

2. Выполнение разделов проекта и составление пояснительной записи

Ниже приведены названия разделов пояснительной записи и примерное их содержание. Во многих разделах приведены примеры описаний и расчетов, относящиеся к этим частям проекта. Примеры в тексте выделены шрифтом.

2.1. Введение

Во введении пояснительной записи коротко освещается актуальность использования сетевых технологий на предприятиях и в организациях, формулируется цель работы и задачи, которые предстоит выполнить при достижении поставленной цели, приводится структура пояснительной записи с указанием содержания каждого раздела.

Примером формулировки цели и задач проекта может быть следующее. "Целью данной работы является разработка проекта локальной сети малой (средней или крупной) организации, обеспечивающей информационные услуги ее пользователям с требуемым уровнем безопасности.

В процессе достижения поставленной цели решались следующие задачи:

- определение месторасположения серверных и кроссовых помещений и количества местоположения телекоммуникационных розеток;
- разработка логической структуры сети;
- выбор активного телекоммуникационного оборудования;
- распределения сетевых адресов;
- разработка структурированной кабельной системы и выбор пассивного сетевого оборудования;
- разработка физической структуры сети и схемы электрических соединений;
- разработка политики безопасности, списков доступа к ресурсам сети и сценариев реализации политики безопасности;
- моделирование сети и коррекция схемы сети по результатам моделирования".

Этот пример вводной части является обобщенным. В каждом конкретном варианте проекта должна быть отражена его специфика, определяемая техническим заданием на разработку.

2.2. Постановка задачи

В этом разделе следует подробно описать структуру организации, для которой проектируется компьютерная сеть: количество рабочих комнат и рабочих мест в них, расположение помещений в здании (количество этажей, комнат на этажах), наличие и месторасположение технических помещений, которые могут быть использованы для размещения коммуникационного оборудования; перечислить основные приложения, с которыми работают сотрудники, используемые

операционные системы, необходимые сервисы Интернет, наличие собственных адресов Интернет, требования по доступу к информационным ресурсам предприятия.

В качестве исходного материала к этому разделу используются данных технического задания. При этом допускается введение проектировщиком по согласованию с руководителем дополнительных условий (изменение числа рабочих групп, расширение или изменение списка доступа пользователей к информационным ресурсам, количество и тип серверов, а также место их расположения, дополнительные условия фильтрации пакетов и т.п.).

Затем в постановке задачи подробное излагается, что конкретно необходимо спроектировать (с учетом варианта технического задания и введенных дополнительных требований, сформулированных в результате изучения особенностей предприятия).

В качестве примера ниже приведен фрагмент описания ситуации на предприятии.

"Организация располагается на одном (или нескольких, планируется расширение) этажах здания. Основные информационные технологии, используемые сотрудниками организации — обработка текстов в MS Word и таблиц в MS Excel (составление отчетов о проделанной работе), довольно частое общение с клиентами посредством электронной почты. Группа сотрудников в количестве N_1 человек работает с 1С бухгалтерией, еще одной небольшой группе сотрудников (указать количество) нужна правовая система "Консультант-плюс", одна основная группа N_2 сотрудников использует две узкоспециализированные расчетные подсистемы. Небольшая группа, состоящая из N_3 , сотрудников занимается скачиванием и рассылкой аудио- и видеофайлов в реальном времени.

Все сотрудники, в большей или меньшей степени используют Интернет. Т.е. всем им необходимо искать, просматривать и скачивать в Интернете какую-то информацию. Для этого на одном из компьютеров установлен ADSL-модем и работа с Интернет возможна только через этот компьютер. Интернетом пользуются не очень активно. Основная работа все-таки локальная.

На предприятии имеется:

- 46 сотрудников, но планируется расширение приблизительно до 100 сотрудников;
- 12 помещений, но предполагается еще один этаж и дополнительно 30 помещений;
- Программное обеспечение (которое используется в настоящее время):
 1. Бухгалтерия 1С (базы в dbf-формате).
 2. Правовая система Консультант плюс (сетевая версия).
 3. MS Word 200x.
 4. MS Excel.
 5. TheBat! (почтовая программа).
 6. Антивирус - Norton Antivirus.
 7. Первая специализированная расчётная система.
 8. Вторая специализированная расчётная система.
 9. Интернет браузеры - Opera, FireFox, IE.

10. Запись CD-дисков – Nero.
11. Мультимедиа - MS Windows Media, WinAmp.
12. MS Windows Server 2008 - сетевая 1С Бухгалтерия и архивы 2-го сервера.
 1. MS Windows Server 2008.
 2. MS Terminal Server 2008.
 3. 1С Бухгалтерия – лицензионная.
13. MS Windows Server 2008 - файловый сервер + Консультант плюс и архивы 1С бухгалтерии.
14. Консультант плюс. И т.д."

2.3. Определение количества и месторасположения кроссовых, серверных помещений и телекоммуникационных розеток сети

В этом разделе необходимо спланировать расположение кроссовых и серверных помещений, рассчитать количество рабочих групп и требуемое количество телекоммуникационных розеток проектируемой сети. Исходным материалом для выполнения этой работы является план размещения предприятия в здании (зданиях), количество и площадь занимаемых помещений. При расчете количества рабочих групп в данном проекте предполагается, что в комнате площадью до 40 м^2 располагаются сотрудники одной рабочей группы, а в помещении площадью свыше 40 м^2 — две. Если организация располагается в нескольких зданиях, то число рабочих групп принимается равным их количеству в здании центрального офиса.

Для того чтобы определить, сколько кроссовых должно быть в здании и где они должны располагаться, следует помнить, что максимальная длина горизонтального кабеля типа "витая пара" в локальной вычислительной сети не может превышать 90 метров.

Международный стандарт EIA/TIA-569 [EcoLAN] требует, чтобы для расположения серверов и коммутационного оборудования выделялось минимум одно специальное служебное помещение на этаж. Кроме того, он устанавливает необходимость наличия дополнительного помещения (распределительного пункта) для коммутационного оборудования на каждые 1000 квадратных метров, если обслуживаемая площадь этажа превышает 1000 квадратных метров или если протяженность горизонтальной кабельной системы больше 90 метров.

Если организация занимает не один этаж, а также если она располагается в нескольких зданиях, то выделяется специальное помещение для распределительного пункта здания, а этажные и распределительные пункты других зданий играют роль промежуточных распределительных пунктов. Распределительные пункт здания (РПЗ) и пункты этажей (РПЭ) соединяются между собой магистральной кабельной системой. При расположении организации в нескольких зданиях, в одном из них оборудуется распределительный пункт комплекса (РПК), который назначается главным коммутационным узлом сети предприятия.

Сети небольших зданий рекомендуется проектировать по принципу централизованной архитектуры. При этом если диаметр сети не превышает 200 метров, достаточно одного пункта коммутации, а все активное оборудование целесообразно размещать в одном месте. Важным преимуществом централизованной архитектуры является то, что она позволяет установить систему кондиционирования сетевого оборудования в единственном помещении. Это снижает расходы на эксплуатацию системы.

Такую же простейшую топологию целесообразно выбрать и в случае объединения в сеть ресурсов компаний, арендующей всего несколько комнат. Если пользователи находятся в удаленных помещениях или на разных этажах, то следует организовать два и более пунктов коммутации. В этом случае часть портов или панелей будет задействована для подключения магистралей, соединяющих распределительные пункты.

В случае, когда требуется просто объединить рабочие места в составе одной структурной единицы предприятия (отдела, службы и т.п.), используется простая рабочая группа компьютеров. Но если рабочей группе требуется повышенная информационная безопасность или нужно дисковое пространство, выделение которого на головном сервере предприятия представляется нецелесообразным, то в этом случае для рабочей группы следует устанавливать отдельный сервер, который выполняет также функции сервера приложений. Рабочая группа с собственным сервером является обособленной в составе сети предприятия и, как правило, выделяется в отдельный домен. Взаимоотношения с основным доменом устанавливаются исходя из целей и задач, решаемых рабочей группой.

В магистральной подсистеме целесообразно планировать не более двух уровней коммутации. Это позволит ограничить искажение сигналов в пассивном оборудовании и упростить администрирование. На пути от РП этажа до РП комплекса должен быть один распределительный пункт. Распределительные пункты магистральной кабельной системы могут располагаться в телекоммуникационных помещениях или аппаратных.

Используемые организацией серверы следует разделить на две отдельных группы: **сервер(ы) предприятия** (enterprise servers) и **серверы рабочих групп** (workgroup servers), а затем разместить их в сети согласно ожидаемому характеру потока данных пользователей и исполняемым функциям. Сервер предприятия поддерживает всех пользователей сети, предоставляя им различные службы, такие как электронная почта, служба доменных имен (DNS) и т.д. Сервер рабочей группы обслуживает определенную группу пользователей и предоставляет им такие службы, как обработка текстов или совместный доступ к файлам, то есть функции, которые могут понадобиться только некоторым группам пользователей.

Серверы предприятия целесообразно размещать на распределительном пункте комплекса — **главной распределительной станции**. В этом случае поток данных на серверы предприятия будет идти только к РПК, не проходя через остальные сети.

В идеальном случае серверы рабочих групп следует располагать на **промежуточных распределительных станциях** — РПЭ, по возможности ближе к

пользователям, использующим приложения этих серверов. Если серверы рабочих групп установить поближе к пользователям, то поток данных будет проходить по инфраструктуре сети прямо к РПЭ, не затрагивая других пользователей в этом сегменте.

При планировании расположения серверного оборудования следует учесть, что одним из случаев удобного и достаточно простого распределения серверов являются **серверы отделов**. Данные устройства могут быть непосредственно подключены к блоку распределения сети, которую они обслуживают. Как правило, такие серверы подключаются непосредственно к этажному коммутатору, который обслуживает данный отдел, либо подсоединяются к коммутаторам распределительного пункта здания. В таком случае также предоставляется возможность создания небольшой серверной группы (серверной фермы) в РПЗ каждого здания. Файловые серверы и серверы печати отделов могут подключаться там, где в централизованной серверной группе могут быть расположены серверы предприятия и высокопроизводительные устройства хранения и обработки данных.

В последнее время широко применяются централизованные **серверные группы** (фермы). *Группа серверов* обычно располагаются в аппаратном помещении с контролируемыми условиями эксплуатации, т. е. это помещение имеет специальное оборудование для фильтрации колебаний силового напряжения и поддержания температуры в заданном диапазоне. Создание группы серверов позволяет сэкономить средства, поскольку некоторое оборудование (например, фильтры питания, источники бесперебойного питания и устройства архивации) могут обслуживать целое помещение, и их не нужно покупать отдельно для каждого хоста и сервера. Кроме того, расположение серверной фермы в одной комнате облегчает защиту от несанкционированного доступа. Однако следует учитывать, что такие серверные группы могут создавать повышенную нагрузку на совместно используемую среду передачи данных, поскольку скорость обработки информации в них может быть чрезвычайно высокой. Поэтому каналы, связывающие серверы и сетевое оборудование, должны быть высокоскоростными, и их следует изолировать от тех сегментов, в которых располагаются рабочие станции. Наличие скоростных каналов обеспечит полосу пропускания, достаточную для всех пользователей, обращающихся к серверам. Изолируя серверы от других сегментов, можно также обеспечить избыточность сети тем самым повысить ее надежность.

Следует принять во внимание, что в некоторых случаях в крупных организациях окажется предпочтительнее размещать серверы так, чтобы они отражали структуру отделов или подразделений. При таком подходе серверами управляют администраторы, имеющиеся в каждом подразделении, благодаря чему эксплуатация ресурсов может учитывать специфику конкретного подразделения. Однако и в таком случае серверы желательно размещать в отдельных помещениях, в частности, в распределительных пунктах этажей.

Программные продукты общего пользования и базы данных целесообразно размещать на головном сервере предприятия. Такое решение позволяет упорядочить логическую структуру сети и упростить ее администрирование и поиск данных.

Управление типовой локальной вычислительной сетью осуществляется, как минимум, группой из трех серверов, включающей:

- **головной сервер** (Main), отвечающий за распределение ресурсов, хранение информации и политику безопасности, с подключенным к нему дисковым массивом;
- **резервный сервер** (Backup), который исполняет роль вторичного контроллера домена и отвечающий за резервное копирование информации;
- **Web-сервер**, на котором размещается Web-сайт предприятия;
- **Почтовый сервер** (Mail) и служба электронной почты.

Кроме того, в группу серверов входит рабочее место администратора сети. К служебным компьютерам относятся сервер доступа, обеспечивающий защиту локальной сети от несанкционированного доступа извне.

Количество пользователей сети предприятия определяется техническим заданием на разработку, а также желанием и возможностями заказчика. С учетом возможного роста сети целесообразно увеличить количество телекоммуникационных розеток не менее чем на 10%, относительно заданного числа пользователей. При отсутствии в техническом задании количества рабочих мест пользователей общее число рабочих мест, определяется из расчета 5 м² на одно место.

Среднее рабочее место рассчитывается следующим образом: 1 розетка телекоммуникационная, 1 розетка телефонная, 2 розетки электрические. На каждое помещение дополнительно предусматривается 4 электрические розетки (2 для бытовых нужд, 1 на кондиционер и 1 на факс) и одна телефонная для подключения факсимильного аппарата.

Распределение рабочих мест по этажам целесообразно представить в форме таблицы (например, таблица 2.1).

Таблица 2.1 – Распределение рабочих мест по этажам

Этаж	Наличное количество рабочих мест	Резерв на развитие	Общее количество телекоммуникационных розеток
1	30	3	33
2	28	3	31
3	47	5	52
Всего	105	11	116

Затем следует распределить телекоммуникационные розетки (разъемы) по помещениям и определить среднюю длину кабеля от розетки до кроссового оборудования. Следует иметь в виду, что высокая плотность установки телекоммуникационных разъемов повышает гибкость сети и облегчает изменения телекоммуникационных ресурсов рабочих мест. Допускается установка розеток одиночно или группами, однако каждое рабочее место должно иметь не менее двух разъемов. На каждом рабочем месте необходимо предусмотреть, по крайней мере, один разъем, терминированный симметричным кабелем с волновым сопротивлением 100 или

120 Ом (предпочтение отдается кабелям 100 Ом). Другие разъемы можно устанавливать на симметричном либо на оптоволоконном кабеле. Симметричный кабель должен иметь две или четыре пары проводников, причем все пары должны быть подсоединенены к контактам телекоммуникационной розетки.

В пояснительной записке следует обосновано и подробно описать план размещения оборудования. Пример фрагмента такого описания приведен ниже.

"Организация, занимающаяся предоставлением услуг предприятиям и населению, располагается в многоэтажном здании и занимает весь этаж (чертеж СевНТУ XXX). На данном этаже имеется 10 помещений, размеры которых указаны на чертеже. Общая протяженность коридора, согласно чертежу, равна 34 м. В центре здания имеется помещение №7 площадью 13 кв.м., которое может быть использовано для технических нужд сети в качестве аппаратной.

Выполним расчет площадей помещений, на основании которого определим количество телекоммуникационных розеток (ТР), подлежащих установке в каждой из комнат, а также число рабочих групп организации. Число компьютеров в рабочей группе не должно превышать 14-ти (из расчета 4 двоичных разряда на нумерацию компьютеров в группе). Расчетные данные сведем в таблицу 2.2.

Таблица 2.2- Площадь помещений и распределение ТР

№ комнаты	Площадь помещения, м ²	Количество ТР	Номера рабочих групп	Примечания
1	15,7	3	2	Зам. директора Гл. бухгалтер
2	46,8	9	3	
3	15,2	3	1	Администратор сети Программисты
4	38	8	4	
5	34	7	5	
6	56	11	6	
7	13	2	1	Аппаратная
8а	6	1	2	Секретарь
8б	9	2	2	Директор
9	32,5	6	5	
10	48,6	10	7	
Итого общее количество:		62	7 групп	

В результате анализа плана этажа и расчетных данных предлагается для размещения администратора сети и технического персонала выделить комнату №3, а помещение №7 использовать в качестве аппаратной, в которой будет установлено активное телекоммуникационное оборудование. В связи с тем, что организация занимает только один этаж, в аппаратной целесообразно установить оборудование

горизонтальной и вертикальной подсистем СКС, а также серверное оборудование рабочих групп и организации.

Для защиты распределительных панелей и активного коммуникационного оборудования от влаги и электромагнитного излучения, проникновения пыли и грязи, а также для ограничения несанкционированного доступа к этим устройствам, в комнате №7 должен быть установлен один 19-дюймовый телекоммуникационный шкаф напольного исполнения.

В этом же помещении монтируется распределительный щит силового питания компьютеров и другого офисного оборудования, находящегося в помещениях. Схема расположения телекоммуникационного шкафа и щита электропитания показана на чертеже размещения компонентов сети (чертеж СевНТУ 6.050101.12.01КП).

В телекоммуникационном шкафу монтируются коммутационные панели (патч-панели) для разделки горизонтальных кабелей, а также могут быть установлены оптические распределительные полки для подключения оптоволоконных кабелей подсистемы вертикальных магистралей. Кроме этого, в телекоммуникационный шкаф помещаются центральный и этажные коммутаторы, серверы приложений, а также источник бесперебойного питания.

2.4. Разработка логической структуры сети и планирование виртуальных сетей

2.4.1. Выбор и обоснование структуры сети

В данном разделе приводятся возможные различные варианты структур локальной сети предприятия, часть из которых рассмотрены в подразделе 2, анализируются их достоинства и недостатки и обосновывается логическая структура проектируемой компьютерной сети, удовлетворяющая поставленным требованиям, в частности, позволяющей масштабирование сети, обеспечивающей повышенную надежность. Здесь же должен быть представлен чертеж логической структуры и его подробное описание (состав и функционирование).

Составим схему сети предприятия для рассмотренного выше примера. В состав сети входит 62 рабочие станции, объединенные в 7 рабочих групп. Пусть сеть должна обеспечить выход в Интернет для внутренних пользователей сети в определенное время. Из внешней сети должен быть предоставлен доступ только к почтовому, FTP- и Web-серверу.

В связи с предъявленными требованиями, все серверы, связанные с Интернет, выносим в отдельную подсеть — демилитаризованную зону (DMZ). В локальной сети будут находиться файловый сервер, сервер печати, сервер авторизации, DHCP-сервер и DNS-сервер локальной сети, а также все рабочие станции. Так как количество рабочих станций достаточно велико, то на уровне доступа необходимо использовать несколько коммутаторов. Для реализации возможности обмена информацией между пользователями функциональных подразделений предприятия

коммутаторы уровня доступа должны соединяться через маршрутизатор или маршрутизирующий коммутатор (коммутатор третьего уровня).

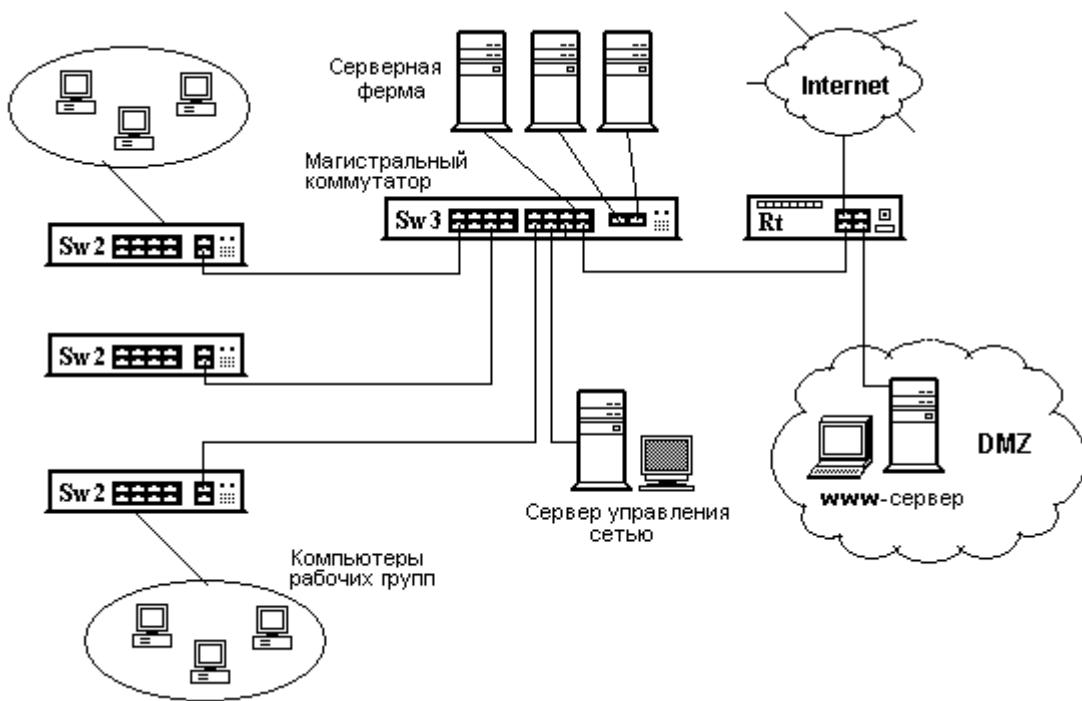


Рисунок 2.1 — Пример реализации логической структуры сети предприятия

Локальная сеть и демилитаризованная зона будут общаться между собой через маршрутизатор, который, собственно, и будет иметь выход в Интернет. На маршрутизаторе будет установлен соответствующий межсетевой защитный экран (файервол) и сервер преобразования адресов NAT, что позволит организации работать с сетью Интернет через один реальный адрес.

С учетом изложенного, структурная схема проектируемой сети имеет вид, изображенный на рисунке 2.1.

В качестве коммутаторов уровня доступа (SW 2) применяются три однотипных коммутатора, имеющие 24 порта FastEthernet. На уровне распределения установлен маршрутизирующий коммутатор третьего уровня (SW 3). Связь по выделенной телефонной линии обеспечивает DSL-модем со встроенным маршрутизатором, который, кроме функций маршрутизации, может выполнять роль защитного экрана и NAT-сервера.

2.4.2. Деление сети предприятия на независимые виртуальные сети

Для достижения максимальной производительности сети и повышения защищенности отдельных рабочих групп всю сеть целесообразно разделить на независимые логические сегменты. Одним из эффективных способов такого разделения является создание виртуальных логических сетей (VLAN).

В данном подразделе пояснительной записки нужно показать, каким образом рабочие станции (клиентские компьютеры) объединяются в виртуальные сети. При этом следует помнить, что в виртуальную сеть могут быть включены клиентские компьютеры, не зависимо от их пространственного положения, т.е., в виртуальную сеть могут входить компьютеры, расположенные не только в одной комнате, но и в различных комнатах одного или разных этажей. На практике вопросы включения компьютеров в ту или иную изолированную виртуальную сеть решаются на основе рекомендаций администрации или службы безопасности предприятия.

В настоящем учебном проекте для упрощения, предполагается, что количество и состав виртуальных сетей определяются рабочими группами пользователей. Таким образом, для рассматриваемого примера сети количество VLAN задаем равным 7. Номера виртуальных сетей в данном случае совпадают с номерами рабочих групп (таблица 2.2). В VLAN1 включим рабочие станции администратора сети, станцию, расположенную в аппаратном (серверном) помещении и компьютеры системных программистов. Во вторую виртуальную сеть VLAN2 включим компьютеры администрации предприятия: директора и его секретаря, заместителя директора и главного бухгалтера. В остальные виртуальные сети войдут компьютеры сотрудников соответствующих рабочих групп.

2.4.3. Обеспечение отказоустойчивости компьютерной сети

При разработке топологии сети необходимо учитывать наличие требований к отказоустойчивости сети, достигаемой способом резервирования, и допустимой величины отказоустойчивости (см. таблицу вариантов приложения А1). Под отказоустойчивостью сети понимается способность продолжения функционирования сети при выходе из строя телекоммуникационного оборудования или нарушениях (обрывах) линий связи. Существует две основные технологии обеспечения отказоустойчивости компьютерной сети: технология изменения топологии сети и технология «бесшовного» резервирования. Суть первой технологии заключается в изменении топологии сети в случае возникновения какой-либо неисправности в процессе функционирования сети. Изменение топологии занимает определенное время (от миллисекунд до секунд, в зависимости от протокола). Это время является основным параметром, характеризующим отказоустойчивость компьютерной сети и называется «временем восстановления». В течение этого времени связи с частью сети нет и, соответственно, данные теряются. По этой причине обеспечить время восстановления в сетях с перестройкой топологии меньше 1 мс не представляется возможным.

При «бесшовной» топологии отказоустойчивость обеспечивается не за счет перестройки топологии сети, а за счет резервирования оборудования и трактов передачи кадров. Подлежащий передаче от источника кадр дублируется отправителем, затем оба кадра передаются разными путями, а принимающий узел обрабатывает кадр, пришедший первым, и отбрасывает второй. Этот способ функционирования не требует выполнения перестройки топологии и, соответственно, данная

технология не требует осуществления определенных действий на стыках фрагментов сети, обеспечивая практически «бесшовность» сети.

В данном курсовом проекте (работе) предполагается обеспечение отказоустойчивости сети за счет введения резервирования. Резервирование в офисных компьютерных сетях — это процесс создания избыточных элементов в сети, от резервных каналов связи до дублирующих серверов и маршрутизаторов, служащий для повышения надёжности и непрерывности работы сети. Основная цель резервирования — обеспечить бесперебойное функционирование сети даже в случае отказа одного или нескольких компонентов. Отказоустойчивость компьютерной сети зависит от наличия резервирования соединений (линков) и телекоммуникационных устройств, а также от качества конфигурации (настройки параметров) оборудования.

При реализации мероприятий по осуществлению резервирования в сети следует учитывать, что каждый логический канал между активным сетевым оборудованием должен иметь как минимум два физические соединений, а каждый функциональный узел уровня ядра и распределения должен состоять из двух физических устройств (коммутаторов, маршрутизаторов или серверов). С целью повышения надежности функционирования сети при возникновении проблем у Интернет-провайдера следует применять подключение к двум провайдерам. Это возможно только при наличии не менее двух каналов с различными Интернет-провайдерами (см. таблицу вариантов приложения А1).

Для обеспечения доступа к серверному оборудованию в случае отказа коммутатора либо обрыва соединения необходимо обеспечить резервирование соединений серверов и коммутаторов за счет их дублирования. В штатном режиме связь с сервером осуществляется через основной коммутатор и одно звено связи. При отказе звена связи или основного коммутатора осуществляется переключение на резервный коммутатор. Топология отказоустойчивой компьютерной сети организации изображена на рисунке 2.2.

Однако наличие параллельных трактов передачи пакетов, характерных при введении резервирования, может привести к появлению петель связи и возникновению зацикливания пакетов, так называемый «широковещательный шторм», что в свою очередь приведет к перегрузке сети и нарушении связи. Для исключения петель связи в сетях с резервированием разработаны специальные протоколы резервирования, задачей которых является мониторинг дублированных каналов связи с целью недопущения зацикливания пакетов и перераспределение трафика в аварийных ситуациях. Протокол резервирования должен гарантировать логическое существование только одного пути доставки сообщения в конкретный момент времени при физическом наличии нескольких. Из существующих физических каналов связи один выбирается основным, остальные находятся в резерве.

Такой принцип был впервые применён в протоколе STP (*Spanning Tree Protocol*), регламентируемый стандартом IEEE 802.1d, согласно предписаниям которого отслеживается состояние каналов связи и при обнаружении обрывов трафик переключается с отказавшего канала на резервный. Во время обнаружения обрыва, определения резервного пути, и переключения портов связь теряется. В

зависимости от размеров сети и сложности её топологии время восстановления связи может занимать от сотен миллисекунд до десятков секунд.



Рисунок 2.2 – Топология отказоустойчивой компьютерной сети

В протоколе связующего дерева STP затраты времени на изменение топологии сети занимает не менее 50 секунд, что не всегда удовлетворяет требованиям к времени восстановления сети. Поэтому для снижения времени восстановления был разработан стандарт IEEE 802.1w – протокол *Rapid Spanning Tree Protocol (RSTP)*. Его целью, кроме повышения быстродействия было преодоления отдельных ограничений STP, которые мешали внедрению ряда новых функций коммутаторов, в частности, функций 3-го уровня, всё больше и больше применяемых в коммутаторах Ethernet. RSTP обеспечивает более быструю сходимость (конвергенцию) за счет введения новых ролей и состояний портов, что сокращает время конвергенции с нескольких секунд до 5-10 миллисекунд. RSTP также поддерживает такие функции, как корректировка стоимости портов, определение типа канала и механизм предложения/согласия для более быстрой конвергенции.

В связи с этим, при допустимом времени восстановления сети >50 с следует использовать протокол STP, а при допустимом времени восстановления менее 50 с необходимо активировать на коммутаторах протокол RSTP.

2.5. Выбор активного телекоммуникационного оборудования

В этом подразделе следует привести соображения, на основании которых было выбрано активное телекоммуникационное оборудование. При обосновании необходимо, кроме технических характеристик, учитывать надежность и стоимость оборудования, пожелания и финансовые возможности Заказчика.

В настоящем проекте рекомендуется в качестве активного оборудования выбирать устройства (коммутаторы и маршрутизаторы) корпорации Cisco. При выборе оборудования следует обращать внимание на новые и перспективные изделия. Следует избегать использования устройств, производство которых уже прекращено или выпуск которых прекращается в ближайшее время. Информацию о таком оборудовании можно получить на официальных сайтах производителей или дистрибуторов. В данном пособии в примерах зачастую используется устаревшее оборудование, снятое с производства. Это сделано преднамеренно для исключения копирования студентами рассмотренных примеров. Студенты же должны использовать модели, выпускаемые взамен устаревших или включать в состав проектируемой сети современные аналоги рассмотренного оборудования.

После обоснования выбора нужно привести все технические и эксплуатационные параметры выбранных устройств. Пример обоснования и выбора активного сетевого оборудования приведен ниже.

"В локальных компьютерных сетях на уровне доступа пользователей к сети целесообразно использовать коммутаторы фирмы Cisco типа Catalyst 29xx. Коммутаторы этой серии представляют собой полнофункциональную линию коммутаторов 10/100 Ethernet с автоматическим выбором скорости передачи и с поддержкой технологии создания виртуальных сетей. Устройства этой серии обеспечивают наилучшее соотношение цена/производительность среди устройств данного класса. Коммутаторы Catalyst 29XX имеют очень высокую производительность, простоту в эксплуатации и гибкость в использовании. Эти устройства могут применяться как для создания высокопродуктивных рабочих групп, так и для объединения групп серверов и коммутаторов предыдущего уровня, например, Catalyst 1900/2820. Коммутаторы серии Catalyst 29XX поставляются с пожизненной гарантией, которая предусматривает бесплатный заводской ремонт оборудования в течение всего времени поддержки устройства.

Для проектируемой компьютерной сети для обеспечения подключения на уровне доступа 62-х рабочих станций целесообразно использовать сетевые коммутаторы настольного типа Cisco Catalyst 2950-24. Коммутатор Catalyst 2950C-24 – это 25-х портовый коммутатор уровня доступа, предназначенный для построения малых и средних локальных сетей. Устройство рассчитано на круглосуточную работу и характеризуется высокой производительностью и широкими функциональными возможностями.

Коммутатор автоматически определяет скорость передачи на каждом порту (10/100 Мбит/с), поддерживает протокол качества обслуживания (QoS), предоставляет возможность управления группой коммутаторов и допускает соединения

коммутаторов в стек. Основные технические параметры коммутатора типа Catalyst 2950 приведены в таблице 2.3.

Таблица 2.3 — Технические характеристики коммутатора доступа

Параметр	Значение
Тип сети	Fast Ethernet Ethernet
Количество базовых портов	24 (24 макс.)
Буфер памяти (на один порт)	8 МБ
Скорость передачи по UPLINK	100 Мбит/с
Индикаторы	- активное соединение - полнодуплекс / полуудуплекс - состояние соединения - уровень загрузки - электропитание
Поддерживаемые стандарты	- IEEE 802.3 (Ethernet) - IEEE 802.3u (Fast Ethernet)
Размер таблицы MAC адресов (L2)	8192
Методы коммутации	store-and-forward
Протоколы удаленного управления	- SNMP - Telnet - Console
Пропускная способность	6,8 Гбит/с
Среда передачи	Ethernet 10/100BaseT - категория 5 НВП - скорость передачи до 100 Мбит/с - длина сегмента до 100 м Ethernet 100baseFX - MMF 62,5 микрон - скорость передачи до 100 Мбит/с - длина сегмента до 2 км
Интерфейсы	24 × Ethernet 10/100BaseT • RJ-45 (half / full duplex mode) 2 × Ethernet 100baseFX • MT-RJ (half / full duplex mode)
Электропитание	встроенный блок питания - 200 ...240 В (переменный ток) - потребляемая мощность 30 Вт
Габариты (Высота × Ширина × Глубина), Вес	44,5 × 4,36 × 24,18 мм, 3 кг

В качестве магистрального коммутатора в проектируемой сети целесообразно использовать коммутаторы третьего уровня типа Cisco Catalyst 3500. В состав семейства коммутаторов Catalyst 3500XL входит три модели:

1) WS-C3512-XL — содержит 12 универсальных портов 10/100 Mbps Ethernet с автоматическим определением скорости и режима передачи, а также два порта Gigabit Ethernet;

2) WS-C3524-XL — содержит 24 универсальных порта 10/100 Mbps Ethernet с автоматическим определением скорости и режима передачи, а также два порта Gigabit Ethernet;

3) WS-C3508G-XL — содержит 8 портов Gigabit Ethernet. Коммутаторы семейств 2900XL, 3500XL могут объединяться в стеки (до 16 устройств) при помощи соединений Fast Ethernet, Fast EtherChannel (агрегирование Fast Ethernet по 2 или 4 канала), а также Gigabit Ethernet и Gigabit EtherChannel. Максимальное количество портов, которое может быть установлено в одном стеке равно 380. Такой стек является единым объектом сетевого управления, которое может выполняться как при помощи командного языка CLI с консоли или при помощи протокола telnet, так и при помощи специализированных систем управления типа CWSI (Cisco Works for Switched Internetworks), так и при помощи WEB-технологии с любой рабочей станции, оснащенной программами просмотра Netscape или Internet Explorer.

Для проектируемой сети, с учетом возможных расширений, достаточно установить 12-портовый маршрутизирующий коммутатор типа WS-C3512-XL. Технические характеристики этого коммутатора приведены в таблице 2.4.

Таблица 2.4 — Технические характеристики коммутатора Catalyst WS-C3512-XL

Параметр	Значение
Тип сети	Fast Ethernet Ethernet
Количество базовых портов	24 (24 макс.)
Производительность	10 Гбит/с
Пропускная способность	7,5 миллионов (64-х байтовых) пакетов в с
Буфер памяти (на один порт)	8 МБ
Скорость передачи по UPLINK	100 Мбит/с
Поддерживаемые стандарты	- IEEE 802.3 (Ethernet) - IEEE 802.3u (Fast Ethernet)
Размер таблицы MAC адресов (L2)	8192
Поддерживаемые стандарты	1) IEEE 802.3x full duplex; 2) IEEE 802.1D Spanning-Tree Protocol; 3) IEEE 802.1Q VLAN; 4) IEEE 802.3z, IEEE 802.3x;

	5) IEEE 802.3u 100BaseTX and 100BaseFX specification; 6) IEEE 802.3 10BaseT specification; 7) IEEE 802.3z, IEEE 802.3x 1000BaseX specification; 8) 1000BaseX (GBIC) — 1000BaseSX, 1000BaseLX/LH, 1000BaseZX.
--	---

2.6. Назначение сетевых адресов коммуникационному оборудованию и подсетям

В данном подразделе необходимо назначить проектируемой сети внешний IP-адрес и сетевую маску, а также присвоить адреса и сетевые маски всем виртуальным сетям и рабочим станциям. Ниже приведен пример назначения и распределения сетевых адресов в проектируемой сети.

"Внешний IP-адрес и сетевая маска выделяется провайдером Интернет-услуг по запросу предприятия. Пусть согласно варианту предприятию выделен в постоянное пользование один бесклассовый адрес 83.221.169.36/30.

Известно, что для внутреннего использования в локальных сетях рекомендованы следующие частные адреса (таблица 2.5).

Таблица 2.5 — Диапазоны частных адресов

Класс	Начальный адрес	Конечный адрес	Число сетей
A	10.0.0.1	10.255.255.255	1
B	172.16.0.0.	172.31.255.255	16
C	192.168.0.0.	192.168.255.25	255

Если предприятие располагается в нескольких многоэтажных зданиях, то для удобства администрирования в качестве адреса сети целесообразно выбрать адрес 10.Z.Y.X с сетевым префиксом длиной 24 бита (рисунок 2.). Десятичное значение символа Z отображает номер здания; Y — рабочей группы, а X — номер компьютера в группе. Таким образом, в рабочую группу можно объединить до 254-х компьютеров. Диапазон адресов компьютеров предприятия для рассмотренного выше примера (12 рабочих групп) представлен в таблице 2.6.

Адреса с нулевой группой целесообразно использовать для присвоения адресов портов маршрутизаторам и портам управления коммутаторов. Таким образом, адреса для коммуникационного оборудования находятся в следующих диапазонах: 10.1.0.1 — 10.1.0.254.

Таблица 2.6 — Диапазон сетевых адресов проектируемой сети

Начальный адрес	10.	1.	0.	1
	00001010	00000001	00000000	00000001
Конечный адрес	10.	1.	254.	254
	00001010	00000001	00000001	11111110

Для портов маршрутизатора выделено два частных адреса. Адрес 10.1.0.1 присвоим порту, соединенному с локальной сетью организации, а адрес 10.1.0.2 — порту, подключенному к серверу демилитаризованной зоны. Интернет-адрес 83.221.169.36 сети предприятия выделен провайдером. В связи с тем, что в соответствии с ТЗ предприятию выделен только один внешний адрес, то для обеспечения выхода пользователей сети в Интернет необходимо использовать процедуру трансляции адресов.

Далее необходимо привести таблицу с адресами всех компьютеров, расположенных в помещениях организации, для которой проектируется сеть. В этой таблице целесообразно указать номера коммутаторов/маршрутизаторов и номера портов, к которым подключаются клиентские компьютеры и серверы. Фрагмент таблицы адресов с номерами портов для рассматриваемого примера представлен в таблице 2.7.

Таблица 2.7 – Распределение адресов

№№ ком- нат	Номер/название рабочей группы	Номер ТР (компью- тера)	Адрес	Устройство / порт	Примечание
3	1/Инф.поддержки	31	10.1.1.1	Sw1-Fa0/2	Админ. сети
3	1	32	10.1.1.2	Sw1-Fa0/3	
3	1	33	10.1.1.3	Sw1-Fa0/4	
7	1	71	10.1.1.4	Sw1-Fa0/5	
7	1	72	10.1.1.5	Sw1-Fa0/6	
1	2/Дирекция	11	10.1.2.1	Sw1-Fa0/7	
1	2	12	10.1.2.2	Sw1-Fa0/8	
1	2	11	10.1.2.3	Sw1-Fa0/9	
8а	2	81	10.1.2.4	Sw1-Fa0/11	Секретарь
8б	2	82	10.1.2.5	Sw1-Fa0/10	Директор
8б	2	83	10.1.2.6	Sw1-Fa0/11	
3	3/Финансовая	31	10.1.3.1	Sw2-Fa0/2	
3	3	32	10.1.3.2	Sw2-Fa0/3	
3	3	33	10.1.3.3	Sw2-Fa0/4	
3	3	34	10.1.3.4	Sw2-Fa0/5	
3	3	35	10.1.3.5	Sw2-Fa0/6	
3	3	36	10.1.3.6	Sw2-Fa0/7	
3	3	37	10.1.3.7	Sw2-Fa0/8	
3	3	38	10.1.3.8	Sw1-Fa0/9	
3	3	39	10.1.3.9	Sw1-Fa0/11	

:	:	:	:		:
7	Сервер внутр.		10.1.1.30		LAN
	:	:	:		
	Сервер внутр.		10.1.7.30		
7	Сервер внеш.		10.1.0.2		DMZ
7	Маршрут-р		83.221.169.36	S1	ISP
7	Коммутатор1		10.1.0.3		
7	Коммутатор2		10.1.0.4		
7	Коммутатор3		10.1.0.5		
7	Коммутатор4				
10	7/Маркетинг	101	10.1.7.1	Sw3-Fa0/2	
10	7	102	10.1.7.2	Sw3-Fa0/3	
:	:	:	:		:
10	7	110	10.1.7.10	Sw3-Fa0/11	

При этом следует помнить, что необходимо зарезервировать адреса для портов маршрутизатора(ов) и портов управления коммутаторов.

2.7. Разработка физической структуры сети

В этом разделе пояснительной записки проекта осуществляется разработка схемы размещения компонентов структурированной кабельной системы (СКС) сети, построение кабельных трасс, а также проводится обоснование и выбор типов кабелей для горизонтальной и вертикальной систем СКС. При этом учитываются требования и нормы международных и национальных стандартов []. Расчет кабельной системы можно выполнять вручную или использовать автоматизированную систему (рекомендуется). В настоящее время практически все локальные сети проектируются на базе медных витых пар и волоконно-оптических кабелей. Поэтому в приведенных примерах обоснования и расчета СКС рассматриваются именно эти типы кабелей.

2.7.1. Выбор типов кабелей

Обоснование и выбор типов кабелей для проектируемой компьютерной сети осуществляется на основе рекомендаций, изложенных в [14]. Схема кабельной подсистемы в целом для любой из подсистем СКС определяется типом сети и выбранной топологией.

Наиболее «подвижной» частью любой локальной сети является горизонтальная подсистема. На этом уровне добавление новых пользователей, перемещение рабочих групп происходят гораздо чаще, чем изменения в вертикальных подсистемах между этажами. Поэтому наиболее рациональным вариантом является применение медных неэкранированного кабеля UTP, так как стоимость установки оптоволокна достаточно велика (в нее входят стоимость сетевых адаптеров и сравнительно высокие затраты на монтажные работы). Оптоволоконный кабель используют в основном в подсистемах кампусов и вертикальных. Однако следует иметь в виду, что хотя по мере развития технологий цены на кабели категорий 6 и 7 снижаются, однако параллельно дешевеют и оптоволоконные системы и оптоволоконные кабели становятся все более конкурентоспособными по отношению к медным кабелям даже на уровне подключения рабочих станций к сети.

Медные кабели для СКС характеризуются рядом параметров, в частности:

- волновое сопротивление (Impedance);
- затухание (Attenuation);
- переходная помеха на ближнем конце NEXT (Near End Cross Talk);
- переходная помеха на дальнем конце FEXT (Far End Cross Talk);
- нормированное (приведенное к уровню полезного сигнала) значение FEXT - ELFEXT;
- характеристики взаимных помех между парами PowerSum FEXT, PowerSum ELFEXT и PowerSum NEXT;
- защищенность от переходных помех ACR (Attenuation to crosstalk Ratio);
- задержка распространения сигнала (Propagation Delay);
- неравномерность задержки распространения сигнала (Delay Skew).

В данном подразделе следует в краткой форме (целесообразно в виде таблиц) представить данные об электрических и стоимостных характеристиках современных медных кабелей 5 – 7 категорий и оптоволоконных одномодовых и многомодовых кабелей и обосновать выбор того или иного типа кабеля. При защите проекта студент должно хорошо представлять физическую суть этих параметров и уметь пояснить влияние их на информационные характеристики компьютерной сети.

Например, в данный подраздел можно включить следующее обоснование. "С учетом того, что на уровне доступа передача данных выполняется преимущественно со скоростью 100 Мбит/с и с учетом возможности в перспективе увеличения скорости передачи для горизонтальной подсистемы, выбираем кабель типа UTP4-C6-SOLID-GY. Это кабель 6-й категории типа неэкранированная витая пара (UTP), состоящий из 4 пар одножильных (solid) медных проводников. Кабель соответствует стандарту пожарной безопасности UL 444 и UL 1581 и имеет следующие технические характеристики:

- диаметр проводника: $0,54 \pm 0,01$ мм (24 AWG);
- изоляция — полиэтилен повышенной плотности, минимальная толщина 0,18 мм;
- диаметр провода в изоляции $0,99 \pm 0,02$ мм;
- цвет витых пар: синий-белый/синий, оранжевый-белый/оранжевый, зеленый-белый/зеленый, коричневый-белый/коричневый;
- 4 витые пары с полиэтиленовым разделителем, покрыты поливинилхлоридной оболочкой (PVC) с минимальной толщиной оболочки 0,4 мм;
- внешний диаметр кабеля равен $6,2 \pm 0,2$ мм;
- рабочая температура кабеля от -20°C до $+75^{\circ}\text{C}$;
- радиус изгиба кабеля: $8 \times \varnothing$ во время инсталляции, $6 \times \varnothing$ при вертикальном кабелировании и 4 диаметра при горизонтальном кабелировании;
- стандартная упаковка размером $21,5 \times 42 \times 42$ см ($\text{Ш} \times \text{В} \times \text{Г}$) — 305 м;
- вес кабеля без упаковки 12.9 кг.

Кабель характеризуется следующими электрическими параметрами:

- максимальное сопротивление проводника при температуре 20°C равно 9,38 Ом/100 м;
- дисбаланс сопротивления не превышает 5%;
- емкостной дисбаланс пары по отношению к земле равен 330 пФ/100 м;
- сопротивление на частоте от 0,772 до 100 МГц составляет 85...115 Ом;
- максимальная рабочая емкость равна 5,6 нФ/м;
- неравномерность задержки 45 нс/100 м;
- задержка распространения <536 нс/100 м.

Частотные характеристики кабеля приведены в таблице 2.8.

Таблица 2.8 — Частотно-зависимые характеристики передачи

Частота МГц	Затухание дБ/100 м	NEXT дБ	ACR дБ/100м	PS NEXT дБ	EL-FEXT дБ/100м	PS EL- FEXT дБ/100м	RL дБ
31,25	11,4	45,9	34,6	42,9	33,9	30,9	23,6
62,5	16,5	41,4	25,8	38,4	27,8	24,8	21,5
100	21,3	38,3	19,0	35,3	23,8	20,8	20,1
155	27,2	35,5	10,8	32,5	19,9	16,9	18,7

Параметры передачи многомодового оптоволоконного кабеля приведены в таблице 2.9, а параметры одномодового — в таблице 2.10

Таблица 2.9 — Оптические параметры многомодового оптоволокна

Тип волокна	Длина волны, нм	Затухание (среднее/ максималь- ное), дБ/км	Коэффициент широко- полосности, МГц·км	Дальность передачи для Ethernet, м		Коэффициент преломления
				1GbE	10 GbE	
62,5/125 OM1	850	3,0/3,2	>200	275	33	1,495
	1300	0,7/0,9	>600	550	—	1,490
50/125 OM2	850	2,6/2,8	>600	550	82	1,481
	1300	0,6/0,9	>1200	550	—	1,476

Таблица 2.10 — Оптические параметры одномодового оптоволокна
ITU-G.652B

Тип волокна	Диаметр, мкм	Длина волны, нм	Затухание (среднее/макси- мальное), дБ/км	Дисперсия, пс/(нм·км)	PMD, пс/км ^{1/2}	Коэфф. прелом- ления
9/125	9,2±0,4	1310	0,35/0,5	< 3,5	—	1,467
	125±0,5	1550	0,21/0,3	< 18	< 0,2	1,467

Параметр PMD (Поляризационная модовая дисперсия) — это дисперсия, вызываемая небольшой асимметричностью поперечного сечения волокна. Асимметричность приводит к тому, что одна из двух основных ортогональных поляризованных мод передается по оптическому каналу связи быстрее, чем другая. В связи с тем, что приемное устройство принимает комбинацию этих двух мод, то результирующий импульс становится шире входного импульса, поскольку он подвергся дисперсии, т. е. происходит расширение импульса.

Для выполнения силовой проводки используем трехжильный медный кабель типа ВВГ 3×1,5 (Виниловая оболочка, Виниловая изоляция, Гибкий). Сечение

кабеля 1,5 мм² выбирается из расчета максимального потребляемого тока 15 А (мощность 3,3 кВт) на одну розетку".

2.7.2. Схема размещения компонентов СКС

В этом подразделе приводится обоснование и описывается схема размещения пассивного и активного телекоммуникационного оборудования проектируемой сети на территории, на которой располагается предприятие. Собственно схема размещения выполняется на чертеже формата А1 в соответствии с требуемыми стандартами и нормативами [28,29]. Фрагменты схемы размещения показаны на рисунках 2.2 и 2.3.

Пример обоснования и описания может иметь следующий вид.

"Схема размещения компонентов сети разрабатывается на основе поэтажных чертежей здания, в котором располагается предприятие или организация. Во всех помещениях на каждом рабочем месте устанавливаются телекоммуникационные розетки (TP) с двумя гнездами типа RJ-45 и по три силовых розетки с напряжением 220 В. Количество TP, рассчитанное на основании соответствующих технических норм, приведено в таблице 2. Телекоммуникационные розетки закрепляются в кабельных коробах на высоте 80 см от уровня пола. Расположение телекоммуникационных и электрических розеток и других компонентов сети в каждом из помещений предприятия с указанием установочных размеров показано на чертеже СевГУ 09.03.02.01.12

Фрагмент схемы размещения компонентов СКС с указанием типов и параметров кабелей в помещении, в котором располагается рабочая группа организации, показан на рисунке 2.3. Все телекоммуникационные кабели прокладываются в декоративных пластмассовых кабельных каналах (коробах), которые закрепляются на стене помещения. Кабельный канал разделен на две секции. Одна служит для укладки телекоммуникационных кабелей, а вторая — для силовых кабелей. Телекоммуникационные розетки монтируются на корпусе короба, либо на стене. Силовые розетки в количестве 3 шт на каждое рабочее место закрепляются на расстоянии 0,8 м от уровня пола. На такой же высоте устанавливаются и телекоммуникационные розетки.

Выход пучка кабелей горизонтальной подсистемы осуществляется через металлический патрубок (конduit) диаметром 80 мм, который пропускается через стену помещения на расстоянии 0,2 м от потолка. В коридоре коммуникационные кабели укладываются в кабельный лоток, который закреплен между потолочным перекрытием и подвесным потолком.

Силовые кабели выводятся через отдельный собственный conduit и укладываются в межпотолочном пространстве в лоток силовых кабелей.

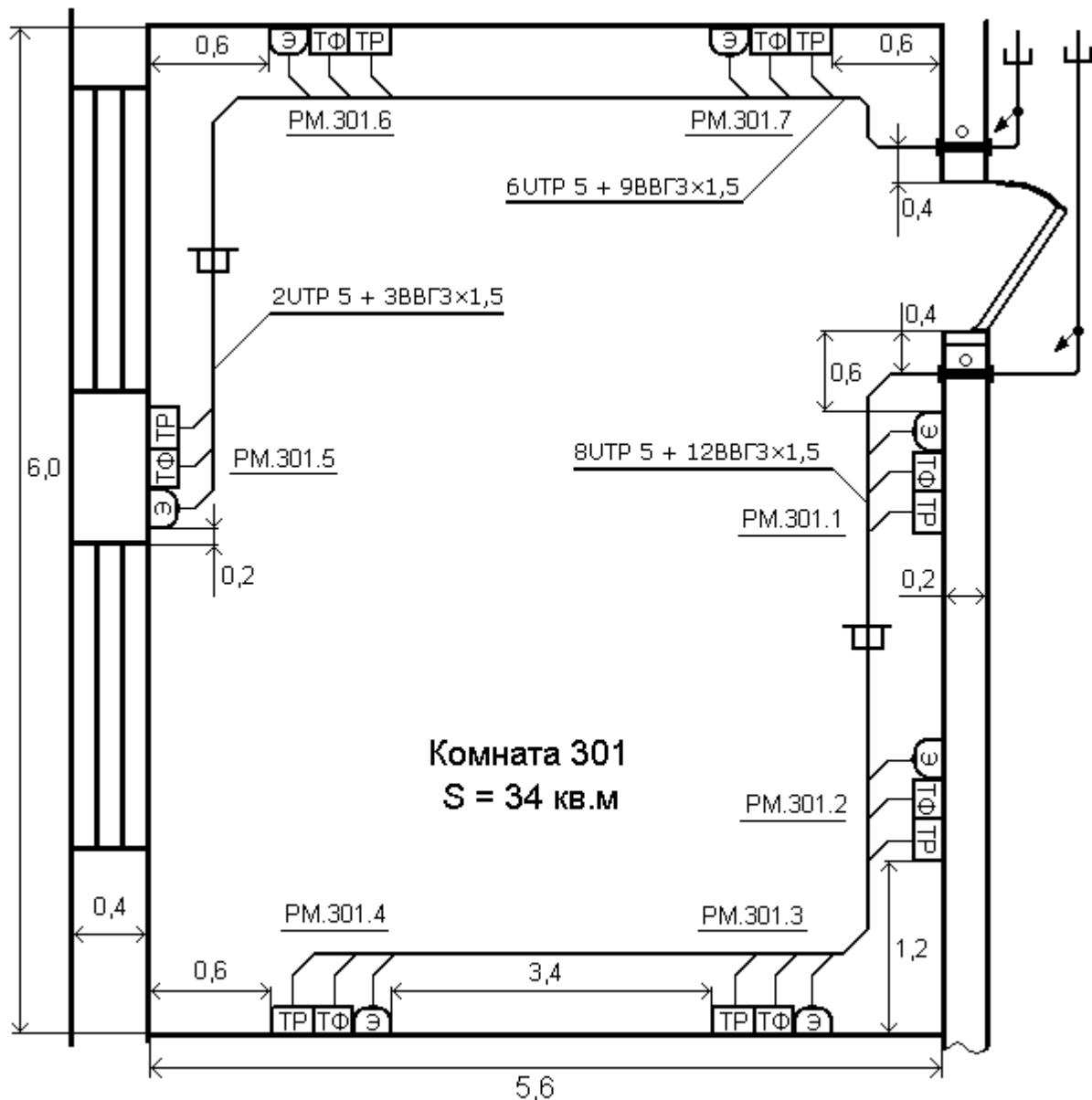


Рисунок 2.2 — Схема размещения компонентов компьютерной сети в помещении 301

На рисунке 2.3 изображена схема размещения компонентов и оборудования сети в техническом помещении, используемом в качестве распределительного пункта этажа (серверной). В этом помещении установлен телекоммуникационный шкаф, в котором устанавливаются распределительные (патч-) панели, коммутаторы канального и сетевого уровней, маршрутизатор, а также серверное оборудование. Здесь же располагается щит силового электропитания. Расстояние между коммуникационным шкафом и стеной помещения выбрано таким образом, чтобы обеспечить доступ к распределительным панелям при монтаже или замене кабелей. Коммуникационные кабели и силовые заводятся в помещение через раздельные кондуиты.

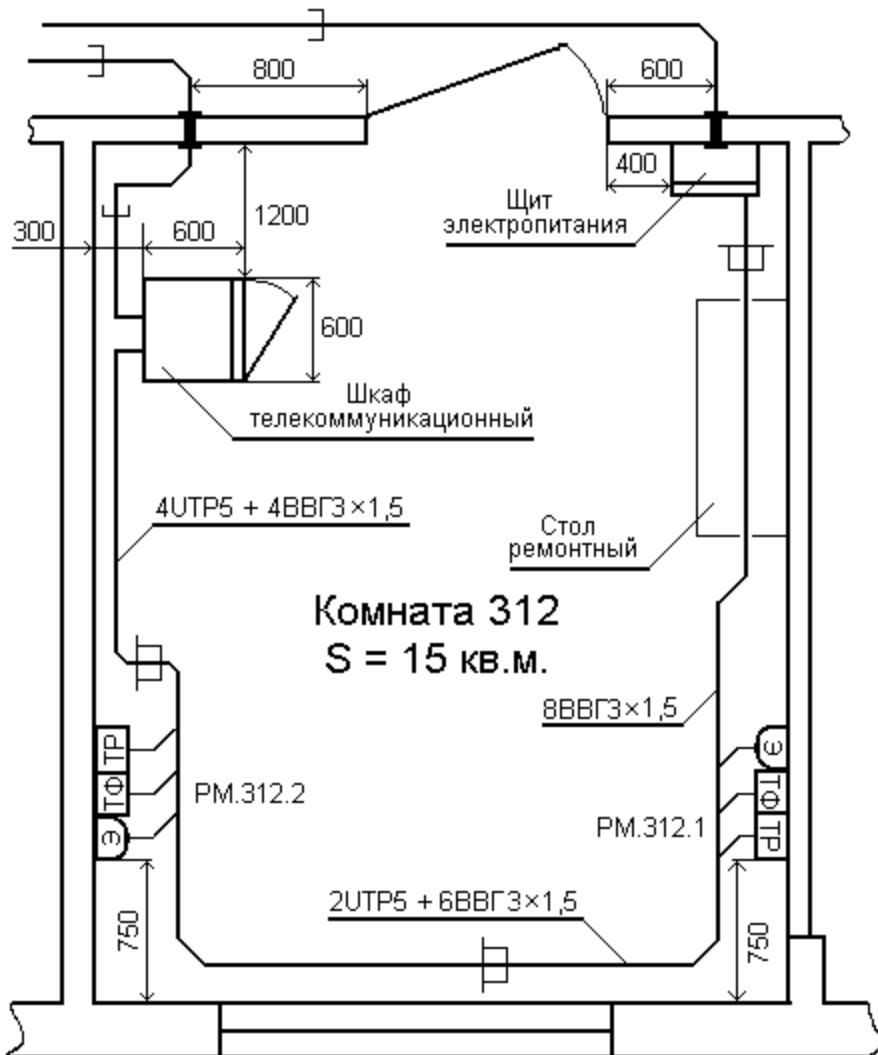


Рисунок 2.3 – Схема размещения компонентов СКС в техническом помещении

Ввод коммуникационных кабелей в шкаф осуществляется через верхнее входное отверстие, имеющееся в его крыше. Кабели подводятся сверху в лотке и затем через верхний вводной люк водятся внутрь шкафа. При этом способе к кабелям нет доступа, и они хорошо физически защищены. Четыре кабеля силового питания типа ВВГ 3 сечением 1,5 мм^2 каждый и 4 телекоммуникационных кабеля, идущих от рабочих мест РМ.301.1 и РМ.301.2, подводятся к телекоммуникационному шкафу в пластмассовом коробе и вводятся в него через нижний вводной люк.

В помещении также оборудовано два рабочих места: одно для администратора сети или лица, выполняющего его функции, а второе — для инженера-электронщика. Телекоммуникационные и силовые розетки рабочих мест закрепляются на стене, на высоте 0,8 м от уровня пола. Остальные установочные размеры показаны на чертеже. Для тестирования и ремонта оборудования установлен специальный стол монтажника.

2.7.3. Расчет величины расхода кабеля

Общая потребность кабеля для реализации сети рассчитывается по методике, изложенной в [16]. При этом учитывается, что наибольшая длина кабеля горизонтальной подсистемы не должна превышать 90 м.

Для определения минимальной L_{\min} и максимальной L_{\max} длины кабелей горизонтальной подсистемы построим профили кабельных трасс на основании планов помещений. Примеры профилей кабельных трасс изображены на рисунках 2.4а) и б) для минимальной и максимальной длин соответственно. Длины отдельных участков кабельных трасс взяты произвольно и не связаны с конкретным планом помещения.

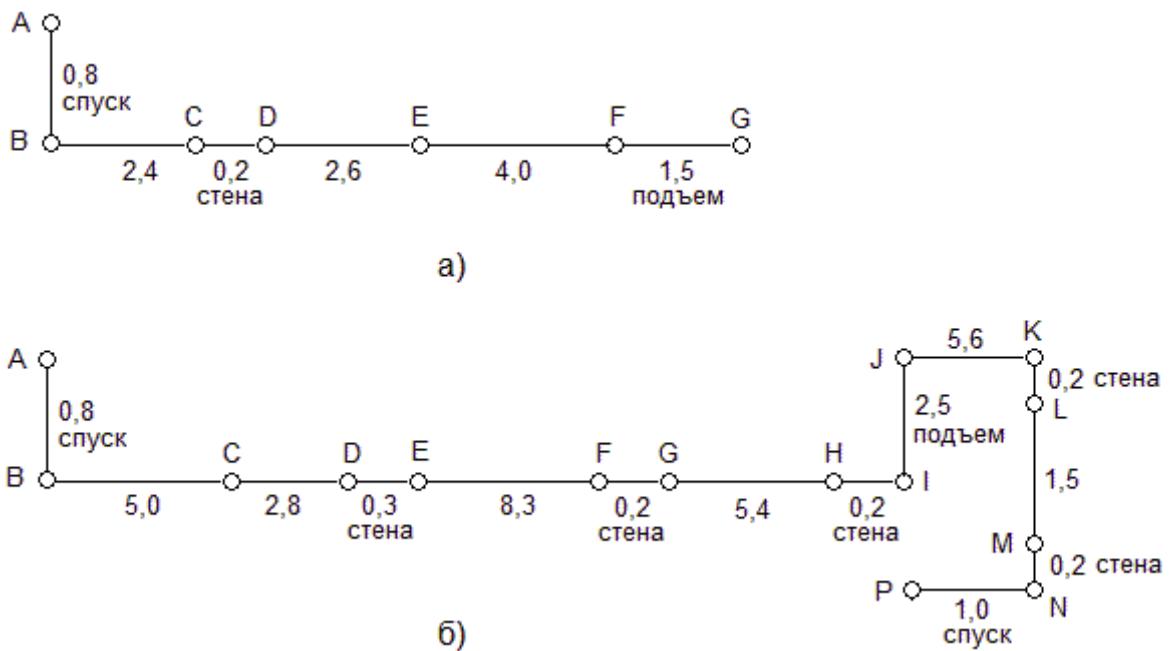


Рисунок 2.4 — Примеры построения профилей кабельных трасс

Эти данные необходимы для расчета потребности в кабельной продукции. Рассчитаем количество кабеля, требуемое для прокладки горизонтальных линий связи для каждого этажа (включая цокольный) 6-этажного здания. Нужное количество кабеля рассчитывается с использованием эмпирического метода [14], основанного на предположении, что рабочие места распределены по обслуживаемой площади равномерно. Средняя длина (L_{cp}) кабельных трасс вычисляется по формуле:

$$L_{cp} = (L_{\max} + L_{\min})/2,$$

где L_{\min} и L_{\max} – соответственно длины кабельной трассы от точки размещения кроссового оборудования до телекоммуникационного разъема самого близкого

и самого далекого рабочего места, посчитанные с учетом технологии прокладки кабеля, всех спусков, подъемов, поворотов и особенностей здания.

При этом учитем, что при определении длины трасс необходимо прибавить технологический запас величиной 10% от $L_{\text{ср}}$ и запас X для процедур разводки кабеля в распределительном узле и телекоммуникационном разъеме.

С учетом сделанных дополнений формула нахождения общей длины кабельных трасс L принимает вид:

$$L = (1,1L_{\text{ср}} + X) N_p,$$

где N_p – количество розеток на этаже.

Для определения величин L_{min} и L_{max} по плану здания и помещений построим профили кабельных трасс для минимальной и максимальной длины кабелей (рисунок 2.4а. и 2.4б).

По профилям трасс находим L_{min} и L_{max} , которые для приведенного примера равны соответственно 29 и 45 метров. С учетом того, что к каждой телекоммуникационной розетке, снабженной двумя гнездами RJ-45, подводится два кабеля одинаковой длины, а общее количество коммуникационных розеток в проектируемой сети равно $N_p = 62$, находим

$$\begin{aligned} L_{\text{ср}} &= (29+45)/2 = 37 \text{ м.} \\ L &= (1,1 \times 37 + 2) \times 2 \times 62 = 5295 \text{ м.} \end{aligned}$$

Таким образом, для горизонтальной подсистемы требуется 5295 м кабеля. Известно, что в стандартной кабельной бухте содержится 305 метров кабеля. Тогда для создания горизонтальной подсистемы нужно 18 ($5295/305=17,4$) бухт, или 5490 м кабеля ($18 \times 305=9455$).

Кабели оканчиваются (терминируются) встраиваемыми в короб телекоммуникационными розетками типа RJ-45, способными подключать также телефонные коннекторы RJ-11. Для подсоединения оборудования рабочих мест СКС укомплектывается патч-кордами.

2.7.4. Расчет габаритных размеров декоративного кабельного короба

При расчетах диаметр горизонтального кабеля категории 5е принимается равным 5,2 мм, что соответствует площади поперечного сечения кабеля $S_{\text{каб}}=21,2 \text{ мм}^2$. Коэффициент использования площади выбирается равным $k_i = 0,5$, а коэффициент заполнения — $k_z = 0,45$.

С целью уменьшения расхода декоративного короба целесообразно использовать двухсекционный короб, в котором одна секция служит для размещения коммуникационных кабелей, а вторая — для силовых. При этом требуется просчитать необходимые габариты каждой из секций.

Таким образом, требуемое сечение короба определяется по формуле

$$S_{\text{крб}} = (\sum S_{i\text{Ккаб}}) / (k_i k_z) + (\sum S_{j\text{Скаб}}) / (k_j k_z),$$

где $S_{i\text{Ккаб}}$ — сечение i -го коммуникационного кабеля; $S_{j\text{Скаб}}$ — сечение j -го силового кабеля.

Схему прокладки декоративных коробов, с целью более экономного их расходования, целесообразно выбрать таким образом, чтобы отдельные сегменты кабельных каналов данной разновидности использовались для прокладки кабелей к двум информационным розеткам.

Результаты расчетов габаритов короба целесообразно свести в таблицу 2.11.

Таблица 2.11 — Параметры кабельного короба

Количество обслуживаемых ТР	2	3	6	8
Количество горизонтальных кабелей	4	6	12	16
Требуемая площадь короба, мм ²	376	565	1130	1507
Габаритные размеры односекционного короба, мм	40×16	40×16	75×20	75×20

После определения суммарного сечения кабелей выбирается стандартный тип короба с сечением, не меньше рассчитанного. На практике наиболее широко используются секции короба стандартной длины 2 м и сечением 40×16 мм, 60×16 мм и 75×20 мм.

2.7.5. Выбор пассивного телекоммуникационного оборудования

Из расчетных данных следует и свидетельствуют о том, что в СКС будут использоваться короба типа NCT1050 двух типоразмеров: 60×16 мм и 75×20 мм, которые позволяют выполнять монтаж корпусов информационных и силовых розеток рядом с коробом на поверхности стены. Две секции короба будут использованы для прокладки горизонтальных информационных кабелей, а одна — двух силовых кабелей (один для системы гарантированного электропитания компьютерного оборудования, другой обеспечивает подключение розеток бытового электроснабжения). Кроме собственно короба для организации кабельных каналов требуется ряд вспомогательных элементов: заглушки, соединители и плоские уголки, соединяющие короба при их поворотах на 90°. Количество уголков и соединителей рассчитывается исходя из стандартной длины секции короба, равной 2-м метрам и количества поворотов кабельных трасс. Общая потребность таких элементов приведена в таблице 2.12.

Таблица 2.12 — Спецификация комплектующих элементов кабельных каналов

Тип	Наименование компонентов	Ед. изм	Кол-во
Кабельные каналы			
NCT1050	Короб 100×50	м	400
NCI1050	Соединитель 100×50	шт	190
NJC1050	Заглушка на шов 100×50	шт	190
NAF1050	Плоский угол 100×50	шт	20
NWP1050	Заглушка внутренняя 100×50	шт	40
YEP4	Заглушка 40×25	шт	65
YAF4	Плоский угол 40×25	шт	130

В качестве коммутационного оборудования для медных кабелей выберем 24-портовые коммутационные патч-панели типа «21-R0-45H024D0-2N1N» категории 5е для разделки кабелей горизонтальной подсистемы. Для подключения кабелей к коммутаторам и маршрутизатору через патч-панели предусмотрены соединительные шнуры (патч-корды) с разъемами «RJ45-RJ45» на обоих концах. Длина соединительных шнуров 1 м.

В качестве кросса для оптоволоконной части подсистемы внутренних магистралей выбираем оптические одномодовые распределительные полки с 8 разъемами типа «SC-AS». Для обеспечения возможности укладки избытка соединительных коммутационных шнуров под оптическими полками предусмотрены организаторы кабеля, имеющие форму пластины с держателями кабеля.

При монтаже оптоволоконной части подсистемы внутренних магистралей предполагается использовать технологию сварки, которая обеспечивает минимальные потери в точке сращивания оптических волокон и наибольшую надежность соединения.

Для размещения коммутационного оборудования СКС и активного оборудования ЛВС в здании предусмотрено техническое помещение 312. В этом помещении устанавливается 19"телекоммуникационный шкаф, в который в соответствии с логической схемой сети устанавливаются:

- 1) одна 19" оптическая панель 24×ST высотой 1U;
- 2) 3 патч-панели на 25 портов RJ-45 для терминирования кабелей горизонтальной подсети;
- 3) 3 патч-панели на 25 портов RJ-45 для терминирования кабелей телефонной связи;
- 4) 4 горизонтальных кабельных органайзеров высотой 1U каждый;
- 5) 2 вертикальных кабельных органайзера;
- 6) два коммутатора Cisco Catalyst 2950 на 12 портов 10/100 RJ-45 высотой 2U каждый;
- 7) маршрутизирующий коммутатор Cisco Catalyst 3500 высотой 2U;
- 8) 2 сервера высотой 3U каждый;
- 9) блок бесперебойного питания высотой 4U;

10) блок электрических розеток высотой 1U;

11) панель вентиляторов потолочная на 2 вентилятора высотой 1U;

В итоге для размещения оборудования в шкафе требуется высота 29U. С учетом 30-процентного запаса требуемая высота шкафа составляет 40U. На основании этого выбираем телекоммуникационный шкаф со стандартной высотой 41U (2030 мм). Для закрытия неиспользуемого пространства шкафа предусмотрим панели заглушки общей шириной 10U. Для коммутации шкаф укомплектовывается патч-кордами длиной 0,5, 1 и 1,5м. Перечень пассивного оборудования спроектированной сети приведен в таблице 2.13.

Таблица 2.13 — Спецификация пассивного оборудования локальной сети

№№	Наименование компонентов	Ед. изм	Кол-во
1	EuroLAN MiNi настенная информационная розетка RJ45, кат.5е, 2-х портовая	шт	70
2	Кабель UTP 4PR-1583	м	5490
3	Кабель ВО 2-х жильный, 62,5/125	м	80
4			
5	19" Патч-панель, 24xRJ45, 568B, UTP	шт	6
6	19" Оptическая панель 24xST	шт	1
7			
8	ST-MM Оptический коннектор	шт	8
9			
10	Модуль вентиляторный потолочный, 380x380 мм, 2 вент	шт	1
11	Шкаф напольный 41U, 2050x600x600, стеклянная дверь в стальной раме, ручка с замком с трёхточечной фиксацией	шт	5

В случае, когда компьютерная сеть разворачивается на нескольких этажах одного или группы зданий, необходимо произвести аналогичные расчеты для распределительных пунктов всех этажей и распределительного пункта здания и выбрать нужное количество и габариты коммуникационных шкафов.

2.8. Разработка политики информационной безопасности в сети предприятия

В данном разделе записи должны быть составлены тексты инструкций, в которых излагаются положения специфической политики для заданных техническим заданием типов сервисов, общие правила доступа пользователей к

информационным ресурсам, а также разработаны правила доступа отдельных категорий пользователей к локальным и глобальным сетевым ресурсам.

2.8.1. Политика информационной безопасности для отдельных видов сервиса.

Техническим заданием на проектирование предусмотрена разработка политики безопасности для одного из видов обслуживания:

- при удаленном доступе к ресурсам предприятия;
- при взаимодействии с Интернет;
- при получении доступа к сетевым ресурсам;
- при выборе и использовании паролей;
- при защите от вирусов.

Рассмотрим ряд примеров составления положений частных политик безопасности. Примерный текст политики удаленного доступа к ресурсам предприятия может иметь вид [www.compdoc.ru/network/internet/politicians_of_safety/]:

"1. Сотрудник компании несет ответственность за последствия неправильного использования удаленного доступа.

2. Высокоскоростной удаленный доступ через каналы сетей ISDN и Frame Relay разрешается только сотрудникам службы безопасности сети, администратору сети, главным специалистам компании, другим специалистам компании, выезжающим в служебную командировку и менеджерам продаж.

3. Сотрудники, менеджеры продаж и выездные специалисты компании, обладающие удаленным доступом к корпоративной сети компании, несут такую же ответственность, как и в случае локального подключения к сети компании.

4. Перед осуществлением удаленного доступа к корпоративной сети следует ознакомиться по расписи в журнале учета со следующими политиками безопасности:

- а) допустимого шифрования;
- б) организации виртуальных частных сетей;
- в) безопасности беспроводного доступа;
- г) допустимого использования.

5. Защищенный удаленный доступ должен постоянно контролироваться. Ответственность за контроль возлагается на начальника службы безопасности.

6. Требуемый уровень безопасности должен обеспечиваться посредством использования однократных паролей или инфраструктуры открытых ключей.

7. Сотрудники, имеющие привилегию удаленного доступа к корпоративной сети, не имеют права использовать адреса электронной почты компании для ведения собственного бизнеса.

6. Сотрудник компании несет личную ответственность за то, чтобы член его семьи не нарушил правила политик безопасности компании, не выполнил противозаконные действия и не использовал удаленный доступ для достижения собственных деловых интересов.

7. Сотрудникам запрещается передавать или посыпать по электронной почте свой пароль на вход в систему, включая членов семьи.

8. Сотрудники, имеющие право удаленного доступа, должны гарантировать, что их компьютеры, которые удаленно подключены к сети, не подключены в то же самое время ни в какую другую сеть, за исключением домашних сетей, которые находятся под полным управлением сотрудника.

9. Для членов семьи сотрудника компании доступ к Internet через сеть компании разрешается только в случае оплаты трафика самим сотрудником.

10. Маршрутизаторы для выделенных ISDN линий, сконфигурированные для доступа к корпоративной сети, должны использовать для аутентификации, как минимум, процедуру CHAP.

11. Для получения дополнительной информации относительно удаленного доступа, включения и отключения услуги, поиска неисправностей и т.д., следует обращаться на сайт службы организации удаленного доступа к информационным ресурсам компании".

Перечень требований данной политики может быть расширен и дополнен.

Другим примером фрагмента политики безопасности по разграничению доступа в локальную вычислительную сеть (ЛВС) является следующий [www.zahist.narod.ru/securelan4.htm].

"1. Каждый персональный компьютер должен иметь "владельца" или "системного администратора", который является ответственным за работоспособность и безопасность компьютера, и за соблюдение всех политик и процедур, связанных с использованием данного компьютера.

2. Пользователи должны быть обучены и обеспечены соответствующими руководствами так, чтобы они могли корректно соблюдать все политики и процедуры безопасности.

3. Все механизмы защиты сервера ЛВС должны находиться под монопольным управлением местного администратора и местного персонала Администраторов ЛВС.

4. Программное обеспечение должно быть лицензированным и является безопасным.

5. За все изменения (замены) программного обеспечения и создание резервных копий данных на серверах отвечают Администраторы ЛВС.

6. Каждому пользователю должен быть назначен уникальный ИДЕНТИФИКАТОР ПОЛЬЗОВАТЕЛЯ и начальный пароль (или другая информация для идентификации и аутентификации) только после того, как закончено оформление надлежащей документации.

7. Пользователям запрещается совместно использовать назначенные им ИДЕНТИФИКАТОРЫ ПОЛЬЗОВАТЕЛЯ.

8. Пользователи должны аутентифицироваться в ЛВС перед обращением к ее ресурсам.

9. ИДЕНТИФИКАТОР ПОЛЬЗОВАТЕЛЯ должен удаляться после продолжительного периода неиспользования.

10. Использование аппаратных средств мониторинга ЛВС, маршрутизаторов или регистраторов трафика должно быть авторизовано и проводиться под контролем Администраторов ЛВС.

11. Служащие, ответственные за управление, функционирование и использование ЛВС предприятия должны пройти курс обучения в области компьютерной безопасности и правил работы на компьютере.

12. Отчеты о безопасности ЛВС должны готовиться и рассматриваться ежедневно".

2.8.2. Общие правила предоставления доступа к информационным ресурсам

На каждом предприятии, использующем сетевые информационные технологии, должны быть разработаны общие правила предоставления доступа к информационным ресурсам. Такие правила разрабатываются персоналом службы безопасности и являются обязательными для каждого пользователя компьютерной сети. Ниже приведены примеры правил доступа к некоторым видам ресурсов [31 - 34].

1. Доступ к ресурсам

Для предоставления доступа к информационным ресурсам пользователи направляют в подразделение информационных технологий (ИТ) заявку в установленной форме с ходатайством непосредственного руководителя заявителя и визой владельца информационного ресурса (В заявке указываются Ф.И.О. пользователя, наименование ресурсов и обоснование необходимости). В случае доступа к информационному ресурсу категории конфиденциально «К» обязательна подпись администратора информационной безопасности.

Для получения доступа к внешним информационным ресурсам, пользователь направляет в подразделение информационных технологий письмо по установленной форме, с ходатайством непосредственного руководителя, согласованное со службой сетевой безопасности. (Данное письмо необходимо для тех организаций, где доступ в Интернет и использования электронной почты требует отдельного разрешения).

1.1. При наличии технической возможности специалисты соответствующих подразделений ИТ производят подключение пользователя к информационному ресурсу с внесением необходимых изменений в терминальное и коммуникационное оборудование (присвоением компьютеру пользователя сетевого имени, выдача соответствующего идентификатора, имени пользователя, пароля и т.д.).

1.2. При работе на одном компьютере нескольких пользователей, каждый из них должен применять свою учетную запись для доступа к информационному ресурсу.

1.3. Каждый пользователь обязан хранить свой пароль в тайне и изменять его по мере необходимости (для информации категории «К» не реже 1 раза в месяц).

1.4. Заявки пользователей на создание учетных записей и на предоставление доступа к информационному ресурсу хранятся в подразделении ИТ в течение времени действия учетной записи пользователя.

1.5. Пользователям запрещается несанкционированно использовать информационные ресурсы, доступа к которым он не имеет. Контроль доступа обеспечивается средствами операционных систем, средствами контроля доступа специализированных приложений, сертифицированными средствами защиты от несанкционированного доступа, а также средствами сетевого мониторинга и аудита.

2. Аннулирование доступа

2.1. В случае увольнения или перевода в другое подразделение (отдел, бюро и т.д.) сотрудника, являющегося пользователем информационного ресурса, его непосредственный руководитель обязан известить соответствующего администратора объекта информатизации для аннулирования доступа к информационному ресурсу.

2.2. Не информирование администратора влечет за собой дисциплинарную ответственность.

2.3. Сверка по увольнениям и перемещениям сотрудников должна осуществляться не реже 1 раза в месяц.

3. Обслуживание информационных систем

Пользователям запрещается использовать информационные ресурсы предприятия и средства вычислительной техники (СВТ) в целях, не связанных с выполнением должностных обязанностей.

3.1. Установка и настройка программного обеспечения.

3.1.1. К установке на СВТ разрешается только программное обеспечение (ПО), включенное в реестр протестированного и разрешенного службой ИТ к применению программного обеспечения.

3.1.2. Подразделение ИТ составляет и обновляет реестр системного и прикладного ПО, разрешенного к установке на СВТ пользователей и пользователей сети. Реестр обновляется в соответствии с потребностями пользователей и тенденциями в развитии программного обеспечения.

3.1.3. Любой пользователь может быть инициатором внесения в реестр новых программных продуктов. Для внесения программного продукта в реестр пользователи направляют заявку.

3.1.4. Программный продукт, указанный в заявке, тестируется специалистами ИТ, после чего принимается решение о включении его в реестр.

3.1.5. Установку и переустановку любого общесистемного, сетевого и антивирусного программного обеспечения, а также всех информационных систем, разрабатываемых на предприятии, на СВТ пользователей и пользователей сети производят только службы ИТ в соответствии со спецификой ПО. Самостоятельно

устанавливать и переустанавливать программные продукты пользователям запрещается.

3.1.6. Пользователям запрещается менять настройки применяемого ПО без согласования с администратором объекта информатизации. Изменение настроек общесистемного, сетевого и антивирусного ПО запрещено без согласования с администратором сети.

3.1.7. Допускается самостоятельная установка и переустановка прикладного ПО пользователями по согласованию с системным администратором сети.

3.2. Устранение сбоев в работе СВТ и неполадок в программном и аппаратном обеспечении.

3.2.1. При возникновении сбоев в работе автоматизированных систем и СВТ пользователи должны сообщить о неполадках диспетчеру подразделения ИТ. Диспетчер сообщает о неполадках в соответствующие службы ИТ и координирует их работу по устранению неисправностей. Устранять неполадки самостоятельно пользователям запрещается.

3.2.2. Ремонтно-профилактические работы на СВТ производят только специалисты ИТ. Работы должны быть организованы таким образом, чтобы исключить возможность несанкционированного доступа к конфиденциальной информации, находящейся на дисках СВТ.

3.2.3. Ремонт компьютера проводится либо на месте, под присмотром ответственного лица, назначенного руководителем подразделения, либо отправляется в стационарный ремонт. В случае отправки в стационарный ремонт вся конфиденциальная информация, хранящаяся на жестком магнитном диске, должна быть удалена с наложением на удаленные сектора незначащих символов (используя специальное программное обеспечение). Допускается снятие жесткого магнитного диска с конфиденциальной информацией на хранение ответственным за безопасность информации сотрудником подразделения до получения компьютера из ремонта.

3.2.4. Бесконтрольный ремонт СВТ с магнитным накопителем, содержащим конфиденциальную информацию, не допускается.

4. Обмен данными

4.1. Пользователи при обмене данными с применением внешних носителей информации обязаны производить проверку носителей на наличие вирусов перед началом работы с данными, содержащимися на них.

4.2. Наличие на компьютерах сетевых пользователей ресурсов общего доступа (доступ «полный», «на чтение», «определяется паролем») не допускается. Обмен информацией осуществляется посредством почтового сервера предприятия или через информационные ресурсы, расположенные на серверах предприятия. Весь почтовый обмен производится только через электронные почтовые ящики, открытые на почтовом сервере предприятия.

4.3. Пользователям запрещается хранить на СВТ, а также на информационных ресурсах, открытых на серверах для обмена и хранения данных, информацию и программные средства, не связанные с выполнением должностных обязанностей.

4.4. При обмене и передачи информации, отнесенной к категории «К», должны применяться сертифицированные средства криптозащиты информации и электронная цифровая подпись.

5. Обеспечение сохранности данных

5.1. Резервное копирование.

5.1.1. Архивирование критически важных данных для обеспечения деятельности предприятия является обязательным. Для архивирования применяются специальные аппаратно-программные средства.

5.1.2. Ответственность за утерю, порчу и сохранность информации, хранящейся на накопителях СВТ, возлагается на пользователя. Для резервного хранения информации пользователям сети могут предоставляться специальные информационные ресурсы на серверах. Информационные ресурсы создаются по заявке, направляемой в центр информационных технологий (ЦИТ) от имени начальника подразделения. В заявке на создание информационного ресурса необходимо указать размер информационного ресурса, ответственного за ресурс, необходимость и периодичность резервного сохранения данных. В заявке на предоставление ресурса можно указать прочих пользователей, доступ для которых к данному ресурсу открыт.

5.1.3. Помимо информационных ресурсов для хранения на серверах сети, для резервного копирования пользователи сети могут использовать внешние носители информации.

5.2. Антивирусная защита

5.2.1. Применение антивирусной защиты на рабочих станциях и серверах является обязательным.

5.2.2. Ответственность за обновление антивирусного ПО и антивирусных баз данных возлагается на системного администратора сети.

5.2.3. Ответственность за установку и настройку антивирусного ПО на СВТ пользователей сети возлагается на подразделения ИТ. На СВТ пользователей в обязательном порядке должна быть установлена программа антивирусной защиты, работающая в фоновом режиме, отслеживающая все операции по открытию, копированию и перемещению файлов на СВТ, а также автоматически производящая ежедневную проверку всех дисков и памяти СВТ на наличие вирусов.

5.2.4. Ответственность за антивирусную защиту информации на СВТ пользователей возлагается на пользователя, за которым закреплено данное СВТ. Пользователи обязаны обратиться в подразделения ИТ для получения действующего на Предприятия антивирусного ПО.

5.2.5. Пользователь СВТ обязан:

- перед началом работы убедиться, что программа антивирусной защиты на его СВТ запущена;

- не допускать использования и хранения на своем рабочем месте автономных носителей информации не проверенных на наличие вирусов;

- при обнаружении вируса произвести его лечение средствами антивирусной защиты, установленными на СВТ пользователя и сообщить об обнаружении вируса системному администратору сети и администратору информационной безопасности.

5.2.6. Пользователям запрещается распространять, хранить и создавать вредоносные программы.

5.3. Обеспечение конфиденциальности информации

5.3.1. Пользователи обязаны принять все возможные меры для предотвращения несанкционированного доступа со стороны посторонних лиц к хранящейся на СВТ конфиденциальной информации.

5.3.2. Администратор информационной безопасности при необходимости получения доступа к ресурсам СВТ, при проведении служебных проверок, обязан поставить в известность пользователя данного СВТ или руководителя подразделения пользователя.

5.4. Обеспечение режима безопасности пользователями

5.4.1. Все пользователи обязаны принимать участие в обеспечении режима информационной безопасности при работе с информационными ресурсами Предприятия и на СВТ, а именно:

- предотвращать возможность несанкционированного доступа посторонних лиц к информации, хранящейся на информационных ресурсах и на СВТ;

- выполнять требования «Инструкции о пропускном режиме» в части автономных носителей информации (дискеты, CD-R, CD-RW, DVD-RW, Flash-memory, сотовые телефоны, цифровые диктофоны, фотоаппараты и видеокамеры) и элементов компьютерной техники;

- немедленно информировать администраторов объектов информатизации о случаях нарушения режима информационной безопасности, в том числе, связанных как с аварийными (сбойными) ситуациями при эксплуатации компьютерной техники, так и с появлением реальных каналов утечки информации путем умышленного разрушения программно-аппаратных механизмов защиты информационных ресурсов;

- магнитные диски и иные носители информации (дискеты, CD-R, CD-RW, DVD-, Flash-memory, сотовые телефоны, цифровые диктофоны, фотоаппараты и видеокамеры), получаемые от других сотрудников или других организаций, перед использованием должны быть подвергнуты обязательному входному контролю на наличие программных вирусов.

5.4.2. Пользователям информационных ресурсов и СВТ запрещается:

- производить очистку журнала аудита;

- самостоятельно изменять аппаратные конфигурации и подключать периферийные внешние устройства;
- несанкционированное копирование информации (файлов) на дискеты и другие внешние носители;
- нерегламентированный просмотр, вывод на печать и т.п. информации ограниченного распространения;
- оставлять без присмотра закрепленную за ним компьютерную технику без ее отключения или блокировки на время отсутствия пользователя, или без установки специального программного обеспечения поддержки дежурного режима (хранители экрана) с обязательной установкой пользователем произвольного пароля, неизвестного другим лицам;
- оставлять на рабочих столах в свое отсутствие автономные носители информации (дискеты, диски всех типов, магнитные ленты стримеров), содержащие данные конфиденциального характера.

Помимо представленных выше документов можно создать инструкции для пользователей и администраторов по отдельным видам деятельности. Например, по работе в Интернет, работе с почтой, архивированию данных и т.д.

2.8.3. Правила доступа персонала к информационным ресурсам

В этом подразделе формулируются конкретные права доступа к сетевым ресурсам каждого их сотрудников предприятия. На практике такие правила составляются на основании требований и пожеланий руководства организацией и ее службы безопасности. Затем эти правила оформляются в форме таблиц доступа, в которых указывается, с каких сетей разрешается доступ к другим сетям, кому и в какое время разрешается доступ к тому или иному ресурсу, а к каким ресурсам доступ запрещается. Формы таких таблиц могут иметь следующей вид.

Таблица 2.14 — Регламентация взаимодействия между виртуальными сетями

Рабочая группа / VLAN	Разрешен доступ к виртуальным сетям						
	Админ. 1/VLAN	Управл. 2/VLAN	3/VLAN	4/VLAN	5/VLAN	6/VLAN	7/VLAN
1/VLAN1	Да	Нет	Нет	Нет	Нет	Нет	Нет
2/VLAN2	Да	Да	Нет	Нет	Нет	Нет	Нет
3/VLAN3	Да	Да	Да	Нет	Нет	Нет	Да
4/VLAN4	Да	Да	Нет	Да	Нет	Нет	Нет
5/VLAN5	Да	Да	Нет	Нет	Да	Нет	Нет
6/VLAN6	Да	Да	Да	Нет	Нет	Да	Нет
7/VLAN7	Да	Да	Нет	Да	Да	Нет	Да

В этой таблице показан пример взаимодействия между рабочими группами, регулируемого на уровне телекоммуникационных устройств (маршрутизаторов и коммутаторов). Разграничение доступа на уровне серверов и клиентских компьютеров осуществляется отдельными установками. В данной таблице отмечено, что сотрудникам группы информационной поддержки разрешается доступ к компьютерам всей сети организации (предприятия). Это объясняется необходимостью осуществления технической и программной поддержки инфраструктуры компьютерной сети. Разрешение доступа из одних сетей в другие предоставляется на основании производственной необходимости и с учетом информационной безопасности.

Следующим регламентируемым видом доступа является доступ сотрудников организации в Интернет. Правила доступа должны регулировать доступ к ресурсам Интернета отдельным сотрудникам, либо группам пользователей. Этими правилами могут быть установлены типы протоколов, виды данных, разрешенных к приему и передаче, разрешен или запрещен доступ к отдельным сайтам, указано время и дни недели, в которые разрешено выходить в Интернет и другие ограничения. В таблице 2.15, в качестве примера, указаны ограничение на доступ в Интернет по дням недели и времени и на виды передаваемых или принимаемых файлов.

Таблица 2.15 — Регламентация доступа к сети Интернет

Ф.И.О.	Должность			Запрещенные типы файлов	Дни доступа	Время доступа
Иванов А.Б.	Директор				1-7	6.00-24.00
Бондарь В.В.	Гл.бухгалт.			mp3; avi; exe	1-6	8.00-22.00
Гонтарь С.П.	Нач. отдела				1-5	8.00-18.00
Репин А.И.	Сет.админ.				1-7	Не огран.
Аулова Д.С.	Бухгалтер				1-5	8.00-18.00
Янин А.П.	Менеджер				1-5	8.00-18.00
Кобзарь И.Г.	Инженер				1-5	8.00-18.00
Бадов Р.П.	Техник				1-5	8.00-18.00
Бадов Р.П.	Техник				1-5	8.00-16.00
Другие служащие					1-5	12.00-13.00

В таблице 2.16 внесены временные ограничения на доступ к внутренним серверам корпоративной сети.

Таблица 2.16 — Регламентация доступа к внутренним серверам

Ф.И.О.	Должность	Доступ разрешен/запрещен + / -			Дни доступа	Время доступа
		Сервер 1	Сервер 2	Сервер 3		
Иванов А.Б.	Директор	+	+	+	1-7	7.00-22.00
Бондарь В.В.	Гл. бухгалт.	+	-	+	1-7	7.00-22.00
Гонтарь С.П.	Нач. отдела	-	+	-	1-6	7.00-20.00
Репин А.И.	Админ.	+	+	+	1-7	0.00-24.00
Аулова Д.С.	Бухгалтер	-	-	+	1-5	8.00-18.00
Янин А.П.	Менеджер	-	+	-	1-5	8.00-18.00
Кобзарь И.Г.	Инженер	-	+	-	1-5	8.00-18.00
Бадов Р.П.	Техник	-	+	-	1-5	8.00-18.00
Другие служащие		-	-	+	1-5	12.00-13.00

Таблицы доступа могут иметь другой вид и содержать иные ограничения (Таблица 2.17) .

Таблица 2.17

Виды ограничений	Ограничения по входящим сообщениям	Ограничения по исходящим сообщениям	Исключения для пользователей / рабочих групп
Максимальный размер письма	100 МБ	5 МБ	Маркетинг
Допустимость зашифрованных файлов	Да Нет	Нет Нет	— Отдел разработок
Запрещение вложенных файлов	avi, mpg, mpeg, wav, exe, com exe, com, dll	avi, mpg, mpeg, wav, exe, com exe, com, dll	Отдел маркетинга Группа ИТ
Ключевые слова	—	Конфиденциально, для служебного пользования	Директор
		Username; id; password	Группа ИТ
	CV, vitae, resume	CV, vitae, resume, резюме, поиск работы	Директор. отдел кадров
	Гороскопы. анекдоты	—	—
Ключевые слова - Отправитель	Anonymous, no one, replay.com	—	Группа ИТ
Ключевые слова - Получатель	—	Список конкурентов	—
Продолжительность сохранения письма в БД	2 года	2 года	Директор, руководители проектов, отдел кадров, бухгалтерия

2.9. Разработка скриптов конфигурации коммуникационного оборудования сети

В данном подразделе необходимо изобразить логическую схему сети с указанием типа оборудования, адресов виртуальных подсетей, интерфейсов маршрутизаторов и коммутаторов. Пример такой схемы показан на рисунке 2.5.

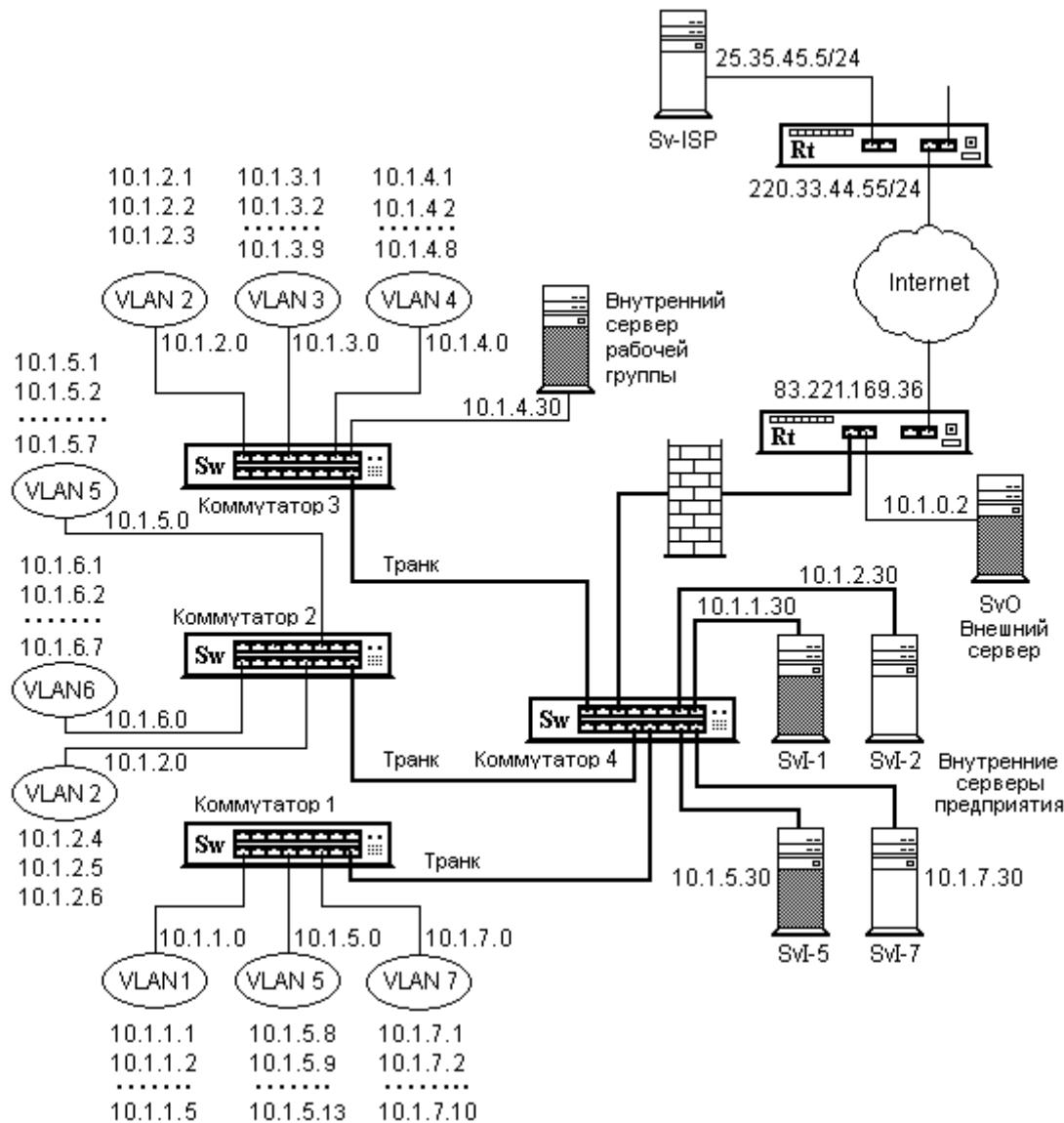


Рисунок 2.5 — Логическая схема сети с IP адресами

Затем приводятся полные тексты сценариев (скриптов) конфигурации оборудования, которое входит в состав разработанной компьютерной сети. Для каждого типа оборудования составляются соответствующие сценарии конфигурации с учетом применяемой в нем сетевой операционной системы (Cisco IOS или CatOS). Составление скриптов следует начинать с оборудования уровня доступа.

В начале каждого скрипта должна быть освещена суть процедуры, а затем следует соответствующий сценарий конфигурации. Все скрипты должны сопровождаться подробными комментариями.

Сценарии должны включать следующие разделы:

- начальная конфигурация устройств;
- настройка интерфейсов;
- создание подсетей или виртуальных сетей;
- обеспечения взаимодействия подсетей;
- просмотр и контроль созданной конфигурации.

При конфигурировании оборудования Cisco следует иметь в виду, что в нем отсутствует заводская установка IP адреса по умолчанию, а вся конфигурация выполняется вручную с консоли через консольный порт устройства.

Ниже приведены примеры разработки сценариев (скриптов) для гипотетической локальной сети предприятия, схема которой показана на рисунке 2.5.

2.9.1. Сценарии конфигурации коммутаторов

Конфигурация коммутатора 4.

Конфигурацию коммутаторов начнем с корневого устройства, с которым непосредственно связаны все остальные коммутаторы сети. Пусть все коммутаторы сети — устройства типа Cisco Catalyst 2950-24, содержащие 24 интерфейса (порта) FastEthernet. К коммутатору 4 посредством магистральных каналов (транков) подключены коммутаторы 1-3, а к портам FastEthernet подсоединены четыре внутренние серверы рабочих групп и сетевой маршрутизатор. Предположим, что внутренние серверы подключаются к следующим портам коммутатора: SvI-1 – Fa0/4; SvI-2 – Fa0/5; SvI-5 – Fa0/6; SvI-7 – Fa0/7. Первый коммутатор соединяется с корневым через магистральный порт Fa0/11, второй — через магистральный порт Fa0/12, третий — через магистральный порт Fa0/13, а соединение коммутатора 4 с маршрутизатором осуществляется через магистральный порт Fa0/24.

Сценарий конфигурации данного коммутатора состоит из следующих команд.

```
!-- Вход в привилегированный режим конфигурации.
```

```
Switch>enable
```

```
Switch#
```

```
!-- Задание пароля для входа в привилегированный режим.
```

```
Switch# configure terminal
```

```
Switch(config)# enable password <Пароль привилегированного режима>
```

-- Установка пароля для входа по telnet по линиям 0...4.

Switch(config)# line vty 0 4

Switch(config-line)#password <Пароль для telnet>

-- Разрешение входа по telnet.

Switch(config-line)# login

Switch(config)# exit

-- Шифрование паролей, чтобы они не показывались в открытом виде.

Switch(config)# service password-encryption

-- Сохранение (при необходимости) текущей конфигурации.

Switch#copy running-config startup-config

-- Стирание (в случае необходимости) текущей стартовой конфигурации.

Switch#erase startup-config

-- Вход в режим глобального конфигурирования.

Switch#configure terminal

Switch(config)#

-- Присвоение имени Cat2950-4 конфигурируемому устройству.

Switch(config)#hostname Cat2950-4

Cat2950-4(config)#

-- Присвоение IP-адреса для управления коммутатором.

Cat2950-4(config)# interface vlan 1

Cat2950-4(config-if)# ip address 10.1.0.4 255.255.255.0

-- Ввод команды exit, чтобы изменения были приняты.

Cat2950-4(config-if)# exit

Cat2950-4(config)#

-- Создание виртуальных сетей.

-- Переход в привилегированный режим.

Cat2950-4(config)# exit

Cat2950-4#

-- Вход в базу данных VLAN для конфигурации виртуальных сетей.

Cat2950-4# vlan database

-- Для облегчения задач администрирования сети применим протокол VTP.

-- Объявление домена, на который распространяется действие протокола VTP.

Cat2950-4(vlan)# vtp domain Victoria

-- Задание коммутатору режима "Сервер".

Cat2950-4(vlan)# vtp server

!-- Если коммутатор уже находится в режиме "сервер" и нужно, чтобы он
!-- оставался в этом режиме, эту команду можно опустить.

!-- Создание на коммутаторе-сервере всех VLAN, имеющихся в данной сети
!-- Первая виртуальная сеть уже имеется по умолчанию. Первоначально в нее
!-- входят все (Fa0/0...Fa0/24) интерфейсы коммутатора.

!-- Создание второй виртуальной сети.

Cat2950-4(vlan)#vlan 2

!-- Аналогично задаются остальные сети.

!--

Cat2950-4(vlan)#vlan 7

Cat2950-4(vlan)#exit

Cat2950-4#

!--

!-- Задание имен сетям (при желании).

Cat2950-4# conf t

Cat2950-4(config)#vlan 2 name buchgalteria

!--

!--

!-- Включение в VLAN 1 порта fa0/4 (сервера первой рабочей группы).

Cat2950-4(config)# interface fa0/4

!--

!-- Задание порту режима коммутации (работы на канальном уровне).

Cat2950-4(config-if)# switchport mode access

!-- Включение в VLAN 2 порта fa0/5 (сервера второй рабочей группы) и

!-- задание порту режима коммутации (работы на канальном уровне).

Cat2950-4(config)# interface fa0/4

Cat2950-4(config-if)# switchport access vlan 2

!-- Аналогично включаются серверы 5-й и 7-й рабочих групп в соответствующие
!-- виртуальные сети VLAN 5 и VLAN 7.

!-- Ввод команды exit для сохранения изменений.

Cat2950-4(config-if)# exit

Cat2950-4(config)#

!-- Перевод портов FastEthernet 0/11, 0/12, 0/13 и 0/24 на коммутаторе 4 в режим
!-- trunk.. Конфигурация порта 0/11.

Cat2950-4(config)#interface FastEthernet0/11

!-- Задание режима инкапсуляции по протоколу 802.1Q

```
Cat2950-4(config-if)#switchport trunk encapsulation dot1q
```

-- Задание магистрального режима

```
Cat2950-4(config-if)#switchport mode trunk
```

-- Разрешение передачи кадров для всех VLAN по магистрали

```
Cat2950-4(config-if)#switchport trunk allowed vlan all
```

```
Cat2950-4(config-if)#exit
```

-- -----

```
Cat2950-4(config)#interface FastEthernet0/24
```

```
Cat2950-4(config-if)#switchport trunk encapsulation dot1q
```

```
Cat2950-4(config-if)#switchport mode trunk
```

```
Cat2950-4(config-if)#switchport trunk allowed vlan all
```

```
Cat2950-4(config-if)#exit
```

```
Cat2950-4(config)#
```

-- Контроль созданных VLAN и принадлежности портов

```
Cat2950-4(config)# exit
```

```
Cat2950-4# show vlan
```

Затем следует определить IP-адреса, которые нужно назначить на VLAN интерфейс, чтобы маршрутизатор был способен выполнять маршрутизацию между VLAN. Когда маршрутизатор принимает пакет, предназначенный для другой сети (VLAN), он просматривает свою таблицу маршрутизации чтобы определить, куда переслать пакет. В результате пакет передается на нужный VLAN интерфейс. Последний в свою очередь посыпает пакет на тот порт, к которому подсоединен целевая рабочая станция. В качестве адреса для всех VLAN выберем адрес соответствующей виртуальной сети с номером в поле хоста равным 100.

-- Конфигурируем VLAN интерфейсы IP-адресами, определенными в

-- предыдущем пункте.

--

```
Cat2950-4#configure terminal
```

```
Cat2950-4(config)#interface vlan 2
```

```
Cat2950-4(config-if)#ip address 10.1.2.100 255.255.255.0
```

```
Cat2950-4(config-if)#no shutdown
```

```
Cat2950-4(config)#interface vlan 5
```

```
Cat2950-4(config-if)#ip address 10.1.5.100 255.255.255.0
```

```
Cat2950-4(config-if)#no shutdown
```

Этот процесс нужно повторить для всех VLAN, которые используются в маршрутизации.

Конфигурация коммутатора 1.

К коммутатору 1 подключаются компьютеры трех виртуальных сетей: VLAN 1, VLAN 5 и VLAN 7. Подключение осуществляется через интерфейсы FastEthernet (fa), работающим в режиме доступа на канальном уровне. Виртуальной сети VLAN 1 выделим интерфейсы fa0/1...fa0/5, сети VLAN 5 — интерфейсы fa0/6...fa0/11, а сети VLAN 7 — fa0/12...fa0/21. Интерфейс fa0/24 настраивается на магистральный (транковый) режим.

-- Сценарий конфигурации первого коммутатора состоит из следующих команд.

--

-- Вход в привилегированный режим конфигурации.

Switch>enable

Switch#

-- Задание пароля для входа в привилегированный режим.

Switch# configure terminal

Switch(config)# enable password <Пароль привилегированного режима>

-- Установка пароля для входа по telnet.

Switch(config)# line vty 0 4

Switch(config-line)#password <Пароль для telnet>

-- Разрешение входа по telnet.

Switch(config-line)# login

Switch(config)# exit

-- Шифрование паролей чтобы они не показывались в открытом виде.

Switch(config)# service password-encryption

-- Сохранение (при необходимости) текущей конфигурации.

Switch#copy running-config startup-config

-- Вход в режим глобального конфигурирования.

Switch#configure terminal

Switch(config)#

-- Присвоение имени Cat2950-1 конфигурируемому устройству.

Switch(config)#hostname Cat2950-1

Cat2950-1(config)#

--

-- Задание режима работы с VTP протоколом.

-- Переход в привилегированный режим.

Cat2950-1(config)# exit

Cat2950-1#

-- Вход в базу данных VLAN.

Cat2950-1# vlan database

-- Включение коммутатора в домен, на который распространяется действие

-- VTP протокола.

Cat2950(vlan)# vtp domain Victoria

-- Задание коммутатору режима "Клиент".

Cat2950-1(vlan)# vtp client

Cat2950-1(vlan)#exit

-- Контроль статуса коммутатора.

Cat2950-1#show vtp status

-- Конфигурация магистрального интерфейса.

Cat2950-1#conf t

Cat2950-1(config)#int fa0/24

Cat2950-1(config-if)#switchport trunk encapsulation dot1q

Cat2950-1(config-if)#switchport mode trunk

Cat2950-1(config-if)#switchport trunk allowed vlan 1-7

Cat2950-1(config-if)#exit

Cat2950-1(config)#exit

-- Проверка того, что информация о виртуальных сетях, созданных на сервере,

-- распространилась на коммутатор-клиент.

Cat2950-1#schow vlan

-- Включение в VLAN 5 группы портов с 6-го по 11-й.

Cat2950-1(config)# interface range FastEthernet 0/6 – 11

-- Задание портам режима коммутации (работы на канальном уровне).

Cat2950-1(config-if)# switchport mode access

-- Включение портов в виртуальную сеть VLAN 5.

Cat2950-1(config-if)# switchport access vlan5

-- Включение поддержки алгоритма STP.

Cat2950-1(config-if)#spanning-tree port FastEthernet

!--

-- Включение в VLAN 7 диапазона портов с 12-го по 21-й.

Cat2950-1(config)# interface range FastEthernet 0/12 – 21

-- Задание портам режима коммутации.

Cat2950-1(config-if)# switchport mode access

!--

-- Включение портов в VLAN 7.

Cat2950-1(config-if)# switchport access vlan 7

```

!--
!-- Сохранение настроек и переход в режим глобальной конфигурации.
Cat2950-1(config-if)#exit

!-- Перевод порта FastEthernet0/24 на коммутаторе 1 в режим trunk..
Cat2950-1(config)#interface FastEthernet0/24
Cat2950-1(config-if)#switchport mode trunk

!-- Задание режима инкапсуляции 802.1Q.
Cat2950-1(config-if)#switchport trunk encapsulation dot1q

!-- Разрешение передачи кадров для всех VLAN по магистрали.
Cat2950-1(config-if)#switchport trunk allowed vlan all
Cat2950-1(config-if)#exit
!--

```

Конфигурация коммутаторов 2 и 3

Процедура конфигурации обоих коммутаторов выполняется аналогично предыдущей. Как следует из логической схемы сети предприятия (рисунок 2.5) к коммутатору 2 подключаются компьютеры виртуальных сетей VLAN 2, 5 и 6. Интерфейс fa0/24 конфигурируется в режиме магистрального.

К коммутатору 3 подключаются компьютеры виртуальных сетей VLAN 2, 3 и 4. Кроме этого, в состав VLAN 4 входит внутренний сервер рабочей группы. Интерфейс fa0/24 конфигурируются в режиме магистрального.

В пояснительной записке необходимо привести полные тексты сценариев конфигурации всех телекоммуникационных устройств.

Правильность создания и конфигурации коммутаторов осуществляется путем задания следующих команд:

```

show vlan;
show vtp status;
show interface;
show running-config.

```

2.9.2. Сценарий минимальной конфигурации маршрутизатора

Для проектируемой сети выбран маршрутизатор типа Cisco 2621 с IOS 12.4. В данном маршрутизаторе имеется два последовательных внешних интерфейса (WAN) Serial0/0 и Serial0/1, один из которых используем для подключения к Интернет-провайдеру, а также два внутренних порта FastEthernet 0/1 – 0/2. К внутренним портам подключаются корневой коммутатор 4 локальной сети и внешний сервер предприятия SvO.

-- Перевод маршрутизатора в привилегированный режим EXEC.

Router> enable

Router#

-- Вход в режим глобального конфигурирования.

Router#configure terminal

Router(config)#

-- Установка пароля входа через виртуальный терминал.

Router(config)#line console 0

Router(config)#password [наш пароль]

-- Вход в режим консоли.

Router(config)#login

Router(config)#exit

Router#wr mem

-- Присвоение имени Cisco2621 конфигурируемому маршрутизатору.

Router(config)#hostname Cisco2621

Cisco2621(config)#

-- Установка пароля входа через Telnet.

-- Задание числа разрешенных сессий равное 5-ти (с 0-й по 4-ю).

Cisco2621(config)#line vty 0 4

Cisco2621(config)#password [наш пароль]

Cisco2621(config)#login

-- Разрешение функционирования SNMP, для возможности получения

-- статистики.

Cisco2621(config)#snmp-server community community_name RO

-- Установка выданного провайдером глобального IP-адреса.

Cisco2621(config)# interface Serial0/1

Cisco2621(config-if)# ip address 83.221.169.36 255.255.255.0

-- Установка IP-адреса интерфейса маршрутизатора в локальной сети

-- (он же шлюз по умолчанию).

Cisco2621(config)# interface FastEthernet0/0

Cisco2621(config-if)# ip address 10.1.0.254 255.255.255.0

-- Конфигурация внутреннего интерфейса FastEthernet0/0, к которому

-- подключена вся сеть организации

Cisco2621(config)#interface FastEthernet0/0

Cisco2621(config-if)# no ip address

--

```

!-- Включение интерфейса.
Cisco2621(config-if)#no shutdown
!--
!-- Сохранение конфигурации.
Cisco2621(config-if)#exit
!--
!-- Создание подинтерфейса и настройка магистрали.
Cisco2621(config)#interface FastEthernet0/0.1
!--
!-- Задание режима инкапсуляции 802.1Q.
Cisco2621(config-subif)#encapsulation dot1Q 1 native
!--
!-- Присвоение подинтерфейсу fa0/0.1 IP адреса.
Cisco2621(config-subif)#ip address 10.1.1.20 255.255.255.0
Cisco2621(config-subif)# no shutdown
Cisco2621(config-subif)#exit
!--
!-- Выполнение аналогичных операций для настройки магистралей
!-- на подинтерфейсах fa0/0.2...fa0/0.7.
Cisco2621(config)#int fastEthernet 0/0.2
Cisco2621(config-subif)#encapsulation dot1Q 2
Cisco2621(config-subif)#ip address 10.1.2.20 255.255.255.0
Cisco2621(config-subif)# no shutdown
Cisco2621(config-subif)#exit
!-- . . . . .
Cisco2621(config)#int fastEthernet 0/0.7
Cisco2621(config-subif)#encapsulation dot1Q 7
Cisco2621(config-subif)#ip address 10.1.7.20 255.255.255.0
Cisco2621(config-subif)# no shutdown
Cisco2621(config-subif)#exit
!--
!-- Контроль состояния интерфейсов
Cisco2621#show int
!--
!-- Конфигурация интерфейса для подключения внешнего сервера
!-- Задание адреса интерфейсу внешнего сервера
Cisco2621#conf t
Cisco2621(config)#int fa0/1
Cisco2621(config-if)#ip address 10.1.0.254 255.255.255.0
!--
!-- Включение интерфейса
Cisco2621(config-if)#no shutdown
Cisco2621(config-if)#exit
Cisco2621(config)#exit
Cisco2621#
!--

```

```

!-- Конфигурация внешнего последовательного интерфейса
Cisco2621#conf t
Cisco2621(config)#int s0
!--
!-- Задание глобального IP-адреса и включение интерфейса
Cisco2621(config-if)#ip address 83.221.169.36 255.255.255.0
Cisco2621(config-if)#no shutdown
Cisco2621(config-if)#exit
Cisco2621(config)#exit
!--
!-- Задание тактовой частоты устройству с кабельным окончанием DCE
Cisco2621#conf t
Cisco2621(config)#int s0
Cisco2621(config-if)#clock rate 1000000
Cisco2621(config-if)#end
Cisco2621#

```

2.9.3. Конфигурирование списков доступа.

Предположим, что политикой доступа в сети данной организации определено, что пользователям сети запрещается доступ к компьютерам рабочей группы дирекции организации (директор, главный инженер, главный бухгалтер и др.), кроме персонала группы технической поддержки (администратор сети, инженеры). Согласно распределению адресов между рабочими группами (таблица 2.), компьютеры рабочей группы дирекции входят в виртуальную сеть с адресом 10.1.2.0/24, а виртуальная сеть рабочей группы технической поддержки имеет адрес 10.1.1.0/24.

Кроме этого, политикой безопасности установлено, что к внешнему серверу организации имеет право доступа клиенты всех рабочих групп, за исключением седьмой.

Реализация данной политики доступа осуществляется путем конфигурации на маршрутизаторе списков доступа.

```

!-- Запрет доступа к компьютерам группы управления (сеть 10.1.2.0), кроме
!-- персонала группы технической поддержки (сеть 10.1.1.0)
!--
!-- Задание расширенного списка доступа
Cisco2621#conf t
!--
!-- Разрешение доступа с виртуальной сети группы поддержки
Cisco2621(config)#access-list 102 permit ip 10.1.1.0 0.0.0.255 10.1.2.0
0.0.0.255
!--
!-- Неявный запрет для всех остальных пользователей
!--

```

```

!-- Привязка списка доступа к подинтерфейсу vlan 2
Cisco2621(config)#int fa0/0.2
Cisco2621(config-subif)#ip access-group 102 out
Cisco2621(config-subif)#exit
!--
!-- Запрет доступа к внешнему серверу пользователей 7-й рабочей группы
!-- (10.1.7.0), всем остальным пользователям сети организации доступ разрешен
!--
Cisco2621(config)#access-list 101 permit tcp any any
Cisco2621(config)#int fa0/1
Cisco2621(config-if)#ip access-group 101 out
Cisco2621(config-if)#exit
Cisco2621(config)#int fa0/1
Cisco2621(config-if)#no ip access-group 101 out
Cisco2621(config-if)#no access-list 101 permit tcp any any
Cisco2621(config)#no access-list 101 deny tcp 10.1.7.0 0.0.0.255 10.1.0.2
0.0.0.0
Cisco2621(config)#exit

!-- Контроль созданного списка доступа
Cisco2621#show access-list

```

Пусть пользоваться Интернетом разрешается сотрудникам, которые находятся в сетях 10.1.5.0 и 10.1.7.0, только в рабочие дни во время перерыва на обед, начало действия данного правила — с 1 июня 2011 г, окончание — не определено. При этом разрешается прохождение только TCP-пакетов, содержащие данные протокола HTTP.

Сотрудникам сети 10.1.2.0 выход в Интернет разрешается в рабочие дни с 7:00 до 22:00 и в выходные дни с 9:00 до 15:00.

В сети 10.1.6.0 установлен сервер с адресом 10.1.6.30, доступ к которому разрешен только для пользователей этой сети по рабочим дням с 8:00 до 17:00. Данное правило должно вступить в действие сразу и закончиться к концу года.

Для защиты от атак типа DDoS предусмотреть закрытие любого TCP-сессии, если он не установлен в течение 30 с.

Сценарий конфигурации маршрутизатора для указанных условий имеет следующий вид.

```

Cisco2621#conf t
Cisco2621(config)#ip access-list 101 permit tcp any any eq 80 time-range allow-
http
!-- Разрешение прохождения TCP пакетов, содержащих данные протокола HTTP,
!-- во всех направлениях.
Cisco2621(config)#interface FastEthernet0/0

    ip access-group 101 in

```

```
time-range allow-http
absolute start 00:01 1 June 2011
periodic weekdays 13:00 to 14:00
```

-- Назначение списка доступа интерфейсу FastEthernet0/0. Приведем пример конфигурации такого списка доступа:

```
interface FastEthernet0/0
ip access-group 102 in
time-range http-ok
absolute end 24:00 31 December 2001
periodic weekdays 08:00 to 17:00
!
ip access-list 102 permit tcp any host 140.11.12.10 eq 80 time-range http-ok
```

-- Закрытие любого TCP-сессии, не установленного в течение 30 секунд
!-- для защиты от flood-атаки SYN с отказом в обслуживании.

```
ip tcp synwait-time 30
```

2.9.4. Конфигурирование процедур трансляции адресов

Выбранный маршрутизатор типа Cisco2621 содержит два порта для подключения локальных сетей (FastEthernet0/0 и FastEthernet0/1) и один последовательный порт s0 для подключения к глобальной сети провайдера Интернет-услуг. Пусть данной организации выделен один глобальный (публичный) IP-адрес (83.221.169.36/24) для внешнего сервера, а также группа глобальных IP-адресов в диапазоне 83.221.169.37 – 83.221.169.40. Для преобразования частного адреса внешнего сервера в глобальный адрес маршрутизатор должен выполнять статическую трансляцию внутреннего адреса 10.1.0.30 сервера во внешний глобальный адрес 83.221.169.36/24. Предположим, что на маршрутизаторе используется протокол маршрутизации RIP.

```
-- Задание протокола маршрутизации
!--
Cisco2621#conf t
Cisco2621(config)#Cisco2621 rip
!--
!-- Указания адреса смежной сети
Cisco2621(config-Cisco2621)#network 83.221.169.0
Cisco2621(config-if)#exit
Cisco2621(config)#exit
!--
Cisco2621> enable
```

```

Cisco2621# configure terminal
Cisco2621 (config)# interface fastethernet 0/0
!--
!-- Указание на внутренний интерфейс
Cisco2621 (config-if)# ip nat inside
Cisco2621 (config-if)# exit
Cisco2621 (config)# interface serial0
!--
!-- Задание последовательного порта в качестве внешнего интерфейса
Cisco2621 (config-if)# ip nat outside
Cisco2621 (config-if)# exit
!--
!-- Задание соответствия локального адреса и глобального
Cisco2621 (config)# ip nat inside source static 10.1.0.2 83.221.169.36
Cisco2621 (config)# exit
!--
!-- Проверка правильности трансляции адреса осуществляется командой
Cisco2621#show ip nat translations
!--
!--
!-- Конфигурация процедуры динамического преобразования адресов
!--
Cisco2621#conf t
!--
!--Задание пула адресов
Cisco2621(config)#ip nat pool 7 83.221.169.37 83.221.169.40 netmask
255.255.255.0
!--
!-- Указание на преобразование адресов из списка 17 в пул адресов 7
Cisco2621(config)#ip nat inside source list 17 pool 7
!-- Создание списка доступа с номером 17, определяющий компьютеры,
!-- для которых разрешается выполнять трансляцию для внутренних адресов
Cisco2621(config)#access-list 17 permit 10.1.0.0 0.0.255.255
!--
!-- Задание последовательного порта в качестве внешнего интерфейса
Cisco2621(config)#int s0
Cisco2621(config-if)#ip nat outside
Cisco2621(config-if)#exit
!--
!-- Указание на внутренний интерфейс
Cisco2621(config)#int fa0/0
Cisco2621(config-if)#ip nat inside
Cisco2621(config)#exit

```

```
!--  
!-- Проверка правильности восприятия команд маршрутизатором  
Cisco2621#show ip nat tr  
Cisco2621 #Show access-list
```

Для сохранения созданной конфигурации маршрутизатора необходимо применить команду

```
Cisco2621# copy running-config startup-config
```

2.10. Компьютерное моделирование функционирования сети

2.10.1. Цели, задачи и особенности моделирования сети

Целью моделирования является проверка функционирования спроектированной компьютерной сети предприятия в соответствии с техническим заданием и корректности разработанных сценариев конфигурирования телекоммуникационного оборудования.

В процессе достижения поставленной цели должны быть решены следующие задачи:

- создания топологии спроектированной сети или ее фрагмента;
- назначение портов телекоммуникационного оборудования для подключения рабочих станций и серверов;
- соединение рабочих станций и серверов сети с портами соответствующего телекоммуникационного оборудования, а также телекоммуникационного оборудования между собой;
- создание виртуальных локальных сетей (Vlan) рабочих групп;
- задание IP-адресов и сетевых масок рабочим станциям и серверам;
- конфигурация коммутаторов и маршрутизатора;
- проверка доступности рабочих станций сети и степени изолированности виртуальных сетей;
- коррекция схемы сети и сценариев конфигурации (в случае необходимости) по результатам проверки функционирования спроектированной сети.

Особенность моделирования состоит в том, что в курсовом проекте, в случае громоздкости схемы спроектированной сети, по согласованию с руководителем проекта, осуществляется моделирование не всей сети, а ее базового фрагмента, в котором содержатся все принципиальные составные части спроектированной сети. Моделирование сети осуществляется в среде сетевого эмулятора Packet Tracer 6.0 или среде Boson версии 7.0 и выше. Для моделирования также возможно использование эмуляторов других типов, в частности OPNET или NetCracker Professional, .

В процессе моделирования вначале составляется упрощенная схема исследуемой сети. В создаваемую схему включаются те типы коммуникационных устройств, которые входят в спецификацию спроектированной сети. В случае отсутствия данного типа устройств в базе данных используемого эмулятора, по согласованию с руководителем проекта, разрешается включать в моделируемую схему коммуникационные устройства, которые по своим свойствам близки к отсутствующим образцам.

После создания топологии сети выполняется конфигурация интерфейсов коммуникационных устройств, формируются виртуальные сети, задаются сетевые адреса, инициируется процедура трансляции адресов и конфигурируются списки доступа. Затем выполняется тестирование сети путем пингования рабочих станций, серверов, просмотра и анализа трасс маршрутизации. Конфигурация сети

осуществляется на основе параметров, полученных в процессе выполнения этапов ее проектирования, освещенных в подразделах 2.7-2.9 данного пособия.

Ниже рассматривается пример моделирования компьютерной сети, топология и параметры которой изображены на рисунке 2.5. Для упрощения процедуры моделирования схема сети, исходная схема упрощается, в частности, уменьшается количество виртуальных сетей и количество рабочих станций в них (рисунок 2.6).

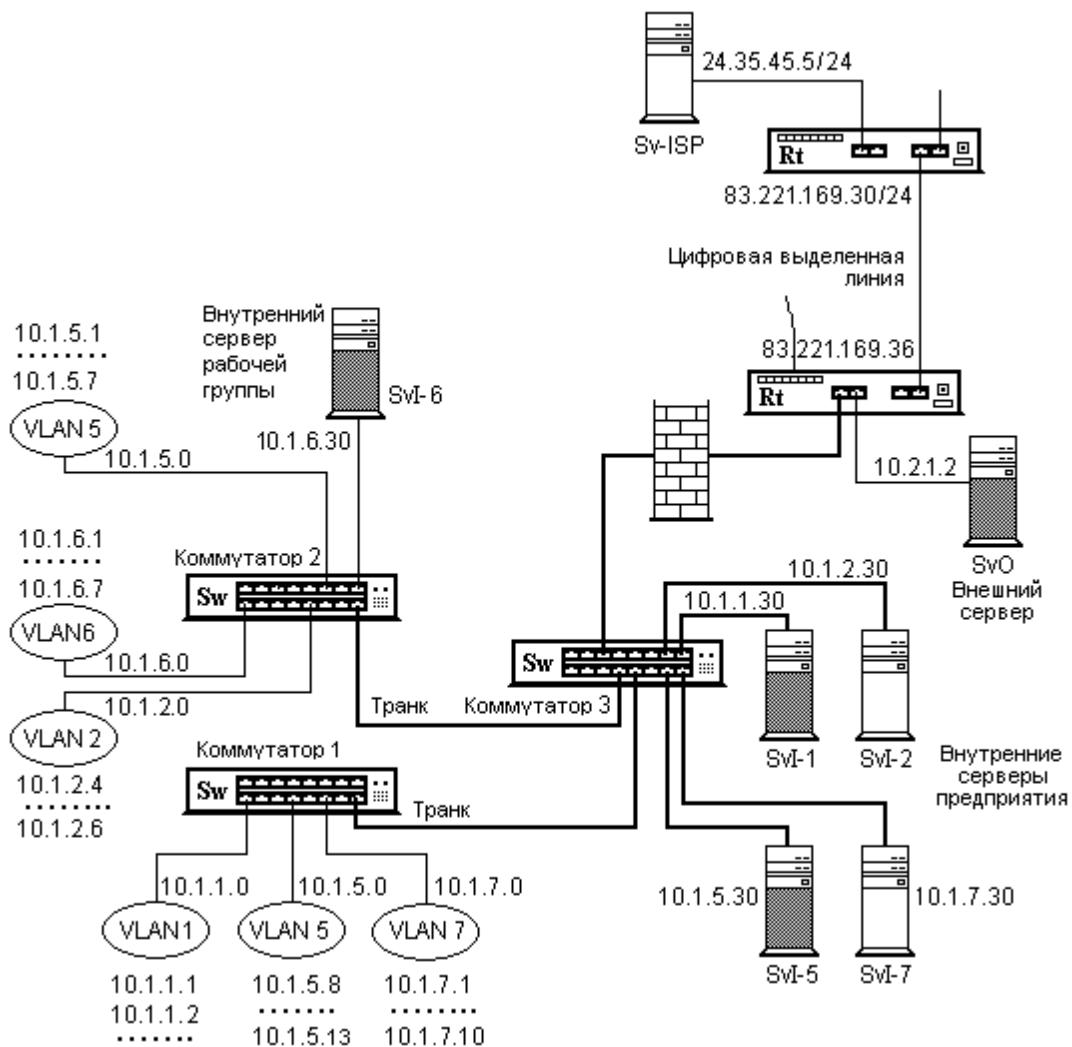


Рисунок 2.6 — Моделируемый фрагмент сети

Такое упрощение позволяет оценить работоспособность сети в целом, соответствие ее параметров техническому заданию и корректность конфигурации устройств, так как отсутствующие элементы имеют аналогичные связи между компонентами сети и сценарии конфигурации с моделируемыми фрагментами сети.

Данный фрагмент включает компьютеры пяти подсетей рабочих групп, каждая из которых представляет собой виртуальную локальную сеть (соответственно VLAN1, VLAN2, VLAN5, VLAN6 и VLAN7), логически отделенную от подсетей

других рабочих групп. Кроме рабочих станций в сети имеется сервер рабочей группы, входящий в пятую подсеть и внешний сервер предприятия.

2.10.2. Создание топологии сети в системе Packet Tracer

Для создания топологии моделируемой сети запускается Network Designer и в меню File выбирается New. При этом открывается новое рабочее окно дизайнера сети. Топология сети создается путем выбора из списка оборудования “Devices and Connectors” маршрутизатора соответствующего типа, нужных типов коммутаторов и рабочих станций и размещения их путем перетягивания с помощью мышки в рабочем поле окна конструктора. Затем распределяются порты коммутаторов по локальным сетям и осуществляется соединение рабочих станций с соответствующими портами коммутаторов, а также коммутаторов между собой и коммутатора с маршрутизатором. Вид созданной топологии сети изображен на рисунке 2.7.

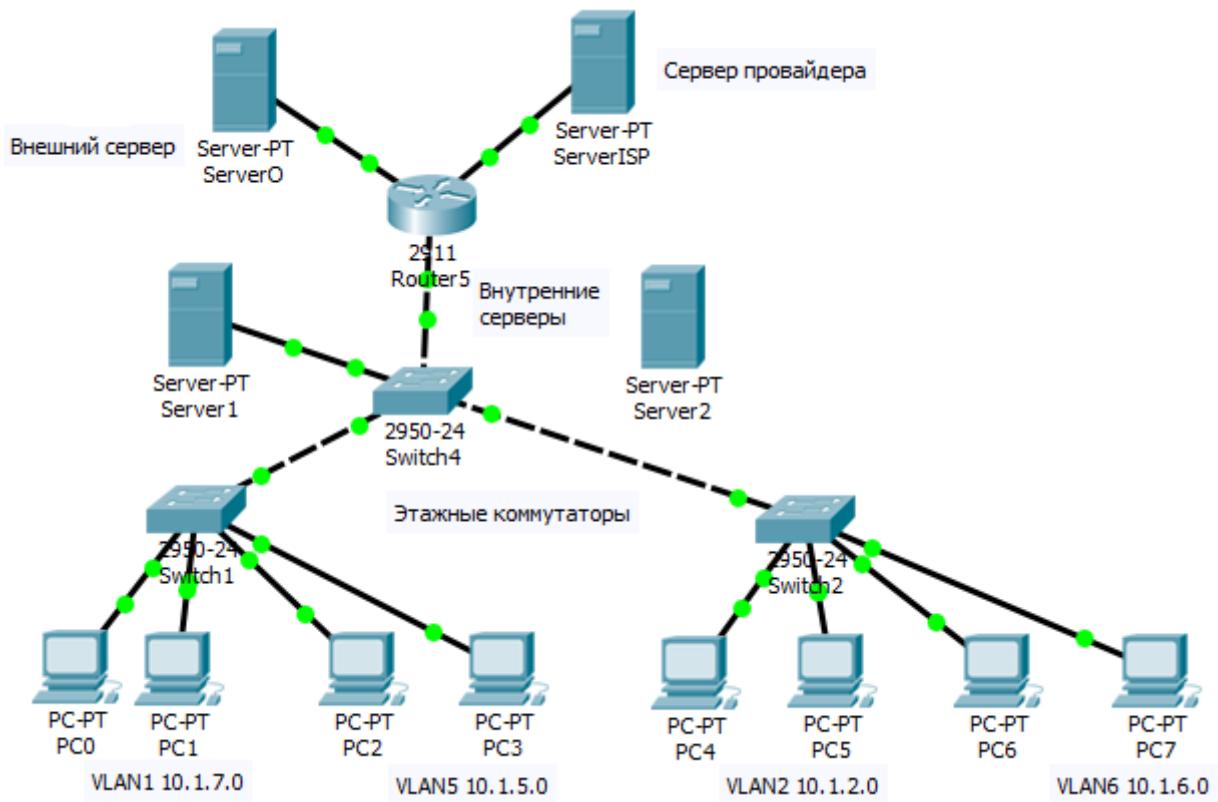


Рисунок 2.7 — Топология моделируемой компьютерной сети в окне Packet Tracer

Модель сети содержит два аналогичных 12-портовых сетевых коммутатора второго уровня типа Cisco Catalyst 2950 — Sw-1 и Sw-2. Все порты коммутаторов являются 100 мегабитовыми портами типа FastEthernet. В первый коммутатор

включены по две рабочих станции 1-й, 5-й и 7-й виртуальных сетей. Обозначение рабочей станции содержит две буквы РС и два цифровых символа. Первый из них отражает номер виртуальной сети, а второй — номер станции в соответствующей сети. Внутренний сервер рабочей группы обозначается символами SvI, а внешний — SvO. Ко второму коммутатору Sw-2 подсоединенны две станции сети VLAN2, две станции VLAN5 и сервер рабочей группы, входящий в эту же виртуальную сеть, а также две рабочих станции VLAN7.

В состав сети входит маршрутизатор типа Cisco-2621, располагающий двумя портами FastEthernet и одним последовательным портом S0. Последовательный порт через выделенную цифровую линию соединен с последовательным портом маршрутизатора провайдера сетевых услуг аналогичного типа. К порту FastEthernet маршрутизатора внешней сети подключен сервер провайдера Sv-ISP.

После создания топологии сети она сохраняется в файле топологии с произвольным именем и расширением *.top. На схеме топологии моделируемой сети, для облегчения ее понимания, отмечены номера портов, через которые выполнено подключение рабочих станций, серверов, а также осуществляется связь коммуникационного оборудования между собой.

Символы в обозначениях портов (fa0/1 и др.) отображают тип интерфейса (FastEthernet), номер модуля и номер порта в соответствующем модуле. Для обозначения последовательного порта маршрутизатора, служащего для соединения его с внешней сетью, используется символ S0.

2.10.3. Конфигурирование и моделирование функционирования локальной сети

Топология конфигурируемой сети изображена на рисунке 2.5. Для упрощения конфигурации и администрирования сети используем VTP режим. Конфигурация осуществляется поэтапно, начиная с создания виртуальных сетей. Для избегания ошибок периодически будет проводиться проверка созданной топологии путем использования команд show и контрольного пингования участков создаваемой сети. Конфигурацию начнем с корневого коммутатора Sw-3.

Конфигурация корневого коммутатора 3. В коммутаторе используется 4 порта в режиме доступа и три в магистральном (транковом) режиме.

```

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Cat2650-3
Cat2650-3(config)#exit
Cat2650-3#vlan database
Cat2650-3(vlan)#vtp server

!-- Задание имени vtp домена

```

```
Cat2650-3(vlan)#vtp domain Victoria
Changing VTP domain from NULL to victoria
Cat2650-3(vlan)#exit
APPLY completed.
Exiting....
```

Проверка статуса коммутатора и режима работы.

```
Cat2650-3#show vtp status
```

VTP Version	:	2
Configuration Revision	:	2
Maximum VLANs supported locally	:	64
Number of existing VLANs	:	5
VTP Operating Mode	:	Server
VTP Domain Name	:	victoria
VTP Pruning Mode	:	Disabled
VTP V2 Mode	:	Disabled
VTP Traps Generation	:	Disabled
MD5 digest	:	0xEE 0xB3 0xDC 0x9F 0xE2 0xE0 0x25 0xDF
Configuration last modified by 0.0.0.0 at 3-1-93 04:55:57		
Local updater ID is 0.0.0.0 (no valid interface found)		

Из представленного сообщения видно, что коммутатор находится в статусе сервера и входит в домен victoria

```
!--
!-- Создание VLAN-сетей на коммутаторе, которые имеются в
!-- спроектированной сети, с учетом того, что сеть VLAN1 существует
!-- по умолчанию и ей принадлежат все порты
```

```
Cat2650-3#vlan database
Cat2650-3(vlan)#vlan 2
VLAN 2 added:
  Name:VLAN0002
Cat2650-3(vlan)#vlan 5
VLAN 5 added:
  Name:VLAN0005
Cat2650-3(vlan)#vlan 6
VLAN 6 added:
  Name:VLAN0006
Cat2650-3(vlan)#vlan 7
VLAN 7 added:
  Name:VLAN0007
Cat2650-3(vlan)#exit
APPLY completed.
```

Exiting....

!--

!-- Контроль созданных виртуальных сетей

Cat2650-3#show vlan

VLAN	Name	Status	Ports						
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12						
2	VLAN0002	active							
5	VLAN0005	active							
6	VLAN0006	active							
7	VLAN0007	active							
1002	fdmi-default	active							
1003	token-ring-default	active							
1004	fdmnet-default	active							
1005	trnet-default	active							
VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1
1	enet	100001	1500	-	-	-	-	-	0
7	enet	100007	1500	-	-	-	-	-	0
5	enet	100005	1500	-	-	-	-	-	0
2	enet	100002	1500	-	-	-	-	-	0
6	enet	100006	1500	-	-	-	-	-	0
1002	fdmi	101002	1500	-	-	-	-	-	0
1003	tr	101003	1500	-	-	-	-	-	0
1004	fdmnet	101004	1500	-	-	-	ieee	-	0
1005	trnet	101005	1500	-	-	-	ibm	-	0

!-- Задание режимов и назначение портов коммутатора для VLAN

Cat2650-3#conf t

!-- Задание портов доступа

Cat2650-3(config)#int fa0/2

Cat2650-3(config-if)#switchport access vlan 2

Cat2650-3(config-if)#exit

Cat2650-3(config)#int fa0/5

Cat2650-3(config-if)#switchport access vlan 5

Cat2650-3(config-if)#exit

Cat2650-3(config)#int fa0/7

Cat2650-3(config-if)#switchport access vlan 7

Cat2650-3(config-if)#exit

!-- Проверка задания портов доступа виртуальным сетям

Cat2650-3#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1,Fa0/3,Fa0/4,Fa0/6,Fa0/8, Fa0/9, Fa0/10, Fa0/11,Fa0/12

2	VLAN0002	active	Fa0/2
5	VLAN0005	active	Fa0/5
6	VLAN0006	active	
7	VLAN0007	active	Fa0/7
1002	fdci-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1
1	enet	100001	1500	-	-	-	-	-	0
2	enet	100002	1500	-	-	-	-	-	0
5	enet	100005	1500	-	-	-	-	-	0
6	enet	100006	1500	-	-	-	-	-	0
7	enet	100007	1500	-	-	-	-	-	0
1002	fdci	101002	1500	-	-	-	-	-	0

Проверка показывает, что все виртуальные сети созданы, порты доступа по виртуальным сетям распределены верно.

-- Задание магистральных портов

```
Cat2650-3#conf t
Cat2650-3(config)#int fa0/10
Cat2650-3(config-if)#switchport mode trunk
Cat2650-3(config-if)#exit
```

```
Cat2650-3(config)#int fa0/11
Cat2650-3(config-if)#switchport mode trunk
Cat2650-3(config-if)#exit
Cat2650-3(config)#int fa0/12
Cat2650-3(config-if)#switchport mode trunk
Cat2650-3(config-if)#exit
Cat2650-3(config)#exit
```

-- Контроль состояния магистральных портов

```
Cat2650-3#show int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/10	on	802.1q	trunking	1
Port		Vlans allowed on trunk		
Fa0/10		1-4094		
Port		Vlans allowed and active in management domain		
Fa0/10		2,5,6,7		
Port		Vlans in spanning tree forwarding state and not pruned		
Fa0/10		2,5,6,7		

Port	Mode	Encapsulation	Status	Native vlan
Fa0/11	on	802.1q	trunking	1
Port		Vlans allowed on trunk		

Fa0/11	1-4094
Port	Vlans allowed and active in management domain
Fa0/11	2,5,6,7
Port	Vlans in spanning tree forwarding state and not pruned
Fa0/11	2,5,6,7

Port	Mode	Encapsulation	Status	Native vlan
Fa0/12	on	802.1q	trunking	1
Port	Vlans allowed on trunk			
Fa0/12	1-4094			
Port	Vlans allowed and active in management domain			
Fa0/12	2,5,6,7			
Port	Vlans in spanning tree forwarding state and not pruned			
Fa0/12	2,5,6,7			

Из этого сообщения следует, что порты Fa0/10 - Fa0/12 находятся в транковом (магистральном) режиме и во включенном состоянии. Поддерживается протокол инкапсуляции 802.1q.

Конфигурация коммутатора 1

```

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Cat2950-1
Cat2950-1(config)#exit
Cat2950-1#vlan database
Cat2950-1(vlan)#vtp client
Cat2950-1(vlan)#vtp domain Victoria
Changing VTP domain from NULL to victoria
Cat2950-1(vlan)#exit
APPLY completed.
Exiting....
```

```
Cat2950-1#show vtp status
```

```

VTP Version : 2
Configuration Revision : 2
Maximum VLANs supported locally : 64
Number of existing VLANs : 9
VTP Operating Mode : Client
VTP Domain Name : victoria
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xEE 0xB3 0xDC 0x9F 0xE2 0xE0 0x25 0xDF
Configuration last modified by 0.0.0.0 at 3-1-93 04:55:57
```

Local updater ID is 0.0.0.0 (no valid interface found)

Из этого сообщения можно убедиться, что коммутатор переключился в клиентский режим и принадлежит домену *victoria*.

Продолжаем конфигурацию магистральных портов и портов доступа коммутатора. По окончании конфигурации осуществляем проверку правильности заданных предписаний.

```
Cat2950-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cat2950-1(config)#int fa0/12
Cat2950-1(config-if)#switchport mode trunk
Cat2950-1(config-if)#exit
Cat2950-1(config)#int fa0/5
Cat2950-1(config-if)#switchport access vlan 5
Cat2950-1(config-if)#int fa0/6
Cat2950-1(config-if)#switchport access vlan 5
Cat2950-1(config-if)#exit
Cat2950-1(config)#int range fa0/7-8
Cat2950-1(config-if-range)#switchport access vlan 7
Cat2950-1(config-if-range)#end
Cat2950-1#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/9, Fa0/10, Fa0/11, Fa0/12
2	VLAN0002	active	
5	VLAN0005	active	Fa0/5, Fa0/6
6	VLAN0006	active	
7	VLAN0007	active	Fa0/7, Fa0/8
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	Bridg- eNo	Stp	BrdgMode	Trans1
1	enet	100001	1500	-	-	-	-	-	0
2	enet	100002	1500	-	-	-	-	-	0
5	enet	100005	1500	-	-	-	-	-	0
6	enet	100006	1500	-	-	-	-	-	0
7	enet	100007	1500	-	-	-	-	-	0
1002	fddi	101002	1500	-	-	-	-	-	0
1003	tr	101003	1500	-	-	-	-	-	0

Контроль созданных виртуальных сетей показал, что все порты распределены по VLAN верно.

Конфигурация коммутатора 2. Конфигурация данного коммутатора выполняется аналогично вышеизложенной процедуре.

```

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname Cat2950-2
Cat2950-2(config)#exit
Cat2950-2#vlan database
Cat2950-2(vlan)#vtp client
Cat2950-2(vlan)#vtp domain Victoria
Changing VTP domain from NULL to victoria
Cat2950-2(vlan)#exit
APPLY completed.
Exiting....
Cat2950-2#show vtp status

Cat2950-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.

Cat2950-2(config)#int fa0/12
Cat2950-2(config-if)#switchport mode trunk
Cat2950-2(config-if)#exit ^Z
%SYS-5-CONFIG_I: Configured from console by console

Cat2950-2#show vlan

```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12
2	VLAN0002	active	
5	VLAN0005	active	
6	VLAN0006	active	
7	VLAN0007	active	
1002	fdci-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Из таблицы видно, что в процессе реализации протокола VTP на коммутаторе активированы все виртуальные сети, объявленные на сервере.

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1
1	enet	100001	1500	-	-	-	-	-	0
5	enet	100005	1500	-	-	-	-	-	0
2	enet	100002	1500	-	-	-	-	-	0

6	enet	100006	1500	-	-	-	-	-	0
7	enet	100007	1500	-	-	-	-	-	0
1002	fddi	101002	1500	-	-	-	-	-	0
1003	tr	101003	1500	-	-	-	-	-	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0
1005	trnet	101005	1500	-	-	-	ibm	-	0

```
Cat2950-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.

Cat2950-2(config)#int range fa0/2-3
Cat2950-2(config-if-range)#switchport access vlan 2
Cat2950-2(config-if-range)#exit
Cat2950-2(config)#int fa0/5
Cat2950-2(config-if)#switchport access vlan 5
Cat2950-2(config-if)#exit
Cat2950-2(config)#int range fa0/6-8
Cat2950-2(config-if-range)#switchport access vlan 6
Cat2950-2(config-if-range)#end
Cat2950-2#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/4, Fa0/9, Fa0/10, Fa0/11, Fa0/12
2	VLAN0002	active	Fa0/2, Fa0/3
5	VLAN0005	active	Fa0/5
6	VLAN0006	active	Fa0/6, Fa0/7, Fa0/8
7	VLAN0007	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Контроль созданных виртуальных сетей показал, что все порты распределены по VLAN верно.

Конфигурация маршрутизатора локальной сети Rt-2621.

```
Router>
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname Rt-2621
Rt-2621(config)#int fa0/0
```

```
!-- Включение интерфейса
Rt-2621(config-if)#no shutdown
```

%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

-- Конфигурация подинтерфейсов с заданием вида инкапсуляции и IP адресов
!-- с целью обеспечения возможности взаимодействия между виртуальными
!-- сетями на третьем уровне.

```
Rt-2621(config-if)#exit
Rt-2621(config)#int fa0/0.2
Rt-2621(config-subif)#encapsulation dot1q 2
Rt-2621(config-subif)#ip address 10.1.2.254 255.255.255.0
Rt-2621(config-subif)#exit
Rt-2621(config)#int fa0/0.5
Rt-2621(config-subif)#encapsulation dot1q 5
Rt-2621(config-subif)#ip address 10.1.5.254 255.255.255.0
Rt-2621(config-subif)#exit
Rt-2621(config)#int fa0/0.6
Rt-2621(config-subif)#encapsulation dot1q 6
Rt-2621(config-subif)#ip address 10.1.6.254 255.255.255.0
Rt-2621(config-subif)#exit
Rt-2621(config)#int fa0/0.7
Rt-2621(config-subif)#encapsulation dot1q 7
Rt-2621(config-subif)#ip address 10.1.7.254 255.255.255.0
Rt-2621(config-subif)#exit
Rt-2621(config)#exit
```

-- Контроль состояния интерфейсов

Rt-2621#show int

-- Задание адреса интерфейсу внешнего сервера

```
Rt-2621#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Rt-2621(config)#int fa0/1
Rt-2621(config-if)#ip address 10.1.0.254 255.255.255.0
Rt-2621(config-if)#no shutdown
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Rt-2621(config-if)#exit
Rt-2621(config)#exit
Rt-2621#
```

-- Конфигурация внешнего последовательного интерфейса

```
Rt-2621#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Rt-2621(config)#int s0
```

-- Задание публичного IP адреса и включение интерфейса

```
Rt-2621(config-if)#ip address 83.221.169.36 255.255.255.0
Rt-2621(config-if)#no shutdown
```

```
%LINK-3-UPDOWN: Interface Serial0, changed state to up
%LINK-3-UPDOWN: Interface Serial0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
changed state to down
Rt-2621(config-if)#exit
Rt-2621(config)#exit
```

-- Интерфейс переключился в состояние down потому, что не указана тактовая
-- частота в звене данных DTE-DCE. Нужно определить, какая из сторон -- является терминальной частью (DTE), а какая коммуникационной
!-- (DCE)? Для этого применяется команда

```
Rt-2621#show controllers s0
HD unit 0, idb = 0x1AE828, driver structure at 0x1B4BA0
buffer size 1524 HD unit 0,V.35 DTE cable
Rt-ISP#show contr s0
HD unit 0, idb = 0x1AE828, driver structure at 0x1B4BA0
buffer size 1524 HD unit 0,V.35 DCE cable
```

-- При установлении соединения точка-точка одно из устройств (DCE) должно
!-- задавать тактовую частоту. Узнать допустимые значения этой частоты
!-- можно путем задания команды `clock rate ?`

```
Rt-ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Rt-ISP(config)#int s0
Rt-ISP(config-if)#clock rate ?
500000
148000
1200
2400
4800
9600
1000000
. . . .
1300000
2000000
4000000
```

-- Задание тактовой частоты устройству с кабельным окончанием DCE

```
Rt-ISP(config-if)#clock rate 1000000
Rt-ISP(config-if)#end
Rt-ISP#
Rt-2621#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Rt-2621(config)#int fa0/1
```

```
Rt-2621(config-if)#ip nat inside source static 10.1.0.2
83.221.169.36
Rt-2621(config-if)#exit
```

```
!-- Задание процедуры трансляции адресов
Rt-2621(config)#int s0
Rt-2621(config-if)#ip nat outside
Rt-2621(config-if)#exit
Rt-2621(config)#exit
```

```
!-- Контроль таблицы трансляции адреса
Rt-2621#show ip nat translation
```

Pro	Inside global	Inside local	Outside local	Outside global
---	83.221.169.36	10.1.0.2	---	---

Проверка трансляции свидетельствует, что преобразование адресов осуществляется верно.

Конфигурация маршрутизатора Интернет-провайдера

```
Rt-ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Rt-ISP(config)#router rip
Rt-ISP(config-router)#network 25.35.45.0
Rt-ISP(config-router)#network 83.221.169.0
Rt-ISP(config-router)#exit
```

```
Rt-2621#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Rt-2621(config)#router rip
Rt-2621(config-router)#network 83.221.169.0
Rt-2621(config-if)#exit
Rt-2621(config)#exit
```

```
Rt-2621#ping 83.221.169.30
```

Конфигурация списков доступа на маршрутизаторе Rt-2621

```
Rt-2621(config)#ip nat inside source list1 int fa0/0 overload ?
Rt-2621(config)#ip nat inside source list 1 interface s0 overload ?
Rt-2621(config)#int s0
Rt-2621(config-if)#ip nat outside
Rt-2621(config-if)#exit
Rt-2621(config)#int fa0/0
```

```
Rt-2621(config-if)#ip nat inside
Rt-2621(config-if)#exit
Rt-2621(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Rt-2621(config)#exit
!
!-- Проверяем созданные vlan и связанные с ними порты коммутатора
Sw-1#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/9, Fa0/10, Fa0/11, Fa0/12
2	VLAN0002	active	
5	VLAN0005	active	Fa0/5, Fa0/6
6	VLAN0006	active	
7	VLAN0007	active	Fa0/7, Fa0/8
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1
1	enet	100001	1500	-	-	-	-	-	0
7	enet	100007	1500	-	-	-	-	-	0
5	enet	100005	1500	-	-	-	-	-	0
2	enet	100002	1500	-	-	-	-	-	0
6	enet	100006	1500	-	-	-	-	-	0
1002	fddi	101002	1500	-	-	-	-	-	0
1003	tr	101003	1500	-	-	-	-	-	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0
1005	trnet	101005	1500	-	-	-	ibm	-	0

Открываем в эмуляторе окно eStations и выбираем рабочую станцию PC1-1.
Присвоим IP–адрес и сетевую маску станции, а также адрес шлюза по умолчанию.

```
Press Enter to begin
C:>
C:>ipconfig /ip 10.1.1.1 255.255.255.0
C:>ipconfig /dg 10.1.1.11
!
! Просмотр созданной конфигурации
!
C:>ipconfig
    Ethernet adapter Local Area Connection:
        IP Address. . . . . : 10.1.1.1
        Subnet Mask . . . . . : 255.255.255.0
        Default Gateway.... . . . . . : 10.1.1.11
```

Аналогичным образом конфигурируем все рабочие станции, включенные в данный коммутатор.

Проверим возможность связи рабочих станций внутри виртуальных сетей, а также логическую изоляцию виртуальных сетей. Для этого воспользуемся процедурой пингования рабочих станций. Пропингуем с PC1-2 рабочие станции PC1-1, PC5-5 и PC7-2. В среде эмулятора это выглядит следующим образом:

```
C:>ping 10.1.1.1
```

```
Pinging 10.1.1.1 with 32 bytes of data:
```

```
Reply from 10.1.1.1: bytes=32 time=60ms TTL=241
```

```
Ping statistics for 10.1.1.1: Packets: Sent =5,
```

```
Received =5, Lost =0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 50 ms, Maximum = 60 ms, Average = 55 ms
```

```
C:>ping 10.1.5.5
```

```
Pinging 10.1.5.5 with 32 bytes of data:
```

```
Request timed out.
```

```
Ping statistics for 10.1.5.5:
```

```
Packets: Sent = 5, Received = 0, Lost = 5 (100% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0 ms, Maximum = 0 ms, Average = 0 ms
```

```
C:>ping 10.1.7.2
```

```
Pinging 10.1.7.2 with 32 bytes of data:
```

```
Request timed out.
```

```
Ping statistics for 10.1.7.2:
```

```
Packets: Sent = 5, Received = 0, Lost = 5 (100% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0 ms, Maximum = 0 ms, Average = 0 ms.
```

Аналогичные действия выполняем для всех рабочих станций виртуальных сетей, включенных в коммутатор.

На основании проведенных исследований можно сделать вывод, что связь между компьютерами внутри виртуальных сетей существует, а передать пакеты в станции других *vlan* не возможно, так как они логически изолированы друг от друга.

Если же тестовые пакеты проходят в другие *vlan*, то необходимо еще раз проверить правильность назначения портов в виртуальные сети и, при наличии ошибки, скорректировать конфигурацию. Далее выполняем конфигурацию маршрутизатора.

Выполним конфигурацию маршрутизатора для обеспечения взаимодействия на сетевом уровне между виртуальными сетями

```

Router>
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#no shutdown
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
!--
Router(config)#int fa0/0.1
Router(config-subif)#encapsulation dot1q 1
Router(config-subif)#ip address 10.1.1.11 255.255.255.0
Router(config-subif)#int fa0/0.5
Router(config-subif)#encapsulation dot1q 5
Router(config-subif)#ip address 10.1.5.11 255.255.255.0
Router(config-subif)#exit
Router(config)#int fa0/0.7
Router(config-subif)#encapsulation dot1q 7
Router(config-subif)#ip address 10.1.7.11 255.255.255.0
Router(config)#int fa0/0.2
Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip address 10.1.2.11 255.255.255.0
Router(config-subif)#exit
Router(config)#exit
!
!-- Проконтролируем состояние интерфейсов и подинтерфейсов
!
Router#show ip int
Serial0 is administratively down, line protocol is down
  Internet protocol processing disabled
FastEthernet0/0 is up, line protocol is up
  Internet protocol processing disabled

```

```

FastEthernet0/0.1 is up, line protocol is up
  Internet address is 10.1.1.11/24
  Broadcast address is 255.255.255.0
  MTU 1500 bytes
:
:
FastEthernet0/0.7 is up, line protocol is up
  Internet address is 10.1.7.11/24
  Broadcast address is 255.255.255.0
  MTU 1500 bytes

```

Проверим возможность передачи пакетов между виртуальными сетями и связь с внешним сервером SvO, в частности, связь рабочей станции PC5-5 с внешним сервером SvO и PC7-1.

```

Ethernet adapter Local Area Connection:
  IP Address. . . . . : 10.1.5.5
  Subnet Mask . . . . . :: 255.255.255.0
  Default Gateway . . . . . : 10.1.5.11

C:>ping 10.1.0.12
Pinging 10.1.0.12 with 32 bytes of data:
Reply from 10.1.0.12: bytes=32 time=60ms TTL=241

Ping statistics for 10.1.0.12:  Packets: Sent = 5,
Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50 ms, Maximum = 60 ms, Average = 55 ms

C:>ping 10.1.7.2
Pinging 10.1.7.2 with 32 bytes of data:
Reply from 10.1.7.2: bytes=32 time=60ms TTL=241

Ping statistics for 10.1.7.2:  Packets: Sent = 5,
Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50 ms, Maximum = 60 ms, Average = 55 ms

```

Как видно из результатов эксперимента, подключение виртуальных сетей к маршрутизатору позволяет осуществлять обмен между хостами различных виртуальных сетей.

Аналогичным образом выполняется конфигурация коммутатора Sw-2 и проверка правильности задания параметров конфигурации. В пояснительной записи необходимо привести тексты сценариев конфигурации всех устройств, входящих в состав моделируемой сети.

2.10.4. Тестирование сети и коррекция схемы по результатам моделирования

Проверим функционирование спроектированной сети в целом. Для этого выполним процедуру пингования с рабочих станций, включенных в виртуальные сети, относящихся ко второму коммутатору. Проведем пингование с первой рабочей станции PC6-1 шестой vlan.

Ethernet adapter Local Area Connection:

```
IP Address . . . . . : 10.1.6.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.1.6.11
```

!-- Пингование станции собственной vlan.

```
C:>ping 10.1.6.2
Pinging 10.1.6.2 with 32 bytes of data:
Reply from 10.1.6.2: bytes=32 time=60ms TTL=241

Ping statistics for 10.1.6.2: Packets: Sent = 5,
Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50 ms, Maximum = 60 ms, Average = 55 ms
```

!-- Пингование интерфейса шлюза по умолчанию.

```
C:>ping 10.1.6.11
Pinging 10.1.6.11 with 32 bytes of data:
Reply from 10.1.6.11: bytes=32 time=60ms TTL=241
```

```
Ping statistics for 10.1.6.11: Packets: Sent = 5,
Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50 ms, Maximum = 60 ms, Average = 55 ms
```

-- Пингование внешнего сервера предприятия

```
C:>ping 10.1.0.12
Pinging 10.1.0.12 with 32 bytes of data:
```

```
Reply from 10.1.0.12: bytes=32 time=60ms TTL=241
```

Пингование шлюза по умолчанию и сервера предприятия показало, что эти устройства достижимы. Следовательно, схема сети составлена корректно, а конфигурация устройств выполнена верно.

Аналогичное тестирование следует провести со всех рабочих станций и серверов. После проведения тестирования всех возможных интерфейсов спроектированной сети можно сделать вывод, что сеть функционирует корректно, либо необходимо провести коррекцию конфигурации или подключения рабочих станций к коммутаторам.

Конфигурация списков доступа.

```
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 10 permit 10.1.1.0 0.0.0.255
Router(config)#access-list 10 deny 10.1.0.0 0.0.255.255
Router(config)#int fa0/0.2
Router(config-subif)#ip access-group 10 out
Router(config-subif)#exit
Router(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
Router#show access-list 10
Standard IP access list 10
    10 permit 10.1.1.0 0.0.0.255 (0 matches)
    10 deny   10.1.0.0 0.0.255.255 (20 matches)
```

Проверка доступа к сети 10.1.2.0. Пингование выполняется с рабочей станции PC5-1 с IP-адресом 10.1.5.1

```
C:>ping 10.1.5.5
Pinging 10.1.5.5 with 32 bytes of data:
```

```
Reply from 10.1.5.5: bytes=32 time=60ms TTL=241
```

```
Ping statistics for 10.1.5.5:    Packets: Sent = 5,
Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50 ms, Maximum = 60 ms, Average = 55 ms
```

C:>ping 10.1.1.1

```
Pinging 10.1.1.1 with 32 bytes of data:
```

```
Reply from 10.1.1.1: bytes=32 time=60ms TTL=241
```

```
Ping statistics for 10.1.1.1:    Packets: Sent = 5,
Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50 ms, Maximum = 60 ms, Average = 55 ms
```

C:>ping 10.1.2.1

```
Pinging 10.1.2.1 with 32 bytes of data:
```

```
Request timed out.
```

```
Ping statistics for 10.1.2.1:
Packets: Sent = 5, Received = 0, Lost = 5 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0 ms, Maximum = 0 ms, Average = 0 ms
```

Тестирование спроектированной сети прошло успешно.

Заключение

В заключительной части записи отмечается, что параметры спроектированной сети полностью соответствуют техническому заданию, а результаты компьютерного моделирования функционирования сети подтверждают ее работоспособность. Отмечается также, что спроектированная сеть рассчитана на такое-то количество рабочих мест, содержит такое-то современное телекоммуникационное оборудование, которое позволит эксплуатировать сеть в течение 10 лет без существенной модернизации аппаратной части.

Библиографический список

1. Александров К.К. Электротехнические чертежи и схемы / К.К. Александров, Е.Г. Кузьмина. — М.: Энергоатомиздат, 1990. — 288 с.
2. Амато В. Основы организации сетей Cisco. Том 1: Пер. с англ./ В.Амато. — М.: Изд-во "Вильямс", 2004. — 512 с.
3. Амато В. Основы организации сетей Cisco. Том 2. : Пер. с англ. / В.Амато.— М.: Изд-во "Вильямс", 2004. — 464 с.
4. Боллапрагада В. Структура операционной системы Cisco IOS: Пер. с англ. / В. Боллапрагада, К.Мэрфи, Р.Уайт: Пер. с англ. — М.: Изд-во "Вильямс", 2002. — 208 с.
5. Гук М. Аппаратные средства локальных сетей. Энциклопедия / М.Гук.- СПб.: Изд-во "Питер", 2000. — 576 с.
6. Кларк К. Принципы коммутации в локальных сетях Cisco: Пер. с англ. / К.Кларк, К. Гамильтон. — М.: Изд-во "Вильямс", 2003. — 976 с.
7. Кульгин М.В. Компьютерные сети. Практика построения. Для профессионалов / М.В. Кульгин. — СПб.: Изд-во "Питер", 2003.— 368 с.
8. Леинванд А. Конфигурирование маршрутизаторов Cisco: Пер. с англ. / А. Леинванд, Б. Пински. — М.: Изд-во "Вильямс", 2001. — 560 с.
9. Мамаев М. Технология защиты информации в Интернете. Специальный справочник / М.Мамаев, С.Петренко.- СПб.: Изд-во "Питер", 2002. — 848 с.
10. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд. / В.Г.Олифер, Н.А.Олифер. — СПб: Изд-во "Питер", 2005. — 864 с.
11. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство: Пер. с англ. — М.: Изд-во "Вильямс", 2005.— 1168 с.
12. Ретана А. Принципы проектирования корпоративных IP-сетей: Пер. с англ. / А. Ретана, Д. Слайс, Р. Уайт — М.: Изд-во "Вильямс", 2002. — 368 с.
13. Семенов А.Б. Структурированные кабельные системы / А.Б. Семенов, С.К. Стрижаков, И.Р. Сунчелей. — М.: Изд-во "Компьютер Пресс", 1999. — 387 с.
14. Семенов Ю.А. Телекоммуникационные технологии ГНЦ ИТЭФ. <http://www.book.iter.ru>
15. Столлингс В. Современные компьютерные сети: Пер. с англ. / В.Столлингс. — СПб.: Изд-во "Питер", 2003. — 783 с.
16. Столлингс В. Основы защиты сетей. Приложения и стандарты: Пер. с англ. / В.Столлингс.— М.: Изд-во "Вильямс", 2002. — 432 с.
17. Структура СКС. http://www.ecolan.ru/st_structure.htm#topology
18. Таненбаум Э. Компьютерные сети: Пер. с англ. / Э.Таненбаум .—СПб.: Изд-во "Питер", 2005. —672 с.
19. Техническая характеристика коммутаторов семейства Catalyst фирмы Cisco [<http://www.bkc.com.ua/product.asp?cid=1276>].

20. Хабракен Дж. Как работать с маршрутизаторами Cisco: Пер. с англ. / Дж. Хабракен. — М.: Изд-во ДМК Пресс, 2005. — 320 с.
21. Хелеби С. Принципы маршрутизации в Internet: Пер. с англ. / С.Хелеби, Д.Мак-Ферсон: Пер. с англ.— М.: Изд-во "Вильямс", 2001.— 448 с.
22. Хьюкаби Д. Руководство Cisco по конфигурированию коммутаторов Catalyst: Пер. с англ. / Д.Хьюкаби, С. Мак-Квери. — М.: Изд-во "Вильямс", 2004. — 560 с.
23. Чернега В.С. Компьютерные сети / В.Чернега, Б.Платтнер. — Севастополь: Изд-во СевНТУ, 2006. — 500 с.
24. Установка и настройка коммутаторов Cisco Catalyst серий 2900XL и 3500 [http://www.network.xsp.ru].
25. СКС малых и домашних офисов [http://www.ecolan.ru/midilan.htm]
26. Структурированные кабельные системы [http://www.bc-group.ru/si/service/scs.shtml]
27. Компьютерные сети и технологии [http://www.xnets.ru/plugins/content/content.php?cat.2]
28. ГОСТ 2.702-69. Правила выполнения электрических схем.
29. ГОСТ 21.614-88. Изображения условные графические электрооборудования и проводок на планах.
30. Cisco Certified Internetwork Expert. Учебное руководство / Д. Шварц, Т. Леммл: Пер. с англ.— М.: Изд-во "Лори", 2002.— 758 с.
31. Политики безопасности компании при работе в Internet. [www.compdoc.ru/network/internet/politicians_of_safety]
32. Политика безопасности ЛВС www.zahist.narod.ru/securelan4.htm
33. Инструкция пользователя компьютерной информационной сетью фирмы <http://www.zahist.narod.ru/instruct.htm>
34. Пример политики доступа
<http://www.cybercontrol.ru/resources/policy.html>

Приложение А1 - Таблица вариантов задания на курсовой проект

Приложение А1 - Таблица вариантов задания на курсовой проект

Номер варианта соответствует номеру студента в списке группы

Исходные данные на проектирование	Варианты								
	1	2	3	4	5	6	7	8	9
Расстояния между зданиями, км	-	-	-	-	-	-	-	-	-
Внутренних/внешних серверов в сети	2/1	4/1	4/2	3/2	2/2	4/1	5/2	2/3	4/3
Место подключения серверов: узел этажа (Э), здания (З), серверная ферма (СФ)	Э	Э	Э	Э	Э	З	З	З	СФ
Деление на VLAN	Да	Да	Да	Да	Да	Да	Да	Да	Да
Адрес шлюза по умолчанию: Приложение Б									
Вид связи с IP: Frame Relay (FR); ATM (A); ВОЛС(В); FastEthernet (FA)	В	А	FA	В	В	FA	А	FA	В
Способ адресации: Класс/ Бесклассовая	Б	Б	Б	К	Б	Б	Б	Б	К
Возможность расширения: Да/Нет	Да	Да	Да	Да	Да	Да	Да	Да	Да
Наличие резервирования	Да	Н	Да	Да	Н	Да	Н	Н	Да
Количество каналов с Интернет- провайдерами	2	1	2	2	1	2	1	1	1
Допустимая отказоустойчивость (время восстановления), сек	0,5	120	0,2	2	60	80	60	120	0,2
Наличие DMZ: Да/Нет	Да	Да	Да	Да	Да	Да	Да	Да	Да
Описание политики безопасности:									
удаленного доступа	+	+	+		+	+	+		+
взаимодействия с Интернет	+	+	+	+	+	+	+	+	+
правила предоставления доступа	+			+		+		+	+
выбора и использования паролей	+	+		+			+		+
инструкция по защите от виру- сов		+			+			+	