МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Индустриальный институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования «Югорский государственный университет»
(ИндИ (филиал) ФГБОУ ВО «ЮГУ»)

УТВЕРЖДАЮ
Заместитель директора по УВР
_____ Гарбар О.В.
«09» сентября 2021 г.

Методические указания

по выполнению практических работ

ПМ.12 ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ

для специальности 09.02.07

Нефтеюганск
2021

РАССМОТРЕНО:
Предметной цикловой
Комиссией специальных технических
дисциплин
Протокол №1 от 09.09.2021
_____Шарипова И.А.

СОГЛАСОВАНО:
заседанием Методсовета
протокол №1 от 16.09.2021
Председатель Методсовета
_____Н.И. Савватеева

Разработчик: Чупракова И.В., преподаватель ИндИ (филиала) ФГБОУ ВО «ЮГУ».

Оглавление

Пояснительная записка

Методические указания выполнению практических работ профессионального модуля ПМ.12 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.07 Информационные системы и программирование. Программа профессионального модуля может быть использована в дополнительном профессиональном образовании и профессиональной подготовке работников по укрупненной группе специальностей 09.00.00 Информатика и вычислительная техника.

Реализация профессионального модуля предусматривает проведение и практических работ в форме практической подготовке обучающихся.

Практическая подготовка при реализации профессионального модуля организуется путем проведения практических занятий, практикумов и иных аналогичных видов учебной деятельности, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью, а также демонстрацию практических навыков, выполнение, моделирование обучающимися определенных видов работ для решения практических задач, связанных с будущей профессиональной деятельностью в условиях, приближенных к реальным производственным.

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля **должен:**

Иметь практический опыт	монтажа, эксплуатации и обслуживания локальных компьютерных сетей; установки и настройки сетевого и серверного оборудования для подключения к глобальным компьютерным сетям (Интернет).
уметь	осуществлять монтаж кабельной, беспроводной сети и оборудования локальных сетей различной топологии; подключать сервера, рабочие станции, принтеры и другое сетевое оборудование к локальной сети; вести отчетную и техническую документацию; устанавливать специализированные программы и драйверы, осуществлять настройку параметров подключения к сети Интернет; осуществлять диагностику подключения к сети Интернет; устанавливать и настраивать программное обеспечение серверов сети Интернет, в том числе web-серверов и серверов электронной почты;
знать	общие сведения о локальных компьютерных сетях, их назначении и области использования; топологию локальных сетей, физическую структуру, способы соединения компьютеров в сеть, виды интерфейсов, кабелей и коннекторов; виды инструментов, используемых для монтажа и диагностики кабельных систем компьютерных сетей; состав аппаратных ресурсов локальных сетей; программное обеспечение для доступа к локальной сети; программное обеспечение для мониторинга и управления локальной сетью; виды серверов, используемых в локальной сети.

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности (ВПД) Разработка модулей программного обеспечения для компьютерных систем, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	**Наименование профессиональных компетенций**[1]
ПК 1.1.	Осуществлять монтаж кабельной сети и оборудования локальных сетей различной топологии.
ПК 1.2.	Осуществлять настройку сетевых протоколов серверов и рабочих станций.
ПК 1.3.	Выполнять работы по эксплуатации и обслуживанию сетевого оборудования.
ПК 1.4	Обеспечивать работу системы регистрации и авторизации пользователей сети.
ПК 1.5.	Осуществлять системное администрирование локальных сетей.
ПК 2.1.	Устанавливать и настраивать подключения к сети Интернет с помощью различных технологий и специализированного оборудования.
ПК 2.2	Осуществлять выбор технологии подключения и тарифного плана у провайдера доступа к сети Интернет
ПК 2.3.	Устанавливать специализированные программы и драйверы, осуществлять настройку параметров подключения к сети Интернет.
ПК 2.4.	Осуществлять управление и учет входящего и исходящего трафика сети.
ПК 2.5.	Интегрировать локальную сеть в сеть Интернет.
ПК 2.6.	Устанавливать и настраивать программное обеспечение серверов сети Интернет.
ПК 3.2	Осуществлять меры по защите компьютерных сетей от несанкционированного доступа.
ПК 3.3.	Применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами.
ПК 3.4.	Осуществлять мероприятия по защите персональных данных.

Освоение профессионального модуля направлено на развитие общих компетенций:

Код	**Наименование общих компетенций**
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3	Планировать и реализовывать собственное профессиональное и личностное развитие.

[1] Перечень профессиональных компетенций (ПК) соответствует Федеральному государственному образовательному стандарту среднего профессионального образования по профессии 230103.03 Наладчик компьютерных сетей, утвержденный приказом Министерства образования и науки РФ от 2 августа 2013 г. N 853

ОК 4	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 5	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 6	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 7	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 9	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

Правила выполнения практических работ

Подготовка к выполнению практических работ. Практические работы в группах проводятся в соответствии с расписанием учебных занятий в колледже в течение определенного времени. Поэтому для выполнения практических работ обучающийся должен руководствоваться следующими положениями:

– Предварительно ознакомиться с графиком выполнения практических работ;

– Внимательно ознакомиться с описанием соответствующей практической работе и установить, в чем состоит основная цель и задача этой работы;

– По лекционному курсу и соответствующим литературным источникам изучить теоретическую часть, относящуюся к данной практической работе;

– Неподготовленные к работе обучающиеся к выполнению практической работы не допускаются.

После окончания работы рабочее место должно быть приведено в порядок. В течение всего времени занятий обучающиеся обязаны находиться на своих рабочих местах. Выходить из помещения во время занятий можно только с разрешения преподавателя.

Оформление отчета по практическим работам.

Составление отчета о проведенных исследованиях является важнейшим этапом выполнения практической работы. По каждой выполненной работе в рабочей тетради составляют отчет, руководствуясь следующими положениями:

– Указать название и порядковый номер лабораторной работы, а так же краткое сформулировать цель работы;

– Схемы и графики чертить с соблюдением принятых стандартных условий обозначений;

– Отчет по каждой практической работе должен содержать основные выводы. В заголовке отчета указывают номер работы и ее полное наименование. При составлении отчета нужно кратко описать цель работы, ее содержание, указать использованные аппаратуру и оборудование.

– При выполнении практической работ необходимо строго следовать правилам техники безопасности.

Критерии оценки работ

Оценка «отлично» ставится, если обучающийся выполнил работу в полном объеме с соблюдением необходимой последовательности действий; в «Отчете к практическим работам» правильно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок.

Оценка «хорошо» ставится, если обучающийся выполнил требования к оценке "5", но допущены 2-3 недочета.

Оценка «удовлетворительно» ставится, если обучающийся выполнил работу не полностью, но объем выполненной части таков, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки.

Оценка «неудовлетворительно» ставится, если обучающийся выполнил работу не полностью или объем выполненной части работы не позволяет сделать правильных выводов.

Практическая работа №1 Анализ структурированных кабельных систем

Цель работы: научиться сопоставлять характеристики кабелей в структуре СКС, исходя из требований нормативно-технической документации.

Теоретические сведения

Структурированная кабельная система (СКС) - это универсальная кабельная система здания, группы зданий, предназначенная для использования достаточно длительный период времени без реструктуризации, СКС подразумевает замену собой всей кабельной системы и систем здания.

Универсальность СКС подразумевает использование ее для различных систем:

- компьютерная сеть;
- телефонная сеть;
- охранная система;
- пожарная сигнализация
- прочие.

Такая кабельная система независима от оконечного оборудования, что позволяет создать гибкую коммуникационную инфраструктуру предприятия. Структурированная кабельная система - это совокупность пассивного коммуникационного оборудования:

- Кабель - этот компонент используется как среда передачи данных СКС. Кабель различают на экранированный и неэкранированный.
- Розетки - этот компонент используют как точки входа в кабельную сеть здания.
- Коммутационные панели - используются для администрирования кабельных систем в коммутационных центрах этажей и здания в целом.
- Коммутационные шнуры - используются для подключения офисного оборудования в кабельную сеть здания, организации структуры кабельной системы в центрах коммутации.

В настоящее время в локальных вычислительных сетях (ЛВС) используются следующие типы кабельной системы:

тонкий и толстый коаксиальный кабель;

четырех- и восьмиконтактная витая пара (UTP - Unshielded twisted-pairwaire);

одно- и многомодовое оптоволокно.

Коаксиальный кабель наиболее давно используется в ЛВС. По структуре он похож на обыкновенный телевизионный антенный кабель (рис. 1), однако имеет сопротивление не 75 Ом, а 50 Ом. Тонкий коаксиальный кабель имеет диаметр 0,5 дюйма. Максимальная длина сегмента тонкого коаксиального кабеля зависит от его характеристик, а точнее от затухания сигнала при передаче и равна примерно 185м, однако чем толще кабель, тем лучше у него характеристики (для толстого коаксиала с диаметром 0,25 дюйма максимальная длина сегмента составляет около 500м.),

но тем сложнее его прокладывать и тем он дороже. Сегментом сетевого кабеля называется участок кабеля между оконечными устройствами.

Достаточно низкая стоимость и относительная простота установки обеспечили в прошлом коаксиальному кабелю высокую популярность до тех пор, пока для используемых приложений хватало скорости передачи данных, которую обеспечивает данный тип кабеля, а именно: 10 Мбит/сек. (10 Mbps). Тонкий коаксиальный кабель дешевле толстого, но за дешевизну кабеля приходится расплачиваться качеством- тонкий коаксиал обладает

худшей помехозащищенностью, худшей механической прочностью и более узкой полосой пропускания.

Оптический кабель может передавать данные с очень высокой пропускной способностью. Оптоволокно обладает отличными трансмиссионными характеристиками, высокой емкостью передаваемых данных, потенциалом для дальнейшего увеличения пропускной способности и устойчивостью к электромагнитным и радиочастотным помехам. Световод состоит из сердцевины и защитного стеклянного внешнего слоя (оболочки). Оболочка служит в качестве отражающего слоя, с помощью которого световой сигнал удерживается внутри сердцевины. Оптический кабель может состоять только из одного световода, но на практике он содержит множество световодов. Световоды уложены в мягкий защитный материал (буфер), а он, в свою очередь, защищен жестким покрытием. В широко распространенных световодах диаметр оболочки составляет 125 микрон. Размер сердцевины в распространенных типах световодов составляет 50 микрон и 62,5 микрон для многомодового оптоволокна и 8 микрон для одномодового оптоволокна. В общем-то, световоды характеризуются соотношением размеров сердцевины и оболочки, например 50/125, 62,5/125 или 8/125. Многомодовое и одномодовое оптоволокно отличаются емкостью и способом прохождения света. Наиболее очевидное отличие заключается в размере оптической сердцевины световода. Более конкретно, многомодовое волокно может передавать несколько мод (независимых световых путей) с различными длинами волн или фазами, однако больший диаметр сердцевины приводит к тому, что вероятность отражения света от внешней поверхности сердцевины повышается, а это чревато дисперсией и, как следствие, уменьшением пропускной способности и расстояния между повторителями. Грубо говоря, пропускная способность многомодового оптоволокна составляет около 2,5 Гбит/с. Одномодовое оптоволокно передает свет только с одной модой, однако меньший диаметр означает меньшую дисперсию, и в результате сигнал может передаваться на большие расстояния без повторителей. Проблема в том, что как само одномодовое оптоволокно, так и электронные компоненты для передачи и приема света стоят дороже.

Одномодовое волокно имеет очень тонкую сердцевину (диаметром 10 микрон или менее). Из-за малого диаметра световой пучок отражается от поверхности сердцевины реже, а это ведет к меньшей дисперсии. Термин "одномодовый" означает, что такая тонкая сердцевина может передавать только один световой несущий сигнал. Пропускная способность одномодового оптоволокна превышает 10 Гбит/с.

Число световодов в кабеле называется числом волокон. Оптический кабель, в котором одна часть световодов одномодовые, а другая - многомодовые, называется гибридным. Оптическое окно - это длина световой волны, которую волокно передает с наименьшим затуханием. Длина волны измеряется обычно в нанометрах (нм). Самые распространенные значения длины волны - 850, 1300, 1310 и 1550 нм. Большинство волокон имеет два окна - т. е. свет может передаваться на двух длинах волн. Для многомодовых световодов это 850 и 1310 нм, а для одномодовых - 1310 и 1550 нм.

Затухание характеризует величину потери сигнала и аналогично сопротивлению в медном кабеле. Затухание измеряется в децибелах на километр (дБ/км). Типичное затухание для одномодового волокна составляет 0,5 дБ/км при длине волны в 1310 нм и 0,4 дБ/км при 1550 нм. Для многомодового волокна эти величины равны 3,0 дБ/км при 850 нм и 1,5 дБ/км при 1300 нм. Благодаря тому, что оно тоньше, одномодовое волокно позволяет передавать сигнал с тем же затуханием на более дальние расстояния, чем эквивалентное многомодовое волокно.

Оптоволоконные кабели обладают отличными характеристиками всех типов: электромагнитными, механическими (хорошо гнутся, а в соответствующей изоляции обладают хорошей механической прочностью). Однако у них есть один серьезный недостаток- сложность соединения волокон с разъемами и между собой при необходимости наращивания (увеличения длины) кабеля.

Кабель "Twisted Pair" - "Витая пара", состоит из "пар" проводов, закрученных вокруг друг друга и одновременно закрученных вокруг других пар, в пределах одной оболочки (рис.2). Каждая пара состоит из провода, именуемого "Ring" и провода "Tip". (Названия произошли из телефонии). Каждая пара в оболочке имеет свой номер, таким образом, каждый провод можно идентифицировать как Ring1, Tip1, Ring2, Tip2, ... Дополнительно к нумерации проводов каждая пара имеет свою уникальную цветовую схему: Синий/Белый для 1-ой пары, оранжевый/белый - для 2-й, зеленый/белый - для 3-й коричневый/белый - для 4-й. Согласно стандартам, провод делится на несколько категорий по своей "пропускной способности".

Обычно на проводе написано, к какой категории он относится. Например: " ...CATEGORY 5 UTP ...". Для защиты от внешних помех кабель с витыми парами может дополнительно экранироваться - в этом случае такой кабель называется экранированной витой парой (STP - Shielded Twisted Pairwaire). Однако на практике такой кабель используется весьма редко.

Максимальная длина сегмента UTP кабеля определяется максимальным затуханием сигнала на пути от источника до приемника и должно быть не более 11,5 Дб. На практике принято считать максимально допустимой длиной сегмента UTP 5-ой категории 100 метров при скорости передачи 100 Mbps. При скорости в 10Mbps длина сегмента может быть гораздо больше.

Для соединения устройств витой парой предусматривается использование провода имеющего две пары: одну для передачи, другую - для приема.

Используются две возможные разводки кабеля в порту. MDI для DTE (Data Terminal Equipment) устройств (т.е. компьютеры, принтеры и т.д.) и MDI-X для хабов (устройства для расширения сети - содержат несколько входов для подключения нескольких компьютеров или других хабов).

При подключении MDI порта к MDI-X порту используется прямая разводка кабеля. А при соединении одинаковых портов MDI и MDI или MDI-X и MDI-X используется "перевернутая" (crossover) разводка кабеля. При этом "передача" соответственно соединяется с "приемом".

Разводка проводов витая пара производится в следующем порядке:

Если кабель содержит только две пары:

Скорость передачи у четырехконтактной витой пары не выше 10Mbps.

Для восьмижильного кабеля (четыре пары) существует два варианта заделки: 568A и 568B. Оба этих варианта эквивалентны. Возможно соединение со скоростями до 100Mbps.

Кабель зачищается с помощью обжимного инструмента или ножа на необходимую длину и затем на него одевается вилка RJ-45.

Вилка RJ-45 похожа на вилку от импортных телефонов, только немного большего размера и имеет восемь контактов (рисунок 3).

Если кабель вставлен правильно, то все жилы должны оказаться над контактами 1 и упереться в правую часть вилки (по рисунку 3а). Внешняя общая изоляция кабеля должна расположиться над фиксатором провода 3.

На новой, неиспользованной вилке, контакты выходят за пределы корпуса вилки0. В процессе обжима, они будут утоплены внутрь корпуса, прорежут изоляцию провода и воткнуться в жилу, а фиксатор провода зажмет внешнюю изоляцию провода.

При отсутствии обжимного инструмента операцию обжима можно провести с помощью острой плоской отвертки. После того, как вилка надета на кабель, производится прижим фиксатора кабеля 3, а затем по очереди вдавливаются в жилы контакты вилки.

Выбор типа сети перед монтажом СКС.

Самое главное перед началом монтажа структурированной кабельной системы, определиться, какой именно тип кабельной системы Вам необходим. После чего можно будет приступать к проектированию СКС. Рабочий проект должен быть составлен в

соответствии со всеми нюансами обследованного объекта, для того, чтобы избежать проблем при монтаже сетей СКС.

Стандарты СКС

Структурированная кабельная система (СКС) - это физическая основа инфраструктуры организации, созданная для того, чтобы свести в одну систему различные информационные сервисы, такие как: вычислительные сети, телефонию, видеонаблюдение, системы безопасности и контроля доступа и другие... Сейчас существуют 3 основных стандарта СКС

1. Американский стандарт EIA/TIA-568-B
2. Международный стандарт ISO/IEC IS 11801
3. Европейский стандарт CENELECEN 50173

01.01.2010 на территории Российской Федерации введены 2 ГОСТа (ГОСТ Р 53246-2008 ГОСТ Р 53245-2008), в которых описаны требования к основным узлам СКС, а также методика сертификации и испытания. Кроме того, кабельная структура СКС должна соответствовать стандартам ANSI TIA/EIA-569 и TIA/EIA-568-B.

Ход работы

1. Ознакомиться с требованиями ГОСТ Р 53246-2008 и ГОСТ Р 53245-2008.
2. Провести исследование наиболее существенных показателей.
3. Разработать требования к кабелям и внести результаты исследования.

Характеристика кабеля	**Кабели на основе витой пары проводников**	**Волоконно-оптические кабели**	**Пункт и обозначение соответствующего стандарта**
Рабочая длина волны		*850-1300 нм*	*4.1.2.2 ГОСТ Р 53246-2008*
Минимальный радиус изгиба	*4 внешних диаметров кабеля*	*25 мм*	*8.2.2 ГОСТ Р 53246-2008*
Максимальная сила натяжения	*110 Н*	*220 Н*	*8.2.3 ГОСТ Р 53246-2008*

4. Исходя из данных таблицы, провести анализ и сделать вывод о показателях качества.

_____
_____
_____
_____
_____
_____

Контрольные вопросы

1. Что такое СКС?

2. В каких областях применяются стандарты на СКС?
3. Что включает в себя СКС?
4. Какие основные стандарты используются для регулировки качества СКС?
5. Какие показатели качества СКС наиболее значимы?

Практическая работа №2. Составление примерной проектной документации с учетом основных требований монтажа компьютерных сетей

Цель работы: научиться составлять техническое задание, проводить его анализ и подбирать коммутационное оборудование согласно техническому заданию учетом основных требований монтажа компьютерных сетей

Теоретические сведения

Техническая и проектная документация

Проектирование ЛВС должно проводиться в соответствии с постановлением Правительства РФ от 16.02.2008 № 87 «О составе разделов проектной документации и требованиях к их содержанию», региональными строительными нормами и требованиями технического задания. Помимо этого, при проектировании ЛВС должны учитываться требования существующего законодательства и нормативных документов по экологии, охране труда и пожарной безопасности.

В начале всех работ исполнителем проводится предпроектное обследование, целью которого является определение комплекса мероприятий и разработка технических предложений с учетом сформированных типовых решений. По результатам обследования разрабатывается техническое задание на проектирование (ТЗ), являющееся основой для создания любого проекта.

В идеальном случае развернутое ТЗ на проектирование компьютерной сети должен предоставить заказчик. В случае отсутствия у заказчика соответствующих специалистов, которые могли бы составить полноценное ТЗ на проектирование ЛВС, включающее все параметры системы, он может обратиться за помощью к специалистам исполнителя. Интернет-ресурс [И8] содержит конкретный пример ТЗ на проектирование ЛВС.

Проектная документация ЛВС (стадия «П»). Состав проектной документации ЛВС регламентируется постановлением Правительства Российской Федерации от 16.02.2008 № 85 «О составе разделов проектной документации и требованиях к их содержанию». Разработанная концепция ЛВС и техническое задание на ее проектирование дают основания для создания эскизного плана ЛВС — единого комплекса решений, предназначенного для обеспечения заданного режима эксплуатации ЛВС. Эскизный проект определяет оптимальную структуру ЛВС и трассу прокладки кабельных проводок, расположение и состав ОСИС организации, представление о бюджете проекта, а также целый ряд других параметров, которые позволят облегчить выбор конкретных решений.

Проектная документация ЛВС представляет собой текстовые и графические материалы, определяющие объемно-планировочные, конструктивные и технические решения для строительства или реконструкции (модернизации) ЛВС. Основой для разработки проекта ЛВС служат архитектурно-строительная, технологическая и инженерные части технического задания.

Рабочая документация ЛВС (стадия «Р»). На следующем этапе разрабатывается рабочая документация ЛВС, которая используется на этапе строительства ЛВС. Составив и согласовав с заказчиком ТЗ на проектирование сети и состав проектной документации, специалисты исполнителя приступают к разработке рабочей документации, включающей все необходимые документы, чертежи, схемы, журналы и описания, необходимые для производства работ на объекте заказчика. Рабочая документация (по сути — рабочий проект) описывает, что, где, каким образом и согласно каким стандартам, нормам и

правилам должно быть установлено на объекте. Перед тем как приступить к работам, сотрудники исполнителя в обязательном порядке согласовывают с заказчиком разработанную рабочую документацию. Далее начинается монтаж ОСИС. За соответствием выполняемых работ рабочему проекту ЛВС в организации исполнителя следят инженеры — авторы проектов ЛВС. Такой контроль называется авторским надзором. Любые изменения и отступления от рабочего проекта ЛВС оперативно согласовываются с заказчиком и вносятся в проект.

По завершении работ выпускается исполнительная документация, которая некоторым образом повторяет рабочий проект ЛВС, но, в свою очередь, учитывает все изменения, внесенные в рабочий проект ЛВС в течение производства монтажных и наладочных работ, а также результаты тестирования телекоммуникационного оборудования и кабельных линий. Исполнительная документация передается заказчику, а также эксплуатационной службе здания, где смонтированы ОСИС. Указанная документация необходима для системных администраторов, службы эксплуатации здания, для обслуживания и возможности дальнейшей модернизации сети.

Заключительным этапом проектирования ЛВС является разработка сметной документации, в которой определяется полная стоимость оборудования, строительно-монтажных и пусконаладочных работ.

После завершения проектирования ЛВС и создания рабочей документации, согласно которой будут осуществляться работы по построению всей сетевой инфраструктуры на объекте, проводится контроль соответствия выполнения работ проектной документации.

Этой цели служит авторский надзор — следующее звено технологической цепочки при создании инженерных систем. Авторский надзор подразумевает постоянное участие и контроль над технологией монтажа со стороны отдела технического контроля компании исполнителя. Наличие данного этапа крайне важно, поскольку позволяет избежать ошибок во время выполнения работ и исключает возможность несоответствия построенной системы и согласованного проекта ЛВС.

В процессе выполнения работ иногда возникает необходимость корректировки рабочего проекта сети. При наличии авторского надзора эти моменты выполняются обычно быстро и безболезненно с последующей фиксацией в исполнительной документации.

Завершается цикл работ по инсталляции ЛВС подписанием акта приемки-сдачи. Порядок безопасной технической эксплуатации ОСИС обычно регламентирует документ «Правила эксплуатации и хранения техники. Эксплуатация ЛВС». В приложении 1 приведен примерный вид указанного документа.

Технические требования заказчика, которые называются в некоторых случаях заданием на проектирование, являются тем первичным документом, с которого начинается работа по созданию СКС.

Документом, обобщающим исходную информацию и являющимся итогом совместной деятельности заказчика и исполнителя в процессе выполнения предпроектных работ, является утвержденное сторонами техническое задание (ТЗ). ТЗ составляется в соответствии со стандартом ГОСТ 34.602-89 и является тем документом, в соответствии с которым производится создание кабельной системы и ее приемка заказчиком в процессе ввода в эксплуатацию.

ТЗ на СКС разрабатывается на систему целиком или как на некоторую часть в составе другой системы. Дополнительно может быть разработано ТЗ на части СКС. В таких ситуациях на основании ГОСТ 34.201-89, пункт 1.2 достаточно часто практикуется название этого документа как частное техническое задание (ЧТЗ).

ТЗ в общем случае содержит следующие разделы:

- общие сведения;
- назначение и цели создания (развития) системы;
- характеристика объекта;
- технические требования к телекоммуникационным и прочим параметрам системы;

- состав и содержание работ по созданию системы;
- порядок контроля и приемки;
- требования к составу и содержанию работ по подготовке здания и внешних коммуникаций к вводу СКС в действие;
- требования к документированию;
- источники разработки.

При необходимости отдельные разделы могут делиться на подразделы. В ТЗ могут включаться также приложения. В зависимости от конкретных местных условий и специфических особенностей объекта допускается оформлять отдельные разделы ТЗ в виде приложений, вводить дополнительные, исключать и объединять разделы ТЗ.

В процессе разработки технического задания проекту присваивается шифр в соответствии с ГОСТ 34.201-89.

Методика расчета необходимого количества портов при проектировании ЛВС

Примерная методика расчета необходимого количества портов ЛВС выглядит следующим образом:

1. Главный корпус.

1.1. 1 порт, исходя из организации 1 рабочего места для каждого сотрудника в кабинете зам. директора по УПР, работающего в одну смену

1.2. 1 порт, исходя из организации рабочего места секретаря (дополнительно по 1 порту в приемной руководителя и у заместителей – при наличии);

1.3. 1 порт, исходя из организации рабочего зам. директора по метод. работе;

1.4. Количество портов в кабинетах, зависит от количества преподавателей, ведущих прием студентов в одну смену;

1.5. Количество портов ЛВС для работы преподавателей рассчитывается исходя из фактического количества пользователей данных информационных систем и соответствующего необходимого количества организуемых рабочих мест.

2. Мастерские.

2.1. Отделения мастерских:

1 порт исходя из организации в рабочего места преподавателя;

1 порт, исходя из организации в рабочего места преподавателя;

2.2. Вспомогательные службы:

2.2.1. Планово-экономический отдел (кол-во портов, исходя из потребности)

2.2.2. Бухгалтерия (кол-во портов, исходя из потребности)

2.2.3. Отдел кадров (кол-во портов, исходя из потребности)

Ход работы

1. Разработать техническое задание.

Техническое задание на проектирование локальных вычислительных сетей в помещениях учреждения _____

1. Общие требования

1. ***Назначение системы***

*Проектируемая ЛВС должна быть предназначена для*_____
_____
_____

1. ***Требования к проектированию ЛВС***

Проектируемая ЛВС должна:

- являться частью комплекса информационно-вычислительных систем, предназначенного для организации единой информационной инфраструктуры;

- обеспечивать передачу сигналов по физическим линиям с активным сетевым оборудованием между компьютерным оборудованием ЛПУ.

Проектирование ЛВС должно предусмотреть следующие виды работ:

- создание новых портов ЛВС, исходя из потребности;
- интеграция уже имеющихся портов ЛВС в учреждении с вновь проектируемыми рабочими местами в единую сеть;

Проектируемые технические решения по созданию ЛВС полностью должны соответствовать действующим нормам и правилам техники безопасности, пожаробезопасности и взрывобезопасности, а также охраны окружающей среды при эксплуатации зданий и сооружений.

Спроектированная СКС должна полностью соответствовать международному стандарту ISO/IES 11801 на слаботочные кабельные системы зданий.

Проектирование ЛВС и оформление результатов работ должны быть произведены в соответствии со следующими нормативно-техническими документами:

- ГОСТ 21.101-97. Основные требования к проектной и рабочей документации;
- СНиП 11-01-95. Инструкция о порядке разработки, согласования, утверждения и составе проектной документации на строительство
- ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы Термины и определения;

1. ***Требования к ЛВС в целом***
    1. **Проектируемая структурная схема построений ЛВС**

ЛВС, являясь слаботочной структурированной кабельной системой ____ категорий кабелей и в соответствии с международным стандартом на кабельные системы _____ должна состоять из следующих подсистем:

- подсистемы внешних магистралей, содержащей внешние магистральные кабели между кроссовыми зданий, коммутационное оборудование в кроссовых зданий, к которому они подключаются, и коммутационные шнуры и перемычки в кроссовых зданий;
- подсистемы внутренних магистралей, содержащей внутренние магистральные кабели между кроссовой здания и кроссовыми помещений, коммутационное оборудование в кроссовой здания и кроссовых помещений, к которому они подключаются, и коммутационные шнуры и перемычки в кроссовой здания.

    1. **Рабочие места**

На рабочих местах должны быть установлены розетки типового рабочего места, содержащие один информационный разъем, используемый для подключения компьютера. К информационной розетке подходит один кабель горизонтальной подсистемы ЛВС.

    1. **Горизонтальная подсистема.**

Для горизонтальной подсистемы должен использоваться_____кабель.

Кабель должен прокладываться, используя топологию _____.

При разработке трасс прокладки кабелей должно быть учтено, что длина каждого отдельного сегмента кабеля от кроссового поля до информационного разъема не должна превышать _____ м.

    1. **Подсистема внутренних магистралей**

Для прокладки кабельных трасс подсистемы внутренних магистралей должен использоваться _____ кабель.

    1. **Подсистема внешних магистралей**

Для прокладки кабельных трасс подсистемы внешних магистралей должен использоваться _____ кабель.

2.6. Маркировка

Концы кабелей в процессе прокладки должны маркироваться на обоих концах липкой маркировочной лентой, на которой должен указываться идентичный для обоих концов уникальный идентификационный код.

    1. **Коммутационное оборудование для медных кабелей**

В качестве коммутационного оборудования для медных кабелей должны быть использованы _____- или _____- парные коммутационные панели с разъемами ____ категории _____ для разделки кабелей горизонтальной подсистемы.

1. **Решения по защите информации от несанкционированного доступа**

Защита информации должна обеспечиваться техническими мероприятиями, затрудняющими считывание передаваемых данных на всем протяжении каналов СКС.

1. **Решения по режимам функционирования системы**

ЛВС должна поддерживать _____ режим функционирования.

2. Провести анализ ТЗ и подобрать оборудование.

Тип оборудования	Марка/обозначение	Количество	Стоимость

Контрольные вопросы

1. Что такое СКС?
2. Какие стандарты СКС можете назвать?
3. Что такое техническое задание?
4. Из каких разделов состоит ТЗ?

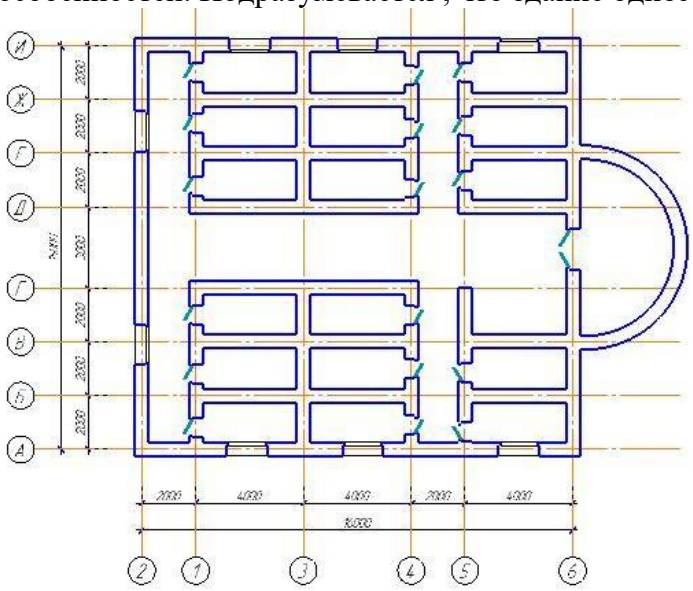
Практическая работа №3. Составление примерной схемы прокладки трасс, расположения оборудования и подключения кабелей.

Цель работы: изучение технологии составления примерной схемы прокладки трасс и подключения кабелей.

Ход работы

На основании выбранного типа и топологии сети, а также выбранного сетевого оборудования и типа кабеля было необходимо разработать план расположения оборудования и прокладки кабеля.

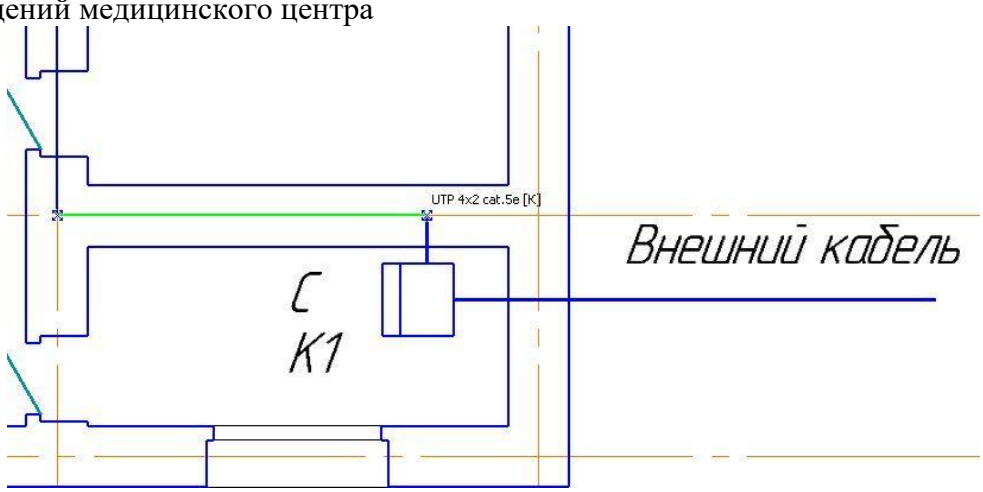
Для разработки плана расположения оборудования и прокладки кабеля для примера разработан план строения объекта с учетом всех его конструктивных особенностей. Подразумевается , что здание одноэтажное.



Сеть согласно заданию необходимо организовать не во всех кабинетах, а лишь в ее части. Так как я выбрал топологию «звезда» , то к организации локально-вычислительной

сети необходимо отнестись , согласно топологическим особенностям. Мне необходимо установить сеть состоящую из 11 персональных компьютеров, объединенных концентратором и сетевым оборудованием для предоставления информационных услуг(согласно условию задачи)

Необходимым условием настройки ЛВС в моем случаи было создание специальной области для оборудования. Для это было необходимо организовать специальное технологическое помещение со специально созданными условия для размещение и функционирования сетевого оборудования. Для этих целей и была выделена одно из помещений медицинского центра



В «серверную» со внешней среды(улицы) проходит кабель оптический внешний бронированный. Этот кабель обеспечивает выход из пределов ЛВС в пределы (в нашем случаи) сети Internet, что просто необходимо, так как локальная сеть согласно заданию курсового проекта просто обязана взаимодействовать с внешним миром.

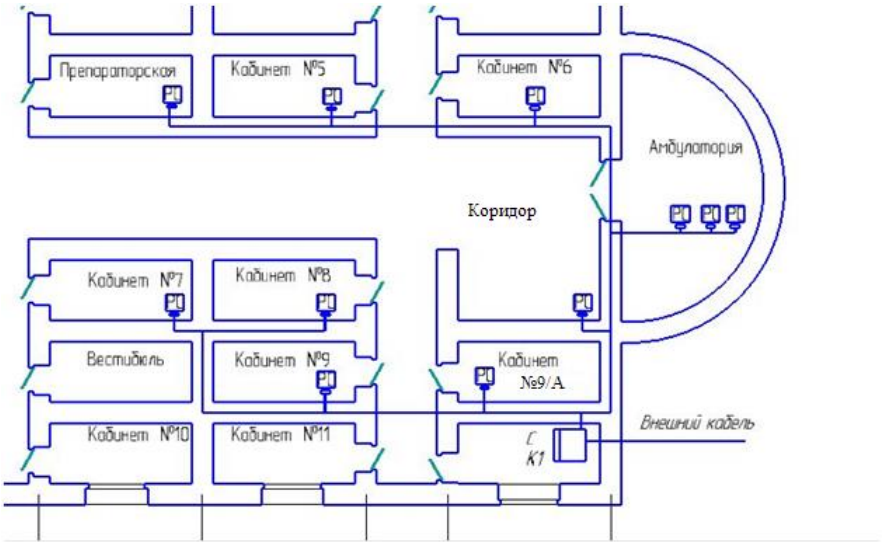
Для удобства и рационализации рабочего пространства рекомендуется поместить все оборудование сетевое в специальное устройство - **шкаф** .В моем случаи сюда поместится 24-портовый **коммутатор**(К) и **маршрутизатор**.

В моем случаи именно это и является «концентратором» для звездной топологии. Также, согласно заданию, сюда рекомендуется установить и иное оборудование(хранилище) – к примеру системы хранения данных (для резервирования и хранения всех данных) и персональный компьютер для более удачного централизованного управления ЛВС.

От шкафа пойдет разводка витой пары, в нашем случаи **UTP 4X2 cat.5e**

При прокладке кабеля преследовались две важные цели:

1. В соответствии со стандартом ISO/IEC 11801 длина кабелей горизонтальной подсистемы не должна превышать 91 м. Кабели прокладываются по кабельным каналам. Принимаются во внимание также спуски, подъемы и повороты этих каналов.
2. Необходимо было сократить и оптимизировать длину кабелей прежде всего из-за экономических и рациональных причин. Чем больше длина - тем больше затухание. Логистическая задача тут также просматривалась. Я обязан подсоединить к одной из «ветвей» звездной топологии как можно больше ПК и с учетом роста этих самых ПК на будущее. Дабы в будущем не возникало проблем у эксплуатирующих сеть при расширении сети .



ти задачи были решены. Помимо прочего было сэкономлено порядка десяти метров сетевого кабеля.

Практическая работа 4. Выбор необходимого оборудования и ПО. Монтаж ЛВС и маркировка кабелей

Цель работы: научиться выбирать необходимое оборудования и ПО для монтажа ЛВС и маркировка кабелей.

Ход работы

Задание. Выбор оборудования В данном случае для прокладки локальной вычислительной сети был выбран кабель витая пара категории 5е. Так как его проще обжимать и прокладывать по сравнению с другими.

1. Выбор кабель канала. Кабель-канал предназначен для прокладывания открытой проводки. Изготавливается кабель канал из различных материалов пластика, стали или алюминия. Для открытой проводки используется пластиковый кабель канал. Самый популярный это - короб, прямоугольный в профиле, с защищающей кабель канал крышкой. Внутри канала для разграничения электро-кабелей на силовые и слаботочные используется перегородка. Монтаж электро-выключателей, электро-розеток и прочих электро-установочных изделий в конструкцию осуществляется несложной защелкой. Сборка и разведение кабельных каналов типа «короб» облегчается через применение деталей-аксессуаров (угол L-образный, угол Т-образный, заглушка, соединитель, угол внешний, угол внутренний), смотреть рисунок 13.

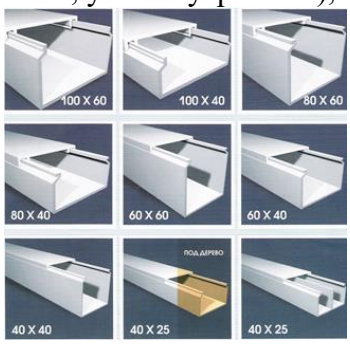


Рисунок 13 - Кабель канал

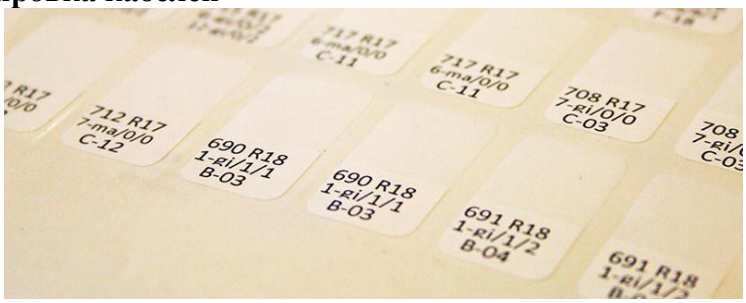
2. Был выбран кабель канал марки "Короб" ценой 220,00 и размерами 40х25.

3. Выбор сетевой розетки. Розетка - конечная точка, к которой подводится кабель-канал или скрытый за стеной кабель - это сетевая розетка. Розетка встраивается в стену и надежно фиксирует подключаемые к ней кабели. Стандартный разъем компьютерной розетки - под коннектор RJ 45 (8P8C), телефонной - RJ 11 или RJ 12. Основная функция розетки - упорядочивать информационные кабели в помещении и обеспечивать надежное подключение патч-корда.
4. Компьютерная розетка VOTO одинарная белая на «липучке». Розетка простая в применении, позволяет быстро организовать подключение по Ethernet для ПК, ресивера, медиа плеера или любого другого устройства. Розетка подключается к витой паре категории 5е.
5. Для максимальной простоты установки, в розетке используется V-образный зажим, благодаря которому не нужно тратить время на зачистку и обжим кабеля. Для правильной распиновки проводов возле каждого зажима есть цветная пометка.
6. В комплекте идет саморез, с помощью которого можно надежно зафиксировать розетку, например, на деревянной или гипсокартонной поверхности. Под «Липучкой» подразумевается скотч двухсторонний пеноакриловый, который надежно зафиксирует розетку на гладкой поверхности и позволяет перенести розетку в случае необходимости, смотреть рисунок 14.

Рисунок 14 - Розетка сетевая

7. Для подключения компьютеров в локальную вычислительную сеть нам потребовались розетки марки VOTO с разъемом для конектора RJ-45.

Маркировка кабелей



Маркировка имеет смысл, когда имеется много проводов и непонятно сразу, какой из них куда ведет. Дело может быть не только в том, что их слишком много.

Как правило, в серверной (или ЦОДе — центре обработки данных) подведены некоторые внешние каналы (Интернет, прямые кабели до других ЦОДов, филиалов компании, и пр.), а также расположено местное оборудование в телекоммуникационных шкафах.

На фото видно верх такого шкафа. Снизу слева подходят кабели от других устройств в стойке, а вверх уходят кабели, которые идут в другие стойки или на внешние каналы. Над стойками есть специальный органайзер для кабелей.

Внутри стойки разделяют активное и пассивное оборудование. Пассивное служит исключительно для целей коммутации. Например, патч-панель:

На такой панели есть 24 или больше портов, она имеет высоту 1U или 2U. С обратной стороны панели все кабели собраны в пучок, который уходит наверх стойки. Как правило, все порты одной патч-панели соответствуют портам другой панели в другой стойке.Таким образом, коммутации подлежат порты в активном и пассивном оборудовании в различных стойках.

Подготовка таблицы коммутации

В такой таблице указывается:

1. номер соединения;
2. исходное активное оборудование;
3. тип разъема на исходном оборудовании;
4. пассивное оборудование в той же стойке;
5. конечное активное оборудование;
6. тип разъема на конечном оборудовании;
7. активное оборудование в той же стойке;

Понятно, что для оборудование в одной стойке пассивные патч-панели могут отсутствовать. Кроме того, при разном типе разъемов могут присутствовать переходники, либо само пассивное оборудование может быть посложнее простой панели с портами. Если все порты одинаковы, можно это опустить.

Для того, чтобы эффективно обозначать оборудование, необходимо ввести некоторые правила обозначений.

Во-первых, все шкафы/стойки в рамках ЦОДа или в рамках нескольких площадок, созданных для общей, но разнесенных территориально, пронумерованы. Поскольку такой шкаф называется rack, то и обозначается: R01, R02, и т.д.

Далее, удобно активное оборудование нумеровать снизу вверх цифрами, а пассивное — сверху вниз буквами A, B, C, и т.д. Соответствующие наклейки наносятся на само оборудование или сбоку на поверхность стойки.

Внутри оборудование тоже нужно ввести нумерацию. Множество сложных устройств имеют в себе модули, поэтому, чтобы использовать нанесенную на них нумерацию, сначала надо указать номер модуля (всегда 1, если там нет никаких модулей), а затем и номер порта в нем. Порты нумеруются слева направо, сверху вниз. Нумерация портов должна быть прозрачна, для каждого типа оборудования нужна в документации картинка с нумерацией, потому что когда кабелей воткнуто много разглядывать циферки не удобно. А недавно встретил Cisco с перевернутыми (вверх ногами) знаками, спасибо китайцам.

Таким образом, для обозначения конкретного порта имеем что-то вроде: R01:2\1\14.

Для пассивного оборудование достаточно: R03:E-21, поскольку для одного устройства нумерация будет наверняка сквозная.

Таким образом, мы имеем таблицу соединений из которой абсолютно понятно сколько кабелей нужно и каких, а также куда их воткнуть.

Что наносить на кабель?

Маркировка нужна для того, чтобы иметь возможность вынуть и воткнуть обратно любой кабель. Кроме того, посмотрев на кабель, имеется возможность понять, куда он идет (или хотя бы должен идти).Что наносить на кабель — дело вкуса.

Возможные варианты:

- номер соединения;
- у порта пассивного оборудования указывать активное (в этой же стойке), а у порта активного — активное в этой же стойке. Удобно для понятия куда же ведет этот кабель, но вставить его в нужный порт невозможно без таблицы, можно применять при маркировке после коммутации;
- писать на обоих концах одно и то же: номер стойки и какие два порта в ней соединяет кабель, удобно для предварительной маркировки, но без таблицы не понять, куда ведет этот кабель, особенно если соответствие патч-панелей не указано;
- другие.

Специальные бирки;

Обычный маркер, номер можно написать прямо на кабеле;

Можно попросить нанести маркировку завод-изготовителей кабелей, если заказ идет напрямую у завода;

Оборудование, которое само печатает маркировку (видео работы по ссылке);

Наборные кольца.

Ход работы

1. Выбираем третий вариант, когда на каждом конце каждого кабеля написано: 123 R01:1\2\12:E-15, где 123 — номер соединения. Тогда можно нанести маркировку на нужное число кабелей и потом брать их по одному и вставлять в оборудование, глядя на маркировку. В принципе, может использоваться что угодно, но нужно учитывать, что обычная клейкая бумага портится от «погодных условий» серверных, а также плохо переносит перегибы проводов. Поэтому лучше подходит плёнка, а ещё лучше специальная.

На такой бумаге есть отдельные наклейки, которые легко отклеиваются и хорошо наклеиваются на кабель. Они называются самоламинирующимися, потому что обклеивание кабеля начинается с бумажной части, а потом пленочная (прозрачная) часть обматывается вокруг кабеля и закрывает саму надпись, тем самым обеспечивая её долговечность. Так же

такая бумага выдерживает сгибания кабеля, но клеить лучше на прямой отрезок, ровнее будет. Печатать на такой бумаге можно на обычном лазерном принтере. Один лист в российских магазинах, к сожалению, стоит от 600 рублей (от 49 до ~200 наклеек на листе, смотря какие нужны). При заказе в США цены будут в 3–5 раз меньше.

2. Для печати необходимо сделать шаблон, удобнее всего — в виде таблицы в Excel. Для бумаги с 13x10 наклейками вот шаблон: ссылка.
3. Необходимо подогнать поля в шаблоне под свой принтер, поскольку отличия на 1-2 мм сказываются значительно. Можно отсканировать и распечатать этот лист на обычной бумаге и попробовать на нем. Можно печатать только на одной наклейке, пока не станет совпадать, но есть опасность, что где-нибудь внизу всё же потом вылезет смещение.
4. Для печати необходимо подготовить таблицу с надписями для кабелей. Столбцы: номер соединения, надпись на одном конце, надпись на другом. Надпись может и совпадать. В моем случае я сделал разбиение надписи на три строчки: номер соединения и шкафа, исходное оборудование, конечное оборудование. Так получился более крупный шрифт, но есть большой минус: надо посмотреть на кабель с почти 270-градусов-сторон, что не всегда легко.

Практическая работа 5. Монтаж пассивного оборудования. Составление таблицы соединений и маркировки

Цель работы: изучить технологию монтажа пассивного оборудования, составить таблицу соединителей и маркировки

Ход работы

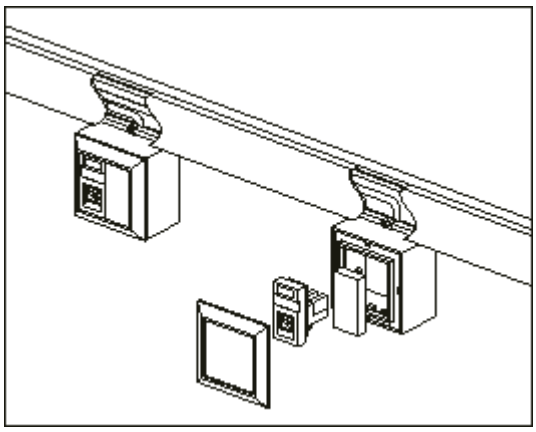
Выбираем кабель-каналы и пассивные компоненты сети.

Постоянство характеристик локальной вычислительной сети достигается за счёт укладки кабелей в специальные кабель-каналы (пластиковые короба).

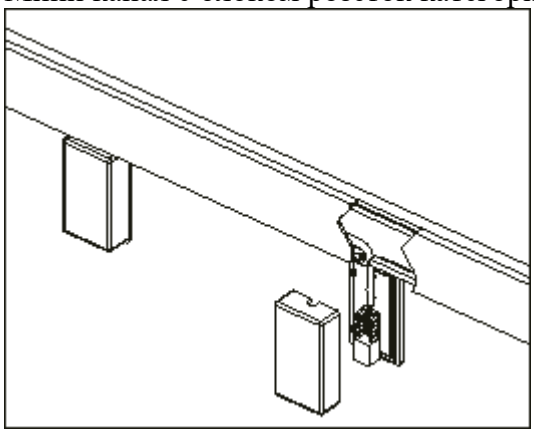
Выясните количество рабочих мест, измерьте длину стен и выберите компоненты нужной категории (рисунки ниже) согласно с требованиями к скорости* работы сети либо исходя из требований к дизайну интерьера.

*Начиная с 5-й категории, прямой зависимости скорости сети от категории компонентов реально нет, всё что выше – даёт лишь запас на «светлое будущее».

Широкий кабель-канал с розетками категории 6.



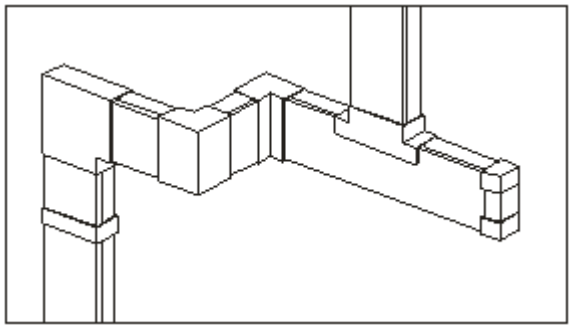
Мини канал с блоком розеток категории 5е



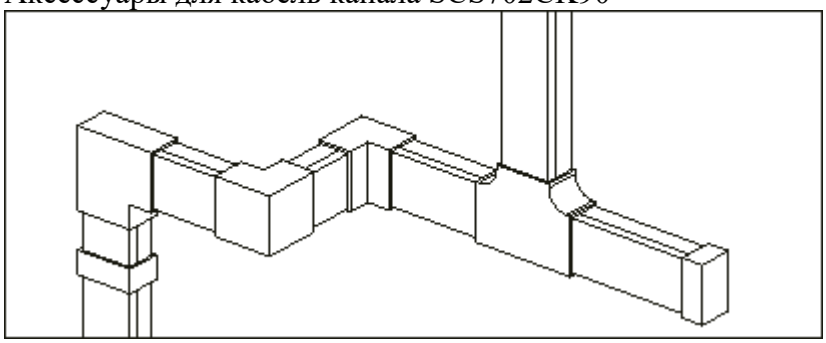
Мини канал с розетками категории 5

Аксессуары к кабель-каналам.

Применение аксессуаров позволяет скрыть огрехи на стыках и ускорить монтаж системы каналов.



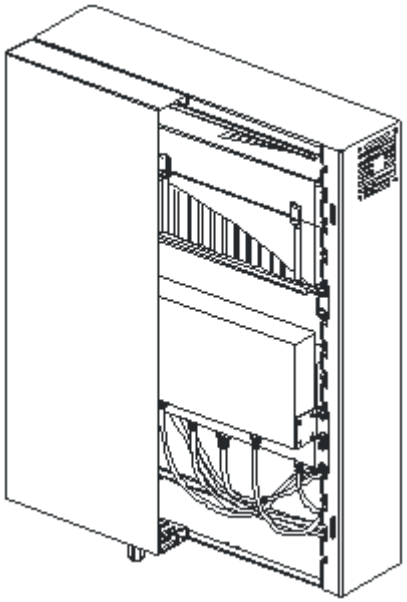
Аксессуары для кабель канала SCS702CK90



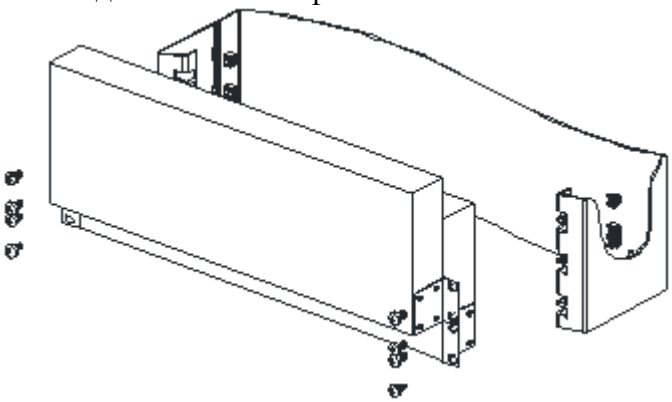
Аксессуары для мини канала SCS702CK40

4. Коммутационный узел локальной сети.

Локальные сети строятся по схеме «звезда» от коммутационного узла. В узле устанавливается многопортовый коммутатор сети. Для защиты портов коммутатора и сокрытия бахромы проводов может использоваться настенный 19» шкафчик.



Коммутатор устанавливается с использованием штатных крепёжных элементов для монтажа в 19 дюймовый шкаф.



Установка коммутаторов.

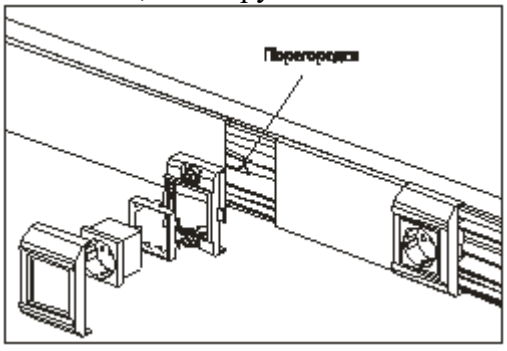
Сети выделенного питания.

Для качественного электроснабжения оборудования рабочих мест организуется сеть выделенного питания. Сеть строится независимо от бытовой сети электроснабжения.

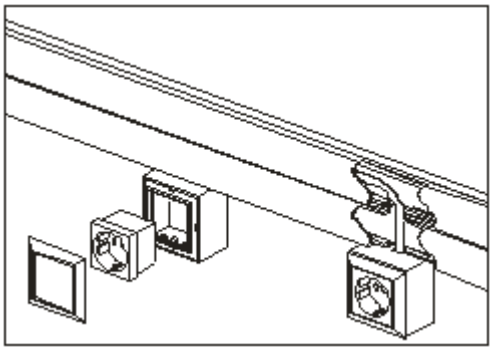
Розетки сети выделенного питания отмечаются красным цветом (розетки бытовой сети имеют белый цвет).

В широкий кабель-канал (короб) устанавливается специальная перегородка, отделяющая кабели сети питания от кабелей локальной сети. По существующим нормативным требованиям установка перегородки является обязательной. Кабели питания размещаются в верхнем отделе канала.

При использовании мини каналов (коробов) кабели сети питания укладываются в отдельный канал, монтируемый над каналом с кабелями локальной сети.



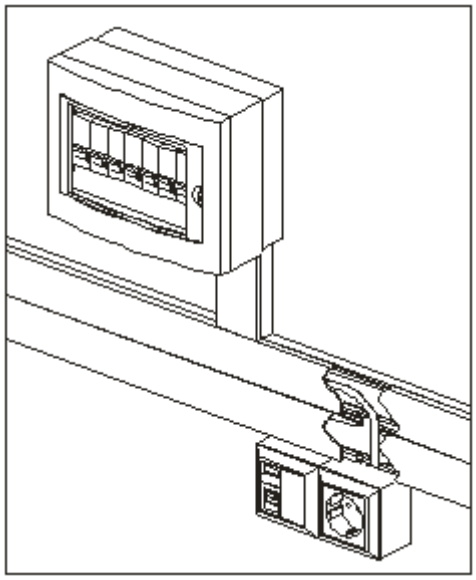
Розетки сети питания для широкого кабель-канала.



Розетки сети питания для мини канала

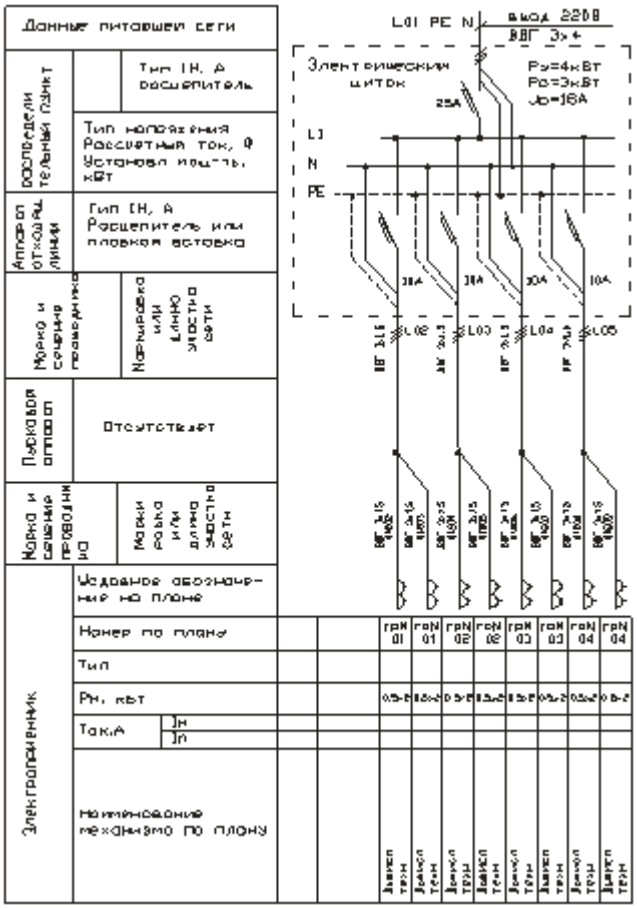
Максимальные нагрузки потребителей определяются путем расчёта в соответствии с «Указаниями РТМ 36.18.324-92». Максимальный ток ограничивается 18А на плечо кабель-канала. В противном случае необходимо разносить каналы питания и локальной сети.

В оснащаемом помещении монтируется распределительный щиток (рисунок ниже). Сеть питания от распределительного щитка до розеток выполняется медным силовым трёхжильным кабелем типа ВВГ.



Распределительный щиток.

Линейная схема сети выделенного питания.



На рисунке приведена линейная схема сети выделенного питания оборудования рабочих мест и питания оборудования сети. По степени бесперебойности электропитания токоприемники, подключаемые к сети выделенного питания, относятся к III категории. Максимальная нагрузка потребителей приведена в табличной части рисунка выше (здесь и далее в разделе приведены данные, служащие исключительно ориентиром для проектировщика, точные цифры должны быть получены путем расчёта, в том числе расчёта сечения жил проводников). Нагрузки по электроснабжению определены по удельному расходу мощности Вт/м2 и по коэффициенту спроса.

Электроснабжение распределительного щитка сети выделенного питания осуществляется от ВРУ (Вводно-Распределительного Устройства) здания. Напряжение низковольтных распределительных сетей 380/220В. В соответствии с ПУЭ по условиям окружающей среды внутренние помещения должны иметь нормальную среду.

Распределение электроэнергии к токоприемникам выполняется при помощи автоматических выключателей, смонтированных на рейке DIN 35 распределительного щитка. Защиту подводящих кабелей от перегрева обеспечивает однофазный автоматический выключатель ВА-101-1/25 номиналом 25А, защиту групповых розеточных сетей — автоматические выключатели ВА-101-1/10 номиналом 10А. Распределительные сети выполняются силовым кабелем марки ВВГ 3х4 от ВРУ до щитка. Групповые розеточные сети от щитка до розеток выполняются силовым кабелем ВВГ 3х1,5. Заземление осуществляется в ВРУ здания. Для заземления используется существующее заземляющее устройство для установок напряжением до 1000В. Сопротивление заземляющего устройства принимается: R=125/Ik.з Ом, но не более 4 Ом, где Ik.з — расчётный ток замыкания на землю (берется по данным энергосистемы), а R — наибольшее сопротивление заземления.

Дополнительные розетки.

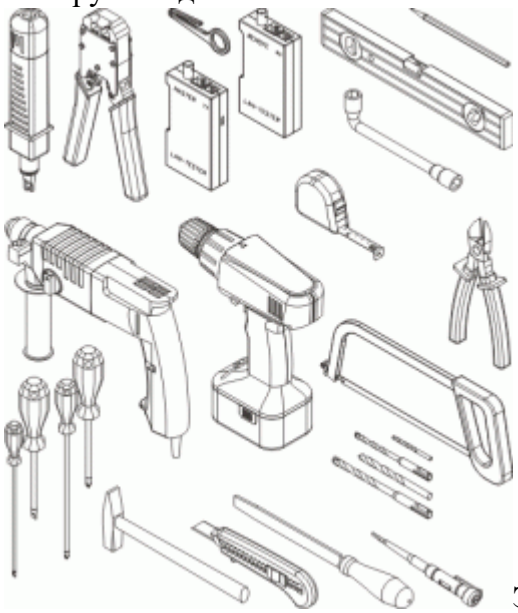
Существует большая вероятность того, что одной информационной розетки и одной розетки сети выделенного питания на каждом рабочем месте будет недостаточно. Без

существенного увеличения стоимости системы, на каждое рабочее место можно установить одну дополнительную информационную розетку и до двух дополнительных розеток сети выделенного питания.

Необходимый инструмент.

Перед началом работ необходимо проверить наличие необходимого инструмента.

Инструмент для монтажа.



Это:

- Нож с ударным механизмом для подключения информационных розеток;
- Клещи для насадки разъемов RJ 45;
- Нож для снятия оболочки UTP кабеля;
- Тестер соединений;
- Ключ торцевой на 13;
- Уровень;
- Карандаш;
- Перфоратор;
- Шуруповёрт;
- Рулетка;
- Бокорезы;
- Ножовка;
- Набор отверток;
- Молоток;
- Монтажный нож;
- Плоский напильник;
- Отвёртка — индикатор напряжения;
- Сверло (шуруповёрт) 5 мм;
- Бур SDS (перфоратор) 6 мм;
- Сверло (шуруповёрт) 10 мм;
- Бур SDS (перфоратор) 10 мм.

Монтаж кабель-каналов (пластиковых коробов).

Работы по монтажу канала выполняются вдвоём или втроём.

Вам потребуются простые дюбели и дюбели для тонких стен (например, для ГКЛ).

Выберите высоту, на которой будет производиться монтаж каналов (выше уровня плинтуса на 20 см, желательно над трубами системы отопления).

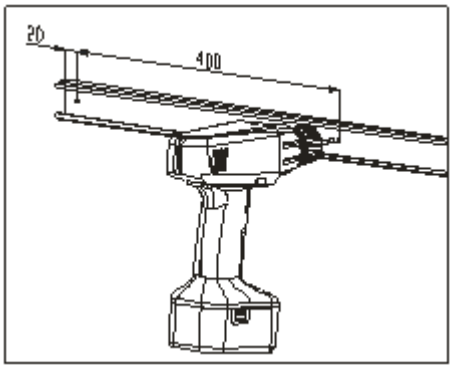
Широкие кабель-каналы рекомендуется располагать выше уровня поверхности столов (80-95 см от пола).

В мини канале, шуруповёртом с пятимиллиметровым сверлом, сделайте отверстия на расстоянии 2 сантиметров от края и далее с шагом около 40 сантиметров.

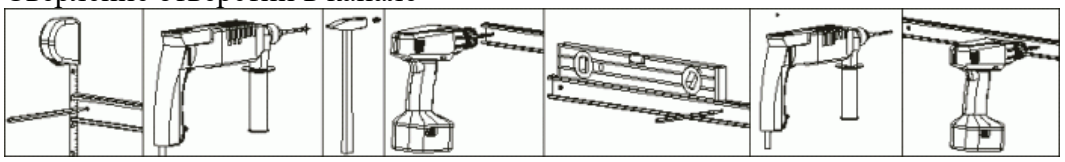
Разместите на выбранной высоте канал и отметьте на стене карандашом место под одно крайнее отверстие.

Просверлите отверстие перфоратором, забейте молотком дюбель и прикрутите короб к стене. Теперь с помощью уровня выравняйте канал по горизонтали и отметьте остальные отверстия. Далее сверлите, забивайте дюбели и крепите канал к стене шурупами с помощью шуруповёрта. При монтаже следующего канала порядок действий повторяется.

Внимание! Сверление отверстий в канале (коробе) перфоратором ведёт к сколам и деформациям пластика.



Сверление отверстий в канале



Монтаж кабель-канала

Для отрезания части канала (короба) следует воспользоваться ножовкой, а затем необходимо снять заусеницы плоским напильником.

Укладка UTP кабелей и кабелей питания.

Работа выполняется вдвоём. Вам потребуются пластиковые хомуты (стяжки) и, возможно, скобы для фиксации кабеля (или, заранее изготовленные, отрезки крышки короба).

Укладка кабелей питания и кабелей локальной сети производится либо в разные мини каналы, либо в разные отделы широкого кабель-канала.

Кабель питания укладывается сверху, кабель локальной сети — внизу. При укладке кабеля локальной сети следует избегать его перегиба и связывания в узел.

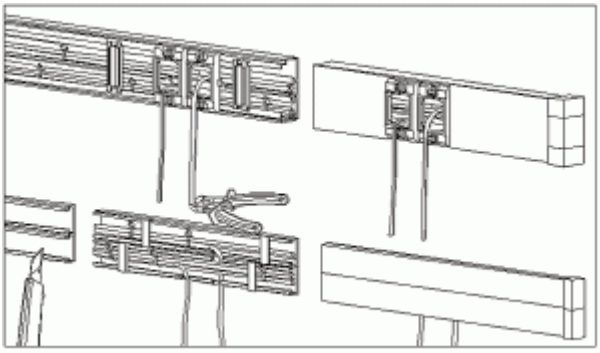
Внимание! Кабели не сращиваются. Если вам не хватило отрезка кабеля – весь кабель необходимо переложить. Места сращивания участков кабеля легко выявляются при измерениях его характеристик.

В районе установки розетки в мини канале делается вырез с помощью монтажного ножа, а на широкий короб монтируется рамка суппорта (рисунок ниже). Кабель укладывается в канал. В вырезанное отверстие или в рамку суппорта выставляется отрезок кабеля длинной 20 сантиметров.

Кабели укладываются по одному, а пучок уложенных кабелей фиксируется скобами (для широкого кабель-канала) или отрезками крышки (для мини канала). Отдельные пучки кабелей удобно стягивать пластиковыми хомутами.

Со стороны узла сети оставляется отрезок кабеля длинной 170 сантиметров для шкафа и 80 сантиметров для кросс бокса.

По окончанию укладки кабеля каналы закрываются крышкой, а стыки и торцы коробов закрываются соответствующими аксессуарами.



Подключение UTP кабелей и кабелей питания.

Работы выполняются в одиночку либо вдвоём.

Перед началом работ необходимо убедиться в том, что распределительный щиток полностью обесточен. Для этого воспользуйтесь отвёрткой-индикатором напряжения.

Для разделки кабеля питания используйте монтажный нож и кусачки. Подключенные кабели фиксируйте пластиковыми хомутами (стяжками).

Назначение проводников кабеля питания обозначается цветом изоляции.

Желто-зеленый проводник — заземление, зажимается центральным заземляющим контактом в розетке или винтом шины заземления электрического щитка; коричневый проводник — фаза, зажимается правым (вид сзади) контактом розетки либо нижней клеммой автоматического выключателя; синий проводник — ноль, зажимается левым (вид сзади) контактом розетки либо винтом нулевой шины электрического щитка.

Информационный кабель локальной сети (UTP) содержит медные одножильные изолированные проводники, сформированные в четыре симметричные витые пары.

Проводники кабеля маркируются разными цветами изоляции.

Модули информационных портов розеток имеют цветовую маркировку, аналогичную маркировке проводников кабеля.

Со стороны розетки локальной сети следует освободить от оболочки 3-4 сантиметра кабеля, используя специальный разделочный нож (рисунок ниже). Далее проводники кабеля вкладываются в ножевые контакты розетки так, чтобы их цвета совпадали с цветами маркеров контактов ряда «В».

Внимание! Важно обеспечить наименьшую длину развива парных проводников и наименьшую длину их участков без оболочки.

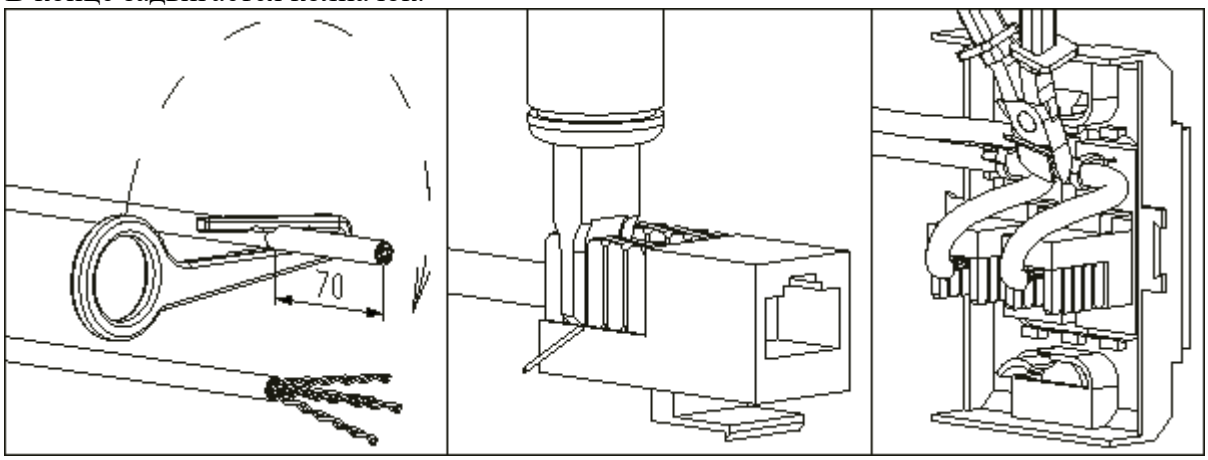
Затем провода забиваются в контакты ножом с ударным механизмом, острая кромка ножа при этом должна отрубать свободные концы проводников. Для этого лезвие ножа вставляется в контакт и ручка ножа плавно смещается в строну контакта до щелчка. После забивки всех проводников модуль устанавливается в суппорт и кабель крепится пластиковым хомутом (стяжкой) к розетке.

Внимание! Стяжка должна лежать на оболочке кабеля.

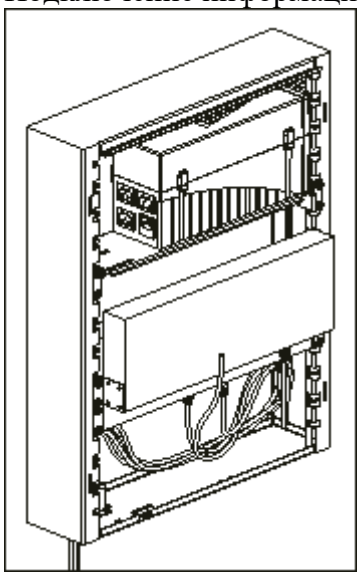
По окончании работы суппорт монтируется в короб и закрывается рамкой.

С противоположной от розетки стороны оставляется отрезок кабеля с длиной, достаточной для подключения к любому порту коммутатора (в шкафу делается кольцо до правой стенки и назад до места расположения портов коммутатора, рисунок ниже). На кабель одевается колпачок. Затем снимается три-четыре сантиметра оболочки (рисунок ниже). Пары раскручиваются до оболочки и проводники аккуратно распрямляются. Проводники выравниваются в одну линию согласно с цветовой схемой и отсекаются обжимочными клещами на расстоянии 15 миллиметров от оболочки. На кабель одевается разъём RJ 45 так, чтобы проводники дошли до конца тонких каналов в разъёме (внимательно следите за соблюдением цветовой схемы), а оболочка кабеля дошла до сужения разъёма (перехода в каналы проводников). Разъём вставляется в обжимочные

клещи, оболочка кабеля проталкивается в глубь разъёма и рукояти клещей сжимаются до упора. В конце задвигается колпачок.



Подключение информационной розетки

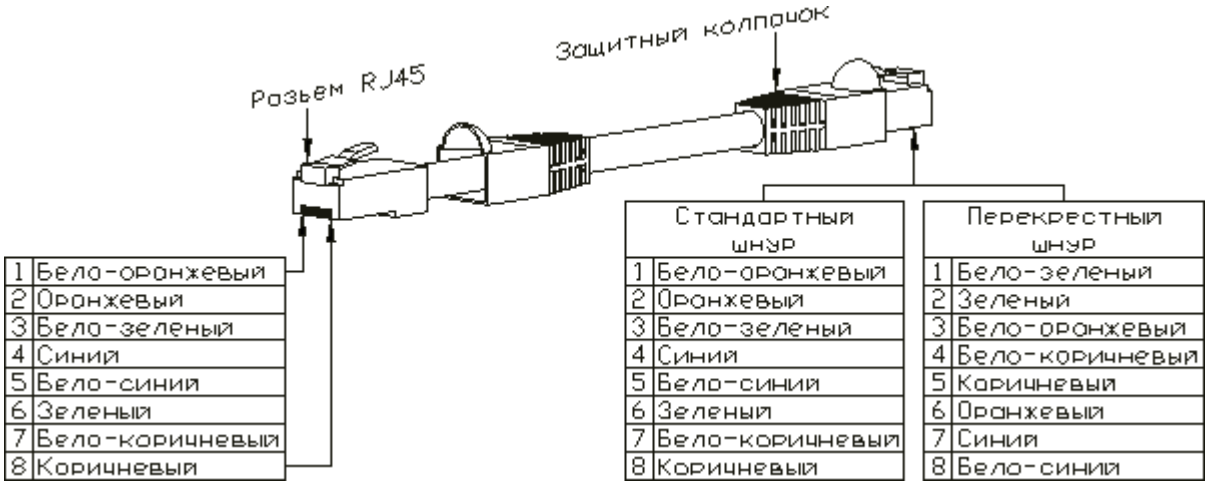


Укладка кабеля локальной сети в 19» настенном шкафчике

Изготовление патчкордов.

Для подключения устройства на рабочем месте используется специальный шнур заводского изготовления с многожильными проводниками (аппаратный шнур, патчкорд, patch cord). При необходимости такой шнур изготавливается вручную. В таблице на рисунке ниже приведена цветовая схема разделки стандартного соединительного шнура и специальной перекрёстной разделки шнура для соединения двух активных устройств (соединения без коммутатора сети, например, компьютер-компьютер, компьютер-сервер, сервер-видеокамера).

Внимание! Разделка перекрёстного шнура «с одной стороны по типу А, с другой стороны по типу Б» является ошибкой.



Разделка шнуров

После насадки разъёмов и подключения розеток проводится проверка правильности монтажа с помощью специального комплекта приборов — тестера соединений. Перед проверкой соединений не забудьте проверить образцовый шнур и сами приборы. Исправность соединений подтверждается последовательным синхронным загоранием индикаторов на ведущем и ведомом приборе (рисунок ниже).

Внимание! Проверка тестером соединений даёт информацию только о правильности выполнения коммутации. Остальное зависит от ответственности и аккуратности монтажника. Если необходимо установить соответствие сети существующим требованиям и сделать распечатку результатов для заказчика, пригласите специалиста с квалификационным тестером.

Проход стен.

Проход капитальных стен осуществляется до начала монтажных работ силами сторонних организаций, обладающих специальным инструментом.

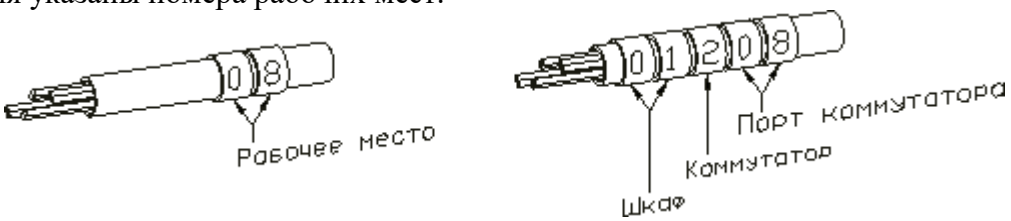
Маркировка ЛВС.

Работа производится одним человеком.

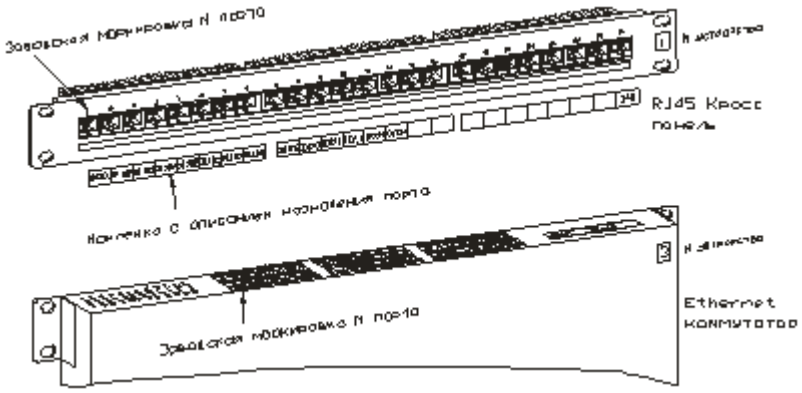
В небольших ЛВС допускаются упрощенная маркировка с указанием только номера рабочего места или маркировка с указанием места назначения кабеля (две цифры — номер шкафа, одна цифра — номер коммутатора и две цифры — номер порта).

Маркировка кабеля производится в начале и конце отрезка кабеля слева направо от места разделки кабеля (см. рисунок ниже).

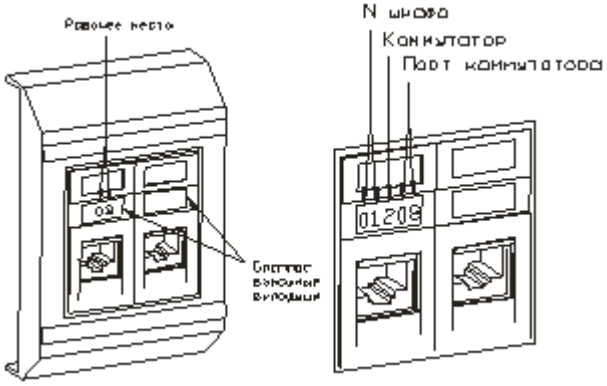
Внимание! Маркировка становится интуитивно понятной, если номер рабочего места и номер порта коммутатора совпадают, а под автоматическими выключателями питания указаны номера рабочих мест.



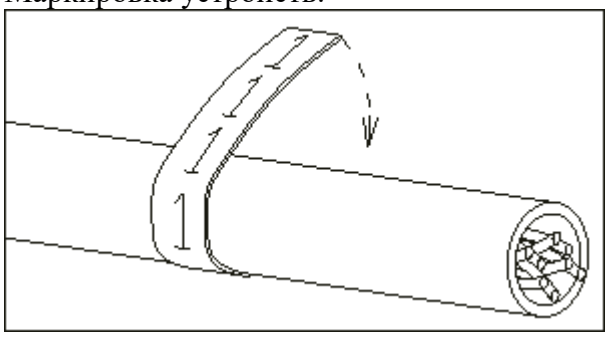
На рисунках ниже приведены маркировка устройств сети и маркировка розеток на рабочих местах.



Маркировка устройств.



Маркировка устройств.



Маркировочные наклейки

Теоретический материал

Пассивное сетевое оборудование - это оборудование не нуждающееся в потребление электроэнергии и не вносящее изменений в сигнал на информационном уровне. Основная функция пассивного оборудования состоит в обеспечении передачи сигнала - это розетки, коннекторы, патч-панели, кабель, патч-корды, кабель-каналы, а также монтажные шкафы, стойки и телекоммуникационные шкафы.

Выбор кабеля. Существует несколько видов сетевых кабелей, основными из которых являются такие как:

- витая пара.
- коаксиальный кабель;
- оптоволокно;

Далее рассмотрим их виды и строения.

Витая пара. Кабель Категории 5е - 4-ех - парный кабель. Скорость передач данных до 100 Мбит/с при использовании 2-ух пар и до 1000 Мбит/с при использовании 4 пар. В СКС самым распространённым является кабель категории 5е. Иногда встречается двухпарный кабель категории 5е. Кабель обеспечивает скорость передач данных до 100 Мбит/с. Преимущества данного кабеля в более низкой себестоимости и меньшей толщине.

Коаксиальный кабель. Предназначен для передачи цифрового аудио сигнала и обладает весьма выгодным соотношением качества и цены. Модель имеет фирменную овальную геометрию, которая обеспечивает равномерную передачу сигнала в широком диапазоне частот. Проводник кабеля выполнен из высококачественной бескислородной меди, при этом центральная жила представляет собой оплетку вокруг диэлектрического «сердечника». Такая конфигурация, в сочетании с овальной формой сечения гарантирует отсутствие скин-эффекта, то есть неравномерного распределения сигналов различных частот по площади его сечения. Этот эффект усиливается с ростом частоты сигнала, и поэтому особенно критичен для джиттера цифровых кабелей, передающих высокоскоростные потоки данных.

Оптоволокно - это сетевой кабель, осуществляющий обмен данными на высокой скорости. Существует понятие ёмкости кабеля, которое определяет количество внутренних волокон. Как правило, внутри кабеля можно найти до 48 и даже больше волокон. Таким образом, этого будет полностью достаточно для большей части выполняемых задач.

Оптоволокно состоит из сердечника из кремния (стекла), отражающего покрытия, защитного лака и буфера. Отражающий слой, являющийся оболочкой, помогает удержать световой сигнал внутри. Для защиты непосредственно волокон используется буфер, который изготавливается из мягких материалов. А поверх наносится дополнительный слой жёсткого покрытия.

Размер сердечника одномодового волокна равен 9 мкм, а многоморового - 50 или 62,5 мкм. Внешний диаметр оболочки равен 125 мкм. Подобные спецификации обеспечивают скорость обмена данными в 1 - 10 Гбит, и даже до 400 Гигагбит в лабораторных условиях на новом оборудовании, вместо традиционных 100 Мбит. А это, как несложно догадаться, значительно увеличивает возможности по обмену данными.

Сердечник волокна состоит из кремния и традиционные схемы соединения волокон невозможны. Поэтому для сращивания двух участков оптического волокна используется сварка оптоволокна с помощью специального сварочного аппарата. При монтаже кабель разделывают на волокна, подготавливает их и сварочный аппарат с помощью роботизированных средств, соединяет волокна на микронном уровне и производит спайку электрической дугой, как показано на рисунке 12.

Рисунок 12 - Оптоволоконный кабель

Практическая работа №6. Создание зон прямого просмотра (основная и дополнительная), перенос зон, настройка параметров TCP/IP для динамической регистрации узлов на сервере DNS, применение команды ipconfig для при¬нудительной регистрации на сервере DNS.

Цель работы: изучить: процесс установки и настройки службы DNS, применение команды ipconfig для принудительной регистрации на сервере DNS. Приобрести навыки применения диагностических утилит для поиска неисправностей и неверных конфигураций протокола TCP/IP и службы DNS.

Теоретический материал

В сетях TCP/IP принято различать адреса сетевых узлов трех уровней

физический (или локальный) адрес узла (MAC-адрес сетевого адаптера или порта маршрутизатора); эти адреса назначаются производителями сетевого оборудования;

IP-адрес узла (например, 192.168.0.1), данные адреса назначаются сетевыми администраторами или Интернет-провайдерами;

символьное имя (например, www.microsoft.com); эти имена также назначаются сетевыми администраторами компаний или Интернет-провайдерами.

Типы адресов

3 типа IP-адресов.

1. Unicast-адрес (единичная адресация конкретному узлу) — используется в коммуникациях «один-к-одному».

2. Broadcast-адрес (широковещательный адрес, относящийся ко всем адресам подсети) — используется в коммуникациях «один-ко-всем». В этих адресах поле идентификатора устройства заполнено единицами. IP-адресация допускает широковещательную передачу, но не гарантирует ее — эта возможность зависит от конкретной физической сети. Например, в сетях Ethernet широковещательная передача выполняется с той же эффективностью, что и обычная передача данных, но есть сети, которые вообще не поддерживают такой тип передачи или поддерживают весьма ограничено.

3. Multicast-адрес (групповой адрес для многоадресной отправки пакетов) — используется в коммуникациях «один-ко-многим». Поддержка групповой адресации используется во многих приложений, например, приложениях интерактивных конференций. Для групповой передачи рабочие станции и маршрутизаторы используют протокол IGMP, который предоставляет информацию о принадлежности устройств определенным группам.

IP-адрес состоит из двух частей — идентификатор сети (префикс сети, Network ID) и идентификатор узла (номер устройства, Host ID).

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.

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 наверх. 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 MAC-адресами (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 узла-отправителя 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.

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.
    - 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.).
    - Протокол ICMP (Internet Control Message Protocol, протокол межсетевых управляющих сообщений) — служит для обмена информацией об ошибках. С помощью специальных пакетов ICMP сообщает сетевым узлам информацию о невозможности доставки пакета, о превышении времени жизни пакета и др.
    - 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.
    - 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.
    - 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.
    - Протоколы для формирования сетевой инфраструктуры (DNS, DHCP, WINS) будут рассмотрены в следующих разделах данного курса.
    - 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.
    - 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.
    - Протокол SNMP (Simple Network Management Protocol, простой протокол управления сетью) используется для организации управления сетевыми узлами.

Ход работы

Задание 1. Настройка параметров протокола TCP/IP

Если вы пропустили этап настройки параметров TCP/IP во время установки системы, настройте эти параметры

Значение IP-адреса и маски подсети необходимо взять из таблицы распределения IP-адресов и имен компьютеров - введите параметры того компьютера, который назначен для вас преподавателем; значения остальных параметров протокола TCP/IP оставьте пустыми. **Параметры протокола зафиксируйте в отчете.**

Задание 2. Проверка коммуникаций с помощью команды ping

Изучите назначение и параметры команды ping

Ping /?

Проверка с помощью команды ping коммуникаций по IP-адресам

Выполните команду ping в таких вариантах:

ping <IP-адрес вашего компьютера>

ping <IP-адрес компьютера партнера в вашем домене>

Примеры: ping 192.168.0.1

ping 192.168.0.2

ping 192.168.0.3

Проверка с помощью команды ping коммуникаций по коротким именам компьютеров (NetBIOS-имена)

Выполните команду ping в таких вариантах:

ping <имя вашего компьютера>

ping <имя компьютера партнера в вашем домене>

Примеры: ping S1

ping S2

Проверка с помощью команды ping коммуникаций по полным именам компьютеров (FQDN-имена)

Выполните команду ping в таких вариантах:

ping <имя вашего компьютера>

ping <имя компьютера партнера в вашем домене>

Примеры: ping S1.world.ru

ping S2.world.ru

Выполните команду ping на компьютере, имеющем выход в интернет:

ping yandex.ru

Определите адрес этого узла воспользовавшись командой ping

Все результаты выполнения команд (проходит или не проходит команда, параметры) зафиксируйте в отчете.

Задание 3. Установка службы dns на сервере

Откройте Панель управления

Выберите пункт "Установка и удаление программ"

Нажмите кнопку "Установка компонентов Windows"

Выберите "Сетевые службы" — кнопка "Дополнительно"

Отметьте службу DNS

ОК (может потребоваться указать путь к дистрибутиву системы)

Задание 4. Создание основной зоны прямого просмотра

Данное упражнение выполняйте на первом компьютере в вашей паре

Откройте консоль DNS

Выберите раздел "Зоны прямого просмотра"

Запустите мастер создания зоны (выбрать: тип зоны — "Основная", динамические обновления — разрешить, остальные параметры — по умолчанию)

Введите имя зоны из таблицы распределения IP-адресов и имен компьютеров — введите имя домена, который назначен для вас преподавателем

Пример (для компьютера S1.world.ru):

имя домена — world.ru

+Разрешите передачу данной зоны на любой сервер DNS (Консоль DNS— ваша зона — Свойства — Закладка "Передачи зон"— Отметьте "Разрешить передачи" и "На любой сервер".

Задание 5. Создание дополнительной зоны прямого просмотра

Данное упражнение выполняйте на втором компьютере в вашей паре

Откройте консоль DNS

Выберите раздел "Зоны прямого просмотра"

+Запустите мастер создания зоны (выбрать: тип зоны — "Дополнительная", IP-адрес master-сервера — адрес первого компьютера в вашей паре, остальные параметры — по умолчанию)

Введите имя зоны из таблицы распределения IP-адресов и имен компьютеров — введите имя домена, который назначен для вас преподавателем

Пример (для компьютера S2.world.ru):

имя домена — world.ru

IP-адрес мастер-сервера — IP-адрес сервера S1

Проверьте появление зоны в окне консоли службы DNS

Задание 6. Настройка параметров tcp/ip для динамической регистрации узлов на сервере dns

Откройте свойства протокола TCP/IP вашего сервера

Укажите в качестве Предпочитаемого сервера DNS IP-адрес первого сервера в вашей паре

Назначьте в качестве суффикса полного имени вашего сервера имя назначенного вашей паре домена ("Мой компьютер"— "Свойства" — Закладка "Имя компьютера"— Кнопка "Изменить"— Кнопка "Дополнительно"— в пустом текстовом поле впишите название вашего домена.— кнопка "0К"(3 раза))

Внимание! Смена имени компьютера потребует его перезагрузки.

Настоятельно рекомендуется перезагружать компьютеры в паре по очереди: сначала первый, затем второй.

Проверьте, что оба сервера в вашей паре зарегистрировались в соответствующей зоне сервера DNS на первом сервере. Если серверы не зарегистрировались в процессе перезагрузки, сделайте принудительную регистрацию с помощью команды

ipconfig /registerdns

Проверьте, что на втором сервере произошла корректная передача зоны для вашего домена. Если автоматическая передача зоны не произошла, то сделайте это вручную в консоли DNS (Консоль DNS — Выбрать вашу зону, щелчок правой кнопки мыши — Выбрать "Все задачи" — Выбрать "Передать зону с основного сервера")

Задание 7. Проверка коммуникаций

Проверка с помощью команды ping коммуникаций по коротким именам компьютеров (NetBIOS-имена)

Выполните команду ping в таких вариантах:

ping <имя вашего компьютера>

ping <имя компьютера партнера в вашем домене>

Примеры (для компьютера S1.world.ru):

ping S1

Проверка с помощью команды ping коммуникаций по полным именам компьютеров (FQDN-имена)

Выполните команду ping в таких вариантах:

ping <имя вашего компьютера>

ping <имя компьютера партнера в вашем домене>

Примеры (для компьютеров world.ru):

ping S2.world.ru

ping S1.world.ru и т.д.

Результаты выполнения команд зафиксируйте в отчете.

Задание 8. Создание основной зоны обратного просмотра

Данное упражнение выполняйте на первом компьютере в вашей паре

Откройте консоль DNS

Выберите раздел "Зоны обратного просмотра"

Запустите мастер создания зоны (выбрать: тип зоны — "Основная", динамические обновления — разрешить, остальные параметры — по умолчанию)

В поле "Код сети (ID)" введите параметры идентификатора сети вашего класса из таблицы распределения IP-адресов и имен компьютеров

Пример 192.168.0

Задание 9. Тестирование регистрации узлов в зоне обратного просмотра

Данное упражнение выполняйте на обоих компьютерах в вашей паре

Выполните принудительную регистрацию вашего сервера в обратной зоне с помощью команды

ipconfig /registerdns

Проверьте, что имя вашего компьютера появилось в зоне обратного просмотра

Протестируйте разрешение IP-адресов компьютеров вашей пары в имена компьютеров командой

ping -a <IP-адрес компьютера>

Результаты выполнения команд зафиксируйте в отчете.

Задание 10. Диагностические утилиты для протокола tcp/ip: ipconfig, arp, ping, netstat, nbtstat, tracert, pathping

10.1 Команда ipconfig - служит для отображения всех текущих параметров сети TCP/IP и обновления параметров DHCP и DNS. При вызове команды ipconfig без параметров выводятся IP-адрес, маска подсети и основной шлюз для каждого сетевого адаптера.

/? - Отобразить справку по команде

/all - Отобразить полную информацию о настройке параметров всех адаптеров

/release - Освободить динамическую IP-конфигурацию

/renew - Обновить динамическую IP-конфигурацию с DHCP-сервера

/flushdns - Очистить кэш разрешений DNS

/registerdns - Обновить регистрацию на DNS-сервере

/displaydns - Отобразить содержимое кэша разрешений DNS

После изучения теоретического материала выполните команду ipconfig с параметрами:

/all

/flushdns

/registerdns

/displaydns

Результаты и пояснения зафиксируйте в отчете

10.2 Команда arp

Отображение и изменение ARP-таблиц.

-a - Отображает текущие ARP-записи

После изучения теоретического материала выполните команду arp с параметром: -a

Результаты и пояснения зафиксируйте в отчете

10.3 Команда ping

Ping - Мощный инструмент диагностики (с помощью протокола ICMP).

Формат команды:

"ping <сетевой узел> параметры"

Параметры: -t - Бесконечная (до нажатия клавиш <Ctrl>+<Break>) отправка пакетов на указанный узел

-a - Определение имени узла по IP-адресу

-n <число> - Число отправляемых запросов

-l <размер> - Размер буфера отправки

-w <таймаут> - Таймаут ожидания каждого ответа в миллисекундах

Команда ping позволяет проверить:

работоспособность IP-соединения;

правильность настройки протокола TCP/IP на узле;

работоспособность маршрутизаторов;

работоспособность системы разрешения имен FQDN или NetBIOS;

доступность и работоспособность какого-либо сетевого ресурса.

После изучения теоретического материала выполните команду ping с параметрами: -t, -a, -n count, -l size, -w timeout

Результаты и пояснения зафиксируйте в отчете

10.4 Команда netstat - используется для отображения статистики протокола и текущих TCP/IP-соединений. Параметры:

-a - Отображение всех подключений и ожидающих (слушающих) портов

-n - Отображение адресов и номеров портов в числовом формате

-o - Отображение кода (ID) процесса каждого подключения

-r - Отображение содержимого локальной таблицы маршрутов

После изучения теоретического материала выполните команду netstat с параметрами: <без параметров>

10.5 Команда nbtstat

Nbtstat - Средство диагностики разрешения имен NetBIOS

–n - Выводит имена пространства имен NetBIOS, зарегистрированные локальными процессами

–c - Отображает кэш имен NetBIOS (разрешение NetBIOS-имен в IP-адреса)

–R - Очищает кэш имен и перезагружает его из файла Lmhosts

–RR - Освобождает имена NetBIOS, зарегистрированные на WINS-сервере, а затем обновляет их регистрацию

После изучения теоретического материала выполните команду nbtstat с параметрами: -c

-n

-r

Результаты и пояснения зафиксируйте в отчете

10.6 Команды tracert, pathping

Tracert - служебная программа для трассировки маршрутов, используемая для определения пути, по которому IP-дейтаграмма доставляется по месту назначения.

-d - Без разрешения IP-адресов в имена узлов

-h <максЧисло> - Максимальное число прыжков при поиске узла

-w <таймаут> - Таймаут каждого ответа в миллисекундах

Pathping - средство трассировки маршрута, сочетающее функции программ ping и tracert и обладающее дополнительными возможностями.

Эта команда показывает степень потери пакетов на любом маршрутизаторе или канале, с ее помощью легко определить, какие маршрутизаторы или каналы вызывают неполадки в работе сети.

-n - Без разрешения IP-адресов в имена узлов

-h максЧисло - Максимальное число прыжков при поиске узла

-q <число_запросов> - Число запросов при каждом прыжке

-w <таймаут> - Таймаут каждого ответа в миллисекундах

Если у вас есть другие сети, для которых существуют маршруты из сети компьютерного класса, то выполните команды:

tracert -d <узел в удаленной 1P-сети>

tracert <узел в удаленной 1P-сети>

pathping -n <узел в удаленной 1P-сети>

pathping <узел в удаленной 1P-сети>

Изучите результаты работы данных команд на компьютере, имеющем выход в другие сети (например интернет), обсудите их с преподавателем. Результаты работы этих утилит зафиксируйте в отчете. Сформулируйте выводы.

Примечания.

Команды netstat, nbtstat полезно повторить после изучения различных сетевых служб (служб каталогов, файлов и печати, DNS, DHCP, WINS). После прохождения соответствующих тем студенты/слушатели будут иметь более четкое представление об использовании таких понятий как IP-адрес и порт, а также понятий сеанс, соединение, слушающий порт, интерфейс NetBIOS и др.

Задание 11. Завершающие действия

1 Удаление зон

Откройте консоль DNS. Удалите все зоны, которые были созданы в процессе выполнений предыдущих упражнений

2 Ссылки на серверы DNS в свойствах протокола TCP/IP

В свойствах TCP/IP вашего компьютера сделайте такие ссылки на серверы DNS:

предпочитаемый сервер DNS — первый компьютер в вашей паре

альтернативные серверы DNS — второй компьютер в паре и компьютер преподавателя

3 Удаление DNS-суффикса

Откройте "Мой компьютер"— "Свойства"— закладка "Имя компьютера"— кнопка "Изменить"— кнопка "Дополнительно"— очистите значение поля "Основной DNS-суффикс компьютера"

Перезагрузите компьютер.

Практическая работа 7. Управление объектами Active Directory утилитами командной строки

Цель работы: изучение способов управления объектами Active Directory утилитами командной строки

Теоретический материал

Современные сети часто состоят из *множества* различных программных платформ, большого разнообразия оборудования и программного обеспечения. Пользователи зачастую вынуждены запоминать большое количество паролей для доступа к различным сетевым ресурсам. *Права* доступа могут быть различными для одного и того же сотрудника в зависимости от того, с какими ресурсами он работает. Все это множество взаимосвязей требует от администратора и пользователя огромного количества времени на *анализ*, запоминание и обучение.

Решение проблемы управления такой разнородной сетью было найдено с разработкой службы каталога. Службы каталога предоставляют возможности управления любыми ресурсами и сервисами из любой точки независимо от размеров сети, используемых операционных систем и сложности оборудования. *Информация* о пользователе, заносится единожды в службу каталога, и после этого становится доступной в пределах всей сети. Адреса электронной почты, принадлежность к группам, необходимые *права* доступа и учетные записи для работы с различными операционными системами — все это создается и поддерживается в актуальном виде автоматически. Любые изменения, занесенные в службу каталога администратором, сразу обновляются *по* всей сети. Администраторам уже не нужно беспокоиться об уволенных сотрудниках — просто удалив учетную *запись* пользователя из службы каталога, он сможет гарантировать автоматическое удаление всех прав доступа на ресурсы сети, предоставленные ранее этому сотруднику.

В настоящее время большинство служб каталогов различных фирм базируются на стандарте *X.500*. Для доступа к информации, хранящейся в службах каталогов, обычно используется протокол *Lightweight Directory Access Protocol* (*LDAP*). В связи со стремительным развитием сетей *TCP/IP*, протокол *LDAP* становится стандартом для служб каталогов и приложений, ориентированных на использование службы каталога.

Служба каталогов Active Directory является основой логической структуры корпоративных сетей, базирующихся на системе *Windows*. Термин " *Каталог* " в самом широком смысле означает " *Справочник* ", а *служба каталогов* корпоративной сети — это централизованный корпоративный справочник. Корпоративный каталог может содержать информацию об объектах различных типов. *Служба каталогов Active Directory* содержит в первую *очередь* объекты, на которых базируется система безопасности сетей *Windows,* — учетные записи пользователей, групп и компьютеров. Учетные записи организованы в логические структуры: *домен, дерево*, *лес*, организационные *подразделения*.

Основные термины и понятия (лес, дерево, домен, организационное подразделение). Планирование пространства имен AD. Установка контроллеров доменов

Модели управления безопасностью: модель "Рабочая группа" и централизованная доменная модель

Как уже говорилось выше, основное назначение служб каталогов — управление сетевой безопасностью. Основа сетевой безопасности — база данных учетных записей (accounts) пользователей, групп пользователей и компьютеров, с помощью которой осуществляется управление доступом к сетевым ресурсам. Прежде чем говорить о службе каталогов Active Directory, сравним две модели построения базы данных служб каталогов и управления доступом к ресурсам.

Модель "Рабочая группа"

Данная модель управления безопасностью корпоративной сети — самая примитивная. Она предназначена для использования в небольших *одноранговых сетях* (3–10 компьютеров) и основана на том, что каждый компьютер в сети с операционными системами Windows NT/2000/XP/2003 имеет свою собственную локальную базу данных учетных записей и с помощью этой *локальной БД* осуществляется управление доступом к ресурсам данного компьютера. *Локальная БД* учетных записей называется база данных *SAM* (*Security Account Manager*) и хранится в реестре операционной системы. Базы данных отдельных компьютеров полностью изолированы друг от друга и никак не связаны между собой.

Пример управления доступом при использовании такой модели изображен на рис. 6.1.

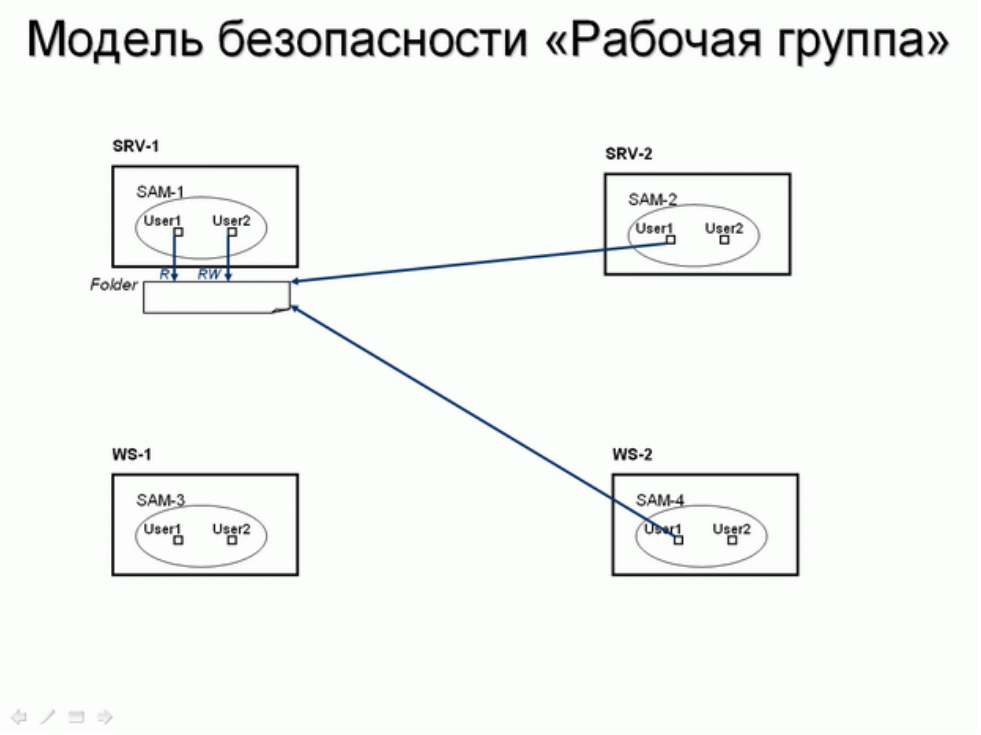


Рис. 6.1.

В данном примере изображены два сервера (SRV-1 и SRV-2) и две рабочие станции (WS-1 и WS-2). Их базы данных SAM обозначены соответственно SAM-1, SAM-2, SAM-3 и SAM-4 (на рисунке базы SAM изображены в виде овала). В каждой БД есть учетные записи пользователей User1 и User2. Полное имя пользователя User1 на сервере SRV-1 будет выглядеть как "SRV-1\User1", а полное имя пользователя User1 на рабочей станции WS-1 будет выглядеть как "WS-1\User1". Представим, что на сервере SRV-1 создана папка Folder, к которой предоставлен доступ по сети пользователям User1 — на чтение (R), User2 — чтение и запись (RW). Главный момент в этой модели заключается в том, что компьютер

SRV-1 ничего "не знает" об учетных записях компьютеров SRV-2, WS-1, WS-2, а также всех остальных компьютеров сети. Если пользователь с именем User1локально зарегистрируется в системе на компьютере, например, WS-2 (или, как еще говорят, "войдет в систему с локальным именем User1 на компьютере WS-2"), то при попытке получить доступ с этого компьютера по сети к папке Folder на сервере SRV-1 сервер запросит пользователя ввести имя и пароль (исключение составляет тот случай, если у пользователей с одинаковыми именами одинаковые пароли).

Модель "Рабочая группа" более проста для изучения, здесь нет необходимости изучать сложные понятия Active Directory. Но при использовании в сети с большим количеством компьютеров и сетевых ресурсов становится очень сложным управлять именами пользователей и их паролями — приходится на каждом компьютере (который предоставляет свои ресурсы для совместного использования в сети) вручную создавать одни и те же учетные записи с одинаковыми паролями, что очень трудоемко, либо делать одну учетную запись на всех пользователей с одним на всех паролем (или вообще без пароля), что сильно снижает уровень защиты информации. Поэтому модель "Рабочая группа" рекомендуется только для сетей с числом компьютеров от 3 до 10 (а еще лучше — не более 5), при условии что среди всех компьютеров нет ни одного с системой Windows Server.

Доменная модель

В доменной модели существует единая база данных служб каталогов, доступная всем компьютерам сети. Для этого в сети устанавливаются специализированные серверы, называемые *контроллерами домена*, которые хранят на своих жестких дисках эту базу. На рис. 6.2. изображена схема доменной модели. Серверы DC-1 и DC-2 — контроллеры домена, они хранят доменную базу данных учетных записей (каждый контроллер хранит у себя свою собственную копию БД, но все изменения, производимые в БД на одном из серверов, реплицируются на остальные контроллеры).

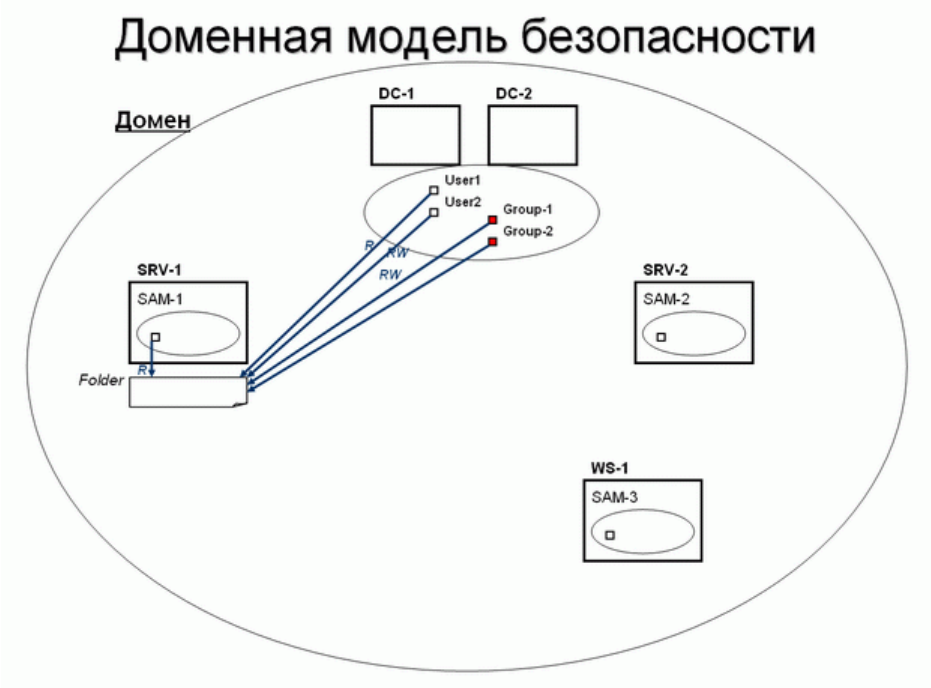


Рис. 6.2.

В такой модели, если, например, на сервере SRV-1, являющемся членом домена, предоставлен общий доступ к папке Folder, то права доступа к данному ресурсу можно назначать не только для учетных записей локальной базы SAM данного сервера, но, самое главное, учетным записям, хранящимся в доменной БД. На рисунке для доступа к папке Folder даны права доступа одной локальной учетной записи компьютера SRV-1 и

нескольким учетным записям домена (пользователя и группам пользователей). В доменной модели управления безопасностью пользователь регистрируется на компьютере ("входит в систему") со своей *доменной учетной записью* и, независимо от компьютера, на котором была выполнена регистрация, получает доступ к необходимым сетевым ресурсам. И нет необходимости на каждом компьютере создавать большое количество локальных учетных записей, все записи созданы *однократно в доменной БД*. И с помощью доменной базы данных осуществляется *централизованное управление доступом* к сетевым ресурсам *независимо от количества компьютеров в сети*.

Назначение службы каталогов Active Directory

Каталог (справочник) может хранить различную информацию, относящуюся к пользователям, группам, компьютерам, сетевым принтерам, общим файловым ресурсам и так далее — будем называть все это объектами. Каталог хранит также информацию о самом объекте, или его свойства, называемые атрибутами. Например, атрибутами, хранимыми в каталоге о пользователе, может быть имя его руководителя, номер телефона, *адрес*, имя для входа в систему, *пароль, группы*, в которые он входит, и многое другое. Для того чтобы сделать хранилище каталога полезным для пользователей, должны существовать службы, которые будут взаимодействовать с каталогом. Например, можно использовать каталог как хранилище информации, *по* которой можно аутентифицировать пользователя, или как *место*, куда можно послать *запрос* для того, чтобы найти информацию об объекте.

Active Directory отвечает не только за создание и организацию этих небольших объектов, но также и за большие объекты, такие как домены, OU (организационные *подразделения*) и сайты.

Об основных терминах, используемых в контексте службы каталогов *Active Directory*, читайте ниже.

Служба каталогов Active Directory (сокращенно — *AD*) обеспечивает эффективную работу сложной корпоративной среды, предоставляя следующие возможности:

- *Единая регистрация в сети* ; Пользователи могут регистрироваться в сети с одним именем и паролем и получать при этом доступ ко всем сетевым ресурсам и службам (службы сетевой инфраструктуры, службы файлов и печати, серверы приложений и баз данных и т. д.);
- *Безопасность информации*. Средства аутентификации и управления доступом к ресурсам, встроенные в службу Active Directory, обеспечивают централизованную защиту сети;
- *Централизованное управление*. Администраторы могут централизованно управлять всеми корпоративными ресурсами;
- *Администрирование с использованием групповых политик*. При загрузке компьютера или регистрации пользователя в системе выполняются требования групповых политик; их настройки хранятся в *объектах групповых политик* (*GPO*) и применяются ко всем учетным записям пользователей и компьютеров, расположенных в сайтах, доменах или организационных подразделениях;
- *Интеграция с DNS*. Функционирование служб каталогов полностью зависит от работы службы DNS. В свою очередь серверы DNS могут хранить информацию о зонах в базе данных Active Directory;
- *Расширяемость каталога*. Администраторы могут добавлять в схему каталога новые классы объектов или добавлять новые атрибуты к существующим классам;
- *Масштабируемость*. Служба Active Directory может охватывать как один домен, так и множество доменов, объединенных в дерево доменов, а из нескольких деревьев доменов может быть построен лес;
- *Репликация информации*. В службе Active Directory используется репликация служебной информации в схеме со многими ведущими (*multi-master*), что позволяет модифицировать БД Active Directory на любом контроллере домена.

Наличие в домене нескольких контроллеров обеспечивает отказоустойчивость и возможность распределения сетевой нагрузки;

- *Гибкость запросов к каталогу*. БД Active Directory может использоваться для быстрого поиска любого объекта AD, используя его свойства (например, имя пользователя или адрес его электронной почты, тип принтера или его местоположение и т. п.);
- *Стандартные интерфейсы программирования*. Для разработчиков программного обеспечения служба каталогов предоставляет доступ ко всем возможностям (средствам) каталога и поддерживает принятые стандарты и интерфейсы программирования (API).

В *Active Directory* может быть создан широкий круг различных объектов. *Объект* представляет собой уникальную сущность внутри Каталога и обычно обладает многими атрибутами, которые помогают описывать и распознавать его. Учетная *запись* пользователя является примером объекта. Этот *тип объекта* может иметь множество атрибутов, таких как имя, фамилия, *пароль*, номер телефона, *адрес* и многие другие. Таким же образом общий принтер тоже может быть объектом в *Active Directory* и его атрибутами являются его имя, местоположение и т.д. Атрибуты объекта не только помогают определить *объект*, но также позволяют вам искать объекты внутри Каталога.

Терминология

Служба каталогов системы *Windows Server* построена на общепринятых технологических стандартах. Изначально для служб каталогов был разработан стандарт *X.500*, который предназначался для построения иерархических древовидных масштабируемых справочников с возможностью расширения как классов объектов, так и наборов атрибутов (свойств) каждого отдельного класса. Однако практическая реализация этого стандарта оказалась неэффективной с точки зрения производительности. Тогда на базе стандарта X.500 была разработана упрощенная (облегченная) версия стандарта построения каталогов, получившая название *LDAP* (*Lightweight Directory Access Protocol*). Протокол *LDAP* сохраняет все основные свойства X.500 (иерархическая система построения справочника, *масштабируемость*, *расширяемость*), но при этом позволяет достаточно эффективно реализовать данный стандарт на практике. Термин " *lightweight* " (" *облегченный* ") в названии *LDAP* отражает основную цель разработки протокола: создать *инструментарий* для построения службы каталогов, которая обладает достаточной функциональной мощью для решения базовых задач, но не перегружена сложными технологиями, делающими реализацию служб каталогов неэффективной. В настоящее время *LDAP* является стандартным методом доступа к информации сетевых каталогов и играет роль фундамента во множестве продуктов, таких как *системы аутентификации*, почтовые программы и приложения электронной коммерции. Сегодня на рынке присутствует более 60 коммерческих серверов *LDAP*, причем около 90% из них представляют собой самостоятельные серверы каталогов *LDAP*, а остальные предлагаются в качестве компонентов других приложений.

Протокол *LDAP* четко определяет круг операций над каталогами, которые может выполнять клиентское *приложение*. Эти *операции* распадаются на пять групп:

- установление связи с каталогом;
- поиск в нем информации;
- модификация его содержимого;
- добавление объекта;
- удаление объекта.

Кроме протокола *LDAP служба каталогов Active Directory* использует также протокол аутентификации *Kerberos* и службу *DNS* для поиска в сети *компонент* служб каталогов (контроллеры доменов, *серверы глобального каталога*, службу Kerberos и др.).

Домен

Основной единицей системы безопасности Active Directory является *домен*. Домен формирует область административной ответственности. База данных домена содержит учетные записи *пользователей, групп* и *компьютеров*. Большая часть функций по управлению службой каталогов работает на уровне домена (аутентификация пользователей, управление доступом к ресурсам, управление службами, управление репликацией, политики безопасности).

Имена доменов Active Directory формируются по той же схеме, что и имена в пространстве имен DNS. И это не случайно. Служба DNS является средством поиска компонент домена — в первую очередь контроллеров домена.

Контроллеры домена — специальные серверы, которые хранят соответствующую данному домену часть базы данных Active Directory. Основные функции контроллеров домена:

- **хранение БД Active Directory** (организация доступа к информации, содержащейся в каталоге, включая управление этой информацией и ее модификацию);
- **синхронизация изменений в AD** (изменения в базу данных AD могут быть внесены на любом из контроллеров домена, любые изменения, осуществляемые на одном из контроллеров, будут синхронизированы с копиями, хранящимися на других контроллерах);
- **аутентификация пользователей** (любой из контроллеров домена осуществляет проверку полномочий пользователей, регистрирующихся на клиентских системах).

Настоятельно рекомендуется в каждом домене устанавливать не менее двух контроллеров домена — во-первых, для защиты от потери БД Active Directory в случае выхода из строя какого-либо контроллера, во-вторых, для распределения нагрузки между контроллерами.

Дерево

Дерево является набором доменов, которые используют единое связанное пространство имен. В этом случае "дочерний" домен наследует свое имя от "родительского" домена. Дочерний домен автоматически устанавливает двухсторонние транзитивные доверительные отношения с родительским доменом. Доверительные отношения означают, что ресурсы одного из доменов могут быть доступны пользователям других доменов.

Пример дерева Active Directory изображен на рис. 6.3. В данном примере домен company.ru является доменом Active Directory верхнего уровня. От корневого домена отходят дочерние домены it.company.ru и fin.company.ru. Эти домены могут относиться соответственно к ИТ-службе компании и финансовой службе. У домена it.company.ru есть поддомен dev.it.company.ru, созданный для отдела разработчиков ПО ИТ-службы.

Корпорация Microsoft рекомендует строить Active Directory в виде одного домена. Построение дерева, состоящего из многих доменов необходимо в следующих случаях:

- для децентрализации администрирования служб каталогов (например, в случае, когда компания имеет филиалы, географически удаленные друг от друга, и централизованное управление затруднено по техническим причинам);
- для повышения производительности (для компаний с большим количеством пользователей и серверов актуален вопрос повышения производительности работы контроллеров домена);
- для более эффективного управления репликацией (если контроллеры доменов удалены друг от друга, то репликация в одном может потребовать больше времени и создавать проблемы с использованием несинхронизированных данных);
- для применения различных политик безопасности для различных подразделений компании;
- при большом количестве объектов в БД Active Directory.

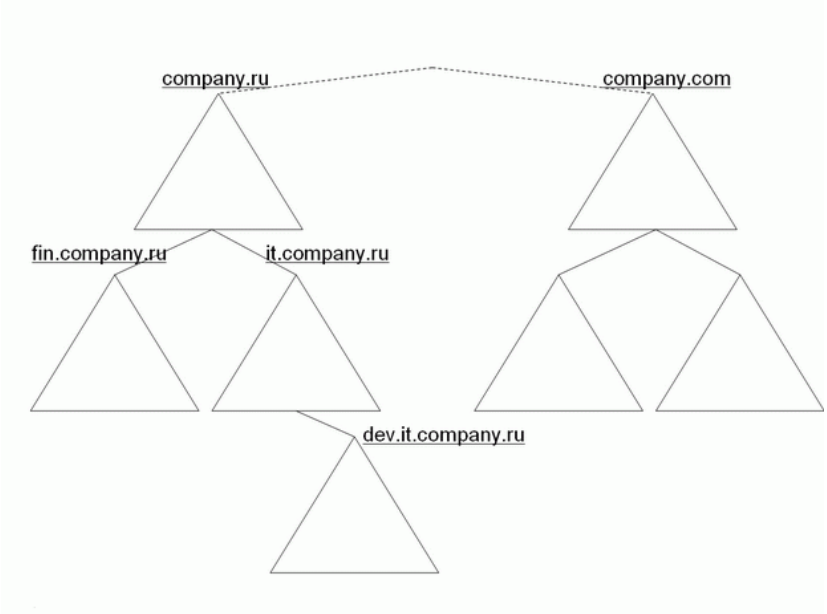


Рис. 6.3.

Лес

Наиболее крупная структура в Active Directory. Лес объединяет деревья, которые поддерживают единую схему (*схема Active Directory* — набор определений типов, или классов, объектов в БД Active Directory). В лесу между всеми доменами установлены двухсторонние транзитивные доверительные отношения, что позволяет пользователям любого домена получать доступ к ресурсам всех остальных доменов, если они имеют соответствующие разрешения на доступ. По умолчанию, первый домен, создаваемый в лесу, считается его корневым доменом, в корневом домене хранится схема AD.

Новые деревья в лесу создаются в том случае, когда необходимо построить иерархию доменов с пространством имен, отличным от других пространств леса. В примере на рис. 6.3 российская компания могла открыть офис за рубежом и для своего зарубежного отделения создать дерево с доменом верхнего уровня company.com. При этом оба дерева являются частями одного леса с общим "виртуальным" корнем.

При управлении деревьями и лесами нужно помнить два очень важных момента:

- первое созданное в лесу *доменов дерево* является *корневым деревом*, первый созданный в дереве домен называется *корневым доменом дерева* (*tree root domain*);
- первый домен, созданный в лесу доменов, называется *корневым доменом леса* (*forest root domain*), данный домен не может быть удален (он хранит информацию о конфигурации леса и деревьях доменов, его образующих).

Организационные подразделения (ОП).

Организационные подразделения (*Organizational Units, OU*) — контейнеры внутри AD, которые создаются для объединения объектов в целях *делегирования административных прав* и *применения групповых политик* в домене. ОП существуют *только внутри доменов* и могут объединять *только объекты из своего домена*. ОП могут быть вложенными друг в друга, что позволяет строить внутри домена сложную древовидную иерархию из контейнеров и осуществлять более гибкий административный контроль. Кроме того, ОП могут создаваться для отражения административной иерархии и организационной структуры компании.

Глобальный каталог

Глобальный каталог является перечнем *всех объектов*, которые существуют в лесу Active Directory. По умолчанию, контроллеры домена содержат только информацию об объектах своего домена. *Сервер Глобального каталога* является контроллером домена, в

котором содержится информация о каждом объекте (хотя и не обо всех атрибутах этих объектов), находящемся в данном лесу.

Именование объектов

В службе каталогов должен быть механизм именования объектов, позволяющий однозначно идентифицировать любой объект каталога. В каталогах на базе протокола LDAP *для идентификации объекта в масштабе всего леса* используется механизм *отличительных имен* (*Distinguished Name, DN*). В Active Directory учетная запись пользователя с именем *User* домена company.ru, размещенная в стандартном контейнере *Users*, будет иметь следующее отличительное имя: "DC=ru, DC=company, OU=Users, CN=User".

Обозначения:

- **DC** (Domain Component) — указатель на составную часть доменного имени;
- **OU** (Organizational Unit) — указатель на организационное подразделение (ОП);
- **CN** (Common Name) — указатель на общее имя.

Если отличительное имя однозначно определяет объект в масштабе всего леса, то для идентификации объекта относительно контейнера, в котором данный объект хранится, существует относительное отличительное имя (*Relative Distinguished Name, RDN*). Для пользователя *User* из предыдущего примера RDN-имя будет иметь вид " *CN=User* ".

Кроме имен DN и RDN, используется *основное имя* объекта (*User Principal Name, UPN*). Оно имеет формат <имя субъекта>@<суффикс домена>. Для того же пользователя из примера основное имя будет выглядеть как User@company.ru.

Имена DN, RDN могут меняться, если объект перемещается из одного контейнера AD в другой. Для того чтобы не терять ссылки на объекты при их перемещении в лесу, всем объектам назначается *глобально уникальный идентификатор* (*Globally Unique Identifier, GUID*), представляющий собой 128-битное число.

Планирование пространства имен AD

Планирование пространства имен и структуры *AD* — очень ответственный момент, от которого зависит эффективность функционирования будущей корпоративной системы безопасности. При этом надо иметь в виду, что созданную вначале структуру в процессе эксплуатации будет очень трудно изменить (например, в *Windows 2000* изменить имя домена верхнего уровня вообще невозможно, а в *Windows* 2003 решение этой задачи требует выполнения жестких условий и тщательной подготовки данной *операции*). При планировании *AD* необходимо учитывать следующие моменты:

- тщательный выбор имен доменов верхнего уровня;
- качество коммуникаций в компании (связь между отдельными подразделениями и филиалами);
- организационная структура компании;
- количество пользователей и компьютеров в момент планирования;
- прогноз темпов роста количества пользователей и компьютеров.

Рассмотрим вопрос пространства имен *AD*.

При планировании имен доменов верхнего уровня можно использовать различные стратегии и правила. В первую *очередь* необходимо учитывать вопросы интеграции внутреннего пространства имен и пространства имен сети *Интернет* — т.к. *пространство имен AD* базируется на пространстве имен *DNS*, при неправильном планировании могут возникнуть проблемы с безопасностью, а также конфликты с внешними именами.

Рассмотрим основные варианты.

1. Один домен, одна зона DNS (рис. 6.4).

На рисунке в левой части — внутренняя сеть компании, справа — сеть Интернет, две сети разделены маршрутизатором " *R* " (кроме маршрутизатора, на границе могут быть также прокси-сервер или межсетевой экран).

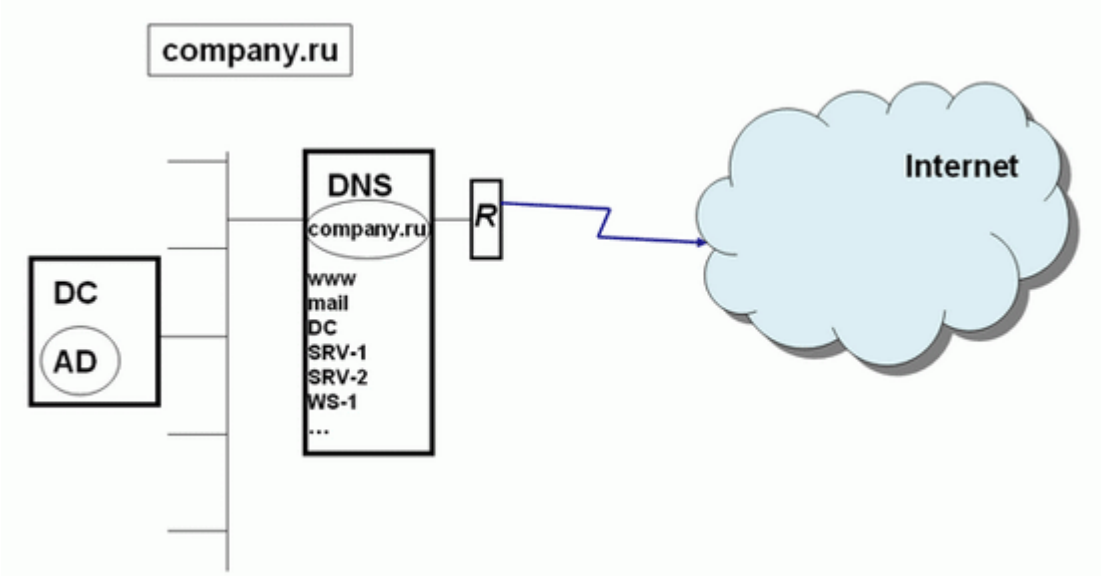


Рис. 6.4.

В данном примере используется одна и та же зона DNS (company.ru) как для поддержки внутреннего домена AD с тем же именем (записи DC, SRV-1, SRV-2, WS-1), так и хранения ссылок на внешние ресурсы компании — веб-сайт, почтовый сервер (записи www, mail).

Такой способ максимально упрощает работу системного администратора, но при этом DNS-сервер, доступный для всей сети Интернет, хранит зону company.ru и предоставляет доступ к записям этой зоны всем пользователям Интернета. Таким образом, внешние злоумышленники могут получить полный список внутренних узлов корпоративной сети. Даже если сеть надежно защищена межсетевым экраном и другими средствами защиты, предоставление потенциальным взломщикам информации о структуре внутренней сети — вещь очень рискованная, поэтому данный способ организации пространства имен AD не рекомендуется (хотя на практике встречается довольно часто).

2. "Расщепление" пространства имен DNS - одно имя домена, две различные зоны DNS(рис. 6.5).

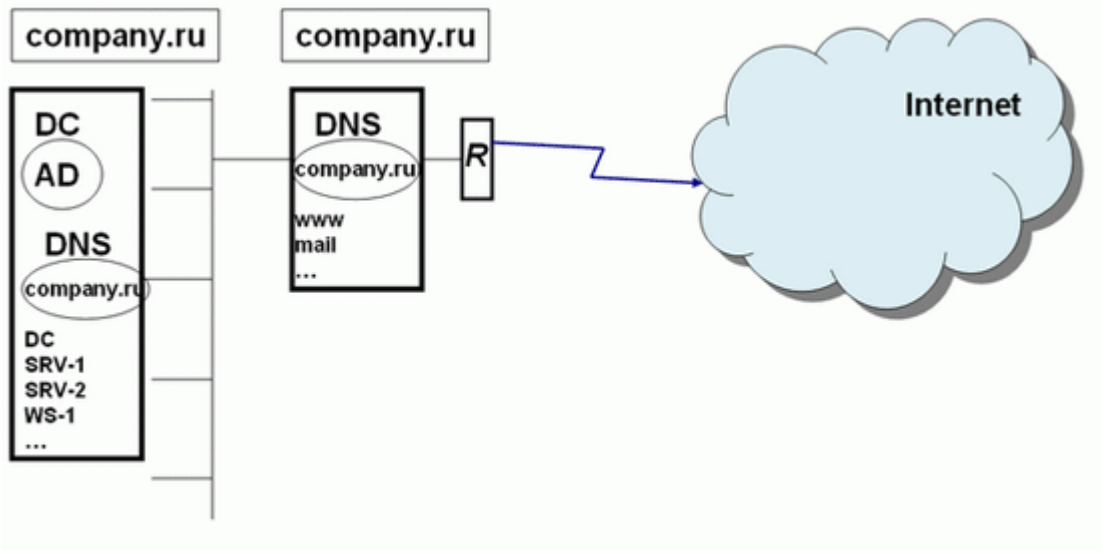


Рис. 6.5.

В данном случае на различных серверах DNS создаются различные зоны с одним и тем же именем company.ru. На внутреннем DNS-сервере функционирует зона company.ru.для Active Directory, на внешнем DNS-сервере — зона с таким же именем, но

для ссылок на внешние ресурсы. Важный момент — данные зоны никак между собой не связаны — ни механизмами репликации, ни ручной синхронизацией.

Здесь во внешней зоне хранятся ссылки на внешние ресурсы, а во внутренней на внутренние ресурсы, используемые для работы Active Directory. Данный вариант несложно реализовать, но для сетевого администратора возникает нагрузка управления двумя разными доменами с одним именем.

3. Поддомен в пространстве имен DNS для поддержки Active Directory (рис. 6.6).

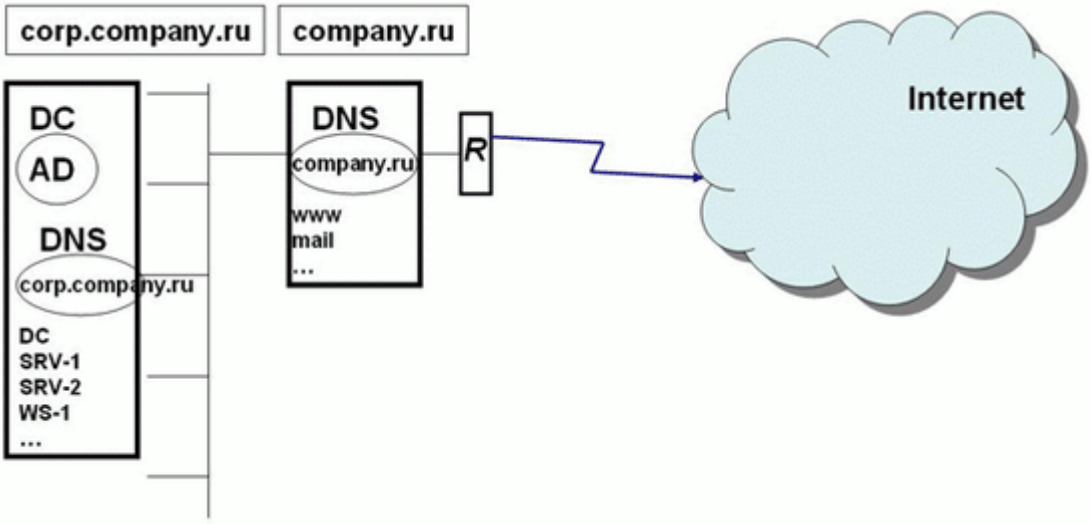


Рис. 6.6.

В данном примере корневой домен компании company.ru служит для хранения ссылок на внешние ресурсы. В домене company.ru настраивается делегирование управление поддоменом corp.company.ru на внутренний DNS-сервер, и именно на базе домена corp.company.ru создается домен Active Directory. В этом случае во внешней зоне хранятся ссылки на внешние ресурсы, а также ссылка на делегирование управления поддоменом на внутренний DNS-сервер. Таким образом, пользователям Интернета доступен минимум информации о внутренней сети. Такой вариант организации пространства имен довольно часто используется компаниями.

4. Два различных домена DNS для внешних ресурсов и для Active Directory (рис. 6.7.).

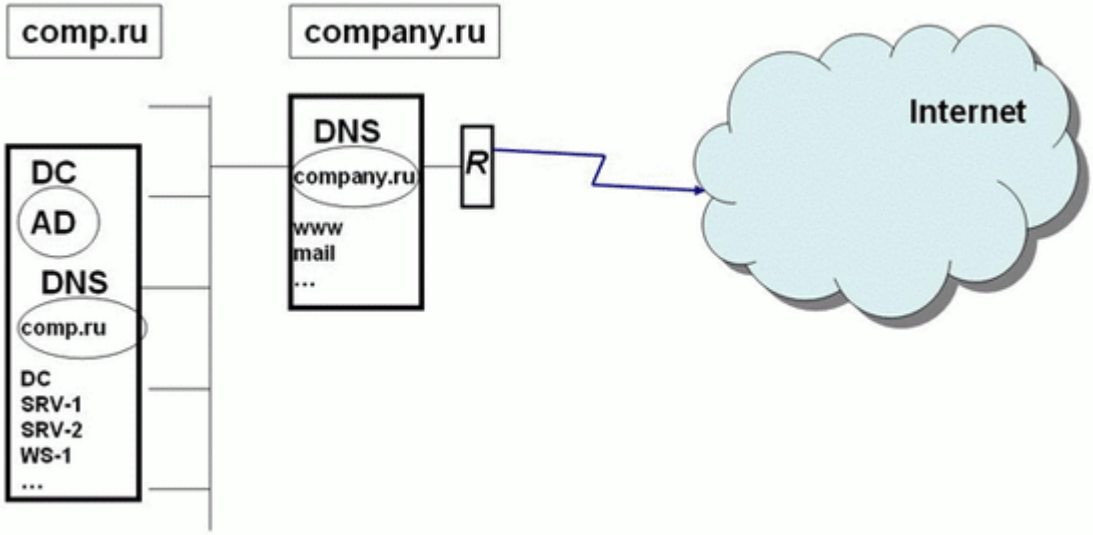


Рис. 6.7.

В этом сценарии компания регистрирует в Интернет-органах два доменных имени: одно для публикации внешних ресурсов, другое — для развертывания Active Directory.

Данный сценарий планирования пространства имен самый оптимальный. Во-первых, имя внешнего домена никак не связано с именем внутреннего домена, и не возникает никаких проблем с возможностью показа в Интернет внутренней структуры. Во-вторых, регистрация (покупка) внутреннего имени гарантирует отсутствие потенциальных конфликтов, вызванных тем, что какая-то другая компания может зарегистрировать в Интернете имя, совпадающее с внутренним именем вашей компании.

5. Домен с именем типа company.local.

Во многих учебных пособиях и статьях используются примеры с доменными именами вида company.local. Такая схема вполне работоспособна и также часто применяется на практике. Однако в материалах разработчика системы Windows, корпорации Microsoft, нет прямых рекомендаций об использовании данного варианта.

Ход работы

Задание Управление Active Directory из командной строки

Большинство утилит, которые будут описаны, работают с объектами службы каталогов, а именование этих объектов осуществляется по определенным стандартам. Поэтому вполне уместным будет посвятить несколько строк правилам именования объектов Active Directory.

Схема Active Directory

1. Схема службы каталогов – это набор классов. Учетные записи пользователей, компьютеров, группы, общие ресурсы – все это классы объектов. Каждый объект имеет определенный набор атрибутов. Например, для учетных записей это имя, фамилия сотрудника, имя входа в домен и другая информация. Конкретно взятый объект, например, учетная запись пользователя Иван Иванов, называется экземпляром класса. Атрибуты и классы определяются независимо, поэтому один атрибут может быть связан с несколькими классами. Каждый атрибут класса имеет свой синтаксис – набор символов, которые могут использоваться в описании атрибута.

Существуют также объекты контейнерного типа. Они могут содержать в себе другие объекты и, как правило, используются для объединения объектов, имеющих одинаковые атрибуты.

2. Опишем принятые в службе каталогов форматы имен.

UPN (User Principal Name) – формат имени, схожий с адресом электронной почты (описанным в RFC 822); такое именование может использоваться для входа пользователя в домен (например, ivanov@domain.com).

3. Следующее в рассмотрении – имена в формате LDAP (Lightweight Directory Access Protocol, облегченная версия протокола X.500 для доступа к каталогу). Каждый объект службы каталогов имеет свое, так называемое уникальное имя (DN, Distinguished Name). Стандарт такого именования описан в RFC 1779 и определяет однозначное нахождение объекта в каталоге. В свою очередь в RFC 2247 описано отображение пространства имен DNS службы каталогов в формате LDAP. Таким образом, пользователь Иван Иванов, принадлежащий группе Managers организационной единицы Office домена domain.com, может иметь следующее DN:

cn=Ivanov, cn=Managers, ou=Office, dc=domain, dc=com;

здесь cn – Common Name, простое имя объекта; ou – Organizational Unit, организационная единица; dc – Domain Component, домен, которому принадлежит объект.

4. Относительное уникальное имя объекта (RDN, Relative Distinguished Name) идентифицирует непосредственно сам объект относительно объекта-контейнера, которому он принадлежит. Здесь RDN объекта Ivanov будет выглядеть как cn=Ivanov, а для родительского объекта Managers – cn=Managers. RND является атрибутом объекта и хранится в каталоге вместе с объектом. Вместе с этим каждый объект имеет атрибут, который является указателем на объект-родитель. Таким образом, имеется возможность создания RDN для любого объекта в каталоге.

5. Аналогично с уникальными именами для однозначного определения местоположения объекта в каталоге можно использовать так называемое каноническое имя. Оно схоже с URL страницы или объекта на веб-сервере и для указанного выше примера выглядит следующим образом:

   domain.com/Office/Managers/Ivanov

6. Есть еще одна вещь, которая однозначно определяет объект в каталоге, – глобальный уникальный идентификатор (GUID, Global Unique Identifier). Это 128-разрядное число, которое является обязательным атрибутом любого объекта. GUID присваивается объекту при его создании, является уникальным и не может измениться ни при каких обстоятельствах. Мы можем переместить объект в схеме, при этом изменится уникальное имя объекта, но его идентификатор останется прежним.

Утилиты для поиска, добавления и модифицирования объектов

7. Операционные системы Windows Server 2003 и Windows XP имеют встроенный набор утилит для осуществления операций над объектами службы каталогов из командной строки. Это утилиты, начинающиеся с латинских букв ds (синтаксис всех команд можно посмотреть, введя в качестве параметра /?):
   - **dsquery** – ищет объект по заданным условиям;
   - **dsget** – получает свойства объекта;
   - **dsadd** – добавляет объект;
   - **dsmod** – изменяет атрибуты объекта;
   - **dsmove** – перемещает объект внутри домена;
   - **dsrm** – служит для удаления объектов из каталога.

Каждая утилита командной строки работает с определенным набором объектов службы каталогов. В таблице указано, с каким объектом может работать утилита, а с каким нет.

Утилиты ds* и объекты, с которыми они могут работать

Объект	**dsquery**	**dsget**	**dsadd**	dsmod	**dsmove**	**dsrm**
User	+	+	+	+	+	+
Contact	+	+	+	+	+	+
Group	+	+	+	+	+	+
Computer	+	+	+	+	+	+
OU	+	+	+	+	+	+
Server	+	+	–	+	+	+
Site	+	+	–	–	+	+
Subnet	+	+	–	–	+	+
Partition	+	+	–	+	+	+
Quota	+	+	+	+	+	+

8. Некоторые команды имеют систему подкоманд, в которых явным образом указывается, с каким объектом вы будете работать, а также перечень параметров. Рассмотрим запрос к службе каталогов.

>dsquery computer -name buh*

Результатом выполнения данного запроса будет список имен компьютеров в домене, начинающихся с buh. Например:

```
"cn=buh01,cn=computers,dc=domain,dc=com"
"cn=buh02,cn=computers,dc=domain,dc=com"
"cn=buhgalter,ou=buhgalters,dc=domain,dc=com"
```

Как видите, результаты выводятся в формате DN.

Синтаксис подкоманд dsquery на первый взгляд может показаться сложным, хотя большинство параметров одинаково, а различаются они лишь расширениями, специфичными для заданного типа объекта.

9. Рассмотрим пример применения утилит dsadd и dsmod (в отличие от dsquery и dsget и наряду с dsmove и dsrm они вносят изменения в Active Directory):

>dsadd user "cn=Ivanov,cn=Users,dc=domain,dc=com" -pwd *

Команда создает пользователя с именем пред-Windows 2000 Ivanov в группе Users домена domain.com. При этом будут запрошены пароль и его подтверждение, потому как в параметре -pwd указана звездочка.

Может сложиться ситуация, когда введенный пароль не будет удовлетворять требованиям безопасности вашего домена (см. настройки политики паролей объекта GPO для домена). В этом случае учетная запись будет создана заблокированной и останется таковой до тех пор, пока вы не смените пароль на такой, который будет отвечать политикам вашего домена.

>dsmod user "cn=Ivanov,cn=Users,dc=domain,dc=com" -upn ivanov@domain.com

Данная команда добавляет логин пользователя в формате UPN.

Утилиту dsquery можно использовать конвейером с другими утилитами, и тогда в качестве входных данных для них будет браться результат команды dsquery. Приведу пример:

>dsquery user -name Ivanov | dsmod user -disabled yes

Dsmod в этом случае отключает учетную запись пользователя Ivanov, получая в качестве входных параметров результат выполнения запроса dsquery. В итоге вход в домен с использованием этой учетной записи будет невозможен.

Помимо встроенных средств Windows Server 2003 и Windows XP существует также ряд утилит, выпущенных сторонними разработчиками – экспертами в области Active Directory. Одним из них является Джо Ричардс – автор целого ряда утилит для мониторинга и управления службой каталогов. Мы рассмотрим лишь две из них. Желающие могут подробнее ознакомиться с остальными на сайте Джо (www.joeware.net).

10. Первая утилита, adfind, фактически является расширенным аналогом стандартной dsquery (скорее даже «солянкой» из dsquery, dsget, ldp и других полезных вещей) и позволяет осуществлять различные запросы к каталогу. Для установки нужно лишь скачать архив с программой и распаковать ее в системный каталог \Windows\system32. Для более подробного ознакомления с параметрами закидываем файл справки в текстовый документ:

>adfind -?? > c:\adfind_help.txt

От стандартных команд, формирующих запросы к каталогу, ее отличает следующее:

- она позволяет выполнять запросы любой сложности;
- полученные с ее помощью результаты запроса можно отсортировать, используя специальные ключи;
- она позволяет увидеть удаленные объекты;
- используя специальный ключ, можно увидеть параметры выполнения запроса, что в свою очередь способствует анализу эффективности конкретного запроса.

11. Рассмотрим простой пример ее применения. Пусть нам нужно найти все компьютеры, имена которых начинаются с buh в организационной единице buhgalteria домена domain.com:

>adfind –b "ou=buhgalteria,dc=domain,dc=com" -f "(&(objectcategory=computer)(name=buh*))"

Здесь мы указываем область поиска и параметры искомого объекта.

12. Вторая утилита от Джо Ричардса, admod, является расширенным аналогом стандартной dsmod (точнее некой смесью dsmod + dsmod + dsrm). В отличие от стандартных команд admod может работать с любыми объектами каталога. Нетрудно догадаться, что с ее помощью можно изменять, перемещать, переименовывать, удалять объекты, используя соответствующие параметры. Также эта утилита позволяет восстанавливать объекты после удаления, однако эта функция действует только в доменах Windows 2003.

Стоит отметить, что результаты запроса команды adfind могут быть использованы в качестве входных параметров команды admod.

Утилиты диагностики неисправностей службы каталогов и сетевой среды

13. Помимо начального планирования, разворачивания и настройки службы каталогов администраторы должны обеспечивать работоспособность и правильное взаимодействие всех компонентов Active Directory. Для решения задач отслеживания и устранения неисправностей существует ряд утилит, которые при обнаружении некорректной работы какого-либо компонента должны быть запущены в первую очередь. Такие инструменты входят в состав Support Tools (находятся на диске с операционной системой) и Resource Kit Tools (их вы найдете на сайте компании Microsoft).

Dcdiag

Эта утилита, входящая в состав Support Tools, позволяет провести диагностику контроллеров домена на предмет обнаружения ошибок в работе служб. Запустить ее можно как с компьютера под управлением Windows XP (при этом указав в параметрах целевой контроллер домена), так и непосредственно на самом контроллере. При запуске без ключей будет выведен результат 27 тестов, предназначение каждого из которых можно узнать, запустив dcdiag с ключом /?. Однозначно можно сказать, что эта утилита является одной из важнейших для администраторов службы каталогов.

Netdiag

«Инструмент», также входящий в состав Support Tools, служит скорее для диагностики проблем в сети, чем напрямую относится к средствам для выявления и устранения неполадок в работе службы каталогов. При его запуске будет проведен ряд проверок, таких как проверка DNS, тест доступности контроллера домена, проверка конфигурации IP-адреса, проверка LDAP, основного шлюза и таблиц маршрутизации и другие важные тесты.

GPOtool

Одна из утилит Resource Kit, которая служит для проверки целостности объектов групповых политик. В предыдущей статье [1] были рассмотрены групповые политики. Напомню, что каждый объект GPO состоит из двух частей – контейнера и шаблона групповой политики. Контейнер хранится в каталоге и содержит параметры объекта GPO, шаблон хранится в папке \Windows\sysvol\ и содержит настройки безопасности, административные политики, скрипты и приложения, которые публикуются при помощи групповых политик. Если версии контейнера и шаблона групповой политики по каким-то причинам не совпадают либо один из них поврежден, групповая политика применена не будет.

Repadmin

Одним из важнейших процессов при функционировании службы каталогов является репликация. Утилита из состава Support Tools, позволяющая увидеть, что происходит при репликации, и выявить возможные причины неполадок.

NTDSutil

Это контекстный инструмент, предназначенный для работы с базой данных службы каталогов, а также для управления ролями FSMO (Flexible Single-Master Operation, одиночный хозяин операций) и удаления метаданных, неправильно вышедших из состава службы каталогов контроллеров домена. С ее помощью можно, например, принудительно захватить роли FSMO, которые принадлежали вышедшему из строя контроллеру домена. Но в этом случае нужно быть уверенным, что этот контроллер уже не вернется к работе, иначе возникнут проблемы в работе службы каталогов, так как некоторые роли FSMO требуют уникальности обладателя в рамках домена. Использование утилиты требует от администратора четкого понимания происходящего, иначе действия, произведенные с помощью NTDSutil, могут повлечь за собой неприятные последствия.

Практическая работа 8. Настройка параметров безопасности (шаблоны безопасности, анализ и настройка безопасности)

Цель работы: изучение настроек параметров безопасности

Управлению безопасностью в сетях Microsoft Windows посвящено немало учебных курсов и хороших книг. В предыдущих разделах мы уже касались политик безопасности, относящихся к учетным записям пользователей (параметры длины и сложности пароля, параметры блокировки учетных записей) и параметрам прав пользователей (в частности, локальный вход в систему на сервере для выполнения лабораторных работ в компьютерном классе).

Оставим подробное изучение безопасности сетей Microsoft за рамками данного курса, но при этом рассмотрим работу с очень полезными оснастками, которые могут помочь начинающему сетевому администратору ознакомиться с некоторыми стандартными шаблонами политик безопасности, которые имеются в самой системе Windows Server, и проводить анализ и текущих настроек сервера в сравнении со этими стандартными шаблонами.

Ход работы

1. Сначала откроем чистую консоль mmc.
   Кнопка " *Пуск* " — " *Выполнить* " — mmc — кнопка " *ОК* ".
1. Добавим в новую консоль оснастки " *Шаблоны безопасности* " и " *Анализ и настройка безопасности* ".

Меню " *Консоль* " — " *Добавить или удалить оснастку* " — кнопка " *Добавить* " — выбрать оснастку " *Анализ и настройка безопасности* " — кнопка " *Добавить* " — выбрать оснастку " *Шаблоны безопасности* " — кнопка " *Добавить* " — кнопка "*Закрыть* " — кнопка " *ОК* ".

В полученной консоли (ее можно будет сохранить и использовать в дальнейшем неоднократно) можно делать следующее:

- изучить параметры стандартных шаблонов безопасности (оснастка "Шаблоны безопасности") и даже попробовать сконструировать собственные шаблоны на основе стандартных (можно сохранить какой-либо шаблон с другим именем и изменить какие-либо параметры шаблона);
- провести анализ (сравнение) текущих параметров безопасности сервера (оснастка " *Анализ и настройка безопасности* ").

Приведем краткие характеристики стандартных шаблонов безопасности:

- **DC security** — используемые по умолчанию параметры безопасности контроллера домена;
- **securedc** — защищенный контроллер домена (более высокие требования к безопасности по сравнению с шаблоном *DC security*, отключается использование метода аутентификации *LanManager*);
- **hisecdc** — контроллер домена с высоким уровнем защиты (более высокие требования к безопасности по сравнению с шаблоном *securedc*, отключается метод аутентификации *NTLM*, включается требование цифровой подписи пакетов SMB);
- **compatws** — совместимая рабочая станция или совместимый сервер (ослабляет используемые по умолчанию разрешения доступа группы "Пользователи" к реестру и к системным файлам для того, чтобы приложения, не сертифицированные для использования в данной системе, могли работать в ней);
- **securews** — защищенная рабочая станция или защищенный сервер (аналогичен шаблону *securedc*, но предназначен для применения к рабочим станциям и простым серверам);

- **hisecws** — рабочая станция или защищенный сервер с высоким уровнем защиты (аналогичен шаблону *hisecdc*, но предназначен для применения к рабочим станциям и простым серверам);
- **setup security** — первоначальные настройки по умолчанию (параметры, устанавливаемые во время инсталляции системы);
- **rootsec** — установка стандартных (назначаемых во время инсталляции системы) NTFS-разрешений для папки, в которую установлена операционная система;

Теперь на примере рассмотрим, как проводить анализ настроек безопасности.

1. Откроем базу данных, в которой будут сохраняться настройки проводимого нами анализа.

Щелкнем правой кнопкой мыши на значке оснастки " *Анализ и настройка безопасности* ", выберем " *Открыть базу данных* ", укажем путь и название БД (по умолчанию БД создается в папках профиля того администратора, который проводит анализ), нажмем кнопку " *Открыть* ", выберем нужный нам шаблон (например, *hisecdc*) и нажмем " *ОК* "

2. Выполним анализ настроек безопасности.

Щелкнем правой кнопкой мыши на значке оснастки " *Анализ и настройка безопасности* ", выберем " *Анализ компьютера* ", укажем путь и название файла с журналом ошибок (т.е. протоколом проведения анализа), нажмем "ОК", будет выполнено сравнение текущих настроек с параметрами шаблона:

Теперь можно провести уже настоящий анализ настроек безопасности.

3. Откроем любой раздел оснастки (например, " *Политики паролей* "):

На рисунке сразу видны расхождения между настройками нашего сервера (столбец " *Параметр компьютера* ") и настройками шаблона (столбец " *Параметр базы данных* ") — видно, как мы понизили настройке безопасности для проведения практических занятий.

4. Аналогично проводится анализ всех остальных разделов политик безопасности.

Этой же оснасткой можно одним действием привести настройки нашего компьютера в соответствии с параметрами шаблона (щелкнуть правой кнопкой мыши на значке оснастки " *Анализ и настройка безопасности* ", выбрать " *Настроить компьютер* "). Не рекомендуем это делать, не изучив в деталях, какие последствия это может повлечь для всей сети. Высокие требования к параметрам безопасности препятствуют работе в домене Active Directory компьютеров с системами Windows 95/98/ME/NT. Например, данные системы поддерживают уровень аутентификации *NTLM* версии 2 (который назначается шаблонами *hisecdc* и *hisecws*) только при проведении определенных настроек на компьютерах со старыми системами. Поэтому, прежде чем принимать решение об установке более высоких параметров безопасности в сети, необходимо тщательно изучить состав сети, какие требования к серверам и рабочим станциям предъявляют те или иные шаблоны безопасности, предварительно установить нужные обновления и настроить нужные параметры на "старых" системах и только после этого применять к серверам и рабочим станциям Windows 2000/XP/2003 шаблоны с высокими уровнями сетевой безопасности.

Заметим дополнительно, что данные оснастки имеются не только на серверах, но и на рабочих станциях под управлением Windows 2000/XP Professional, и они позволяют производить аналогичный анализ и настройки на рабочих местах пользователей.

Первая часть описывает задачи служб каталогов корпоративной сети и основные понятия служб каталогов Active Directory:

- домен;
- дерево;
- лес;
- организационное подразделение.

Вторая часть дает углубленные знания по логической и физической структуре службы каталогов Active Directory.

Третья часть посвящена практическим вопросам управления системой безопасности корпоративной сети — учетными записями пользователей, компьютеров, групп, организационными подразделениями. Описан также механизм групповых политик — мощное средство управлением настройками пользовательской среды и параметров компьютеров в большой корпоративной сети.

В четвертой части описаны технологии управления сетевой безопасностью — протокол аутентификации Kerberos и применение шаблонов безопасности для настройки параметров безопасности серверов и рабочих станций.

Задачи сетевого администратора при управлении инфраструктурой службы каталогов:

- планирование и реализация пространства доменных имен компании или организации для службы каталогов Active Directory;
- планирование и реализация IP-сетей и сайтов AD для управления процессами репликации контроллеров домена и аутентификации пользователей в сети;
- планирование и размещение в сети контроллеров домена, выполняющих функции хозяев операций;
- планирование и реализация правил создания и именования учетных записей пользователей, компьютеров и групп;
- планирование и реализация стратегии использования групп для управления доступом к сетевым ресурсам;
- планирование и реализация иерархии организационных подразделений для делегирования административных полномочий и применения групповых политик;
- планирование и разработка набора групповых политик для управления рабочей средой пользователей и параметров компьютеров;
- проведение анализа сетевой безопасности, настройка требуемого уровня сетевой безопасности на серверах и рабочих станциях.

5. При помощи шаблонов безопасности вы можете настраивать параметры политики, которые отвечают за следующие компоненты безопасности:

- **Политики учетных записей**. Вы можете настраивать политики паролей, политики блокировки учетной записи, а также политики Kerberos;
- **Локальные политики**. Доступны настройке политики аудита, назначения прав пользователей, а также параметры безопасности, аналогичные параметрам политики оснастки **«Редактор объектов групповых политик»**;
- **Журналы событий**. Вы можете изменять настройки журналов **«Приложения»**, **«Система»** и **«Безопасность»**, такие как политики создания файлов журналов, максимальный размер и прочее;
- **Группы с ограниченным доступом**. Настройки ограничений доступа пользователей, которые являются членами различных групп;
- **Настройки системных служб>**. Вы можете управлять типом запуска и разрешением доступа всех системных служб, которые можно найти в оснастке **«Службы»**;
- **Настройки системного реестра**. Можно добавлять разрешения на доступ к разделам реестра;
- **Настройки безопасности файловой системы**. У вас есть возможность задавать разрешения доступа на файлы и папки.

Рекомендуется не вносить изменения в предустановленный шаблон Setup security.inf, так как при помощи этого шаблона у вас есть возможность восстановления параметров безопасности, используемых по умолчанию. Также, чтобы избежать многих проблем, желательно перед внедрением созданного шаблона в эксплуатацию, протестировать его на отдельном компьютере.

Использование оснастки «Шаблоны безопасности»

Откройте оснастку **«Шаблоны безопасности»**. Для этого выполните следующие действия:

1. Откройте **«Консоль управления ММС»**. Для этого нажмите на кнопку **«Пуск»**, в поле поиска введите *mmc*, а затем нажмите на кнопку **«Enter»**;
2. Откроется пустая консоль ММС. В меню **«Консоль»** выберите команду **«Добавить или удалить оснастку»** или воспользуйтесь комбинацией клавиш **Ctrl+M**;
3. В диалоге **«Добавление и удаление оснасток»** выберите оснастку **«Шаблоны безопасности»** и нажмите на кнопку **«Добавить»**;
4. В диалоге **«Добавление или удаление оснасток»** нажмите на кнопку **«ОК»**.

При первом открытии данной оснастки, в папке Documents вашей учетной записи создается папка Security с вложенной папкой Templates. Именно в папке Templates и хранятся созданные вами шаблоны безопасности. На следующей иллюстрации отображена оснастка «Шаблоны безопасности», открытая впервые:

Создание нового шаблона безопасности

Для последующей работы с шаблонами безопасности создайте новый шаблон. Для этого вам предстоит выполнить действия, описанные в следующей процедуре:

1. В дереве консоли щелкните правой кнопкой мыши на узле, предоставляющем путь поиска шаблона. По умолчанию путь %Userprofile%\Documents\Security\Templates;
2. В появившемся контекстном меню выберите команду **«Создать шаблон»**;
3. Введите название нового шаблона в текстовое поле **«Имя шаблона»** появившегося диалогового окна. В том случае, если вы создаете несколько различных шаблонов безопасности, я вам рекомендую добавлять подробное описание назначения шаблона в поле **«Описание»**. Например, на следующей иллюстрации вы можете увидеть диалог создания шаблона с названием **«Конфигурация системных служб»**. В связи с тем, что на пользовательских компьютерах могут быть установлены разные ОС, в описании указана версия операционной системы, для которой создается текущий шаблон.

При желании вы можете изменить путь для поиска шаблонов, созданный по умолчанию. Для этого, в дереве консоли, нажмите правой кнопкой мыши на узле **«Шаблоны безопасности»** и выберите команду **«Найти путь для поиска шаблонов…»**. В диалоговом окне **«Обзор папок»** выберите папку, в которой будут сохраняться новые шаблоны безопасности и нажмите на кнопку **«ОК»**.

Изменение настроек шаблона безопасности

После создания нового шаблона, в оснастке вы увидите набор групповых политик, подобный тем, которые отображаются в оснастке **«Редактор объектов групповых политик»**. Не стоит также забывать, что оснастка шаблонов безопасности представляет собой только редактор набора групповых политик и не влияет на изменение текущей конфигурации. То есть, после полного изменения политик, предоставленных в данной оснастке, вам не стоит волноваться о том, что настройки на вашем рабочем месте будут изменены. Далее мы рассмотрим набор политик системных служб, добавление параметров реестра, а также редактирование групп с ограниченным доступом.

На следующей иллюстрации отображен новый шаблон безопасности:

Настройка системных служб

Узел **«Системные службы»** предназначен для последующего изменения конфигурации системных служб средствами групповых политик при развертывании. Содержимое этого узла сильно напоминает оснастку **«Службы»**, однако между ними есть одна существенная разница. При помощи оснастки **«Службы»** вы настраиваете тип запуска служб на локальном компьютере, а используя шаблоны безопасности, вы можете распространить указанные настройки системных служб одновременно на несколько компьютеров. Рассмотрим подробно применение содержимого данного узла на простом примере:

На компьютерах вашего малого офиса, в котором нет домена, никогда не будут использоваться планшетные ПК, устройства BlueTooth и смарт-карты. Допустим, вы опасаетесь вторжения на компьютеры недоброжелателей, поэтому хотите отключить возможность удаленного управления системного реестра, службы удаленных рабочих столов, а также вашим пользователям нельзя на рабочих местах использовать Windows Media Center. По этой же причине необходимо полностью отключить на компьютерах вашей сети все эти службы. Чтобы развернуть эти настройки служб на всех компьютерах, выполните следующие действия:

1. В оснастке **«Шаблоны безопасности»** перейдите на узел **«Системные службы»**;
2. Выберите службу, тип запуска которой вы планируете настроить, например, **«Служба ввода планшетного ПК»** и откройте свойства этой службы;
3. В диалоговом окне **«Свойства: Служба ввода планшетного ПК»** установить флажок на опции **«Определить следующий параметр службы в шаблоне»** и установите переключатель на опции **«запретить»**;
4. Нажмите на кнопку **«ОК»**. Настройте остальные службы.

Настройка системного реестра

После подробного изучения параметров групповых политик, вы можете обнаружить, что, несмотря на использование групповых политик и шаблонов безопасности, пользователи умудряются изменять некоторые системные параметры при помощи реестра. Вы знаете раздел системного реестра, отвечающий за определенную настройку, но хотите дать возможность вносить изменения в этот раздел только указанной группе пользователей. Допустим, вам нужно дать полный доступ на изменение параметров раздела реестра, отвечающего за компонент **«Дата и время»** только для групп **«Система»** и **«Администраторы»**, причем пользователям, которые являются членами группы **«Пользователи»** нужно запретить даже просмотр данного раздела. Для этого выполните следующие действия:

1. В оснастке **«Шаблоны безопасности»** перейдите на узел **«Реестр»**;
2. Вызовите контекстное меню для узла **«Реестр»** и выберите команду **«Добавить раздел»**;
3. В диалоговом окне **«Выбор раздела реестра»** разверните раздел [MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation] или введите путь к разделу в поле **«Выбранный раздел»** и нажмите на кнопку **«ОК»**;
4. В появившемся диалоговом окне **«Безопасность данных для <Выбранный_раздел_реестра>»** установите разрешения для всех групп и нажмите на кнопку **«ОК»**;
5. В диалоге **«Добавление объекта»** вы можете распространить указанные настройки безопасности на все дочерние подразделы, запретить замену разрешений в указанном разделе, или изменить параметры вручную.
6. По нажатию на кнопку **«ОК»**, данные изменения будут отображены в оснастке **«Шаблоны безопасности»**, как показано на следующей иллюстрации:

Настройка групп с ограниченным доступом

При помощи групп с ограниченным доступом вы можете указывать пользователей, которые будут принадлежать к определенной группе. Политики, применяемые с шаблонами безопасности, будут распространяться на всех пользователей, которые входят в группы с ограниченным доступом. Для того чтобы указать членов группы с ограниченным доступом, выполните следующие действия:

1. В оснастке **«Шаблоны безопасности»** перейдите на узел **«Группы с ограниченным доступом»**;
2. Нажмите правой кнопкой мыши на узле и из контекстного меню выберите команду **«Добавить группу»**;
3. В диалоговом окне **«Добавление группы»** введите название новой группы или выберите существующую, используя кнопку **«Обзор»**;

4. В диалоговом окне свойств новой группы вы можете добавить пользователей, которые будут входить в состав этой группы, а также выбрать родительскую группу. Причем, политики не применяются на те группы, к которым принадлежит созданная вами группа;
5. По нажатию на кнопку **«ОК»** новая группа будет создана и добавлена в узел групп с ограниченным доступом.

По окончании изменения шаблона безопасности, вам нужно его сохранить для дальнейшего использования. Для сохранения шаблона безопасности нажмите правой кнопкой мыши на наименовании узла шаблона безопасности и выберите команду **«Сохранить»** или **«Сохранить как»** из контекстного меню. Шаблон будет сохранен с расширением ***.inf**.

Практическая работа 9. Управление доступом к файловым ресурсам (сетевые права доступа, локальные права доступа, взятие во владение)

Цель работы: настройка управления доступа к файловым ресурсам (сетевые права доступа, локальные права доступа, взятие во владение).

Ход работы

Права доступа, наследование прав доступа, взятие во владение

1. Определение прав доступа к файловым ресурсам осуществляется на основе *разрешений* (*permissions*). При определении разрешений к ресурсам, предоставленным в совместный доступ в сети, используются два типа разрешений: *сетевые разрешения* (*shared folder permissions*) и *разрешения, заданные в файловой системе NTFS* (*NTFS-permissions*).
2. Рассмотрим сначала сетевые разрешения. Данный вид разрешений не зависит от типа файловой системы. *Сетевые разрешения применяются только при доступе к ресурсам через сеть*. Если пользователь локально вошел в систему (локально зарегистрировался в системе), то, какие бы ни были назначены сетевые разрешения для определенной папки, эти разрешения не будут применяться ни к самой папке, ни к размещенным в ней файлам. В случае локальной регистрации пользователя, если данные размещены на томе с системой FAT, пользователь имеет *полный доступ* к этим данным, если данные размещены на томе NTFS, права доступа будут определяться разрешениями NTFS.
3. Предоставление общего доступа к папке.

Предоставить папку на жестком диске в общее пользование можно двумя основными способами.

Открыть *Свойства* папки, закладку «*Доступ*», выбрать пункт «*Открыть общий доступ к этой папке*»

Открыть оснастку «*Общие папки*» в консоли «*Управление компьютером*», выбрать раздел «*Общие ресурсы*», щелкнуть правой кнопкой мыши и выбрать пункт «*Новый общий ресурс*»

Будет запущен «*Мастер создания общих ресурсов*»

Нужно указать путь к папке (ввести с клавиатуры или найти с помощью кнопки «*Обзор*»), дать название общему ресурсу (по умолчанию это название совпадает с именем папки, хотя надо иметь в виду, что не все приложения могут воспринимать длинные сетевые имена с символами не из английской раскладки; рис):

Далее нужно задать *сетевые разрешения* на доступ к информации, хранящейся в данной папке. По умолчанию назначаются разрешения «*Чтение*» группе «*Все*».

Могут быть назначены сетевые разрешения трех видов:

- **Чтение** (**Read**) — чтение списка файлов и папок, чтение данных и запуск программ;

- **Изменение** (**Change**) — кроме чтения данных позволяет также создавать новые файлы и папки, удалять файлы и папки, изменять данные;

- **Полный доступ** (**Full control**) — в добавление к перечисленным выше разрешениям можно также изменять NTFS-разрешения (если общая папка хранится на томе NTFS) и получать статус владельца папки или файла (тоже для томов NTFS).

Определение суммарных сетевых разрешений

Напомним, что при регистрации пользователя домена на каком-либо компьютере контроллер домена выдает пользователю т.н. *маркер доступа* (см. Раздел 4), который состоит из набора идентификаторов безопасности (SID) пользователя и групп, членом которых он является. Именно этот маркер доступа и определяет, какой именно доступ получит пользователь к сетевому ресурсу. В том случае, если некий пользователь имеет разрешение на доступ к папке по сети, а также доступ определен для каких-либо групп, членом которых он является, то определение суммарных разрешений производится по следующей схеме:

- сначала проверяется, нет ли запретов на тот или иной вид доступа для пользователя и групп, в которые он входит, если в сетевых разрешениях имеются запреты для пользователя или хотя бы одной из групп, в которые он входит, то данные виды доступа пользователю не будут предоставлены;

- если на какие-либо виды доступа запретов нет, то действующим разрешением будет наибольшее разрешение, выданное пользователю или какой-либо группе, членом которой он является.

Например, в ситуации, изображенной на рис. 5.33 имеются следующие разрешения:

- группа «*Все*» — «Чтение»;

- пользователь *User1* — «Чтение»;

- группа *Group-1* (в которую входит пользователь User1) — «Изменение».

В данной ситуации пользователь User1 получит разрешение на «Изменение» данных в папке и файлах.

Оснастка «*Общие папки*» позволяет также просматривать, кто из пользователей и какие именно файлы и папки использует в настоящий момент.

Есть несколько способов подключения пользователей к сетевым файловым ресурсам:

- самый любимый пользователями, но не самый эффективный с точки зрения системы, — найти сначала сервер, а затем ресурс с помощью просмотра «*Сетевого окружения*»;

- то же самое можно сделать, если в командной строке ввести т.н. *UNC-имя* сетевого ресурса (*UNC — Universal Naming Convention*, способ именования сетевых ресурсов), для этого нужно нажать кнопку «*Пуск*» — выбрать пункт меню «*Выполнить*» — ввести UNC-имя в виде \\<*имя сервера*>\<*имя сетевого ресурса*> (например, *DC1**Folder1*);

- назначить букву диска к сетевому ресурсу; это можно сделать в командной строке командой вида «*net use <буква диска> <UNC-имя >*» (например, «*net use X: \\DC1\Folder1*») либо же, открыв окно «*Мой компьютер*» можно назначить букву диска для сетевого ресурса с помощью мастера подключения сетевого диска (меню «*Сервис*» — выбрать пункт меню «*Подключение сетевого диска*»).

4. Специальные сетевые ресурсы

В любой системе на базе технологий Windows NT существуют специальные сетевые ресурсы. Имена некоторых ресурсов заканчиваются символом **$**, такие сетевые ресурсы через «*Сетевое окружение*» или при открытии ресурсов сервера с помощью команды «\\<*имя сервера*>» не будут видны. Однако, если указать полное UNC-имя сетевого ресурса, то можно увидеть данные, размещенные в нем.

Перечислим эти ресурсы:

- ресурс вида «**\\<имя сервера>\admin$**» (например, \\DC1\admin$) — предназначен для удаленного администрирования компьютера; путь всегда соответствует

местоположению папки, в которой установлена система Windows; к этому ресурсу могут подключаться только члены групп *Администраторы*, *Операторы архива* и *Операторы сервера*;

- ресурс вида «**<имя сервера>\< буква диска>$**» (например, \\DC1\C$) — корневая папка указанного диска;. к сетевым ресурсам такого типа на сервере Windows могут подключаться только члены групп *Администраторы*, *Операторы архива* и *Операторы сервера*; на компьютерах с Windows XP Professional и Windows 2000 Professional к таким ресурсам могут подключаться члены групп *Администраторы* и *Операторы архива*;

- ресурс «**<имя сервера>\IPC$**» (например, \\DC1\IP$) — используется для удаленного администрирования;

- ресурс «**<имя сервера>\NETLOGON**» (например, \\DC1\NETLOGON) — используется только на контроллерах домена, в данной сетевой папке хранятся скрипты (сценарии) для входа пользователей в систему, совместимые с предыдущими версиями операционными системами Microsoft;

- ресурс «**<имя сервера>\SYSVOL**» — используется только на контроллерах домена, в данной сетевой папке хранится файловая часть групповых политик;

- ресурс «**<имя сервера>\ PRINT$**» — ресурс, который поддерживает совместно используемые принтеры, в частности, в данной папке хранятся драйверы для совместно используемых принтеров.

Просмотреть полный список ресурсов, предоставляемых данным сервером для совместного использования, можно в оснастке «*Общие папки*», в разделе «*Общие ресурсы*»

В этом же разделе данной оснастки можно отключать ресурсы от совместного использования в сети, менять сетевые разрешения, создавать новые сетевые ресурсы.

Кроме специальных сетевых ресурсов с символом $ в конце названия ресурса, предоставленных группам с высокими полномочиями, с этим символом можно предоставить доступ к любому другому ресурсу, которые предоставляется в сетевой доступ самим администратором. В этом случае сетевой ресурс также будет скрыт при обычном просмотре сети, но будет доступен при указании полного UNC-имени, причем доступ можно разрешить тем группам пользователей, которым нужен данный ресурс.

5. Разрешения NTFS

Еще раз подчеркнем, что сетевые разрешения действуют только при доступе к ресурсам через сеть. Если пользователь вошел в систему локально, то теперь управлять доступом можно только с помощью разрешений NTFS. На томе (разделе) с системой FAT пользователь будет иметь полный доступ к информации данного тома.

Разрешения NTFS можно установить, открыв *Свойства* папки или файла и перейдя на закладку «*Безопасность*» (*Security*), набор видов NTFS-разрешений намного богаче, чем набор сетевых разрешений.

На томе NTFS можно назначать следующие виды разрешений для папок:

- **Полный доступ**;
- **Изменить**;
- **Чтение и выполнение**;
- **Список содержимого папки**;
- **Чтение**;
- **Запись**;
- **Особые разрешения**.

6. Для файлов отсутствует вид «*Чтение содержимого папки*».

Если на закладке разрешений нажать кнопку «*Дополнительно*», то можно осуществлять более тонкую настройку разрешений.

7. Разрешения NTFS могут быть *явными* или *унаследованными*. По умолчанию все папки или файлы наследуют разрешения того объекта-контейнера (*родительского объекта*), в котором они создаются. Использование унаследованных разрешений облегчает работу по управлению доступом. Если администратору нужно изменить

права доступа для какой-то папки и всего ее содержимого, то достаточно сделать это для самой папки и изменения будут автоматически действовать на всю иерархию вложенных папок и документов. На рис. 5.36. видно, что группа «*Администраторы*» имеет унаследованные разрешения типа «*Полный доступ*» для папки *Folder1*. А на рис. 5.37. показано, что группа «*Пользователи*» имеет набор явно назначенных разрешений:

Изменить унаследованные разрешения нельзя. Если нажать на кнопку «*Дополнительно*», то можно отменить наследование разрешений от родительского объекта. при этом система предложит два варианта отмены наследования: либо скопировать прежние унаследованные разрешения в виде явных разрешения, либо удалить их совсем.

8. Механизм применения разрешений

Каждый файл представляет собой набор атрибутов. Атрибут, который содержит информацию об NTFS-разрешения, называется *списком управления доступом* (*ACL, Access Control List*). Структура ACL приведена в таблице 5.4. Каждая запись в ACL называется *элементом управления доступом* (*ACE, Access Control Entry*).

ACL		Идентификаторы безопасности	Разрешения
ACE_1	SID_1	Разрешения для SID_1	
ACE_2	SID_2	Разрешения для SID_2	
ACE_3	SID_3	Разрешения для SID_3	
,,,	,,,	,,,	
ACE_n	SID_n	Разрешения для SID_n	

В таблице перечислены идентификаторы безопасности учетных записей пользователей, групп или компьютеров (SID) и соответствующие разрешения для них. вместо SID-ов показаны имена занесенных в ACL пользователей и групп. В разделе 4 говорилось, что при входе пользователя в сеть (при его регистрации в домене) в текущую сессию пользователя на компьютере контроллер домена пересылает маркер доступа, содержащий SID-ы самого пользователя и групп, членом которых он является. Когда пользователь пытается выполнить какое-либо действие с папкой или файлом (и при этом запрашивает определенный вид доступа к объекту), система сопоставляет идентификаторы безопасности в маркере доступа пользователя и идентификаторы безопасности, содержащиеся в ACL объекта. При совпадении тех или иных SID-ов пользователю предоставляются соответствующие разрешения на доступ к папке или файлу.

Заметим, что когда администратор изменяет членство пользователя в группах (включает пользователя в новую группу или удаляет из какой-либо группы), то маркер доступа пользователя при этом автоматически НЕ изменяется. Для получения нового маркера доступа пользователь должен выйти из системы и снова войти в нее. Тогда он получит от контроллера домена новый маркер доступа, отражающий смену членства пользователя в группах

9. Порядок применения разрешений

Принцип применения NTFS-разрешений на доступ к файлу или папке тот же, что и для сетевых разрешений:

- сначала проверяются запреты на какие-либо виды доступа (если есть запреты, то данный вид доступа не разрешается);
- затем проверяется набор разрешений (если есть разные виды разрешений для какого-либо пользователя и групп, в которые входит данный пользователь, то применяется суммарный набор разрешений).

Но для разрешений NTFS схема немного усложняется. Разрешения применяются в следующем порядке:

- явные запреты;

- явные разрешения;
- унаследованные запреты;
- унаследованные разрешения.

Если SID пользователя или SID-ы групп, членом которых является данный пользователь, не указаны ни в явных, ни в унаследованных разрешения, то доступ пользователю будет запрещен.

10. Владение папкой или файлом

Пользователь, создавший папку или файл, является *Владельцем* данного объекта. Владелец объекта *обладает правами изменения NTFS-разрешений* для этого объекта, даже если ему запрещены другие виды доступа. Текущего владельца объекта можно увидеть, открыв *Свойства* объекта, затем закладку «*Безопасность*», затем нажав кнопку «*Дополнительно*» и перейдя на закладку «*Владелец*» (рис. 5.38):

Внимание! Администратор системы *может сменить владельца* объекта, выбрав нового владельца из предлагаемого в данном окне списка или из полного списка пользователей (нажав кнопку «*Иные пользователи или группы*»). Эта возможность предоставлена администраторам для того, чтобы восстановить доступ к объекту в случае утери доступа по причине неправильно назначенных разрешений или удаления учетной записи, имевшей исключительный доступ к данному объекту (например, уволился единственный сотрудник, имевший доступ к файлу, администратор удалил его учетную запись, вследствие этого был полностью потерян доступ к файлу, восстановить доступ можно единственным способом — передача владения файла администратору или новому сотруднику, исполняющему обязанности уволившего сотрудника).

11. Совместное использование сетевых разрешений и разрешений NTFS

При доступе по сети к файловым ресурсам, размещенным на томе NTFS, к пользователю применяется комбинация сетевых разрешений и разрешений NTFS.

При доступе через сеть сначала вычисляются сетевые разрешения (путем суммирования разрешений для пользователя и групп, в которые входит пользователь). Затем также путем суммирования вычисляются разрешения NTFS. Итоговые действующие разрешения, предоставляемые к данному конкретному объекту, будут представлять собой *минимум* из вычисленных сетевых и NTFS-разрешений.

12. Управление доступом с помощью групп

Группы пользователей созданные специально для того, чтобы более эффективно управлять доступом к ресурсам. Ели назначать права доступа к каждому ресурсу для каждого отдельного пользователя, то, во-первых, это очень трудоемкая работа, и во-вторых, затрудняется отслеживание изменений в правах доступа при смене каким-либо пользователем своей должности в подразделении или переходе в другое подразделение.

13. Для более эффективного управления доступом рекомендуется следующая схема организации предоставления доступа:

1) учетные записи пользователей (*accounts*) включаются в глобальные доменных группы (*global groups*) в соответствии со штатной структурой компании/организации и выполняемыми обязанностями;

2) глобальные группы включаются в доменные локальные группы или локальные группы на каком-либо сервере (*domain local groups, local groups*) в соответствии с требуемыми правами доступа для того или иного ресурса;

3) соответствующим локальным группам назначаются необходимые разрешения (*permissions*) к конкретным ресурсам.

Данная схема по первым буквам используемых объектов получила сокращенное название *AGLP* (***A****ccounts* → ***G****lobal groups* → ***L****ocal groups* → ***P****ermissions*). При такой схеме, если пользователь повышается или понижается в должности или переходит в другое подразделение, то нет необходимости *просматривать все сетевые ресурсы*, доступ к которым необходимо изменить для данного пользователя. Достаточно изменить

соответствующим образом *членство пользователя в глобальных группах*, и права доступа к сетевым ресурсам для данного пользователя *изменятся автоматически*.

Добавим, что в основном режиме функционирования домена Active Directory (режимы «*Windows 2000 основной*» или «*Windows 2003*») с появлением вложенности групп и универсальных групп схема **AGLP** модифицируется в схему **AGG…GULL…LP**.

Аудит доступа к ресурсам

Файловая система NTFS позволяет осуществлять *аудит доступа к файловым ресурсам*, т.е. отслеживать и регистрировать события, связанные с получением или неполучением доступа к тому или иному объекту.

Для того, чтобы включить аудит, необходимо выполнить два действия:

1) включить политику аудита доступа к объектам в домене или том ОП, в котором размещен файловый сервер;

2) после применения политики включить аудит доступа на самом объекте — папке или файле.

Первое действие выполняется с помощью редактора групповых политик:

- откроем раздел «Параметры безопасности» в политике для соответствующего ОП, далее — «Локальные политики» и «Политика аудита»;
- откроем параметр «Аудит доступа к объектам»;
- включим механизм аудита для успешного доступа и отказа предоставления доступа

Второе действие выполняется на закладке «*Аудит*» после нажатия кнопки «*Дополнительно*» в параметрах безопасности объекта. Нужно добавить списки пользователей и групп, попытки доступа которых будут отслеживаться для данной папки или файла, указав при этом, какие именно виды доступа надо регистрировать. На рис. 5.40 показано, что будет регистрироваться доступ к папке *Folder1*группы «*Пользователи домена*», на рис. 5.41 показаны виды доступа, которые будут регистрироваться для данной папки. Для того, чтобы можно было регистрировать попытки несанкционированного доступа к файловым ресурсам, необходимо включить в процесс регистрации и удачные, и неудачные попытки доступа.

После включения механизма аудита все события доступа, перечисленные в настройках аудита, будут регистрироваться в журнале безопасности данного сервера (оснастка «*Просмотр событий*», журнал «*Безопасность*», категория «*Доступ к объектам*»). Пример одной из записей журнала, регистрирующей доступ к файлу в папке *Folder1*. В данном примере показано событие *успешного доступа* к файлу *Text.txt* пользователя *Администратор*:

В заключении данного пункта отметим, что включать аудит большого количества файловых ресурсов следует с большой осторожностью. При большом количестве пользователей и обрабатываемых ими файлов, если включить аудит доступа к файлам, в журнале безопасности будет создаваться очень много событий. В случае какого-либо инцидента, например, при несанкционированном доступе к закрытой информации, найти нужную запись будет очень трудно. Поэтому, прежде чем включить аудит доступа, его необходимо очень тщательно спланировать. Необходимо определить:

- доступ к какой информации необходимо отслеживать;
- какие виды доступа (*Чтение, Модификация, Удаление, Изменение разрешений* и т.д.);
- типы событий (*успешный* и *неуспешный* доступ);
- для каких пользователей необходимо отслеживать доступ;
- как часто будет просматриваться журнал безопасности;
- по какой схеме будут удаляться «старые» события из журнала.

Практическая работа 10. Сжатие и шифрование файлов

Цель работы: изучить способы сжатия и шифрования файлов

Ход работы

Сжатие информации

1. Для экономии дискового пространства можно какие-либо папки или файлы сделать сжатыми. Процесс сжатия выполняется драйвером файловой системы NTFS. При открытии файла в программе файловая система распаковывает файл, после внесения изменений в файл при сохранении на диск файл снова сжимается. Делается это совершенно прозрачно для пользователя и не доставляет пользователю никаких хлопот.
2. Для того, чтобы сделать папку или файл сжатым, необходимо открыть страницу Свойств соответствующей папки или файла, нажать кнопку «Другие» и оставить галочку у параметра «Сжимать содержимое для экономии места на диске».
3. Сжимать целесообразно файлы, которые при сжатии сильно уменьшаются в размере (например, документы, созданные программами из пакета MS Office). Не следует сжимать данные, которые по своей природе являются сжатыми — например, файлы графических изображений в формате JPEG, видеофайлы в формате MPEG-4, файлы, упакованные программами-архиваторами (ZIP, RAR, ARJ и другие).
4. Ни в коем случае не рекомендуется сжимать папки с файл-серверными базами данных, т.к. такие БД содержат большое количество файлов и при их совместном использовании многими пользователями могут возникать ощутимые задержки, неизбежные при распаковке открываемых и сжатии сохраняемых файлов.

Шифрование информации

5. Системы семейства Windows 2000/XP/2003 и более поздние позволяют шифровать данные, хранящиеся на томе с системой NTFS. Шифрование данные осуществляется так же легко, как и их сжатие. В примере на рис. 5.43 можно вместо поля «*Сжимать содержимое…*» отметить галочкой поле «*Шифровать содержимое для защиты данных*» (заметим, что эти два параметра являются взаимоисключающими — можно в данный момент времени либо сжать данные, либо их зашифровать). Шифрование является надежным средство предотвращения несанкционированного доступа к информации, даже если будет похищен компьютер с этой информацией или жесткий диск из компьютера. Если данные зашифрованы, то доступ к ним имеет (с небольшим исключением) только тот пользователь, который выполнил шифрование, независимо от установленных разрешений NTFS. Шифрование производится компонентой «*Шифрованная файловая система*» (EFS, Encrypted File System), являющейся составной частью файловой системой NTFS.
6. Процесс шифрования производится по следующей схеме:

1) при назначении файлу атрибута «*Зашифрованный*» драйвер системы EFS генерирует «*Ключ шифрования файла*» (FEK, File Encryption Key);

2) блоки данных файла последовательно шифруются по симметричной схеме (одним из алгоритмов симметричного шифрования, встроенных в систему);

3) ключ шифрования файла (FEK) шифруется по асимметричной схеме открытым ключом *агента восстановления* (*RA, Recovery Agent*);

4) зашифрованный ключ шифрования файла сохраняется в атрибуте файла, называемом «*Поле восстановления данных*» (*DRF, Data Recovery Field*).

Поле восстановления данных необходимо для защиты от потери доступа к зашифрованной информации в том случае, если будет удалена (вместе с ключом шифрования данных) учетная запись пользователя, зашифровавшего эти данные. Агент восстановления — это специальная учетная запись, для которой EFS создает т.н. «*сертификат агента восстановления*», в состав которого входят открытый и закрытый ключи этого агента. особенность асимметричного шифрования заключается в том, что для шифрования и дешифрования данных используются два ключа — одним ключом данные шифруются, другим дешифруются. Открытый ключ агента восстановления доступен любому пользователю, поэтому, если пользователь шифрует данные, то в зашифрованных файлах всегда присутствует поле восстановления данных. Закрытый ключ агента

восстановления доступен только учетной записи этого агента. Если войти в систему с учетной записью агента восстановления зашифрованных данных, то при открытии зашифрованного файла сначала расшифровывается закрытым ключом агента восстановления хранящийся в DRF ключ шифрования данных, а затем уже извлеченным ключом шифрования дешифруются сами данные.

7. По умолчанию агентом восстановления на каждом отдельно взятом компьютере является локальная учетная запись *Администратор* данного компьютера. В масштабах домена можно установить службу сертификатов, сгенерировать для определенных доменных учетных записей соответствующие сертификаты, назначить эти учетные записи агентами восстановления (с помощью групповых политик) и установить эти сертификаты на тех файловых серверах, на которых необходимо шифровать данные. При использовании в масштабах корпоративной сети технологии шифрования данных следует предварительно спланировать все эти действия (развертывание служб сертификатов, выдача и хранение сертификатов, назначение агентов восстановления, процедуры восстановления данных в случае удаления учетной записи, с помощью которой данные были зашифрованы).

Кроме того, во многих ситуациях необходимо также учитывать требования законодательства РФ об использовании только разрешенных на территории России алгоритмов шифрования данных. В таких случаях может потребоваться приобрести соответствующие разрешенные модули шифрования и встроить их в систему.

Следует также помнить, что данные хранятся в зашифрованном виде только на жестком диске. При передаче по сети данные передаются с сервера на ПК пользователя в открытом виде (если не включены политики IPSec).

Квоты

8. Квоты — это механизм ограничения доступного пользователям пространства на файловом сервере. Если а файловых хранилищах отсутствует механизм квот, то пользователи очень быстро засоряют доступное дисковое пространство файлами, не имеющими отношения к работе, или различными версиями и копиями одних и тех же документов.

В системах Windows Server используется механизм квотирования «*На том/На пользователя*» (*Per volume/Per user*). Т.е нельзя установить квоты на отдельные папки тома или для групп пользователей. Размер использованного пользователем места на диске вычисляется по атрибуту «*Владелец файла*».

Механизм квот включается на закладке «*Квота*» *Свойств* тома. Если отметить галочкой поле «»*Включить управление квотами*», то включается самый «мягкий» режим управления квотами. В этом режиме не включается запрет на использование дискового пространства сверх установленной квоты, не устанавливаются сами размеры квот, не регистрируются события, связанные с превышением пользователями квот.

Если на этой закладке нажать кнопку «*Записи квот*», то можно получить информацию о том, какой объем дискового пространства использовал в данный момент каждый пользователь

Если включить самый жесткий механизм квот то будет установлен запрет на превышение установленной квоты, в системных журналах будут регистрироваться предупреждения о превышении определенного порога, а также события, отражающие достижение пользователем допустимого предела.

Если на этой странице щелкнуть двойным щелчком мыши на какой-либо записи квот, то для соответствующего пользователя можно установить индивидуальную квоту, отличную от общих установок:

Если пользователь в процессе сохранения информации на том, управляемый квотами, превысит допустимый размер, то ему будет выдано сообщение:

При этом в системном журнале данного сервера для источника данных «*ntfs*» и категории «*Диск*» появится соответствующая запись

Дефрагментация

9. В процессе использования файловых ресурсов возникает фрагментация дискового пространства. Возникает она из-за того, что при удалении файлов в образовавшееся свободное место записываются новые файлы. Если в освободившемся месте новый файл целиком не помещается, то файловая система выделяет файлу кластеры в другом свободном участке. Считывание такого фрагментированного файла с диска требует большего времени. При длительном использовании тома/раздела степень фрагментации увеличивается, производительность службы доступа к файлам снижается, поэтому время от времени требуется производить *дефрагментацию* тома/раздела, которая заключается в том, что кластеры, выделенные файлам, перераспределяются на томе так, чтобы каждый файл занимал смежные кластеры.

Файловые системы семейства FAT сильнее подвержены фрагментации, т.к. вновь создаваемому файлу всегда выделяется первые найденные свободные кластеры (а в процессе удаления файлов, на томе создается много свободных фрагментов небольшого размера). В файловой системе NTFS новым файлам выделяются в первую очередь участки со смежными кластерами, и только в том случае, когда на томе нет непрерывного участка дискового пространства необходимого размера, тогда файлу выделяются не смежные кластеры.

10. Для осуществления дефрагментации дискового пространства используется оснастка «*Дефрагментация диска*» (которая запускается нажатием кнопки «*Выполнить дефрагментацию*» на закладке «*Сервис*», доступной в окне *Свойств* тома/раздела, или утилита командной строки *defrag.exe*.

Оснастка «*Дефрагментация диска*» выполняет две операции: анализ степени фрагментации тома и сам процесс дефрагментации.

Для проведения анализа необходимо нажать кнопку «*Анализ*» в оснастке. В результате анализа будет выведен краткий отчет (рис. 5.53) о степени фрагментации. При нажатии кнопки «*Вывести отчет*» будет выведен подробный отчет со списком фрагментированных файлов.

На картинке используются следующие цветовые обозначения:

- *красный цвет* — участки с фрагментированными файлами;
- *синий цвет* — нефрагментированные файлы;
- *зеленый цвет* — неперемещаемые файлы (это участки с системными файлами, которые нельзя перемещать в процессе дефрагментации, например, файл подкачки);
- *белый цвет* — свободное пространство на томе.

11. При нажатии на кнопку «*Дефрагментация*» начнется процесс дефрагментации, его длительность зависит от размера тома, степени его фрагментированности, степени загруженности сервера. Очень рекомендуется производить дефрагментацию в нерабочее время, т.к. фрагментация требует значительных ресурсов сервера и замедляет работу службы предоставления файлов в общее пользование. По окончании процесса фрагментации картинка в оснастке «*Дефрагментация диска*» будет выглядеть следующим образом На рисунке очень хорошо показана стратегия файловой системы NTFS — размещать файлы в *непрерывных* свободных участках тома. Здесь видно, что большие фрагментированные файлы, находившиеся примерно в середине тома, были перемещены в свободный участок в конце тома.

Практическая работа 11. Установка принтера, настройка свойств и параметров печати. Настройка протокола IPP

Цель работы: способы установки и настройки принтера, настройка протокола IPP/

Ход работы

Системы семейства Windows Server предоставляют богатые возможности совместного использования принтеров, а также средства управления данным процессом.

В системе Windows Server имеются следующие основные возможности управления печатью:

- предоставление совместного доступа к принтерам;
- публикация принтеров в Active Directory для быстрого поиска имеющихся в сети принтеров;
- автоматическая загрузка клиентом с сервера печати драйвера принтера со всеми настройками данного принтера;
- перенаправление порта принтера на другое устройство печати (позволяет быстро восстановить возможности печати при выходе одного из устройств печати из строя);
- создание пула принтеров (привязка одного принтера к нескольким устройствам печати для повышения быстродействия печати);
- привязка нескольких принтеров к одному устройству печати (для более гибкого управления доступом к принтерам);
- печать через Интернет (Internet Printing Protocol).

Определим сначала основные термины, используемые в данном пункте.

- **Устройство печати** (**Print device**) — физическое устройство, на котором осуществляется вывод информации на бумагу или иные виды носителей;
- **Принтер** (**Printer**) — объект операционной системы (программный интерфейс между системой и *портом*);
- **Порт** (**Port**) — объект системы, связывающий *принтер* и *устройство печати*;
- **Драйвер принтера** (**Printer driver**) — программная компонента, преобразующая информацию из компьютера в набор команд, соответствующий данной модели *устройства печати*;
- **Сервер печати** (**Print server**) — компьютер, получающий от приложений, работающих на компьютерах в сети, задания на печать документов;
- **Очередь печати** (**Print queue**) — очередь документов, ожидающих вывода на *устройство печати*;
- **Спулер** (**Spooler**) — компонента системы, которая временно сохраняет на жестком диске сервера документы, содержащиеся в *очереди печати*.

Такая терминология и соответствующая организация управления печатью позволяет очень эффективно использовать сетевые принтеры, быстро восстанавливать функционирование принтера при выходе из строя устройства печати, создавать пулы принтеров, гибко управлять доступом к принтерам для различных пользователей.

Следует иметь в виду, что все эти термины относятся не только к серверным редакциям системы Windows, но и к Windows 2000/XP Professional, которые содержат в себе службы файлов и печати, но с ограничением на 10 одновременных клиентских подключений.

Ход работы

1. *Установка драйверов, настройка принтеров*

Рассмотрим на примерах и обсудим как общие, так и частные вопросы установки и настройки различных компонент сетевой службы печати:

- установка и настройка принтера, предоставление общего доступа к принтеру по сети;
- настройка сервера печати;
- подключение клиентского ПК к серверу печати, загрузка драйверов;
- перенаправление портов;
- создание пула принтеров;
- привязка нескольких принтеров к одному устройству печати и управление доступом к принтерам.

Напомним, что в нашей учебной конфигурации имеется домен *world.ru*, в котором установлены два сервера (оба являются контроллерами домена) — *DC1* и *DC2*.

2. Установка принтера на сервере.

1. Запустим мастер установки принтера на сервере DC1: кнопка «*Пуск*» — «*Принтеры и факсы*» — «*Установка принтера*» — кнопка «*Далее*».

2. Выберем тип принтера — «*Локальный*» (если принтер подключен к какому-либо физическому порту сервера и система Windows может определить этот принтер с помощью технологии «Plug and Play», то нужно отметить галочкой соответствующее поле), нажмем кнопку «*Далее*»:

Если выбираем вариант «*Сетевой принтер*», то нужно будет либо найти принтер в Active Directory, либо указать точный UNC-путь к принтеру в формате «*server**printer*», либо указать путь к принтеру в Интернете:

3. Продолжим установку локального принтера. Выберем порт LPT1:

На данном этапе можно создать новый локальный порт и выбрать, например, порт TCP/IP. Таким образом, на данном сервер будет считаться локальным принтер, имеющий свой сетевой адаптер и подключенный к сети по протоколу TCP/IP.

4. Если принтер автоматически не определился системой, то выберем модель принтера из списка, например, HP LaserJet 5Si (можно указать путь к драйверу принтера, нажав кнопку «*Установить с диска*»), нажмем кнопку «*Далее*»:

5. Введем имя принтера, например, «*Printer1*», нажмем «*Далее*»:

6. Разрешим сетевой доступ к этому принтеру, нажмем «*Далее*»:

7. Далее можно заполнить необязательные поля «*Размещение*» и «*Комментарий*», которые могут оказаться очень полезными, когда на сервере установлено несколько принтеров, нажмем «*Далее*».

8. Затем система предложит напечатать пробную страницу (мы этот шаг пропустим). Кнопка «*Далее*» (система при этом скопирует из дистрибутива в системные папки драйвер принтера), кнопка «*Готово*».

Выполним аналогичную последовательность действий на сервере DC2, выбрав для принтера имя *Printer2*.

4. Подключение к сетевому принтеру с клиентского ПК

В качестве клиента будем использовать компьютер DC1. Подключимся с сервера DC1 к принтеру, установленному на сервере DC2. Можно это сделать с помощью того же мастера установки принтера, указав в нужном месте UNC-путь к принтеру в виде «*DC2**Printer2*», а можно просто открыть в командной строке ресурсы сервера DC2 («*Пуск*» — «*Выполнить*» — «*DC2*») и подключиться к установленному на сервере принтеру

Еще один вариант — найти в Active Directory принтер, установленный на сервере DC2 и подключиться к нему. Откроем «*Пуск*» — «*Поиск*», выберем поиск принтеров, найдем все принтеры в сети и подключимся к притеру

В процессе установки клиентская часть системы выполнит все необходимые подключения и, самое главное, *автоматически загрузит с сервера драйвер принтера* (если он не был установлен на клиентском компьютере). *Все операционные системы на базе технологий Windows NT* автоматически загружают драйверы принтера с сервера при подключении к принтеру. Кроме того, при каждом новом подключении, например, при отправке задания на печать, клиент проверяет, не обновилась ли версия драйвера на сервере, и в случае обновления также автоматически загружает к себе обновленный драйвер. Те драйверы, которые содержатся в базе данных драйверов Windows Server 2003, работают только в системах Windows 2000/XP/2003. Драйверы для более ранних систем на базе Windows NT, то их нужно установить на сервере с дискеты или CD, поставляемых производителем принтера.

Общие параметры сервера печати

5. Откроем папку «*Принтеры и факсы*», выберем в меню «*Файл*» пункт «*Свойства сервера*».

Закладка «*Порты*». На данной закладке можно изменить настройки какого-либо порта, удалить ненужный порт или добавить новый порт, например, локальный TCP/IP-порт. Заметим, что в качестве локального порта можно указать порт в виде UNC-имени «*\\server\printer*».

Закладка «*Драйверы*». На данной закладке можно добавить, обновить или удалить драйвер для какого-либо принтера.

Закладка «*Дополнительные параметры*». На данной закладке можно указать путь к *папке очереди печати* (*файлу спулинга*), отличный от пути по умолчанию. Это целесообразно делать в том случае, если сервер печати предназначен для печати большого объема документов. Не рекомендуется размещать файл спулинга специализированного и очень нагруженного сервера печати на том же жестком диске, что и операционная система и файл подкачки.

6. Свойства принтера

Выберем в папке «*Принтеры и факсы*» нужный принтер, откроем его *Свойства*.

Закладка «*Общие*». Кнопка «*Настройка печати*» — настройка параметров печати (лотки с подачей бумаги, разрешение печати и др.); кнопка «*Пробная печать*» — печать пробной страницы.

Закладка «*Доступ*». Управление доступом к принтеру по сети — предоставление или отмена общего доступа, публикация принтера в Active Directory. Кнопка «*Дополнительные драйверы*» — установка на сервере дополнительных драйверов для различных операционных систем на базе Windows NT.

Закладка «*Порты*». На этой закладке можно переназначить принтер на другой порт (фактически — на другое устройство печати), если текущее используемое устройство печати вышло из строя. Если отметить поле «*Разрешить группировку принтеров в пул*», то можно выбрать для данного принтера одновременно несколько портов; в этом случае конкретные документы будут выводиться на печать на том устройстве, которое будет свободно.

Закладка «*Дополнительно*». Здесь можно настроить расписание, в которое доступен данный принтер (по умолчанию принтер доступен круглые сутки). Если, например, создать на сервере различные объекты принтеров, привязать их к одному и тому же устройству печати, назначить им различное расписание доступности, а на закладке «*Безопасность*» дать доступ различным группам пользователей, то одно и то же устройство печати будет доступно различным группам пользователей в различное время.

На этой же закладке есть настройки использования очереди печати (файла спулинга), рекомендуем оставить данные настройки без изменений, в системе выбран наиболее оптимальный вариант. Если отметить поле «*Сохранять документы после печати*», то напечатанные документы не будут удаляться из очереди (их нужно будет удалять вручную). Данный параметр может быть полезен в том случае, если требуется время от времени делать повторную печать документов (без запуска соответствующих приложений) или необходимо ежедневно контролировать, какие документы печатаются на принтере.

7. Кнопка «*Страница-разделитель*» позволяет вставлять между документами специальные страницы, которые разделяют документы и, кроме того, позволяют менять режим работы принтера. Шаблоны страниц-разделителей хранятся в файлах с расширением «*.sep*». В системе имеются 4 стандартных страницы-разделителя:

- **pcl.sep** — переключает принтер в режим печати PCL и печатает страницу-разделитель перед каждым документом;
- **pscript.sep** — переключает принтер в режим печати PostScript, не печатает страницу-разделитель перед документами;
- **sysprint.sep** — переключает принтер в режим печати PostScript и печатает страницу-разделитель перед каждым документом;

- **sysprtj.sep** — печатает страницу-разделитель перед каждым документом с указанием параметров задачи.

Использование страниц-разделителей целесообразно тогда, когда необходимо разделять задания, отправленные разными пользователями, или в случае, когда необходимо переключать режим работы принтера для различных жокументов.

Закладка «*Безопасность*» — управление разрешениями на доступ к принтеру.

Закладка «*параметры устройства*» — настройка параметров устройства печати.

8. Управление очередью печати

Откроем конкретный принтер в папке «*Принтеры и факсы*», например, *Printer1*. В окне принтера будут видны задания, стоящие в очереди печати. На рисунке показаны названия документов, состояние документа в очереди, имя пользователя, печатающего данный документ, количество страниц, размер документа, дата и время отправки задания на печать.

Раздел меню «*Принтер*», кроме настроек принтера, рассмотренных ранее, позволяет выполнять следующие действия с очередью печати:

- «*Приостановить печать*» — приостановка процесса печати, данное действие может оказаться необходимым для каких-либо действий с устройством печати (например, заправка бумаги);

- «*Очистить очередь печати*» — удалить все здания из очереди печати.

Раздел меню «*Документ*» позволяет выполнить такие операции с документами в очереди:

- «*Приостановить*» — приостановить процесс печати документа;

- «*Продолжить*» — продолжить печатать документ, печать которого была приостановлена;

- «*Перезапустить*» — повторный запуск документа на печать;

- «*Отменить*» — отменить печать документа.

9. Если щелкнуть двойным щелчком мыши на документе в очереди, то откроется окно свойств печатаемого документа, из которых наиболее важное — «*Приоритет*», задаваемый в диапазоне от 1 до 99. Если повысить приоритет задания, то оно будет печататься раньше, чем задания с более низким приоритетом.

Замечание. При управлении очередью печати бывают случаи, когда документ «зависает» в очереди и не удаляется из нее, особенно если возникли какие-либо ошибки во время печати.

Чтобы очистить очередь от таких «зависших» документов, необходимо перезапустить службу «*Диспетчер очереди печати*» (*Spooler*).

10. Протокол IPP (Internet Printing Protocol)

Системы семейства Windows Server поддерживают *протокол печати через Интернет* (*IPP, Internet Printing Protocol*), работающий поверх протокола HTTP и позволяющий пользователям подключаться к принтерам, размещенным в сетях Интернет/интранет. Поддержка данной технологии актуальна в больших корпоративных сетях, состоящих из большого числа IP-сетей, в которых не всегда эффективно работают стандартное взаимодействие между пользователем и сервером через *вызовы удаленных процедур* (*RPC, Remote Procedure call*).

11. Установка службы печати через Интернет

Служба печати через Интернет устанавливается достаточно просто, как и большинство других компонент системы Windows Server.

1. Нажмем кнопку «*Пуск*», далее — «*Панель управления*» — «*Установка и удаление программ*» — кнопка «*Установка компонентов Windows*».

2. Выберем в списке строку «*Сервер приложений*», но не будем ставить галочку для этой строки, а нажмем кнопку «*Состав*»:

3. Выберем «*Службы IIS*», не ставя галочку, также нажимаем кнопку «*Состав*», отмечаем поле «*Печать через Интернет*», все необходимые компоненты система добавит автоматически. Далее нажимаем нужное количество раз кнопки «*ОК*», «*Далее*» и «*Готово*».

12. Подключение клиента

Подключение пользователя и управление заданиями — все эти операции выполняются через Обозреватель Интернета.

1.Для подключения к серверу печати необходимо в строке адреса Обозревателя ввести адрес в формате «*http://<server>/printers*». В нашей учебной сети это будет выглядеть как «*http://dc1.world.ru/printers*» или «*http://dc2.world.ru/printers*». После подключения увидим веб-страницу сервера печати:

2. Щелкнем мышью на ссылке, указывающей на нужный принтер (в примере — Printer2), затем щелкнем по ссылке «*Подключить*» (эта ссылка выделена жирным шрифтом), система произведет подключение к принтеру, причем драйвер принтера автоматически загрузится и установится на клиентский ПК:

3. Теперь принтер подключен на клиентском ПК, и им можно пользоваться для печати документов из любого приложения.

13. Управление очередью печати

Управление документами в очереди также осуществляется в Обозревателе Интернета. Отправим на печать несколько документов и проверим состояние очереди (рис.:

В окне Обозревателя мы можем приостанавливать и продолжать печать выбранного документа, отменять печать документа, очищать очередь печати.

Первая часть данного раздела описывает управление дисками, разделами и томами, а также структуру файловых систем FAT16, FAT32 и NTFS.

Вторая часть описывает управление доступом к файловым ресурсам: сетевые разрешения, разрешения NTFS, аудит доступа.

Третья часть раздела приведено описание дополнительных функций по управлению файловыми ресурсами: сжатие и шифрование данных, квоты, дефрагментация дискового пространства.

Четвертая часть посвящена управлению ресурсами сетевой печати: установка принтера на сервере, настройка параметров печати, предоставление общего доступа к сетевому принтеру, подключение клиентов к сетевым принтерам, перенаправление портов принтера, создание пула принтеров, предоставление доступа к сетевым принтерам по протоколу IPP (протокол печати через Интернет).

Задачи сетевого администратора при управлении ресурсами файлов и печати:

- планирование необходимого объема дискового пространства;
- планирование и реализация необходимых дисковых конфигураций (базовые или динамические диски);
- планирование и реализация прав доступа к файловым ресурсам (сетевые разрешения и разрешения NTFS);
- планирование и реализация аудита доступа к ресурсам;
- планирование и реализация механизмов сжатия и шифрования данных;
- планирование и реализация квот пользователей на дисковое пространство;
- анализ степени фрагментации дискового пространства и осуществление дефрагментации в случае необходимости;
- планирование и размещение сетевых принтеров, управление доступом к принтерам, подключение рабочих мест к сетевым принтерам.

Практическая работа 12. Составление сметы для подключения к сети Интернет

Цель работы: Научиться создавать проект локальной сети с учетом предлагаемых требований. Обосновать выбор сетевого оборудования.

Ход работы:

В настоящее время довольно часто бывает необходимым проявить знания и умения выполнения проектов локальной сети. Обычно, для проектирования сети в крупных фирмах и организациях приглашают сотрудников фирм, занимающихся проектированием и монтажом сетей. Если фирма небольшая, то иногда целесообразно проводить проектирование и монтаж сети «своими» силами. Поэтому, рассмотрим основные этапы проектирования локальной сети для небольшой фирмы, состоящей из определенного количества сотрудников, которая занимает определенное количество комнат и этажей.

Основные этапы проектирования локальной сети:

1. Определение количества сотрудников, использующих компьютеры.
2. Определение планируемого расширения штата фирмы (при проектировании локальной сети необходимо предусмотреть планируемое расширение фирмы, чтобы в дальнейшем была возможность подключения дополнительных узлов к сети).
3. Определение количества комнат и этажей, занимаемых фирмой с возможностью дальнейшего расширения.
4. Выбор физической топологии сети.
5. Выбор оптимального сетевого оборудования (коммутаторов, маршрутизаторов) с учетом планируемого расширения и бюджета фирмы.
6. Выбор сетевого кабеля и предварительный подсчет метража в соответствии с метражом комнат.
7. Возможность использования сетевых коробов, пач-панелей, патчкордов, розеток, коммуникационных шкафов для размещения свитчей, управляемых свитчей, маршрутизаторов, серверов, если необходимо ограничить физический доступ к оборудованию сотрудников фирмы.
8. Выбор типа сети - одноранговая сеть, сеть на основе сервера, комбинированная сеть.
9. Определение типов серверов для сети на основе сервера и комбинированной сети (файловый сервер, сервер приложений, сервер- маршрутизатор, почтовый сервер, принт-сервер). Возможность совмещения услуг, предоставляемых серверами (например, можно объединить почтовый сервер и сервер-маршрутизатор, или файловый сервер и принт-сервер).
10. Определить уровень безопасности, необходимый для нормального функционирования фирмы и хранения коммерческой информации, исходя из этого, выбрать, под какой операционной системой будут работать рабочие станции локальной сети и сервера.
11. Выбрав коммуникационное оборудование и дополнительное оборудование для монтажа сети, произвести с учетом текущих цен на сетевое оборудование расчет примерной сметы расходов проекта локальной сети фирмы (прайсы по сетевому оборудованию можно найти на сайтах фирм, например, «Компьютерные технологии»).

Основные рекомендации к выполнению практической работы.

При выполнении проектирования локальной сети в соответствии с вариантом заданий для проводной сети рекомендуется:

- при выборе физической топологии использовать «звезду» или иерархическую звезду» (с несколькими коммутаторами);
- для обеспечения возможности фильтрации трафика на канальном уровне и обеспечения дополнительных средств безопасности использовать управляемый коммутатор;

- - если предполагается выход в Internet или соединение с другими сетями, использовать маршрутизатор.
- при выборе сетевого кабеля обратить внимание на то, необходим ли экранированный кабель, или достаточно выбрать неэкранированную витую пару;
- кабель рекомендуется выбирать также с учетом того, будет ли использоваться у вас для укладки кабеля сетевые короба, патчпанели, сетевые розетки, или это оборудование не будет использоваться.
- при расчете примерной сметы расходов самостоятельно определить метраж комнат, чтобы в дальнейшем расчитать метраж сетевого кабеля;
- при расчете сметы расходов на проект локальной сети обратить внимание на конфигурацию серверов и конфигурацию рабочих станций. Объяснить необходимость закупки серверов и рабочих станций выбранной вами конфигурации;
- обосновать выбор операционных систем для компьютеров сотрудников фирмы и серверов.
- обосновать использование коммутационных шкафов в каждой комнате под коммутаторы, сервера; для удобства подключения в напольных шкафах использовать патч-панели. Коммутационные шкафы, патч-панели, сетевые розетки, инструмент для монтажа локальной сети учесть в смете расходов.

Задание к практической работе (часть 1)

Небольшую фирму, состоящую из «А» сотрудников, занимающую «В» этажей в одном здании, размещающуюся в «С» комнатах (количество комнат на этажах выбрать из указанного количества самостоятельно), необходимо обеспечить локальной сетью.

Последнее время увеличился объем работы и в будущем планируется расширение штата (D человек).

У каждого сотрудника есть компьютер. Информация конфиденциальна. Одновременно с установкой сети планируется установка лазерного принтера (выбрать оптимальное количество принтеров для нормальной работы фирмы). Планируется, что будет использоваться сетевая база данных, необходим сервер для хранения информации.

Предложите проект локальной сети для этой фирмы. Необходимо привести примерный план размещения сотрудников по комнатам, перечислить сетевое оборудование, обосновать выбор данного сетевого оборудования, необходимого для нормальной работы сети, описать топологию, которой Вы будете придерживаться, проектируя сеть, обосновать выбор. Описать обязанности сотрудников по отношению к сети (будет ли ими производиться настройка адаптеров и т.д.). Какие меры безопасности Вы бы предложили для сохранения конфиденциальности информации. Посчитать стоимость проекта с учетом выбранного сетевого оборудования.

Варианты лабораторной работы приведены таблице 1.

Таблица 1 - Варианты заданий

№ варианта	«А» сотрудники	«В» этажи	«С» комнаты	«Д» расширение
1	10	2	3	5
2	12	1	4	5
3	12	2	3	8
4	10	1	2	5
5	7	1	2	3

6	8	1	4	5
7	9	1	3	7
8	10	2	2	5
9	12	2	5	5
10	12	1	2	8
11	10	1	4	5
12	7	1	2	3
13	8	1	2	5
14	9	1	2	7
15	15	2	4	8
16	15	2	4	10
17	17	2	4	12
18	20	3	5	12
19	20	3	5	10
20	17	2	3	12
21	16	1	4	5
22	16	2	5	6
23	18	1	4	7
24	22	2	5	8
25	22	1	4	9
26	17	2	3	10
27	30	2	4	5
28	31	2	5	5
29	32	2	4	7
30	33	1	2	8

Задание к практической работе (часть 2)

Предложите проект локальной сети для этой фирмы, план размещения сотрудников которой приведен на рисунке 1. Необходимо перечислить сетевое оборудование, обосновать выбор данного сетевого оборудования, необходимого для нормальной работы сети, описать топологию, которой Вы будете придерживаться, проектируя сеть, обосновать выбор. Описать обязанности сотрудников по отношению к сети (будет ли ими

производиться настройка адаптеров и т.д.). Какие меры безопасности Вы бы предложили для сохранения конфиденциальности информации.

Исходные данные взять из рисунка 1.

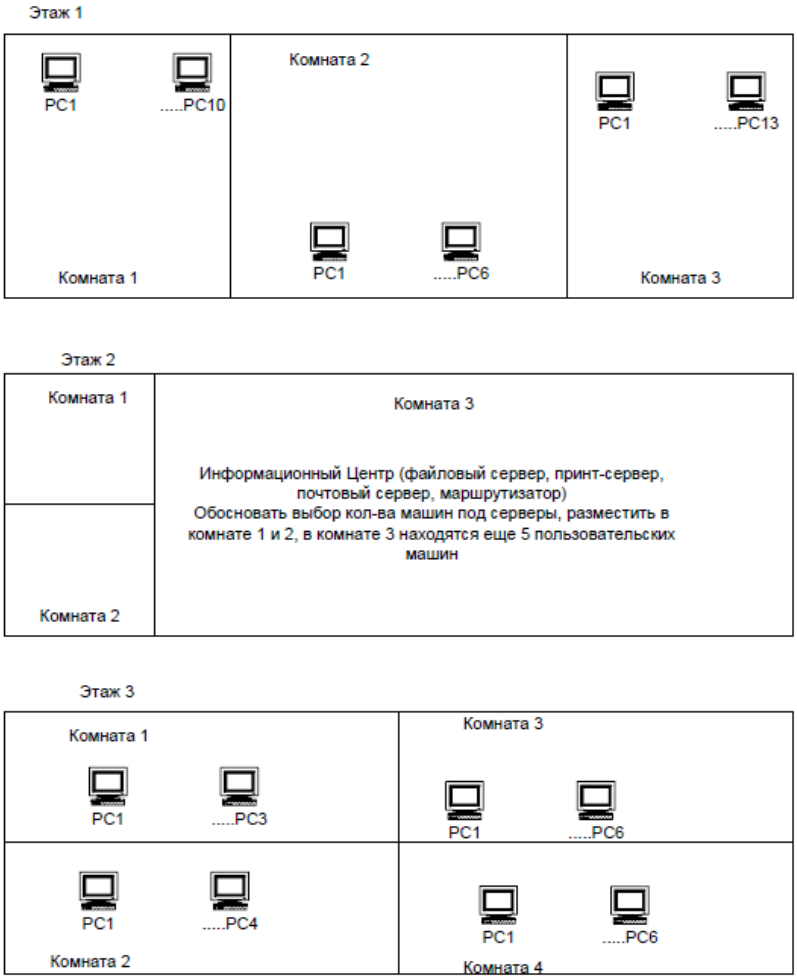


Рисунок 1- План размещения PC для проектирования ЛВС (задача 2 - вариант один для всех)

Отчет по практической работе должен содержать:

- схему размещения сотрудников фирмы по отделам (с отделами определиться самостоятельно);
- схему подключения узлов сети к коммутаторам, маршрутизатору (с учетом серверов и рабочих станций);
- описание выбранной Вами типовой конфигурации для серверов, рабочих станций, с указанием выбранной ОС и аппаратуры (тип процессора, память, жесткий диск - использовать готовую конфигурацию, предлагаемую фирмами);
- перечень сетевого оборудования (коммутаторы, маршрутизаторы, кабель, пассивное сетевое оборудование), его кол-во, цена за единицу и общая стоимость (взять из прайса сетевого оборудования);
- типы серверов (сервер приложений, файловый сервер, прин-сервер и т.д.);
- действия сотрудников фирмы по настройке и поддержанию работоспособности локальной сети.
- какие средства безопасности сети можно использовать?

Задание к практической работе (часть 3)

План-проект учебной компьютерной сети школы

Описание задания

Необходимо спроектировать сегмент учебной компьютерной сети для школы. В школе уже существует две сети:

- административная сеть, объединяющая компьютеры директора, секретаря и бухгалтерии;
- компьютеры кабинетов информатики, имеющих выделенный сервер (обычный компьютер под управлением Windows 10).

Кроме этого еще в 3-ти кабинетах имеются демонстрационные компьютеры с проекторами и 1 компьютер в учительской.

Планируется одновременная трансляция видео и передача голосовых данных

Исходные данные

1. Цели использования сети:

- Обучение школьников различным дисциплинам с использованием сетевых технологий.
- Доступ к информационным ресурсам (библиотека, Интернет).
- Демонстрация видео уроков.
- Голосовое общение по сети.

2. Требуемые характеристики сети:

- скорость передачи достаточная для поддержания видеовещания и голосового общения;
- выход в интернет.
- отделение учебной сети от имеющейся административной сети;
- ограничение доступа пользователей к ресурсам сети.
- масштабируемость.

3. Характеристики существующих компьютеров и других устройств:

В организации имеется уже существующая сеть с выделенным сервером, объединяющая компьютеры в кабинетах информатики.

- количество компьютеров — 26:
- кабинет информатики 1 (10 ученических + 1 учительский);
- кабинет информатики 1 (10 ученических + 1 учительский + 1 сервер);
- по одному компьютеру в 3 кабинетах (история, география, биология);
- один компьютер в учительской.

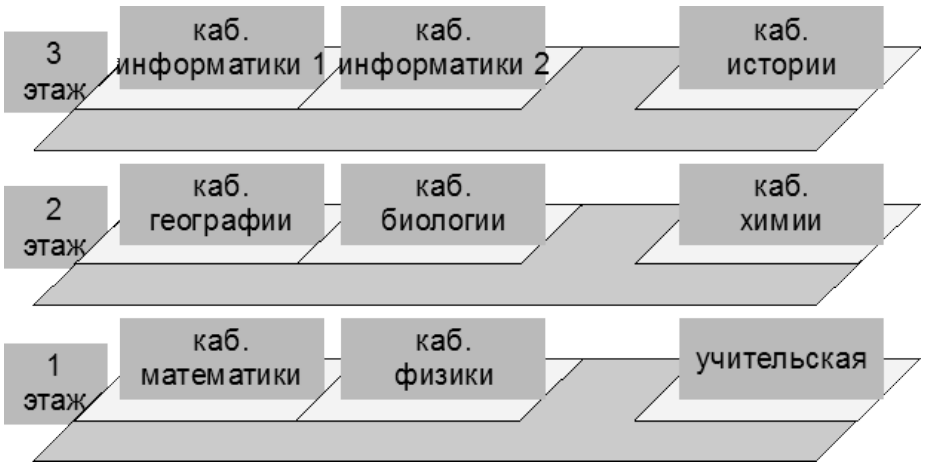
Все компьютеры типовые и имеют следующие характеристики:

- Процессор — Athlon XP 1600+;
- Оперативная память — 256 Мб;
- Жесткий диск — 40 Гб;
- Сетевой адаптер — встроенный (100 Мб, Ethernet).
- количество принтеров — 2 (Samsung ML-1015).
- модемы — аналоговый модем HSP56 MicroModem.

4. Характеристики используемого программного обеспечения:

- Операционные системы:
- Windows10 professional.

Примерная схема здания.



Проектирование сети

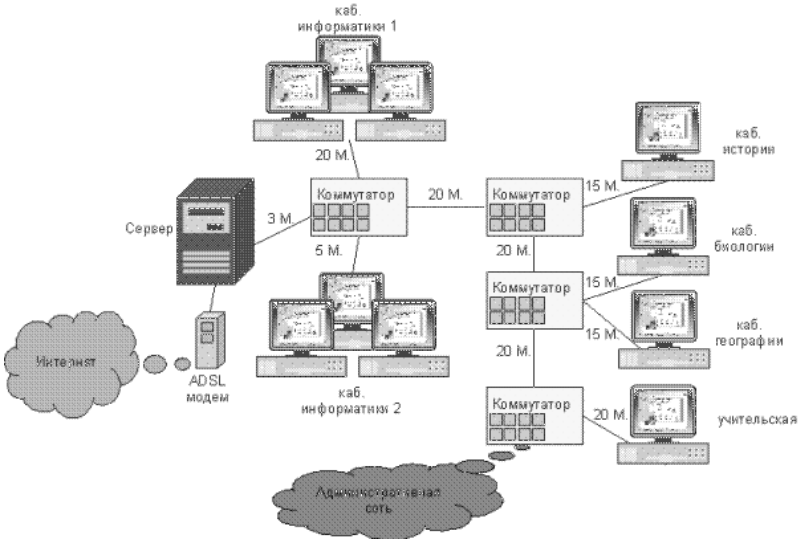
1. Способ сегментирования и объединения сегментов:
- целесообразно использовать концентраторы, т.к. планируется объединять в сеть не большое количество компьютеров (менее 30).
- целесообразно расположить на каждом этаже по концентратору, т.к. в будущем планируется покупка компьютеров для других кабинетов и подключение их к учебной компьютерной сети.

2. Тип кабеля— не экранированная витая пара 5-й категории.

3. Активные устройства— ADSL модем с встроенным брандмауэром.

4. Программное обеспечение:
- ОС для рабочих станций — Windows 10 (уже имеется на компьютерах);
- ОС для сервера — Windows 2003 server (необходимо купить для установки на 1 компьютер);
- прокси-сервер — TrafficInspector (необходимо купить для установки на 1 компьютер);
- антивирусное программное обеспечение — Dr.Web (необходимо купить на каждый компьютер используемый в сети)

Разработка схемы сети.



Определение стоимости

1. Анализ основных направлений затрат:
- сетевое оборудование (концентраторы, не экранированная витая пара 5-й категории, ADSL модем, подключение по технологии ADSL, и т.д.);
- модернизация сервера (оперативная память, жесткий диск);
- монтажное оборудование и инструменты (клещи, короба и т.д.);
- программное обеспечение (Windows 2003 server, TrafficInspector, Dr.Web).

Составление сметы примерных затрат.

Наименование	Цена руб.	Кол-во	Всего
Оперативная память 512 Мб			
Жесткий диск 160 Gb			
Витая пара			
Концентраторы			
ADSL модем			
Клещи			
Разъемы RJ-45			
Короб			
Windows 2003 server			
TrafficInspector			
Dr.Web			
ADSL интернет			
		ИТОГО	

Примерный план проведения работ

Наименование работ	Кол-во дней	Примечание
Уточнение необходимой длины кабелей		
Покупка материалов		
Монтаж локальной сети		
Установка программного обеспечения		
Всего		

Контрольные вопросы:

1. Что такое сеть на основе сервера?
2. Какие физические топологии Вы знаете?
3. Какие категории кабеля «витая пара» Вы знаете?
4. Какие еще типы кабеля Вы знаете?
5. Что такое 8P8C?
6. В чем отличие концентратора от коммутатора?
7. Для чего используется управляемый коммутатор?
8. В чем отличие маршрутизатора от коммутатора?
9. От чего зависит, на сколько портов выбрать коммутатор?
10. Для чего используются патч-панели?
11. Какие средства защиты сети Вы предложили бы для своего проекта?

Практическая работа 13. Настройка ПК для выхода в сеть Интернет

Цель работы: изучение основных способов подключения и настройки соединения к сети Интернет в различных операционных системах.

Ход работы

Сетевые технологии

Наиболее распространенными сетевыми технологиями являются беспроводная технология, Ethernet, HomePNA и Powerline.

Существует несколько видов оборудования, используемого в домашних сетях.

- **Сетевые адаптеры.** Эти адаптеры (также называемые сетевыми интерфейсными платами (NIC)) подключают компьютеры к сети, чтобы те могли обмениваться данными. Сетевой адаптер можно подключить к порту USB или Ethernet на компьютере или установить внутри компьютера в свободное гнездо расширения PCI.

- **Сетевые концентраторы и коммутаторы.** Концентраторы и коммутаторы подключают два или большее число компьютеров к сети Ethernet.

Концентратор Ethernet

Задание 1. Настройка общего доступа к подключению Интернета

Для того чтобы настроить общий доступ и подключение к сети интернет необходимо:

1. На сервере:

Войдите на сервер с учетной записью администратора или владельца. Нажмите кнопку Пуск и выберите пункт «Панель управления». Щелкните пункт «Сеть и подключения к Интернету». Щелкните ссылку «Сетевые подключения». Щелкните правой кнопкой мыши подключение, которое должно использоваться для выхода в интернет. Например, если доступ в Интернет осуществляется через модем, щелкните правой кнопкой мыши требуемое подключение в разделе «Удаленный доступ». Нажмите кнопку «Свойства». Откройте вкладку «Дополнительно». В разделе Общий доступ к подключению Интернета установите флажок «Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера».

При использовании удаленного общего подключения к Интернету установите флажок «Устанавливать вызов по требованию», чтобы разрешить компьютеру автоматическое подключение к Интернету. Нажмите кнопку «ОК».

Когда общий доступ к Интернету будет разрешен, сетевой плате локальной сети будет назначен IP-адрес 192.168.0.1. При этом связь с другими компьютерами сети может быть потеряна. Если другие компьютеры используют статические IP-адреса, следует настроить их на использование динамических адресов. Вы действительно хотите разрешить общий доступ к подключению Интернета? Нажмите «Да».

Для сетевой платы локальной сети устанавливается статический IP-адрес 192.168.0.1 и маска подсети 255.255.255.0.

2. На клиентском компьютере:

Для подключения к Интернету через общее соединение, необходимо проверить настройки IP для сетевой платы локальной сети и затем настроить клиентский компьютер. Для проверки настроек IP для сетевой платы локальной сети, выполните указанные ниже действия.

Войдите на клиентский компьютер с учетной записью администратора или владельца.

Нажмите кнопку «Пуск» и выберите пункт «Панель управления».

Щелкните пункт «Сеть и подключения к Интернету».

Щелкните ссылку «Сетевые подключения».

Щелкните правой кнопкой мыши значок «Подключение по локальной сети» и выберите команду «Свойства».

На вкладке «Общие» выберите параметр «Протокол Интернета (TCP/IP)» в списке «Компоненты, используемые этим подключением» и нажмите кнопку «Свойства».

В диалоговом окне «Свойства»: Протокол Интернета (TCP/IP) выберите пункт «Получить IP-адрес автоматически» (если он еще не выбран) и нажмите «ОК».

Примечание. Можно также назначить уникальный статический IP-адрес в диапазоне от 192.168.0.2 до 192.168.0.254. Например, возможно назначение следующей комбинации статического IP-адреса, маски подсети и шлюза по умолчанию: IP-адрес 192.168.0.2 Маска подсети: 255.255.255.0

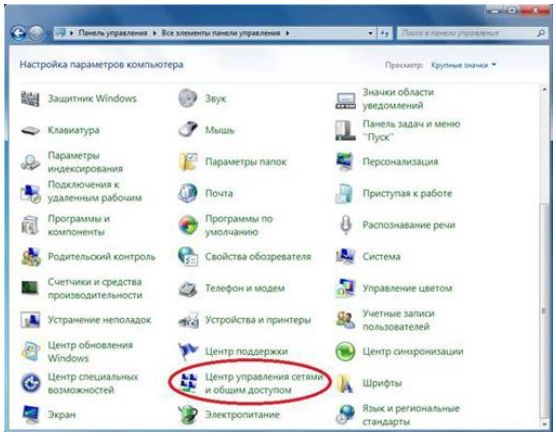
Шлюз по умолчанию: 192.168.0.1. В диалоговом окне Подключение по локальной сети - свойства нажмите кнопку «ОК». Закройте панель управления.

Задание 2. Настройка интернет на Windows 7

Прежде чем приступать к настройке интернет соединения, Вам необходимо установить драйвера на модем, сетевую карту или другое устройство, с помощью которого Вы осуществляете доступ в Интернет. Для начала Вам необходимо запустить Панель управления (Пуск и выбрать Панель управления):

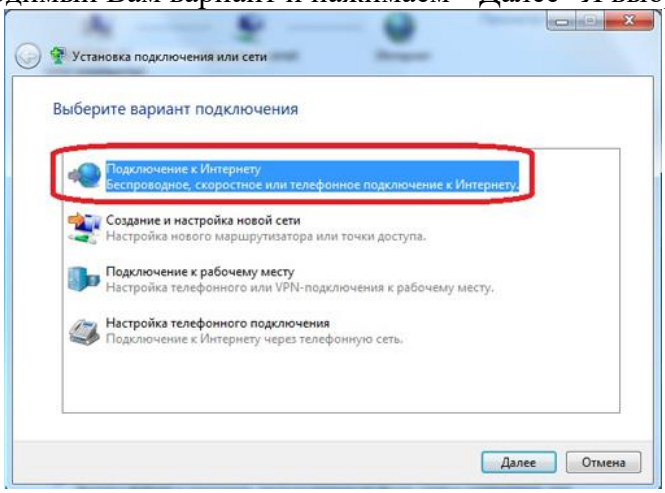
У вас появится окно Настройки параметров компьютера, в котором нужно переключить вид по категориям:

После этого в появившемся списке выбирайте "Центр управления сетями и общим доступом":



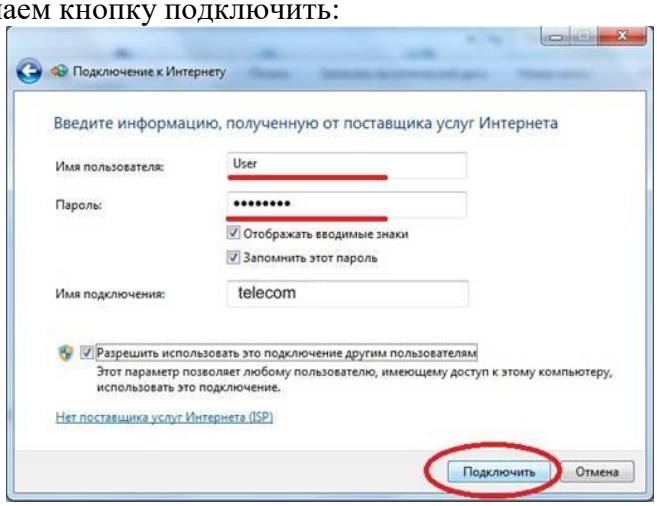
В "Центре управления сетями и общим доступом" Вам необходимо выбрать пункт "Настройка нового подключения или сети":

На следующем этапе установки нужно быть внимательным! Здесь операционная система Windows 7 предлагает нам выбрать вариант подключения к Интернету. В случае если Вы используете ADSL подключение, то Вам необходимо выбрать первый пункт: "Подключение к Интернету". Если Вы используете например 3G Интернет, то вам необходимо выбрать пункт "Настройка телефонного подключения". Выбираем необходимый Вам вариант и нажимаем "Далее" Я выбрал первый вариант:



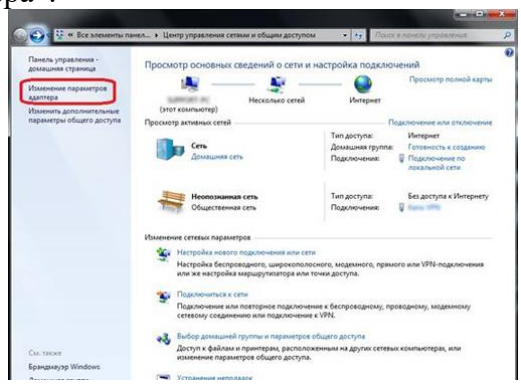
В следующем окне нам нужно просто нажать на "Высокоскоростное (с PPPoE)" (Если Вы настраиваете 3G интернет, то на этой стадии у Вас появится окно выбора модема):

После этого необходимо ввести информацию от поставщика интернет услуг. Здесь пишем имя пользователя и пароль. Если Вы настраиваете 3G интернет, то у Вас будет ещё одно дополнительное поле "Набираемый номер". После того как данные были введены, нажимаем кнопку подключить:



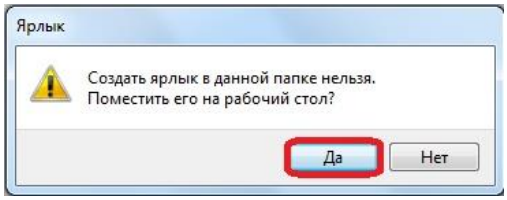
Если все настроено правильно, то у вас появится надпись: "Подключение к Интернету готово к использованию".

Следующим этапом **настройки интернета на Windows 7** будет создание ярлыка подключения на рабочем столе. Для этого опять переходим в панель управления ->Центр управления сетями и общим доступом и кликаем по пункту "Изменение параметров адаптера":



В появившемся окне кликаем правой кнопкой мыши на созданном соединении и выбираем пункт "Создать ярлык":

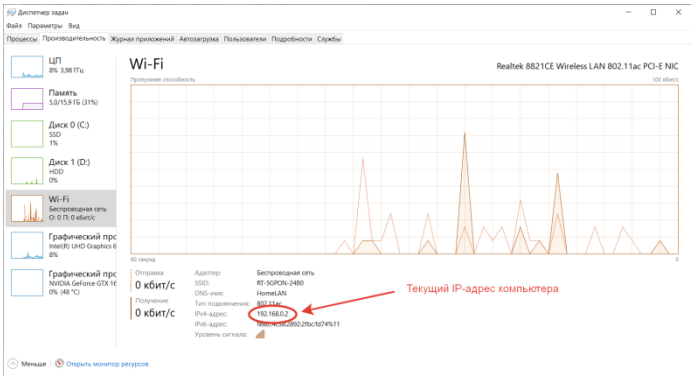
Теперь кликаем на кнопку "Да" тем самым, подтверждая помещение ярлыка на рабочий стол:



Задание 3. Настройка сети в Windows 10

Возможности домашней локальной сети в Windows 10

Локальная сеть поддерживается во всех версиях Windows, включая последние релизы «десятки». Различие касается лишь некоторых ограничений, допускаемых для «домашних» версий, но и в них есть решения для подключения сетевого оборудования (по проводам или через Wi-Fi). К домашней сети обычно подключаются как компьютеры, так и смартфоны или планшеты.



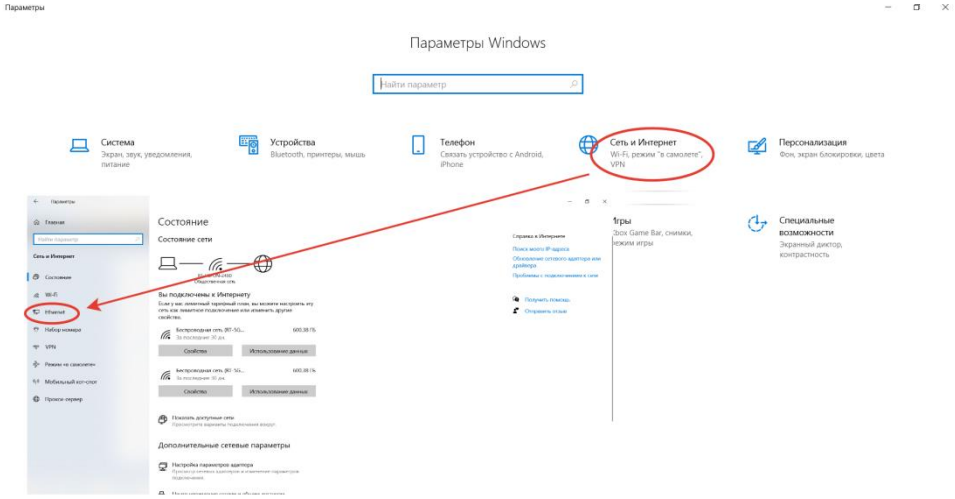
Возможности локальной сети:

1. Общий доступ со всех устройств к расшаренной папке или внешнему накопителю.
2. Совместное использование функционала принтера, сканера, МФУ.
3. Подключение к мультимедийным устройствам, настройка сетевых игр.

Как именно использовать возможности сети, зависит от пользователя. Одни закидывают на внешний диск фильмы и смотрят их на телевизоре с Wi-Fi, другие создают резервные копии корпоративных данных или печатают фотографии со смартфонов. Главное – первоначально настроить сеть и добиться видимости нужного оборудования со всех подключенных устройств.

Выбор статического IP-адреса

Первый шаг к настройке сети – это установка постоянного (статического) IP-адреса для каждого компьютера, который будет подключен к ней. В принципе, большая часть приложений и приборов работает с динамическим адресом, но гарантии стабильного коннекта не будет. Тем более выбор «статики» занимает всего пару минут.



Последовательность действий:

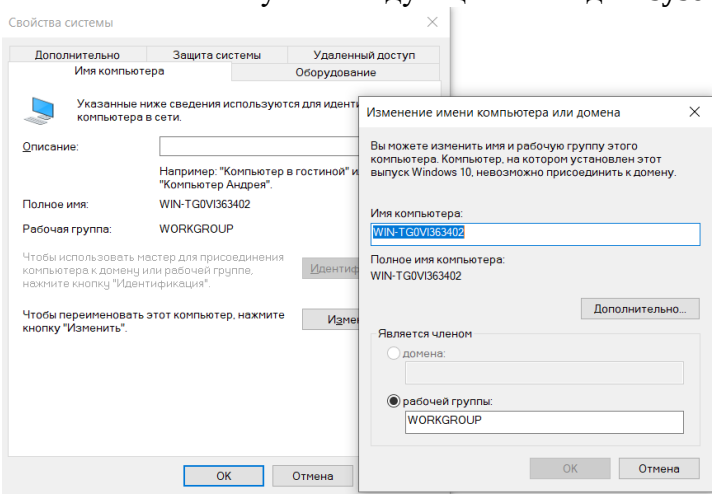
1. Через встроенный поиск найти и открыть утилиту «Параметры».
2. Выбрать пункт «Сеть и Интернет», зайти в раздел Ethernet или Wi-Fi.
3. Щелкнуть на названии текущего сетевого подключения.
4. Прокрутить окно вниз до раздела «Параметры IP».
5. Изменить значение с «Автоматически (DHCP)» на вручную.
6. Включить режим IPv4 или IPv6 в зависимости от задачи.
7. Внести IP-адрес, длину префикса подсети и шлюз.

Здесь же возможно указание DNS-сервера (предпочтительного и дополнительного). После нажатия кнопки «Сохранить» рекомендуется перезагрузить компьютер. В качестве IP-адреса выбирается одно значение из диапазона 192.168.0.1-192.168.255.255. Главное, чтобы каждое устройство приобрело уникальный адрес (начиная с роутера, который часто «висит» на 192.168.0.1 или 192.168.1.1).

В поле «Длина префикса подсети» нужно ввести значение 24, а в качестве DNS-адреса служебного хоста или общедоступного сервера от Google – 8.8.8.8 и 8.8.8.4. То же указывается при выборе IPv6, хотя «устаревший» протокол IPv4 остается практически стандартом де-факто. Его гарантированно поддерживает оборудование, приобретенное даже лет 5-10 назад.

Настройка локальной сети Windows 10

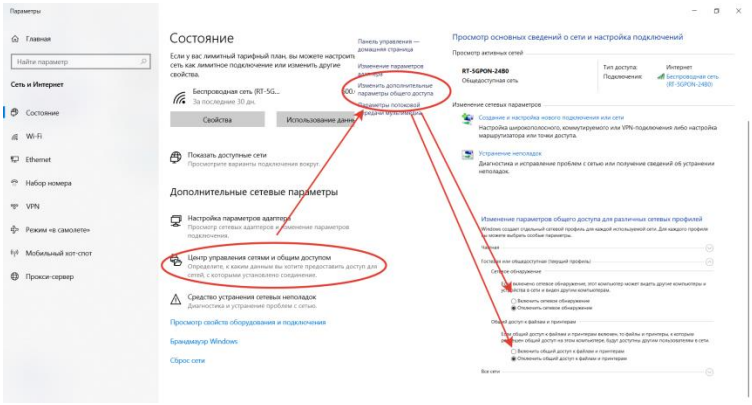
Второй шаг, после назначения компьютерам уникального IP, заключается в назначении одной и той же «рабочей группы», а также индивидуального имени, по которому будет проще определять, к какому именно ПК осуществляется доступ. На всех релизах Windows используется следующая команда – **sysdm.cpl**.



В открывшемся окне нужно нажать кнопку «Изменить» и внести выбранные наименования, а после подтвердить их кликом «ОК» в обеих вкладках. После перезагрузки техника гарантированно войдет в общую рабочую группу и сможет обмениваться файлами, подключаться к сетевым устройствам и использовать их функционал.

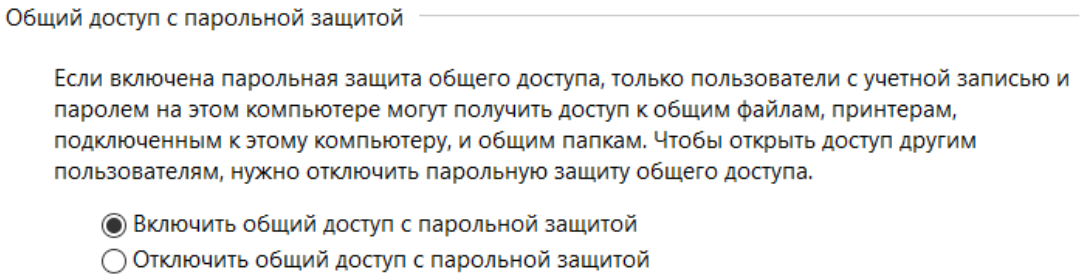
Общий доступ к папкам

Пользователь вправе открыть доступ ко всем накопителям, подключенным к компьютеру, но это небезопасно. Оптимально предоставлять общий доступ только к специально созданному каталогу, в котором и хранятся общедоступные файлы. Это особенно важно, если к локальной сети получают доступ «посторонние» – гости, соседи и пр.



Последовательность действий:

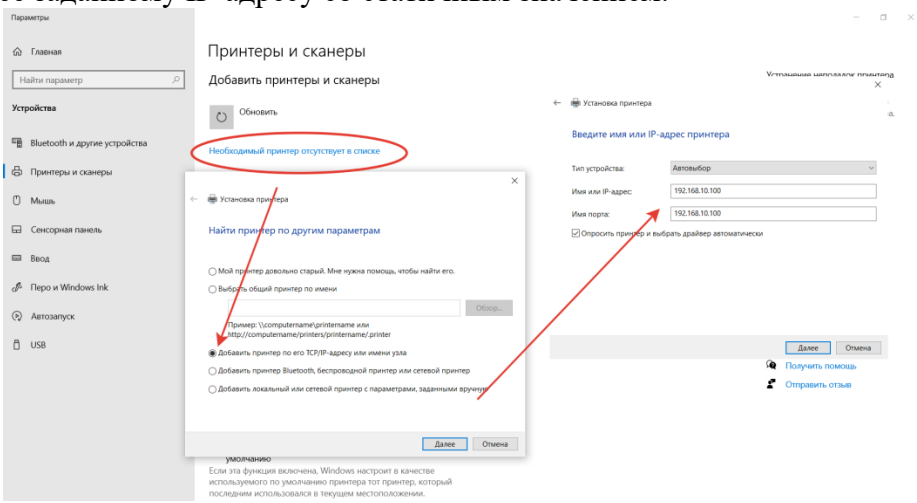
1. Открыть меню кликом правой кнопкой мышки по «Пуску».
2. Выбрать пункт «Сетевые подключения».
3. Кликнуть раздел «Центр управления сетями и общим доступом».
4. Перейти в подраздел «Изменить дополнительные параметры общего доступа».
5. Включить сетевое обнаружение и общий доступ к файлам и принтерам.
6. Перейти в раздел «Все сети» и отключить парольную защиту.



Остается нажать на кнопку «Сохранить изменения» и перезагрузить компьютер. Теперь все доступные устройства будут видны в разделе «Сеть» Проводника. Но пока на них ресурсы не «расшарены»: при попытке обращения система выдаст ошибку, и воспользоваться сетевыми функциями не получится. Чтобы активировать тот же принтер, нужно настроить сетевой доступ отдельно для него.

Настройка сетевого принтера

Предварительно печатающее устройство подключается и настраивается на одном из локальных ПК. В идеале это компьютер, который в течение дня включен постоянно, потому что при выключении доступ к сетевому аппарату пропадет. Обращение к нему происходит по ранее заданному IP-адресу со статичным значением.



Последовательность действий:

1. Запустить приложение «Принтеры и сканеры».
2. Нажать на кнопку «Добавить принтер или сканер».
3. Выбрать пункт «Необходимый принтер отсутствует в списке».
4. Переключить режим определения в TCP/IP.
5. Перейти в следующее окно и внести нужный IP-адрес.

Остается нажать на кнопку «Далее» и дождаться сообщения Windows о завершении процедуры поиска и подключения. Теперь можно распечатать тестовую страницу, чтобы убедиться в качестве работы и соответствии желаемых настроек. Если система не обнаружила принтер автоматически, будет предложен список поддерживаемых моделей для ручного соединения.

Как принудительно отключить сетевое подключение

На практике иногда возникают ситуации, когда приходится экстренно прерывать соединение через локальную сеть. Например, когда соседи начали пользоваться общим диском или принтер «вдруг» начал самопроизвольно печатать. Такое часто происходит в многоквартирных домах, где мощности Wi-Fi роутера часто достаточно для коннекта даже «через этаж».

Варианты:

1. Отключить сетевой кабель или питание роутера.
2. Произвести «обратную» настройку с отключением доступа.

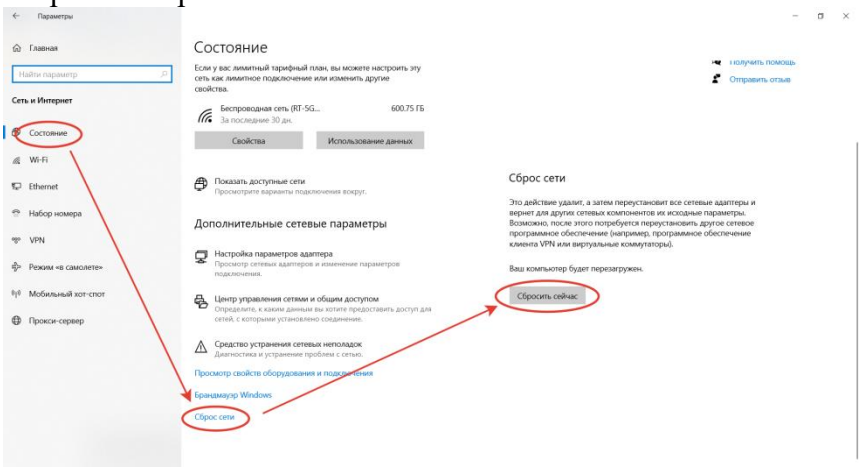
3. Включить парольную защиту для критически важных ресурсов.

Также есть вариант ручного редактирования системного реестра. Это позволит увидеть перечень всех ранее подключенных устройств и вручную удалить ресурсы, к которым хочется заблокировать внешний доступ. Нужно запустить редактор реестра и найти ветку:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

Типовые проблемы с сетевым подключением

Большая часть неполадок, связанным с сетью, разрешается путем перезагрузки активных устройств (роутера, компьютера, принтера). Но иногда пользователю приходится сталкиваться с проблемами после обновления Windows, подключения нового оборудования в качестве замены сломанного. Наиболее универсальное решение неполадок заключается в полном сбросе настроек.

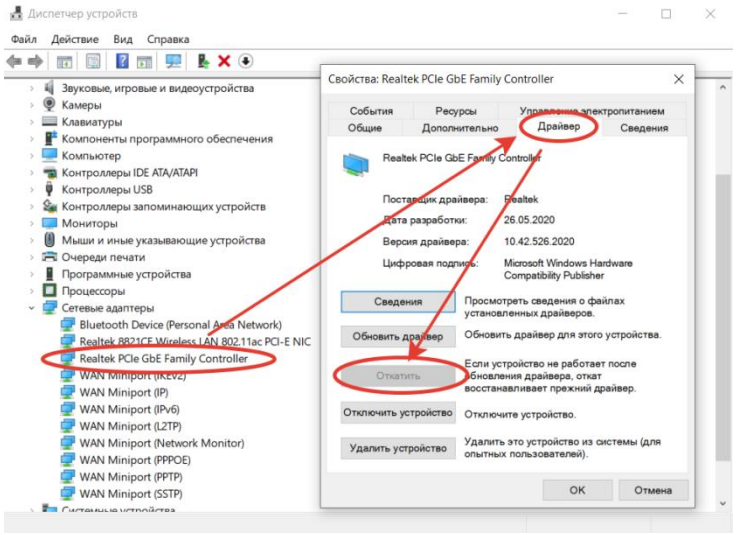


Последовательность действий:

1. Запустить приложение «Параметры».
2. Зайти во вкладку «Сеть и Интернет».
3. Выбрать пункт «Состояние».
4. Прокрутить до «Сброс сети».
5. Кликнуть по пункту.
6. Подтвердить задачу.

Второй «универсальный» вариант, не требующий квалификации в сетевых настройках, состоит в использовании встроенного в Windows инструмента «Диагностики неполадок». Открывается они при клике правой кнопкой мыши на сетевом подключении. В открывшемся окне выбирается один из адаптеров, по вине которого, как считает пользователь, возникли неполадки.

Система сканирует сетевые устройства и пытается обнаружить техническую проблему, выявить ее причину. По завершении процедуры отображается резюме с рекомендациями или заключение, что никаких неполадок не обнаружено. Если предложенные методики не помогли разрешить ситуацию, придется погружаться в детали. Например, разбираться, как откатить драйвер сетевого адаптера.



Выполняется это в «Диспетчере устройств» – нужно выбрать устройство, кликнуть по нему правой кнопкой мышки и далее по пункту «Свойства». В открывшейся вкладке следует переключиться на блок «Драйвер» и нажать на кнопку «Откатить». Она активна только при наличии в архиве системы старой версии драйвера. Если это так, стоит попробовать кликнуть на «Обновить драйвер».

При отсутствии эффекта от отката/обновления стоит принудительно дезактивировать отключение модуля для экономии энергии. Такой режим часто устанавливается «по умолчанию» при инсталляции или обновлении операционной системы. В большинстве случаев он никак не влияет на стабильность сети, но нельзя исключать вероятность несовместимости с конкретной моделью адаптера.

Выполняется отключение также через «Диспетчер устройств», только во вкладке «Управление электропитанием». Там достаточно снять галочку с «Разрешить отключение этого устройства для экономии энергии» и перезагрузить компьютер. Изменения остальных настроек (вроде включения стандарта FIPS или ручного редактирования системного реестра) лучше избегать.

Контрольные вопросы

1. Перечислить необходимое оборудование для подключения сети?
2. Настройка интернет на Windows 7?
3. Настройка сети в Windows 10?

Практическая работа 14. Настройка FTP – сервиса

Цель работы: получение навыков практической работы с FTP-сервисом Internet, формирование умений создания простых HTML-документов

Ход работы

FTP-сервис разработан для того, чтобы позволить пользователю установить соединение с компьютером в Internet (работает по протоколу FTP- протокол передачи файлов (File Transfer Protocol)), просмотреть доступные на нем и скопировать на локальную машину или на сервер необходимые файлы.

Для работы с FTP-сервером требуется иметь специальное имя пользователя, зарегистрированное на сервере, и пароль для установления соединения. Однако существует весьма популярная разновидность этого сервиса, именуемая «анонимный FTP». Для работы с такими серверами в качестве имени используется anonymous, а в качестве пароля – любой выдуманный адрес электронной почты (пример: nnn@nnn.com).

WWW-страницы создаются с помощью специального языка HTML (HyperText Markup Language), являющегося по существу языком компоновки документов и спецификации гиперссылок. Средствами HTML задаются синтаксис и размещение специальных встроенных указаний (теги, заключенные в <> скобки), в соответствии с

которыми браузер отображает содержимое документа: текст, изображения и данные других типов, поддерживаемые данным браузером. Базовый синтаксис и семантика языка HTML определены в стандарте HTML, который можно найти по адресу http://www.w3.org, там же есть ссылки на переводы этих стандартов на различные языки http://www.w3.org/Consortium/Translation/ .

В Internet существует большое количество русскоязычных описаний языка HTML, учебников по разработке WWW-страниц, специализированных серверов для WEB-мастеров и т.д. Большая подборка соответствующих материалов находится на сервере www.webclub.ru .

Практические задания

Задание 1

1. Создать каталог (F7) на локальном диске в каталоге своей группы (\home\students\группа\имя), для локальной работы с сайтом.
2. Запустить редактор Amaya .
3. Создать главную страницу сервера (**index.htm** или index.html), на которой разместить информацию:

- Фамилия И.О. студента
- номер группы
- название и ссылка на страницу своей кафедры
- название и ссылка на страницу своего факультета
- название и ссылка на сервер своего ВУЗа
- ссылку на главную страницу курса "Интернет - технологии"

не забудьте выставить кодировку UTF-8!!!

4. Разместить на этой странице какую-нибудь картинку (для вставки изображения щелкните по кнопке Insert Image и укажите нужное).
5. Подключиться к FTP серверу ipm.kstu.ru (IP 83.149.236.170), используя Krusader (аналог Total Commander) под своим логином и паролем (инструменты=>сетевое соединение). **В целях безопасности не оставляйте свое имя и пароль постоянно прописанными в** Krusader**, а лучше его совсем не прописывать, а при каждом соединение вводить заново!!!**
6. Скопировать страницу на сервере (все содержимое локального каталога копируем на сервер) и просмотреть в браузере, проверить работоспособность всех ссылок и открывание всех картинок. Просмотреть можно по адресу **http://ipm.kstu.ru/students/группа/свой_логин/** . Если ссылка или картинка не открывается, щелкнуть правой кнопкой мыши по этому объекту, выбрать в появившемся меню свойства объекта, проверить появившийся URL на наличие ошибок и исправить.

Задание 2

1. Открыть в браузере перевод спецификации HTML 4.01, расположенный по адресу http://ipm.kstu.ru/internet/doc/.
2. Открыть первую страницу.
3. Выбрать режим работы с исходником страницы. В исходнике страницы укажите, в виде комментариев, для чего предназначена каждая группа тегов (каждый открывавший тег) и их свойства (атрибуты). **Пояснение:**

** - открывающий тег.**

** - закрывающий тег.**

Примеры:

**
**

<!-- Перевод строки -->

****

<!-- Шрифт, имеющий цвет=0000a0, размер=3 -->
****

К сдаче практической предоставляются: *работающая страница на сервере с комментариями каждого тега и его свойств* (атрибуты) *в исходнике.*

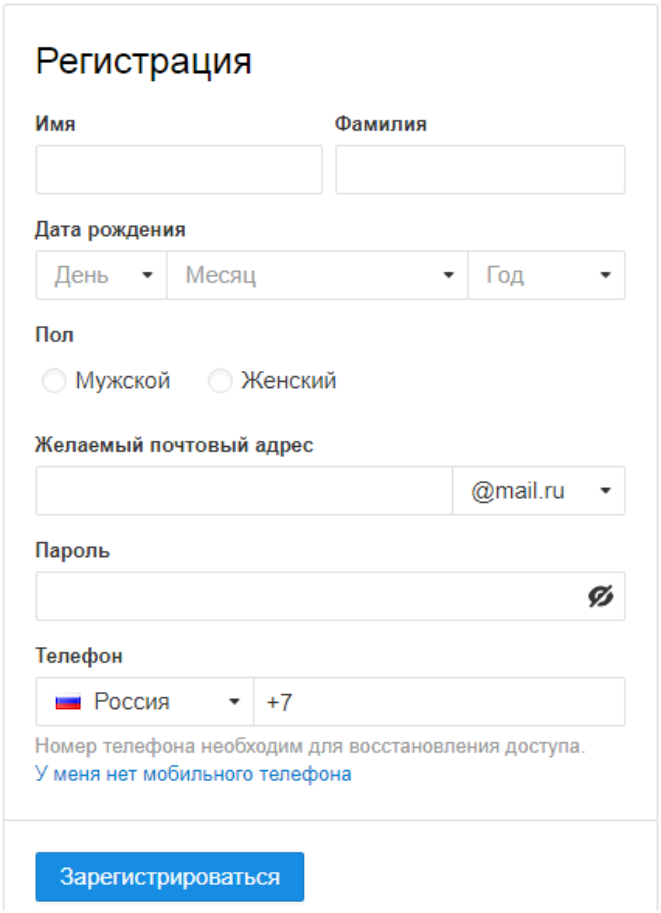
Практическая работа 15. Обмен сообщениями через сервисы Майл, ICQ, Skype.

Цель работы: научиться использовать технологию сбора, размещения, хранения, накопления, преобразования и передачи данных в профессионально ориентированных информационных системах;

Ход работы

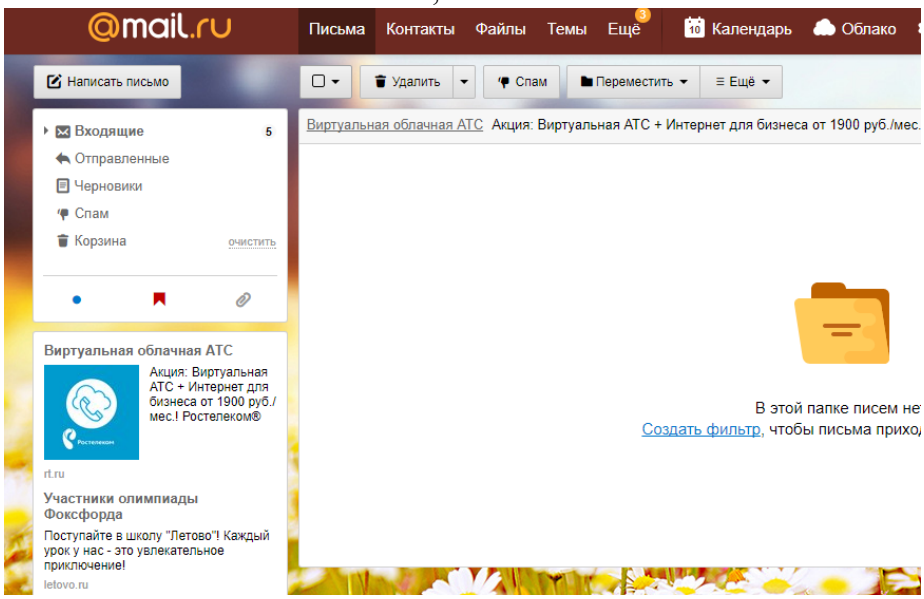
Задание № 1. Создание электронного ящика

1. Запустить браузер **Internet Explorer или Google Chrome** (или любой другой браузер).
2. В окне адресов ввести адрес почтового web-сервера **mail.ru**

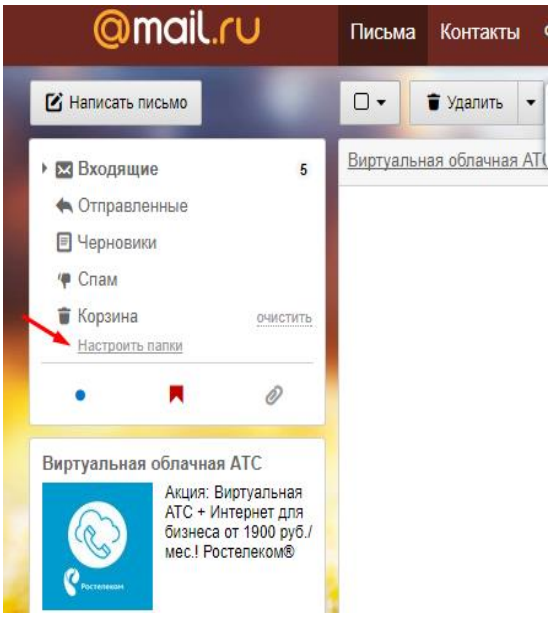


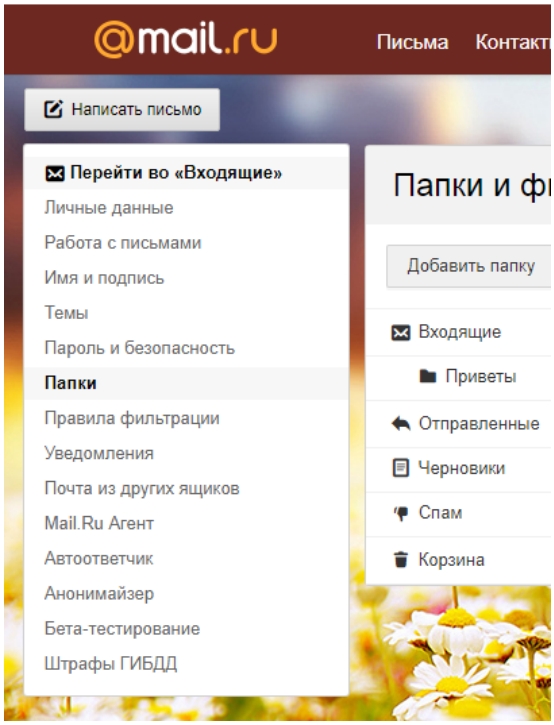
3. Произвести регистрацию:
   - Заполните анкетные данные (имя, фамилия, день рождения, пол).
   - В поле **желаемый почтовый адрес** придумайте запоминающийся вам имя электронного адреса.
   - Выберите и введите пароль.
   - Введите телефон
4. Нажать ссылку **Зарегистрировать почтовый ящик**

5. Войти в почтовый бокс, познакомиться с меню почтовой службы.

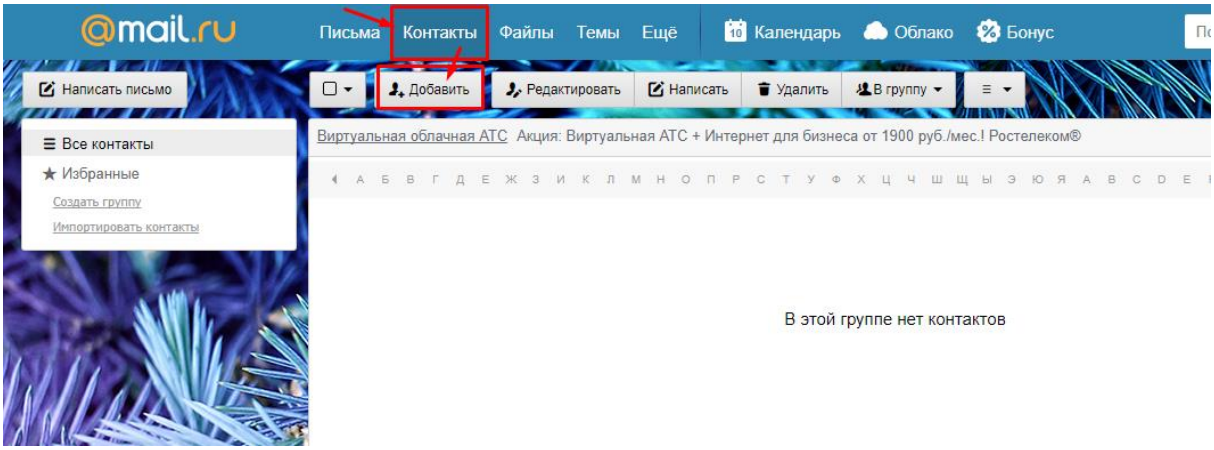


6. Настройте ваш почтовый ящик. Для этого нажмите **Настроить папки.**

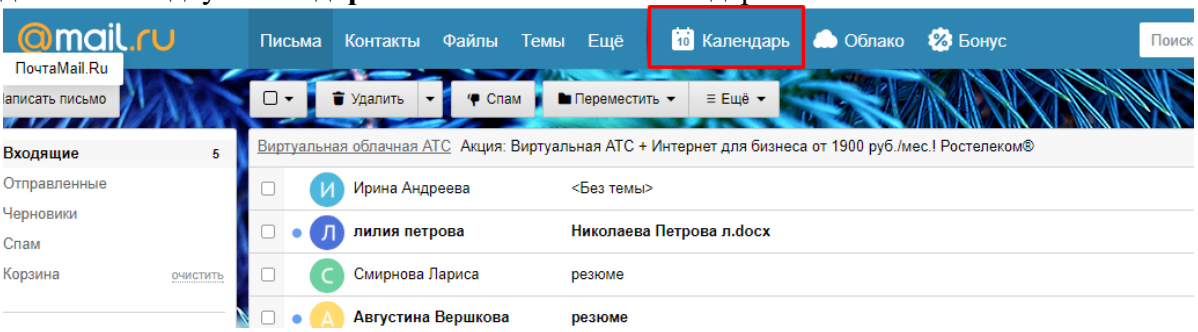




7. Добавьте папки **Важное**, **Друзья**, **Учёба**.
8. Измените фон, выбрав **Тему**
9. При необходимости измените данные в разделе **Личные данные**
10. Измените порядок получения писем и уведомлений в разделе **Работа с письмами**
11. Добавьте **Имя и подпись** для отправляющих писем. Чтобы составить правильно подпись к письму, ознакомьтесь с информацией в интернете: «Как правильно добавить имя и подпись к письму»
12. Добавьте **Контакты** (адрес электронной почты преподавателя), а так же адрес электронной почты соседа слева и справа).



13. Зайдите во вкладку **Календарь** и ознакомьтесь с его содержанием



Задание № 2. Создание и отправление электронного письма с прикрепленными файлами

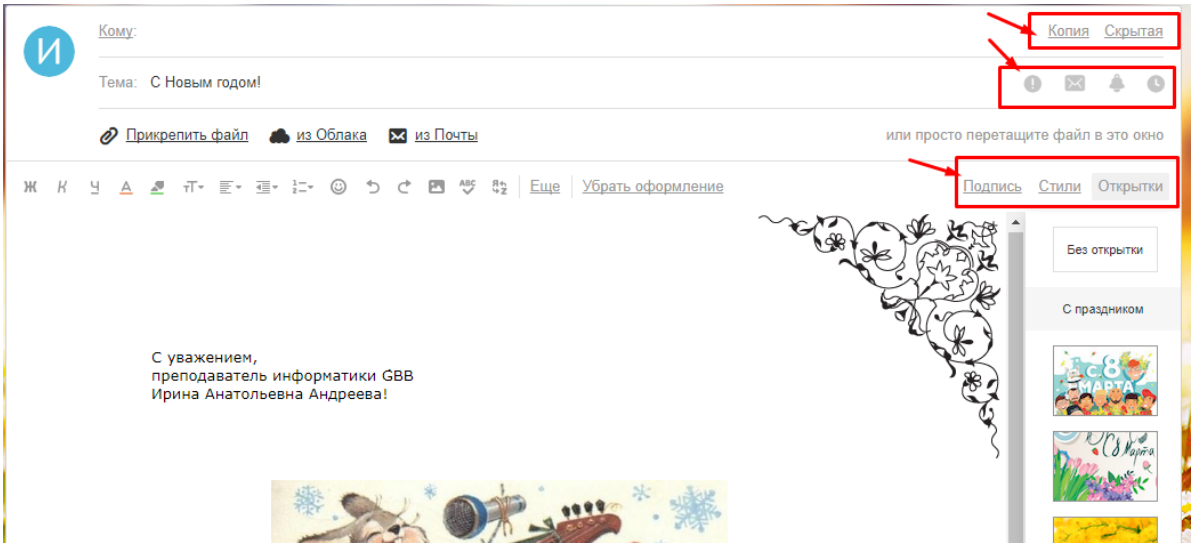
1. Напишите письмо преподавателю на электронный адрес.

с сообщением о том, что Вы поздравляете его с наступающим праздником:

- В окне своего почтового ящика вызовите команду **Написать письмо**.
- Введите адрес получателя электронного письма **(адрес почтового ящика преподавателя)**
- Заполните поле **Тема**, например: *№ Компьютера Поздравляем с Новым годом!!!*
- Напишите текст письма: «*Уважаемая, Ирина Анатольевна! _____ (фамилия, имя студента) поздравляет Вас с наступающим праздником!*».

Нажмите на флажки **копия** и укажите электронный адрес соседа справа, а где **скрытая –** электронный адрес соседа слева.

- Измените **подпись** (если нужно), **стиль** и добавьте **открытку** по соответствующей тематике отправляемого письма.



- Укажите, что письмо **важное** и отметьте, что оно **с уведомлением**
- Установить флажок **Сохранить копию письма в папке Отправленные**.
- Отправьте письмо.

2. Подготовьте и отправьте письмо-резюме с прикрепленным файлом-резюме на электронный адрес преподавателя. Полностью оформите электронное письмо (тема, прикреплённый файл с резюме, сопроводительное письмо) и отправьте его. Для правильного написания резюме найдите в интернете информацию и ответьте на вопросы:
    - Как правильно написать резюме?
    - Как правильно написать сопроводительным письмом к резюме?

Задание № 3. Проверка почты на наличие новых электронных писем

Порядок выполнения задания:

1. Проверить папку **Входящие** на наличие новых писем.
2. Составить отчет о полученных 5 последних письмах (оформите таблицу в MS Word):

Автор	Тема	Дата	Размер
Администрация Mail.Ru	Добро пожаловать на Mail.Ru	25 Февр	11Кб

3. Найдите ответы на вопросы и запишите в документ MS Word:
    - Преимущества и недостатки электронной почты по сравнению с обычной почтой?
    - Какие данные надо знать об адресате для того, чтобы отправить ему электронное письмо?
    - Укажите 3 основных правила телекоммуникационного этикета?
    - Какой электронный адрес президента РФ?
    - Какой электронный адрес президента ЧР?

- Какой электронный адрес ГАПОУ «ЧТТПиК»?

4. Полученный отредактированный документ MS Word отправьте на электронный адрес преподавателя с темой: *№ Компьютера Отчёт.*

Форум – это тематическое общение. В отличие от чата, на форуме обсуждают какую-то определенную тему. Можно сказать, что форум – это клуб по интересам. То есть форум – это такое место в Интернете, где собираются люди, которых объединяет одно увлечение или идея, и общаются на интересующую их тему. Они помогают друг другу советами и подсказками, обмениваются жизненным опытом, поддерживают друг друга.

Для того чтобы найти форум на интересующую тему, можно воспользоваться поисковой системой. Например, открыть сайт yandex.ru и напечатать в оранжевой строке поиска «форум интересующая тема». Например, «форум кошки».

Для общения в системе мгновенных сообщений ICQ каждому пользователю необходимо иметь специальный идентификационный номер, называемый ICQ UIN.

ICQ – служба передачи мгновенных сообщений в Интернете.

Регистрация в системе ICQ

1. Перейдите на страницу **http://www.icq.com/join/ru**
2. Перейдя на страницу регистрации ICQ, вы увидите стандартные поля, которые вы должны будете заполнить и после нажать кнопку Регистрация. Для успешной регистрации заполнять придётся все поля. Рекомендуем обращать внимание на всплывающие подсказки справа - они достаточно полезны при возникновении трудностей.
    - имя, Фамилия - до 20 символов в каждое поле;
    - адрес электронной почты может быть использован для входа в систему или восстановления забытого пароля;
    - Пароль - у большинства при регистрации возникают проблемы с его выбором. Происходит это из-за того, что сервис ICQ установил некие рамки для вводимого пароля - он не может быть короче 6 и длиннее 8 символов включительно. Он может состоять из заглавных и строчных латинских букв и цифр;
    - Дата рождения - эта информация необходима для большей безопасности вашего ICQ UIN, она будет доступна только вашим друзьям(изменить это правило можно в настройках приватности ICQ);
    - Пол;
    - Защита от роботов - 5-6 цифр, обычно раза с 2-3 получается распознать их.
    - Заполнив все поля, нажмите кнопку Регистрация.
3. Если все поля были заполнены верно, вы увидите страницу, на которой написано, что для завершения процесса регистрации номера аськи нужно нажать на ссылку в письме и чуть ниже кнопку для перехода в свой почтовый ящик - жмите её.
4. В своей почте во Входящих должно появиться новое письмо от ICQ Support, откройте его и нажмите ссылку в этом письме. Обычно оно приходит в течение 10 минут. Если письмо так и нет во Входящих, поищите его во вкладке Спам.
5. Итак, вы перешли по ссылке, подтвердив тем самым регистрацию, и теперь введите страницу, на которой вас информируют о том, что вы успешно зарегистрировались в ICQ.
6. Для того, чтобы узнать какой номер UIN вами зарегистрирован, нужно нажать Скачать в верхнем меню сайта и на открывшейся странице в правом верхнем углу вы увидите свою фамилию и имя. Кликнув по этой надписи и вы увидите, какой ICQ номер вы только что зарегистрировали.
7. После успешной регистрации, чтобы пользоваться новым ICQ номером, вам необходимо скачать бесплатную версию ICQ.

Skype – программное обеспечение с закрытым кодом, обеспечивающее шифрованную голосовую связь и видеосвязь через Интернет между компьютерами, а также платные услуги для звонков на мобильные и стационарные телефоны.

Программа также позволяет совершать конференц-звонки (до 25 голосовых абонентов, включая инициатора), видеозвонки (в том числе видеоконференции до 10 абонентов), а также обеспечивает передачу текстовых сообщений (чат) и передачу файлов. Есть возможность вместо изображения с веб-камеры передавать изображение с экрана монитора

Регистрация в скайп:

1. Для начала вам необходимо скачать программу Скайп. После того как программа загрузилась, нажмите на файл установки «SkypeSetup».
2. Далее после распаковки должно открыться окно, в котором надо выбрать русский язык и нажать на кнопку «Я согласен - установить».
3. Дожидаемся конца установки.
4. В открывшемся окне, предварительно проверив соединение с интернетом, нажмите на надпись «У вас нет логина?».
5. Далее появится окно, в котором и произойдет регистрация Скайп. Вам необходимо заполнить все поля (Имя, пароль, электронная почта, а также надо будет придумать уникальный логин) и нажать на кнопку «Я согласен (-на). Создать учетную запись».
6. В появившимся окне вводим свой логин и пароль, который указали при регистрации.

Настройка Скайпа - основные настройки Скайпа включают в себя настройку аудио параметров (микрофон и наушники) и видео (веб-камера). Обычно пользователям самостоятельно не приходиться в ручную настраивать Скайп, все необходимые настройки происходят автоматически. Но, не стандартный, старый и слабый микрофон или наушники могут потребовать вашего вмешательства.

Для начала попробуйте тестовый звонок, он совершенно бесплатен. Вам предложат прослушать сообщение, чтобы оценить качества звука через наушники или колонки, после этого Вам предложат оставить свое голосовое сообщение, которое Вы же потом и прослушаете. Это позволяет оценить качество работы вашего микрофона и качество передачи звука через интернет.

Если есть проблемы с качеством звука или качеством интернет соединения, то обычно Скайп сам вам об этом сообщит после тестового звонка и предложит пути решения проблемы.

Если все ж вас не устроило качество, то имеет смысл попытаться отключить автоматическую настройку микрофона и вручную установить уровень звука

Настройка камеры в Скайпе

Если камера уже работала до Скайпа, то проблем обычно не возникает, Скайп сам корректно найдет и настроит веб-камеру. Если веб-камера подключается впервые, то следует подключить камеру, а после установить драйвера с диска, который шел с камерой.

Задания

Задание 1. Найти с помощью одной из поисковых систем Интернета форумы по следующим темам:

- Компьютеры
- Информатика
- Информационные технологии в строительстве
- Железнодорожный транспорт
- Информационные технологии на железнодорожном транспорте

Зарегистрироваться на форуме. Предложить на форуме обсуждение интересующего вас вопроса по теме форума. Сохранить скрин окна форума в текстовом документе под именем ПР35-36_задание_1.doc.

Задание 2. Зарегистрироваться в системе ICQ, настроить систему, найти в системе троих одногруппников, передать им текстовые сообщения.

Задание 3. Создайте онлайн-анкету по следующим тематикам

- *Интернет-зависимость*
- *Жизнь современной молодежи*
- *Здоровый образ жизни*

Количество вопросов – 10,

Возможные сайты для создания онлайн-анкет

- http://webanketa.com/ru/
- http://www.survio.com/ru/
- https://anketolog.ru/

Практическая работа 16. Состав мероприятий по защите персональных данных

Цель работы: разработать политику безопасности для конкретного предприятия

Ход работы

Концепция ИБ в общих чертах определяет, что необходимо сделать для защиты информации. Политика ИБ детализирует положения Концепции, и говорит как, какими средствами и способами они должны быть реализованы. Концепция информационной безопасности используется для:

- принятия обоснованных управленческих решений по разработке мер защиты информации;
- выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
- координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;
- и, наконец, для формирования и реализации единой политики в области обеспечения информационной безопасности.

Политика безопасности трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. На практике политика безопасности трактуется несколько шире – как совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса. Результатом политики является высокоуровневый документ, представляющий систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Если предприятие не является изолированным, цели и задачи рассматриваются в более широком контексте: должны быть оговорены вопросы безопасного взаимного влияния локальных и удаленных подсистем.

Данный документ представляет методологическую основу практических мер (процедур) по реализации ОБИ и содержит следующие группы сведений.

1. Основные положения информационной безопасности.
2. Область применения.
3. Цели и задачи обеспечения информационной безопасности.
4. Распределение ролей и ответственности.
5. Общие обязанности.

Цели, задачи, критерии ОБИ вытекают из функционального назначения предприятия. Например, для режимных организаций на первое место ставится соблюдение

конфиденциальности. Для сервисных информационных служб реального времени важным является обеспечение доступности (оперативной готовности) подсистем. Для информационных хранилищ актуальным может быть обеспечение целостности данных и т. д. Здесь указываются законы и правила организации, которые следует учитывать при проведении работ по ОБИ.

Типовыми целями могут быть следующие:

- обеспечение уровня безопасности, соответствующего нормативным документам предприятия;
- следование экономической целесообразности в выборе защитных мер;
- обеспечение соответствующего уровня безопасности в конкретных функциональных областях АС;
- обеспечение подотчетности всех действий пользователей с информационными ресурсами и анализа регистрационной информации;
- выработка планов восстановления после критических ситуаций и обеспечения непрерывности работы АС и др.

В рассматриваемом документе могут быть конкретизированы некоторые стратегические принципы безопасности (вытекающие из целей и задач ОБИ). Таковыми являются стратегии действий в случае нарушения политики безопасности предприятия и сторонних организаций, взаимодействия с внешними организациями, правоохранительными органами, прессой и др. В качестве примера можно привести две стратегии ответных действий на нарушение безопасности:

- «выследить и осудить», когда злоумышленнику позволяют продолжить действия с целью его компрометации и наказания (данную стратегию одобряют правоохранительные органы!);
- «защититься и продолжить», когда организация опасается за уязвимость информационных ресурсов и оказывает максимальное противодействие нарушению.

Задание 1: Составить политику безопасности предприятия, придерживаясь вышеизложенного плана.

Задание 2. Разработать концепцию информационной безопасности компании по следующему примерному плану

1. Цели системы информационной безопасности
2. Задачи системы информационной безопасности.
3. Объекты информационной безопасности.
4. Вероятные нарушители.
5. Основные виды угроз информационной безопасности.
6. Классификация угроз.
    a. Основные непреднамеренные искусственные угрозы.
    b. Основные преднамеренные искусственные угрозы.
7. Мероприятия по обеспечению информационной безопасности.
8. Средства защиты от потенциальных угроз.
9. Разработайте вариант политики паролей
10. Предложите ПО для антивирусной защиты (проведя сравнительный анализ цен, возможностей и пр)

Контрольные вопросы

1. Что такое политика безопасности?
2. Перечислите цели и задачи политики безопасности на предприятии.
3. Дайте определение понятию объект и субъект политики безопасности.
4. Назовите основное назначение политики информационной безопасности.

Литература

1. Колдаев, В. Д. Архитектура ЭВМ : учебное пособие / В.Д. Колдаев, С.А. Лупин. — Москва : ФОРУМ : ИНФРА-М, 2021. — 383 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0868-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1136788
2. Кузин, А. В. Компьютерные сети : учебное пособие / А.В. Кузин, Д.А. Кузин. — 4-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2020. — 190 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-453-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1088380
3. Максимов, Н. В. Компьютерные сети : учебное пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2022. — 464 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-454-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1714105
4. Организация сетевого администрирования : учебник / А.И. Баранчиков, П.А. Баранчиков, А.Ю. Громов, О.А. Ломтева. — Москва : КУРС : ИНФРА-М, 2020. — 384 с. - ISBN 978-5-906818-34-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1069157