Содержание

[ВВЕДЕНИЕ 4](#_Toc325955061)

[ТЕХНИЧЕСКОЕ ЗАДАНИЕ 6](#_Toc325955062)

[1. Схема информационных потоков культурно-спортивного центра и расчет объема потоков между отделами 7](#_Toc325955063)

[1.2. Расчет объема потоков между отделами 8](#_Toc325955064)

[2. Схема информационных потоков с учетом серверов. 9](#_Toc325955065)

[2.1. Распределение трафика к серверам 14](#_Toc325955066)

[3. Проектирование структурной схемы корпоративной сети. 15](#_Toc325955067)

[4. Защита сети от несанкционированного доступа 16](#_Toc325955068)

[4.1. Обзор различных методов защиты информации 16](#_Toc325955069)

[4.1.1 Физическая зашита объектов информатизации от несанкционированного доступа 16](#_Toc325955070)

[4.1.2. Программные методы защиты 16](#_Toc325955071)

[4.2. Защита сети от внутреннего НСД 16](#_Toc325955072)

[4.2.1 Политика доступа. 16](#_Toc325955073)

[4.3 Защита от внешнего несанкционированного доступа 23](#_Toc325955074)

[4.3.1 Применение межсетевого экрана 23](#_Toc325955075)

[4.3.2 Аутентификации в Интернет 23](#_Toc325955076)

[Разграничим доступ к сети в зависимости от пользователя (см. таблицу 4.4) 24](#_Toc325955077)

[4.3.3 Теоретические основы SSH 24](#_Toc325955078)

[4.3.4 Теоретические основы SSL 27](#_Toc325955079)

[4.3.5. Реализация защиты данных с помощью протокола. 28](#_Toc325955080)

[5.Организация связи с филиалами. 29](#_Toc325955081)

[5.1. Краткий обзор технологии Metro Ethernet. 29](#_Toc325955082)

[5.1.1. Реализация связи с помощью Metro Ethernet. 31](#_Toc325955083)

[5.2. Краткий обзор технологии ISDN. 31](#_Toc325955084)

[5.2.1. Реализация связи с помощью ISDN. 33](#_Toc325955085)

[6.Распределение адресов рабочих станций с учётом структурной схемы. 34](#_Toc325955086)

[7.Выбор сетевых протоколов 36](#_Toc325955168)

[8. Выбор активного и пассивного оборудования 38](#_Toc325955169)

[8.1. Кабели 38](#_Toc325955170)

[8.1.1. Витая пара 38](#_Toc325955171)

[8.1.2. Волоконно-оптический кабель 38](#_Toc325955172)

[8.2. Выбор коммутаторов 40](#_Toc325955173)

[8.3. Выбор сетевых адаптеров 44](#_Toc325955249)

[8.4. Выбор маршрутизатора 45](#_Toc325955250)

[8.5. Выбор конфигурации серверов 46](#_Toc325955251)

[8.6. Выбор IP-телефонии 47](#_Toc325955252)

[8.7. Выбор IP-камер 48](#_Toc325955253)

[8.8. Выбор датчиков температуры и дыма. 49](#_Toc325955254)

[9.Выбор программного обеспечения. 50](#_Toc325955255)

[9.1. Выбор сетевой операционной системы 50](#_Toc325955256)

[9.2. Операционная система на рабочих станциях 50](#_Toc325955257)

[9.3. Система управления базами данных 50](#_Toc325955258)

[9.4. E-Mail – сервер 51](#_Toc325955259)

[9.5. Web – сервер 51](#_Toc325955260)

[9.6. Антивирусный сервер 52](#_Toc325955261)

[10.Разработка имитационной модели. 53](#_Toc325955262)

[10.1. Расчет задержки в каналах. 53](#_Toc325955263)

[10.2. Расчет задержки в коммутаторах. 53](#_Toc325955264)

[10.3. Расчет задержки на серверах и компьютерах. 54](#_Toc325955265)

[10.4. Расчет времени генерации. 55](#_Toc325955266)

[10.5. Результат и анализ моделирования. 56](#_Toc325955267)

[11.Разработка плана монтажной прокладки соединений сети и расположения сетевого оборудования в зданиях организации и разработка кабельных трасс между зданиями 58](#_Toc325955268)

[12.Смета разработки проекта сети 59](#_Toc325955269)

[ЗАКЛЮЧЕНИЕ. 60](#_Toc325955270)

[Приложение А 61](#_Toc325955271)

[Приложение Б 62](#_Toc325955272)

[Приложение В 69](#_Toc325955273)

[ПРИЛОЖЕНИЕ Г 75](#_Toc325955274)

[СПИСОК ЛИТЕРАТУРЫ. 79](#_Toc325955275)

ВВЕДЕНИЕ

Корпоративная сеть – это сеть, главным назначением которой является поддержание работы конкретного предприятия, владеющего данной сетью. Вопрос о том, что дает предприятию использование сетей, естественным образом порождает другие вопросы: в каких случаях развертывание на предприятии вычислительных сетей предпочтительнее использования автономных компьютеров или многомашинных систем? Какие новые возможности появляются на предприятии с появлением там вычислительной сети? И, наконец, всегда ли предприятию нужна сеть?

Концептуальным преимуществом сетей, которое вытекает из их принадлежности к распределенным системам, перед автономно работающими компьютерами является их *способность выполнять параллельные вычисления*. За счет этого может быть достигнута производительность, превышающая максимально возможную на данный момент производительность любого отдельного, сколь угодно мощного процессора.

Еще одно достоинство распределенных систем – это их принципиально более *высокая отказоустойчивость*. Основой повышенной отказоустойчивости является избыточность. Избыточность обрабатывающих узлов позволяет при отказе одного узла переназначать приписанные ему задачи на другие узлы.

Использование территориально распределенных вычислительных систем больше соответствует *распределенному характеру прикладных задач* в некоторых предметных областях. Во всех этих случаях имеются рассредоточенные по некоторой территории отдельные потребители информации – сотрудники, организации или технологические установки. Эти потребители автономно решают свои задачи, поэтому рациональнее предоставлять им собственные вычислительные средства, но в то же время, поскольку решаемые ими задачи логически тесно связаны, их вычислительные средства должны быть объединены в единую систему. Адекватным решением в такой ситуации является использование вычислительной сети.

Для пользователя распределенные системы дают еще, кроме выше названных, и такие преимущества, как *возможность совместного использования данных и устройств*, а также возможность гибкого распределения работ по всей системе. Подобное разделение дорогостоящих периферийных устройств, таких как дисковые массивы большой емкости, цветные принтеры, графопостроители, модемы, оптические диски, во многих случаях является основной причиной развертывания сети на предприятии.

В последнее время стал преобладать другой побудительный мотив развертывания сетей, гораздо более важный в современных условиях, чем экономия средств за счет разделения между сотрудниками корпорации дорогой аппаратуры или программ. Этим мотивом стало стремление обеспечить сотрудникам *оперативный доступ к обширной корпоративной информации*. В условиях жесткой конкурентной борьбы в любом секторе рынка выигрывает, в конечном счете, та компания, сотрудники которой могут быстро и правильно ответить на любой вопрос клиента – о возможностях их продукции, об условиях ее применения, о решении любых возможных проблем и т.п.

Наличие сети приводит к совершенствованию коммуникаций между сотрудниками предприятия, а также его клиентами и поставщиками. Сети снижают потребность предприятий в других формах передачи информации, таких как телефон или обычная почта. Все большее распространение получают новые технологии, позволяющие передавать по сетевым каналам связи не только компьютерные данные, но голосовую и видеоинформацию. Корпоративная сеть, которая интегрирует данные и мультимедийную информацию, может использоваться для организации аудио- и видеоконференций, кроме того, на ее основе может быть создана собственная внутренняя телефонная сеть.

Конечно, вычислительным сетям присущи и свои проблемы. Эти проблемы в основном связаны с организацией эффективного взаимодействия отдельных частей распределенной системы.

Во-первых, это сложности, связанные с программным обеспечением – операционными системами и приложениями. Сетевая операционная система, выполняя в общем случае все функции по управлению локальными ресурсами компьютера, сверх того решает многочисленные задачи по предоставлению сетевых сервисов. Много забот доставляет обеспечение совместимости программного обеспечения, устанавливаемого в узлах сети.

Во-вторых, много проблем связано с транспортировкой сообщений по каналам связи между компьютерами. Основные задачи здесь - обеспечение надежности и производительности.

В-третьих, это вопросы, связанные с обеспечением безопасности, которые гораздо сложнее решаются в вычислительной сети, чем в автономно работающем компьютере.

Можно приводить еще много «за» и «против» использования сетей, но главным доказательством эффективности является бесспорный факт их повсеместного распространения.

Для культурно-спортивного центра введение сети актуально, т.к. уже имеется большое количество различных данных в электронном формате, например, различные базы данных. Очень удобно сделать работу с этими источниками доступной для всех пользователей сети, кроме того, так как эти данные быстро меняются и пополняются нужно, чтобы каждый пользователь имел доступ к наиболее полной и современной версии данных. Все это достаточно легко решается при создании сетевой базы данных.

Для клиентов культурно-спортивного центра было бы очень удобно иметь возможность узнать о том, когда и какие мероприятия будет проводить культурно-спортивный центр, есть ли на него билеты и т.д.

# ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Спроектировать корпоративную сеть для автоматизации документооборота подсистемы сбыта производственного предприятия. Предусматривается наличие филиала в данном городе, для которого обеспечивается удаленный доступ к сети, и удаленного филиала в другом городе.

Учесть организацию почтового сервера, WEB - сервера, PROXY - сервера, серверов баз данных, файл - серверов.

При проектировании необходимо учесть:

* Два семиэтажных здания - 10х150;
* Расстояние между зданиями 150м;
* Высота этажей, подвалов, чердаков и колодцев: 3м.
* Количество обслуживаемых рабочих станций около 80;
* Наличие филиала в данном городе;
* Наличие филиала в другом городе;
* Обеспечение выхода в Интернет;
* Обеспечение защиты от НСД.
* Наличие логических серверов:

- web – сервер;

- почтовый сервер;

- proxy – сервер;

- file – сервер;

- PDC(первичный контроллер домена);

- BDC(вторичный контроллер домена);

- сервера баз данных;

- сервер приложений;

- Call-менеджер;

- print – сервер;

- Exchange сервер;

- Видеосервер;

# 1. Схема информационных потоков культурно-спортивного центра и расчет объема потоков между отделами

Имеется несколько отделов культурно-спортивного центра, расположенных в нескольких зданиях и на нескольких этажах. Необходимо соединить их в общую локальную сеть, учитывая, что каждый сотрудник центра имеет рабочее место с ПК.

Культурно-спортивный центр состоит из следующих отделов:

1. Администрация (2 компьютера)
2. Бухгалтерия (8 компьютеров)
3. Отдел охраны (5 компьютеров)
4. Отдел технического обслуживания (11 компьютеров)
5. Отдел кадров (7 компьютеров)
6. IT отдел (3 компьютеров)
7. Отдел по проведению спортивных мероприятий (3 компьютеров)
8. Касса оплаты услуг (3 компьютеров)
9. Тренерский отдел (15 компьютеров)
10. Отдел маркетинга (15 компьютеров)
11. Филиал в городе
12. Филиал в другом городе

## 1.2. Расчет объема потоков между отделами

В таблице 1.1 представлен средний объем информации за один рабочий день (8 часов) в Мбайт.

Таблица 1.1.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Ф1 | Ф2 | Сумма исход. |
| 1 | 20 | 25 | 25 | 10 | 10 | 15 | - | - | - | - | 20 | 20 | 125 |
| 2 | 25 | 40 | 30 | 5 | 5 | - | - | - | - | - | - | - | 65 |
| 3 | 15 | 15 | 7 | 5 | 2 | - | 30 | 30 | 30 | 30 | 15 | 15 | 187 |
| 4 | 15 | 5 | 5 | 12 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 65 |
| 5 | 8 | 8 | 8 | 8 | 10 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 74 |
| 6 | 15 | - | 15 | 5 | 5 | 15 | - | - | - | - | - | - | 40 |
| 7 | - | - | 35 | 5 | 5 | 15 | 17 | 25 | 25 | 25 | 25 | 25 | 185 |
| 8 | - | - | 15 | 5 | 5 | - | 15 | 20 | - | - | - | 15 | 55 |
| 9 | - | - | 15 | 5 | 5 | - | 15 | - | 25 | - | - | - | 40 |
| 10 | - | - | 15 | 5 | 5 | - | 15 | - | - | 19 | - | - | 40 |
| Филиал1 | 15 | - | 8 | 5 | 5 | - | 15 | - | - | - | - | - | 48 |
| Филиал2 | 15 | - | 8 | 5 | 5 | - | 15 | 15 | - | - | - | - | 63 |
| Сумма вход. | 108 | 53 | 179 | 63 | 57 | 41 | 116 | 81 | 66 | 66 | 71 | 86 |  |
|  | 125 | 65 | 187 | 65 | 74 | 40 | 185 | 55 | 40 | 40 | 48 | 63 |  |
| Вход+исход | 233 | 118 | 366 | 128 | 131 | 81 | 301 | 136 | 106 | 106 | 119 | 149 |  |

Суммарная информационная нагрузка всех организационных связей центра в среднем составляет ИНΣmax=43909 бит/сек.

# 2. Схема информационных потоков с учетом серверов.

*Физический сервер* - это отдельно стоящая, физически доступная электронная вычислительная машина, выделенная для выполнения на ней сервисного программного обеспечения, которое предоставляет пользователю доступ к определённым ресурсам или услугам.

*Виртуальный сервер* - это не доступный физически электронный вычислительный раздел, созданный с помощью некоторой программы на физическом сервере.

*Клиенты* – компьютеры, использующие общие сетевые ресурсы, предоставляемые серверами.

**Типы сетей:**

*Сети на основе серверов (server-based)* – сети, в которых большинство компьютеров являются клиентами, а лишь немногие серверами. Сервер специально оптимизирован для быстрой обработки запросов. С увеличением объема трафика необходимо увеличивать число серверов и разделять их по функциональным признакам.

Преимущества сети на основе серверов: разделение ресурсов (централизовано), защита, резервное копирование, избыточность (redundancy), количество пользователей.

*Сеть с равноправными узлами (peer-to-peer)* – сети, в которых все компьютеры равноправны и являются как серверами, так и клиентами. Нет назначенных серверов. Пользователь компьютера решает сам, какие данные можно сделать общими. Нет выраженного администратора сети.

Преимущества сети с равноправными узлами: не требуется дополнительное обучение персонала, безопасность определяется в основном паролем на ресурс – отсутствие централизованного административного контроля, каждая рабочая станция должна иметь дополнительные ресурсы для поддержки удаленных пользователей.

**Определение логических серверов**

***Контроллер домена*** - главный компьютер в домене (т.е. локальной сети с иерархической структурой), которому "подчиняются" рабочие. Контроллер домена хранит данные о пользователях и компьютерах в домене и позволяет централизованно управлять ими.

*BDC (Backup Domain Controller)* - предназначен для хранения данных. При пропуске N-го числа репликаций, если PDC отказал, BDC занимает место PDC и работа продолжается.

Резервный контроллер BDC обеспечивает отказоустойчивость. Когда автономным серверам или рабочим станциям  необходимо подтверждение имени пользователя и пароля, они ищут доступный контроллер домена, независимо от того, PDC это или BDC. Следовательно, если PDC недоступен, но доступен BDC в режиме только для чтения,   использование ресурсов домена возможно. BDC сокращает время ответа при одновременной регистрации множества пользователей.

*PDC**(Primary Domain Controller)*– предназначен для хранения всех учетных записей.

Контроллеры доменов хранят данные каталога и управляют связью между пользователями и доменами, в том числе процессом регистрации пользователей, аутентификацией и поиском в каталоге. Контроллеры домена синхронизируют данные каталога, применяя множественную репликацию, гарантируя соответствие информации по прошествии времени.

*DNS (Domain Name System)* – это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.

Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес. Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет - то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос, либо передать его другому DNS-серверу. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов, для повышения надежности своей работы.

*DHCP (Dynamic Host Configuration Protocol).* – автоматизирует процесс назначения IP-адресов узлам сети.

Протокол DHCP работает в соответствии с моделью клиент-сервер. Во время старта системы компьютер, являющийся DHCP-клиентом, посылает в сеть широковещательный запрос на получение IP-адреса. DHCP-cepвер откликается и посылает сообщение-ответ, содержащее IP-адрес. Предполагается, что DHCP-клиент и DHCP-сервер находятся в одной IP-сети.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, называемое временем аренды, что дает возможность впоследствии повторно использовать этот IP-адрес для назначения другому компьютеру. Основное преимущество DHCP — автоматизация рутинной работы администратора по конфигурированию стека TCP/IP на каждом компьютере. Иногда динамическое разделение адресов позволяет строить IP-сеть, количество узлов в которой превышает количество имеющихся в распоряжении администратора IP-адресов.

DHCP обеспечивает надежный и простой способ конфигурации сети TCP/IP, гарантируя отсутствие дублирования адресов за счет централизованного управления их распределением. Администратор управляет процессом назначения адресов с помощью параметра «продолжительность аренды», которая определяет, как долго компьютер может использовать назначенный IP-адрес, перед тем как снова запросить его от DHCP-сервера в аренду.

Для каждой подсети нужен свой DHCP-сервер.

*Файловый сервер* (FS) предоставляет компьютерам сети услуги по обработке файлов для организации внутреннего документооборота. *Протокол обмена* представляет собой набор вызовов, обеспечивающих приложению доступ к файловой системе на файл-сервере.

*Сервер баз данных* (DBS) обслуживает базы данных и обрабатывает запросы на поиск, выборку и обработку данных, посылаемые прикладной системой, находящейся на рабочей станции (клиенте).

*Application Server* **–** реализует трехуровневую модель доступа к базе данных.

Клиентское приложение взаимодействует с БД через сервер приложений (прикладной компонент). Эта модель имеет большой плюс, который позволяет удаленным клиентам работать с БД без затруднений. Скорость по линии удаленной связи может быть разной по разным причинам, а с БД нужно работать всем. Если БД будет работать с удаленным клиентом «долго», это вызовет недоброжелательный отзыв коллег по работе в сторону филиалов. И если удаленный клиент пошлёт запрос к БД, то этот запрос будет обработан сервером приложений. Затем сервер приложений поработает с базой данных и сформирует ответ на запрос, который отправиться удаленному клиенту.

*Почтовый сервер*– предназначен для приёма и отправки внешней электронной почты. Каждому пользователю системы присваивается почтовое "имя" - псевдоним, определяющий, фактически, адрес индивидуального электронного почтового ящика (логин).

*Exchange сервер* – сервер внутренней почты для быстрого обмена сообщениями внутри сети.

*Web-сервер* – выполняет информационно-рекламную функцию.

*Proxy-сервер* **–** это сервер, который управляет доступом клиентских компьютеров в глобальную сеть. Proxy-сервер создает для сети вымышленное имя, под которым она известна внешнему миру, в силу чего пользователям трудно ее отслеживать, а хакерам сложно получить доступ к конкретным машинам. Proxy-сервер можно назвать сторожем. Обычно proxy-сервер размещается с внутренней стороны межсетевого экрана, между браузером и реальным сервером, перехватывая Internet-запросы, передаваемые от клиентов, в силу чего последние не могут напрямую взаимодействовать с Internet.

*Антивирусный сервер* **–** это необходимая часть любой сети. Антивирусный сервер выполняет проверку передаваемой по сети информации от вредоносных программ (вирусов и троянских программ).

*Firewall*- используется для защиты компьютера от несанкционированного доступа через сеть или Интернет. Брандмауэр отличается от антивирусного программного обеспечения, однако их совместная работа обеспечивает надежную защиту сети.

В данном курсовике межсетевой экран будет находиться на маршрутизаторе.

*Call-менеджер (диспетчер, VoIP)* – это программное обеспечение для организации IP-телефонии. Выполняет функции аутентификации и авторизации абонента, распределения вызовов между абонентами. Диспетчер необходим в любой сети IP-телефонии, содержащей более двух абонентов.

*Print-сервер* - необходим для организации работы сетевых принтеров. В каждом отделе будет по крайней мере один сетевой принтер, подключенный через print-сервер.

*Видеосервер* - предназначен для обработки, архивирования и хранения видеоинформации от IP-камер.

**Описание физических серверов.**

Сервер1: база данных бухгалтерии, база данных отдела кадров, база касс

Сервер2: видеосервер

Сервер3: Внешний DNS, WEB-сервер, mail-server.

Сервер4: File-server, PDC, DHCP, DNS внутренний, антивирусный сервер, Call-manager, Exchange-manager, PRINT

Сервер5: Сервер приложений, BDC, PROXY.

Информационные потоки отделов с учетом физических серверов представлены на рис. 2.2.

Рис2.2. Схема информационных потоков с учетом серверов.

Администрация

Бухгалтерия

Отдел кадров

Отдел охраны

Филиал 2

IT отдел.

Транспорт. отдел

Отдел сбыта

Отдел снабж.

Производственный отдел

Филиал 1

Технологический отдел

**Сервер 1**

БД Бухгалтерии

БД Сбыта

БД Снабжения

БД Отдела кадров

**Сервер 2**

Видеосервер

**Сервер 3**

WEB-server

Mail-server

Внешний DNS

**Сервер 4**

File-server

PDC,DHCP

ES,DNS(внут.)

Antivirus-server

Call-менеджер

Print-server

**Сервер 5**

BDC

Proxy-server

Сервер приложений

# 3. Проектирование структурной схемы корпоративной сети.

По техническому заданию имеем 2 семиэтажных здания. Расстояние между зданиями равно 150 метров.

Разделим отделы по зданиям:

Здание 1 (первый этаж):

* Бухгалтерия.
* Администрация.
* Отдел охраны.

Здание 2 (первый этаж):

* Отдел кадров.
* Отдел технического обслуживания.
* Тренерский отдел.

Здание 3 (первый этаж):

* Отдел физвоспитания.
* Кассы оплаты услуг.

Здание 4 (первый этаж):

* Отдел по проведению спортивных мероприятий.
* Отдел маркетинга.

В целях экономии ресурсов сети, сервер системы безопасности лучше поставить на отдельный коммутатор.

Связь с филиалом в городе, где расположен центральный офис, осуществляется через технологию **Metro Ethernet**. С филиалом, расположенным за городом, через - **ISDN**.

Учитывая вышеперечисленные замечания, структурная схема сети принимает вид, приведенный в приложении А.

# 4. Защита сети от несанкционированного доступа

## 4.1. Обзор различных методов защиты информации

## 4.1.1 Физическая зашита объектов информатизации от несанкционированного доступа

Физический контроль доступа в серверные помещения (помещения, где расположены сервера, консоли управления, оборудование АТС, входы каналов связи и т.п.), обеспечивается системами контроля доступа в помещения (включая организационные меры), а также, при наличии технической возможности, системами видеонаблюдения.

Физический контроль доступа к аппаратной части средств защиты от НСД. установленных на объектах ЛВС, обеспечивается также средствами маркирования и блокировки разъемных соединений  
корпусов и блоков оборудования.  
 Физический контроль доступа к пассивному сетевому оборудованию дополнительно может обеспечиваться также средствами маркирования и блокировки разъемных сетевых соединений.

## 4.1.2. Программные методы защиты

Программные способы применяются для шифрования информации, хранящейся на магнитных носителях (дисках, лентах). Программные способы шифрования сводятся к операциям перестановки, перекодирования и сложения по модулю 2 с ключевыми словами. При этом используются команды ассемблера TR (перекодировать) и XC (исключающее ИЛИ).

Особое место в программах обработки информации занимают операции кодирования. Преобразование информации, в результате которого обеспечивается изменение объема памяти, занимаемой данными, называется кодированием. На практике кодирование всегда используется для уменьшения объема памяти, так как экономия памяти ЭВМ имеет большое значение в информационных системах.

## 4.2. Защита сети от внутреннего НСД

## 4.2.1 Политика доступа.

Внутрисетевую защиту реализуем на административном уровне с использованием политики пользователей (политика учетных записей и политика прав пользователей). Всех пользователей объединим в подгруппы с учетом того, в каком отделе он работает. Каждой подгруппе назначим права в соответствии с таблицей. А так же расставим приоритеты для каждого пользователя в использовании информационных ресурсов сети.

Внутри баз данных также создадим роли и пользователей, наделив их правами. Это обеспечит безопасность на уровне базы данных. При этом в рассмотрении возьмем сервера:

Сервер 1, где находятся базы данных; Сервер 4 с основными службами и протоколами, сервер 5 и сервер 3. Видеосервер рассматривать не будем.

Cервер1: разграничить доступ к базам данных

Сервер 5: разграничить доступ к BDC, PROXY, серверу приложений.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Отдел** | **С1 С3** | | | | | | **С4** | | | | | | | |
| **БД бухгалтер** | **БД отд. кадров** | **БД касс** | **WEB** | **MAIL** | **DNS внеш** | **file-serv** | **PDC** | **DHCP** | **DNS-внут** | **PRINT** | **Антив-с** | **exchange** | **call** |
| **Администрация** | R | R | R | + | + | + | + | R | R | R | R | R | + | + |
| **Бухгалтерия** | RW | R | R | - | - | - | + | R | R | R | R | R | + | + |
| **Отдел охраны** | - | - | - | - | - | - | + | R | R | R | R | R | + | + |
| **Отдел тех.обсл.** | mE | mE | mE | + | + | + | + | + | + | + | + | + | + | + |
| **Отдел кадров** | - | RW | - | - | - | - | + | R | R | R | R | R | + | + |
| **Отдел физвосп.** | - | - | - | + | + | + | + | R | R | R | R | R | + | + |
| **Отд. по провед. спорт. меропр.** | - | - | - | + | + | + | + | R | R | R | R | R | + | + |
| **Кассы оплаты** | - | - | RW | + | + | + | + | R | R | R | R | R | + | + |
| **Тренерский от.** | - | - | - | + | + | + | + | R | R | R | R | R | + | + |
| **От. маркетинга** | - | - | - | + | + | + | + | R | R | R | R | R | + | + |
| **AS** | + | + | + | - | - | R | - | - | - | - | - | - | - | - |
| **Web-server** | - | - | - | - | - | R | - | - | - | - | - | - | - | - |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | **С5** | | | **С2** |
| **Отдел** | **BDC** | **PROXY** |  | **AS** | **Видео** |
| **Администрация** | r | r |  | + | r |
| **Бухгалтерия** | r | r |  | + | r |
| **Отдел охраны** | r | r |  | + | + |
| **Отдел кадров** | r | r |  | + | r |
| **Отдел тех.обсл.** | r me | r me |  | r me | + |
| **Отдел физвосп.** | r | r |  | + | r |
| **Отд. по провед. спорт. меропр.** | r | r |  | + | - |
| **Кассы оплаты** | r | r |  | + | - |
| **Тренерский от.** | r | r |  | + | - |
| **От. маркетинга** | r | r |  | + | - |
| **AS** | - | - |  | + | - |
| **Web-server** | - | - |  | - | - |

* + 1. Применение VLAN

Виртуальная локальная сеть (виртуальная частная сеть; Virtual LAN, VLAN) — разновидность Интрасети, представляющая собой логическое объединение узлов большой (распределенной) локальной вычислительной сети, которые могут принадлежать к ее различным физическим сегментам, подключенным к разным концентраторам. Сеть организуется при помощи коммутирующих концентраторов или маршрутизаторов. Специальное программное обеспечение системы управления позволяет разделить сеть на несколько логических частей (виртуальных сегментов). Администратор сети может по своему усмотрению создавать виртуальные сегменты, добавлять или удалять отдельные узлы. Данные, предназначенные для конкретных узлов виртуальной сети, благодаря коммутации пакетов, передаются только в рамках заданного логического сегмента. Этим предотвращаются перегрузки в сети, обеспечивается повышение ее безопасности. Метод создания виртуальных ЛВС используется в сетях типа Ethernet. Принцип логического объединения узлов разнородных сетей (в том числе Token Ring, FDDI, ATM) в виртуальные сегменты используется в распределенных и глобальных сетях, в частности в ATM.

Для торгового предприятия, имеем следующее распределение объектов по VLAN:

VLAN1: K11, K1(Администрация), K2(Бухгалтерия), K3(Отдел охраны), C2(Сервер2).

VLAN2: K12, K5(отдел кадров ), K4(Тренерский отдел), K6(отдел технического обслуживания).

VLAN3: K13, K7(Кассы оплаты услуг), K8(Отдел физвоспитания).

VLAN4: K10, K14(Отдел по проведению спортивных мероприятий), K9(отдел маркетинга), Ф1(филиал 1), Ф2(филиал 2), C1(Сервер 1), C3(Сервер 3),

C4(Сервер 4), C5(Сервер 5), M1(маршрутизатор).

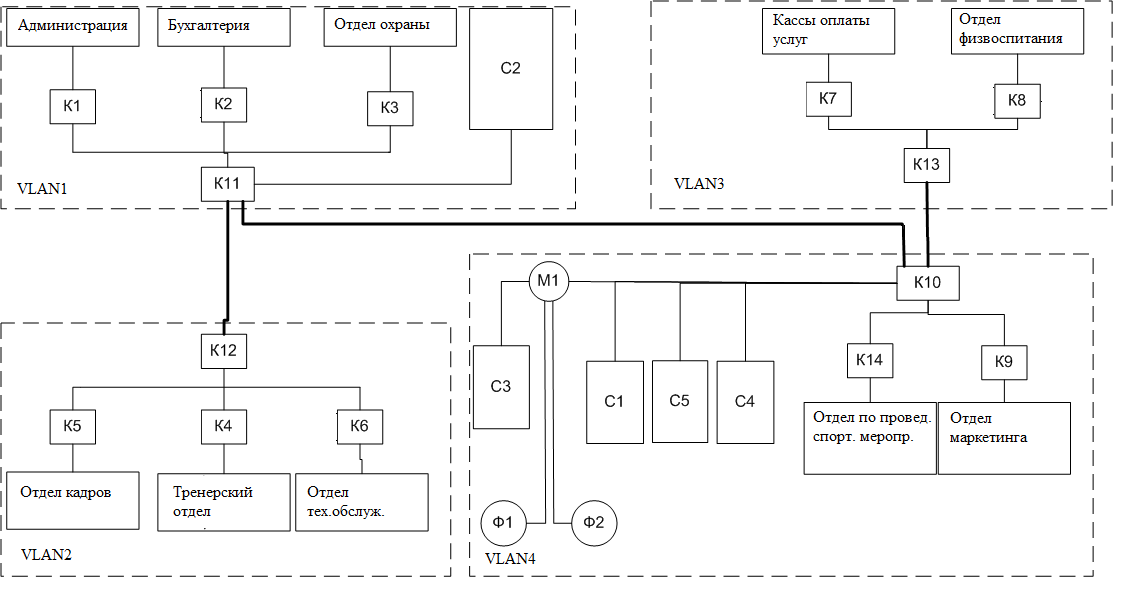
VLAN5(Video): К коммутаторам в отделах: Администрация, бухгалтерия, отдел охраны, отел кадров, тренерский отдел, отдел технического обслуживания, кассы оплаты услуг, отдел физвоспитания, отдел по проведению спортивных мероприятий, отдел маркетинга.

VLAN6(VoIP): К коммутаторам в отделах: Администрация, отдел физвоспитания

Такое распределение допустимо, так как:

1. Отдел по проведению спортивных мероприятий выгружает расписание и программы мероприятий на file-server, поэтому их необходимо объединить в один VLAN: VLAN4.
2. Отдел охраны должен иметь доступ к видео серверу, который находится в VLAN1, поэтому они объединены в один VLAN.

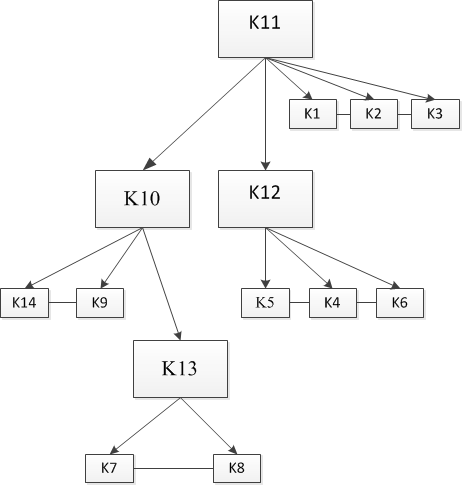
Схема VLAN:



* + 1. Использование STP для защиты от циклов в сети
    2. Описание протокола

Spanning Tree Protocol (STP) (протокол cоставного дерева) — сетевой протокол. Основной задачей STP является устранение петель (циклов) в топологии произвольной сети Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями. STP решает эту задачу, автоматически блокируя соединения, которые в данный момент для полной связности коммутаторов являются избыточными. Наличие топологических петель в реальной сети Ethernet с коммутатором неизбежно приводит к бесконечным повторам передачи одних и тех же кадров Ethernet одним и более коммутатором, отчего пропускная способность сети оказывается почти полностью занятой этими бесполезными повторами; в этих условиях, хотя формально сеть может продолжать работать, на практике её производительность становится настолько низкой, что может рассматриваться как полный отказ сети.

* + 1. Принцип действия
* В сети выбирается один корневой мост (англ. *Root Bridge*).
* Далее каждый, отличный от корневого, мост просчитывает кратчайший путь к корневому. Соответствующий порт называется корневым портом (англ. *Root Port*). У любого не корневого коммутатора может быть только один корневой порт.
* После этого для каждого сегмента сети, к которому присоединён более чем один порт моста, просчитывается кратчайший путь к корневому порту. Мост, через который проходит этот путь, становится **назначенным** для этой сети (англ. *Designated Bridge*), а соответствующий порт — **назначенным портом** (англ. *Designated port*).
* Далее во всех сегментах, с которыми соединены более одного порта моста, все мосты блокируют все порты, не являющиеся корневыми и назначенными. В итоге получается древовидная структура (математический граф) с вершиной в виде корневого коммутатора.
  + 1. Применение STP для нашей сети



## 4.3 Защита от внешнего несанкционированного доступа

## 4.3.1 Применение межсетевого экрана

Межсетевой экран или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Решение о том, фильтровать ли с помощью межсетевого экрана конкретные протоколы и адреса, зависит от принятой в защищаемой сети политики безопасности. Межсетевой экран представляет собой набор компонентов, настраиваемых для реализации выбранной политики безопасности.

В настоящее время не существует единой и общепризнанной классификации межсетевых экранов. Выделяют следующие классы межсетевых экранов:

* Фильтрующие маршрутизаторы.
* Шлюзы сеансового уровня.
* Шлюзы уровня приложений.

## 4.3.2 Аутентификации в Интернет

При удаленном доступе к сети также применяются процедуры идентификации и аутентификации.

*Аутентификация* - идентификация источника информации.

Существует различные классы аутентификации, начиная с полного ее отсутствия до очень строгих механизмов контроля:

* Отсутствие аутентификации

Простейшая аутентификационная система не имеет аутентификации вовсе.

* Аутентификационные механизмы, уязвимые для пассивных атак

Простая проверка пароля является наиболее общей формой аутентификации. Простые аутентификационные проверки имеют различные формы: ключ может быть паролем, запомненным пользователем, он может быть физическим или электронным объектом, принадлежащим пользователю, он может быть уникальной биологической характеристикой. Простые аутентификационные системы считаются "раскрывающими", так как, если ключ передается по сети, он может быть перехвачен злоумышленником. Механизмы раскрывающей аутентификации уязвимы для атак “воспроизведения”. Ключи доступа могут быть запомнены в атакуемой машине и при наличии бреши в системе безопасности можно получить доступ ко всем паролям. Обычно форма хранения паролей допускает их сверку, но не чтение.

* Аутентификационные механизмы, уязвимые для активных атак

Нераскрывающие парольные системы созданы для предотвращения атак воспроизведения. Разработано несколько систем для генерации не раскрываемых паролей. Система аутентификации S/Key (TM), разработанная в Bellcore генерирует много одноразовых паролей из одного секретного ключа [Haller94]. Она не использует физических объектов (token), поэтому удобна для аутентификации машина-машина. Аутентификация S/Key не требует запоминания секретного ключа пользователя, что является преимуществом при работе с ненадежными вычислительными системами. В ее сегодняшнем виде система S/Key уязвима для переборных атак со словарем в случае неудачного выбора пароля.

* Аутентификационные механизмы, неуязвимые для пассивных атак

Более мощные аутентификационные системы используют вычислительные возможности партнеров, участвующих в процессе аутентификации. Аутентификация может быть однонаправленной, например аутентификация пользователей в вычислительной системе, или она может быть взаимной, когда оба партнера должны идентифицировать друг друга. Некоторые системы аутентификации используют криптографические методы и формируют общий секретный код (например, ключ сессии), который может быть использован при последующем обмене. Эти системы аутентификации могут также обеспечить, когда требуется, конфиденциальность (используя шифрование) при передаче данных по незащищенным сетям.

Разграничим доступ к сети в зависимости от пользователя (см. таблицу 4.4)

Таблица 4.4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Пользователи** | **Web** | **Mail** | **AS** | **DNS**  **внеш** |
| Филиал 1 | r/w | r/w | r/w | + |
| Филиал 2 | r/w | r/w | r/w | + |
| Мобильный сотрудник | r/w | r | r/w | + |
| Гости | r/w | r | - | + |

В данной работе для защиты передаваемых данных используется протокол SSH:

## 4.3.3 Теоретические основы SSH

SSH ([англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Secure SHell — «безопасная оболочка») — [сетевой протокол](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) [прикладного уровня](http://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%BD%D0%BE%D0%B3%D0%BE_%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D1%8F&action=edit&redlink=1), позволяющий производить удалённое управление [операционной системой](http://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) и [туннелирование](http://ru.wikipedia.org/wiki/%D0%A2%D1%83%D0%BD%D0%BD%D0%B5%D0%BB%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8)) TCP-соединений (например, для передачи файлов). Схож по функциональности с протоколами [Telnet](http://ru.wikipedia.org/wiki/Telnet" \o "Telnet) и [rlogin](http://ru.wikipedia.org/wiki/Rlogin" \o "Rlogin), но, в отличие от них, [шифрует](http://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) весь трафик, включая и передаваемые пароли. SSH допускает выбор различных[алгоритмов](http://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC) шифрования. SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем.

SSH позволяет безопасно передавать в незащищённой среде практически любой другой сетевой протокол. Таким образом, можно не только удалённо работать на компьютере через [командную оболочку](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%B0%D0%BD%D0%B4%D0%BD%D0%B0%D1%8F_%D0%BE%D0%B1%D0%BE%D0%BB%D0%BE%D1%87%D0%BA%D0%B0), но и передавать по шифрованному каналу звуковой поток или видео (например, с [веб-камеры](http://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D0%BA%D0%B0%D0%BC%D0%B5%D1%80%D1%8B)). Также SSH может использовать [сжатие](http://ru.wikipedia.org/wiki/%D0%A1%D0%B6%D0%B0%D1%82%D0%B8%D0%B5_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) передаваемых данных для последующего их шифрования, что удобно, например, для удалённого запуска клиентов [X Window System](http://ru.wikipedia.org/wiki/X_Window_System).

Большинство [хостинг-провайдеров](http://ru.wikipedia.org/wiki/%D0%A5%D0%BE%D1%81%D1%82%D0%B8%D0%BD%D0%B3-%D0%BF%D1%80%D0%BE%D0%B2%D0%B0%D0%B9%D0%B4%D0%B5%D1%80%D1%8B) за определенную плату предоставляют клиентам доступ к их [домашнему каталогу](http://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B0%D1%88%D0%BD%D0%B8%D0%B9_%D0%BA%D0%B0%D1%82%D0%B0%D0%BB%D0%BE%D0%B3) по SSH. Это может быть удобно как для работы в командной строке, так и для удалённого запуска программ (в том числе графических приложений).

SSH — это протокол сеансового уровня. SSH-сервер обычно прослушивает соединения на TCP-порту 22. Спецификация протокола SSH-2 содержится в [RFC 4251](http://tools.ietf.org/html/rfc4251). Для аутентификации сервера в SSH используется протокол аутентификации сторон на основе алгоритмов [электронно-цифровой подписи](http://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C) [RSA](http://ru.wikipedia.org/wiki/RSA) или [DSA](http://ru.wikipedia.org/wiki/DSA). Для аутентификации клиента также может использоваться ЭЦП RSA или DSA, но допускается также аутентификация при помощи пароля (режим обратной совместимости с [Telnet](http://ru.wikipedia.org/wiki/Telnet" \o "Telnet)) и даже ip-адреса хоста (режим обратной совместимости с [rlogin](http://ru.wikipedia.org/wiki/Rlogin" \o "Rlogin)). Аутентификация по паролю наиболее распространена; она безопасна, так как пароль передается по зашифрованному виртуальному каналу. Аутентификация по ip-адресу небезопасна, эту возможность чаще всего отключают. Для создания общего секрета (сеансового ключа) используется [алгоритм Диффи — Хеллмана](http://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%94%D0%B8%D1%84%D1%84%D0%B8_%E2%80%94_%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%D0%B0) (DH). Для шифрования передаваемых данных используется [симметричное шифрование](http://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D0%BE%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), алгоритмы [AES](http://ru.wikipedia.org/wiki/Advanced_Encryption_Standard), [Blowfish](http://ru.wikipedia.org/wiki/Blowfish" \o "Blowfish) или [3DES](http://ru.wikipedia.org/wiki/3DES). Целостность переданных данных проверяется с помощью [CRC32](http://ru.wikipedia.org/wiki/CRC32) в SSH1 или [HMAC](http://ru.wikipedia.org/wiki/HMAC)-[SHA1](http://ru.wikipedia.org/wiki/SHA1)/[HMAC](http://ru.wikipedia.org/wiki/HMAC)-[MD5](http://ru.wikipedia.org/wiki/MD5) в SSH2.

Для сжатия шифруемых данных может использоваться алгоритм LempelZiv ([LZ77](http://ru.wikipedia.org/wiki/LZ77)), который обеспечивает такой же уровень сжатия, что и архиватор [ZIP](http://ru.wikipedia.org/wiki/ZIP). Сжатие SSH включается лишь по запросу клиента, и на практике используется редко.

**Рекомендации по безопасности использования SSH:**

* Запрещение удаленного root-доступа.
* Запрещение подключения с пустым паролем или отключение входа по паролю.
* Выбор нестандартного порта для SSH-сервера.
* Использование длинных SSH2 RSA-ключей (2048 бит и более). Системы шифрования на основе RSA считаются надёжными, если длина ключа не менее 1024 бит.
* Ограничение списка IP-адресов, с которых разрешен доступ (например, настройкой файервола).
* Запрещение доступа с некоторых потенциально опасных адресов.
* Отказ от использования распространенных или широко известных системных логинов для доступа по SSH.
* Регулярный просмотр сообщений об ошибках аутентификации.
* Установка систем обнаружения вторжений ([IDS](http://ru.wikipedia.org/wiki/IDS) — Intrusion Detection System).
* Использование ловушек, подделывающих SSH-сервис ([honeypots](http://ru.wikipedia.org/wiki/Honeypot_(%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C)" \o "Honeypot (информационная безопасность))).

**Недостатки и достоинства:**

Криптографическая защита протокола SSH не фиксирована, возможен выбор различных алгоритмов шифрования. Клиенты и серверы, поддерживающие этот протокол, доступны для различных платформ. Кроме того, протокол позволяет не только использовать безопасный удалённый shell на машине, но и туннелировать графический интерфейс — X Tunnelling (только для Unix-подобных ОС или приложений, использующих графический интерфейс X Window System). Так же SSH способен передавать через безопасный канал (Port Forwarding) любой другой сетевой протокол, обеспечивая (при надлежащем конфигурировании) возможность безопасной пересылки не только X-интерфейса, но и, например, звука.  
Однако протокол SSH не решает всех проблем сетевой безопасности. Он лишь фокусирует свое внимание на обеспечении безопасной работы таких приложений, как эмуляторы терминала. Использование реализаций протокола SSH на серверах и в клиентских приложениях помогает защитить данные лишь в процессе передачи. Протокол SSH ни коим образом не является заменой брандмауэров, систем обнаружения вторжений, сетевых сканеров, систем аутентификации и других инструментов, позволяющих защитить информационные системы и сети от атак.

Безопасность SSH:  
Клиентские приложения обычно посылают запрос на открытие сессии серверу на определенный порт, который прослушивается запущенными на сервере сервисами на поступающие специфические запросы. Самые известные из них:

21 – ftp

80 – http

25 – smtp

23 – telnet

Многие из этих клиентских приложений осуществляют запросы прямым текстом. Протокол SSH позволяет обезопасить такие подключения. Сначала пакеты будут посланы на некий известный на сервере порт, после чего они будут переадресованы на 22 порт (который обслуживается сервером SSH) и там будут преобразованы в защищенные SSH пакеты, инкапсулированные в защищенное соединение.  
OpenSSH (Open Secure Shell - открытый безопасный shell) - набор программ, предоставляющих шифрование сеансов связи по компьютерным сетям с использованием протокола SSH. Он был создан под руководством Тео де Раадта как открытая альтернатива проприетарного ПО от SSH Communications Security. Разработчики OpenSSH утверждают, что он более безопасен чем оригинальный Secure Shell, благодаря их политике чистки и аудита кода. Хотя исходный код также доступен для оригинального SSH, различные ограничения, накладываемые на его использование, делают OpenSSH более привлекательным проектом для большинства программистов.  
PuTTY (от TTY — телетайп, англ. putty — замазка) - свободно распространяемый клиент для протоколов SSH, Telnet, rlogin и чистого TCP. Изначально разрабатывался для Windows, однако позднее портирован на Unix. В разработке находятся порты для Mac OS и Mac OS X. Сторонние разработчики выпустили неофициальные порты на другие платформы, такие как мобильные телефоны под управлением Symbian OS. Программа выпускается под лицензией MIT. Незаменимая вещь для системных администраторов.

## 4.3.4 Теоретические основы SSL

SSL ([англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Secure Sockets Layer — уровень защищённых сокетов) — [криптографический протокол](http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB), который обеспечивает установление безопасного соединения между клиентом и сервером. SSL изначально разработан компанией [Netscape Communications](http://ru.wikipedia.org/wiki/Netscape_Communications). Впоследствии на основании протокола SSL 3.0 был разработан и принят [стандарт RFC](http://ru.wikipedia.org/wiki/RFC#.D0.A1.D0.BE.D0.B4.D0.B5.D1.80.D0.B6.D0.B8.D0.BC.D0.BE.D0.B5_RFC), получивший имя[TLS](http://ru.wikipedia.org/wiki/TLS).

Протокол обеспечивает конфиденциальность обмена данными между клиентом и сервером, использующими TCP/IP, причём для шифрования используется асимметричный алгоритм с[открытым ключом](http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%BC). При шифровании с открытым ключом используются два ключа, причем любой из них может использоваться для шифрования сообщения. Тем самым, если используется один ключ для шифрования, то соответственно для расшифровки нужно использовать другой ключ. В такой ситуации можно получать защищённые сообщения, публикуя открытый ключ, и храня в тайне секретный ключ.

Протокол SSL состоит из двух подпротоколов: протокол SSL записи и рукопожатия. Протокол SSL записи определяет формат, используемый для передачи данных. Протокол SSL включает рукопожатие с использованием протокола SSL записи для обмена сериями сообщений между сервером и клиентом во время установления первого соединения. Для работы SSL требуется, чтобы на сервере имелся SSL-[сертификат](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%82_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)).

SSL предоставляет канал, имеющий 3 основных свойства:

* Аутентификация. Сервер всегда аутентифицируется, в то время как клиент аутентифицируется в зависимости от алгоритма.
* Целостность. Обмен сообщениями включает в себя проверку целостности.
* Частность канала. Шифрование используется после установления соединения и используется для всех последующих сообщений.

Основные цели протокола в порядке приоритетности:

* Криптографическая безопасность: SSL устанавливает безопасное соединение между двумя сторонами.
* Совместимость: Программисты, независимо друг от друга могут создавать приложения, использующие SSL, которые впоследствии будут способны успешно обмениваться криптографическими параметрами без всякого знания кода чужих программ.
* Расширяемость: SSL стремится обеспечить рабочее пространство, в котором новые открытые ключи и трудоемкие методы шифрования могут быть включены по мере необходимости.
* Относительная эффективность: работа протокола на основе SSL требует больших скоростей от CPU, в частности для работы с открытыми ключами. По этой причине SSL протокол был включен в необязательную сессию схемы кеширования для уменьшения числа соединений, которые необходимо устанавливать с нуля. Кроме того, большое внимание уделяется тому, чтобы уменьшить сетевую активность.

## 4.3.5. Реализация защиты данных с помощью протокола.

Офисы филиалов предприятия соединяются с главным офисом при помощи постоянных VPN-подключений между маршрутизаторами, которые работают круглосуточно.

Используется двусторонне инициируемое VPN-подключение [13]. Подключение может быть инициировано как маршрутизатором в главном офисе, так и маршрутизатором в дочернем подразделении. Двусторонне инициируемые подключения требуют создания интерфейсов вызова по требованию, политики удаленного доступа, пулов IP-адресов и фильтров пакетов на маршрутизаторах с обеих сторон.

В филиале на маршрутизаторе используется протокол SSH для создания постоянного VPN-подключения «маршрутизатор-маршрутизатор» с главным офисом. Подключение является постоянным. Отключение не выполняется, даже если отсутствует обмен данными.

При подключении маршрутизатора филиала к интрасети компании, на него с помощью автозаявки был установлен сертификат компьютера.

# 5.Организация связи с филиалами.

Связь с филиалами осуществляется с помощью двух технологий: Metro Ethernet и ISDN.

## 5.1. Краткий обзор технологии Metro Ethernet.

Metro Ethernet – мультисервисная сеть Ethernet масштаба города.

Растущая конкуренция на рынке телекоммуникаций заставляет операторов искать новые решения, которые позволят расширить спектр предлагаемых услуг, снизить расходы на сопровождение сети, повысить прибыльность и привлечь новых клиентов. Такие решения также должны обеспечивать хорошую масштабируемость и быть рассчитаны на быстрый рост клиентской базы и внедрение новых приложений, требующих поддержки функций качества обслуживания и значительной полосы пропускания.

Всем этим требованиям наилучшим образом отвечает решение Metro Ethernet. Появление Metro Ethernet как серьезной альтернативы другим вариантам сетей городского масштаба обусловлено следующими факторами:

* ростом требований к полосе пропускания в связи с появлением новых типов приложений;
* высокой концентрацией абонентов в офисных и жилых зданиях;
* ростом интереса к массовому рынку домашних абонентов вследствие высокой насыщенности рынка корпоративных клиентов и падения доходности услуг на этом рынке;
* низкой стоимостью первоначальных затрат (CAPEX) и затрат на поддержку (OPEX);
* большим количеством специалистов, имеющих опыт работы с Ethernet.

Решение Metro Ethernet обеспечивает:

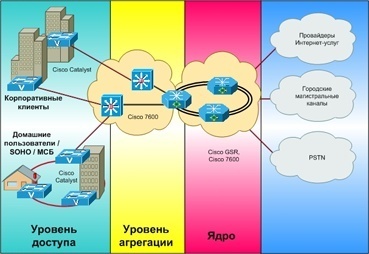
* мультисервисность и высокую надежность инфраструктуры, обеспечивающие поддержку соглашений об уровне обслуживания, необходимых для критичных приложений;
* низкую стоимость развертывания сети;
* исключительно низкую цену за Гбит/c;
* стандартный интерфейс с возможностью предоставления пакета услуг на одном клиентском порту (мультиплексирование сервисов);
* модульность и высокую плотность агрегации- решение рассчитано на быстрое внедрение в районах с высокой плотностью клиентов;
* отличную масштабируемость по количеству портов, производительности узлов и скорости каналов (до 80 Гбит/c);
* единую технологию, механизмы сигнализации и управления для всей сети;
* максимальную автоматизацию управления сетью и активации услуг, поддержку средств самообслуживания клиентов.

Рост требований к емкости городских сетей и успех существующих операторов Metro Ethernet ясно показывают, что данная модель предоставления телекоммуникационных услуг на базе Ethernet в городских сетях конкурентоспособна, востребована и прибыльна для операторов связи. И так же позволяет обеспечить основу для value-added сервисов, таких как IDS, хранение информации, VoIP и IPTV.

Архитектура сети Metro Ethernet разработана с учетом следующих требований:

* масштабируемость;
* высокая надежность и доступность;
* поддержка качества услуг и соглашений об уровне обслуживания, необходимых для критичных бизнес-приложений, голосового трафика и широкополосного видео;
* высокая производительность;
* модульность и возможность быстрого развертывания;
* управляемость;
* поддержка наиболее полного набора услуг, как для бизнес клиентов, так и для домашних абонентов, возможность быстрого внедрения новых услуг;
* безопасность

Типовая сеть Metro Ethernet строится по трехуровневой иерархической схеме и включает ядро, уровень агрегации и уровень доступа.



В ядре и на уровне агрегации обеспечивается резервирование компонентов устройств, а также топологическое резервирование, что позволяет повысить доступность сети и сделать предоставление услуг непрерывным при сбоях каналов и узлов. Поддерживаемые современные механизмы резервирования (Statefull Switchover, Non-stop forwarding, Route Processor Redundancy) и защитной коммутации (Fast Reroute) обеспечивают время восстановления, сравнимое с сетями SDH и позволяют минимизировать потери трафика при сбоях на сети.

На уровне доступа реализуется полный комплекс мер безопасности, обеспечивающих идентификацию и изоляцию клиентов, а также защиту инфраструктуры оператора. В сети реализуются сквозные механизмы качества обслуживания (QoS) и поддерживаются различные типы прозрачного туннелирования клиентской QoS-маркировки трафика. На всех уровнях сети поддерживается эффективная многоадресная передача (multicast), что важно при реализации таких услуг, как телевидение поверх IP.

## 5.1.1. Реализация связи с помощью Metro Ethernet.

Для построения ядра сети Metro Ethernet используется маршрутизатор **Ethernet Router 8000 компании Alcatel-Lucent.**

Он поддерживает множество сетевых протоколов, используемых в городских магистралях. Маршрутизатор оснащен интерфейсами Ethernet, ATM, TDM и SDH, что позволяет операторам плавно переходить от унаследованных технологий городских сетей к Metro Ethernet. Ethernet Router 8000 обеспечивают всю необходимую функциональность, включая MPLS и VPLS, поддерживают механизмы SLA и QoS.   
Коммутационная производительность модели 8000 составляет 16 Гбит/с при пропускной способности 16,7 млн. пакетов в секунду. Резервирование процессоров, коммутационных матриц, блоков электропитания наряду с поддержкой протокола VRRP (Virtual Router Redundancy Protocol), отказоустойчивой маршрутизации и алгоритмов реконфигурации маршрутизации (OSPF multi-path, MLPPP, MPLS Fast Reroute и Port Trunking) обеспечивают время наработки на отказ порядка 200 тыс. ч. Это гарантирует надежность ядра 99,999%.

## 5.2. Краткий обзор технологии ISDN.

ISDN ([англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Integrated Services Digital Network) — цифровая сеть с интеграцией служб. Позволяет совместить услуги телефонной связи и обмена данными.

Основное назначение ISDN — передача [данных](http://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5) со скоростью до 64 кбит/с по абонентской проводной линии и обеспечение интегрированных телекоммуникационных услуг ([телефон](http://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BB%D0%B5%D1%84%D0%BE%D0%BD" \o "Телефон),[факс](http://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%BA%D1%81), и пр.). Использование для этой цели телефонных проводов имеет два преимущества: они уже существуют и могут использоваться для подачи питания на терминальное оборудование.

Выбор 64 кбит/c стандарта определяется следующими соображениями. При полосе частот 4 кГц, согласно [теореме Котельникова](http://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BE%D1%80%D0%B5%D0%BC%D0%B0_%D0%BE%D1%82%D1%81%D1%87%D1%91%D1%82%D0%BE%D0%B2_%D0%A3%D0%B8%D1%82%D1%82%D0%B0%D0%BA%D0%B5%D1%80%D0%B0_%E2%80%94_%D0%9D%D0%B0%D0%B9%D0%BA%D0%B2%D0%B8%D1%81%D1%82%D0%B0_%E2%80%94_%D0%9A%D0%BE%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2%D0%B0_%E2%80%94_%D0%A8%D0%B5%D0%BD%D0%BD%D0%BE%D0%BD%D0%B0), частота дискретизации должна быть не ниже 8 кГц. Минимальное число двоичных разрядов для представления результатов стробирования голосового сигнала при условии логарифмического преобразования равно 8. Таким образом, в результате перемножения этих чисел (8 кГц \* 8 (число двоичных разрядов) = 64) и получается значение полосы [B-канала](http://ru.wikipedia.org/wiki/B-%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB) ISDN, равное 64 кб/с. Базовая конфигурация каналов имеет вид 2 × B + D = 2 × 64 + 16 = 144 кбит/с. Помимо B-каналов и вспомогательного [D-канала](http://ru.wikipedia.org/wiki/D-%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB) ISDN может предложить и другие каналы с большей пропускной способностью: канал Н0 с полосой 384 кбит/с, Н11 — 1536 кбит/c и Н12 — 1920 кбит/c (реальные скорости цифрового потока). Для первичных каналов (1544 и 2048 кбит/с) полоса D-канала может составлять 64 кбит/с.

Для объединения в сети ISDN различных видов трафика используется технология [TDM](http://ru.wikipedia.org/wiki/TDM) ([англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Time Division Multiplexing*, *мультиплексирование по времени*). Для каждого типа данных выделяется отдельная полоса, называющаяся *элементарным каналом* (или *стандартным каналом*). Для этой полосы гарантируется фиксированная, согласованная доля полосы пропускания. Выделение полосы происходит после подачи сигнала *CALL* по отдельному каналу, называющемуся *каналом внеканальной сигнализации*.

В стандартах ISDN определяются базовые типы каналов, из которых формируются различные пользовательские интерфейсы.

|  |  |  |
| --- | --- | --- |
| **Тип** | **Полоса** | **Описание** |
| A | — | Аналоговая телефонная линия, 4кГц. |
| B | 64 кб/с | передача данных или 1 телефонная линия (1 поток оцифрованного звука) |
| C | 8/16 кб/с | передача данных |
| D | 16/64 кб/с | Канал внеканальной сигнализации (управление другими каналами) |
| E | 64 кб/с | Внутренняя сигнализация ISDN |
| H0 | 384 кб/с | передача данных |
| H10 | 1472 кб/с | передача данных |
| H11 | 1536 кб/с | передача данных |
| H12 | 1920 кб/с | передача данных |

В большинстве случаев применяются каналы типов *B* и *D*.

Сеть ISDN состоит из следующих компонентов:

* сетевые терминальные устройства (NT, [англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Network Terminal Devices*)
* линейные терминальные устройства (LT, [англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Line Terminal Equipment*)
* терминальные адаптеры (TA, [англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Terminal adapters*)
* Абонентские терминалы
* Абонентские терминалы обеспечивают пользователям доступ к услугам сети. Существует два вида терминалов: TE1 (специализированные ISDN-терминалы), TE2 (неспециализированные терминалы). TE1 обеспечивает прямое подключение к сети ISDN, TE2 требуют использования терминальных адаптеров (TA).

## 5.2.1. Реализация связи с помощью ISDN.

Для обеспечения связи с филиалом, расположенным в другом городе, используется маршрутизатор D-Link DI-106M, предназначенный для объединения локальных сетей и подключения к Internet по сети ISDN.

**Содержит:**

* 6-портовый Ethernet-хаб 10Base-T (1 аплинк-порт);
* 2 порта для подключения аналоговых телефонов, модемов или факсов G2/3;
* интерфейс RS-232 для управления и настройки;

Возможности:

* Маршрутизация IP, IPX, функции моста;
* Сервер удаленного доступа с протоколом авторизации PAP/CHAP, поддержка RADIUS;
* Черный список, бюджеты, история звонков;
* Динамическое изменение числа используемых каналов в зависимости от трафика;
* Callback для входящих звонков;
* Возможность работы с выделенной линией;
* Сжатие по алгоритму STAC - эффективная полоса пропускания может быть расширена до 512 Кбит/с;
* NAT с возможностью доступа к одному из определенных адресов внутренней сети (например, WEB-серверу)
* Фильтрация трафика (simple firewall);
* Встроенный DHCP-сервер;
* Протоколы маршрутизации RIP-I, RIP-II;
* Удаленное управление: telnet, SNMP, Syslog;
* Удаленное и локальное обновление ПО;

# 6.Распределение адресов рабочих станций с учётом структурной схемы.

Каждая рабочая станция в сети имеет свой уникальный 4-х байтный IP-адрес, который состоит из номера сети и номера узла в сети.

IP-адрес обычно записывается в виде 4-х чисел, представляющих значение каждого байта в десятичной форме и разделенных точками.

Количество компьютеров - 72. Количетсво серверов - 5. Итого: 77 машин. Назначение IP-адресов может происходить в ручную путём прописывания на каждой машине. При этом администратор должен помнить, какие адреса он уже использовал для других интерфейсов, а какие ещё свободные. Протокол DHCP освобождает администратора от этой проблемы автоматизируя назначении IP- адресов.

DHCP обеспечивает надежный и простой способ конфигурации сети TCP/IP, гарантируя отсутствие дублирования адресов за счет централизованного управления их распределением.

При этом, на серверах будем прописывать адреса вручную. Также необходим некоторый запас IP адресов, чтобы в дальнейшем, при расширении сети, не приходилось переписывать уже созданные IP адреса.

Разбиваем нашу сеть на 4 подсети: здание1, здание2, здание3, здание4.

Маска подсети: 255.255.255.192.

Представим распределение IP адресов в виде таблиц.

Первая подсеть (здание1):

|  |  |  |
| --- | --- | --- |
| Отдел | Количество устройств | IP-адрес |
| Администрация | 2 рабочие станции | 192.14.1.4-192.14.1.7 |
| Бухгалтерия | 8 рабочих станций | 192.14.1.8-192.14.1.17 |
| Отдел охраны | 5 рабочих станций | 192.14.1.18-192.14.1.25 |
| Сервер | Сервер2 | 192.14.1.1 |
| Широковещательный адрес | - | 192.14.1.63 |
| Адрес подсети | - | 192.14.1.0 |

Вторая подсеть (здание2):

|  |  |  |
| --- | --- | --- |
| Отдел | Количество устройств | IP-адрес |
| Тренерский отдел | 15 рабочих станций | 192.14.1.66-192.14.1.84 |
| Отдел кадров | 7 рабочих станций | 192.14.1.85-192.14.1.95 |
| Отдел тех.обслуж. | 11 рабочих станций | 192.14.1.96-192.14.1.111 |
| Широковещательный адрес | - | 192.14.1.127 |
| Адрес подсети | - | 192.14.1.64 |

третья подсеть (здание3):

|  |  |  |
| --- | --- | --- |
| Отдел | Количество устройств | IP-адрес |
| Кассы оплаты услуг | 3 рабочих станции | 192.14.1.130-192.14.1.135 |
| Отдел физвоспитания | 3 рабочих станции | 192.14.1.136-192.14.1.141 |
| Широковещательный адрес | - | 192.14.1.191 |
| Адрес подсети | - | 192.14.1.128 |

Четвертая подсеть (здание4):

|  |  |  |
| --- | --- | --- |
| Отдел | Количество устройств | IP-адрес |
| Отдел маркетинга | 15 рабочих станций | 192.14.1.198-192.14.1.219 |
| От. по провед. спор. меропр. | 3 рабочих станций | 192.14.1.220-192.14.1.225 |
| Сервер | Сервер 1 | 192.14.1.193 |
| Сервер | Сервер 3 | 192.14.1.194 |
| Сервер | Сервер 4 | 192.14.1.195 |
| Сервер | Сервер 5 | 192.14.1.196 |
| Широковещательный адрес | - | 192.14.1.255 |
| Адрес подсети | - | 192.14.1.192 |

Также необходимо выделить следующие подсети:

* сервер - коммутатор
* сервер – маршрутизатор
* маршрутизатор – филиал 1
* маршрутизатор – филиал 2

|  |  |  |
| --- | --- | --- |
| Адрес подсети  Маска подсети | Широковещательный адрес | IP-адрес |
| 192.14.1.64  255.255.255.192 | 192.14.1.127 | 192.14.1.61-112.14.1.113­­ |
| 192.14.1.0  255.255.255.252 | 192.14.1.3 | 192.14.1.1-192.14.1.2 |
| 10.10.10.0  255.255.255.252 | 10.10.10.3 | 10.10.10.1  10.10.10.2 |
| 10.10.11.4  255.255.255.252 | 10.10.11.3 | 10.10.11.5  10.10.11.6 |

# 7.Выбор сетевых протоколов

*Протокол* – это совокупность специальных правил, а также технических процедур, которые регулируют порядок и способ осуществления связи между компьютерами, которые объединены в какую-либо сеть.

Сетевые протоколы управляют адресацией, маршрутизацией, проверкой ошибок и запросами на повторную передачу пакета (в случае обнаружения ошибки в процессе передачи). Наиболее популярны из них следующие:

* IP (Internet Protocol) – протокол межсетевого взаимодействия.
* TCP (Transmission Control Protocol) - протокол управления передачей.
* TCP/IP протокол содержит стек протоколов, необходимо определиться с тем, какие протоколы этого стека мы будем использовать.

На транспортном уровне существуют следующие протоколы: TCP, UDP. Поскольку нам нужна надежная доставка информации, то лучшим может быть TCP.

На прикладном уровне существуют следующие протоколы: FTP, Telnet, IPSec, SMTP, TFTP, DNS, HTTP.

*Протокол FTP (File Transfer Protocol)* – протокол передачи файлов пользуется транспортными услугами TCP. Пользователь FTP может вызывать несколько команд, которые позволяют ему посмотреть каталог удаленной машины, перейти из одного каталога в другой, а также скопировать один или несколько файлов.

*Протокол SMTP (Simple Mail Transfer Protocol* – простой протокол передачи почты) поддерживает передачу сообщений (электронной почты) между произвольными узлами сети Internet. Имея механизмы промежуточного хранения почты и механизмы повышения надежности доставки, протокол SMTP допускает использование различных транспортных служб. Над модулем SMTP располагается почтовая служба конкретных вычислительных систем.

*IPSec (сокращение от IP Security)* — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет.

*Протокол DNS (Domain Name System)* – протокол разрешения имен.

*Протокол HTTP (Hyper Text Transfer Protocol)* – гипертекстовой транспортный протокол.

Протоколы FTP, SMTP, DNS, TFTP, HTTP – будут использоваться на всех машинах сети.

# 8. Выбор активного и пассивного оборудования

## 8.1. Кабели

## 8.1.1. Витая пара

Скрученная пара проводов называется витой парой. Витая пара существует в экранированном варианте (Shielded Twisted Pair, STP), когда пара медных проводов обертывается в изоляционный экран, и неэкранированном (Unshielded Twisted Pair, UTP), когда изоляционная обертка отсутствует. Скручивание проводов снижает влияние внешних помех на полезные сигналы, передаваемые по кабелю.

В зависимости от наличия защиты — электрически заземлённой медной оплетки или алюминиевой фольги вокруг скрученных пар, определяют разновидности данной технологии:

* неэкранированная витая пара (UTP — Unshielded twisted pair)
* экранированная витая пара (STP — Shielded twisted pair)
* фольгированная витая пара (FTP — Foiled twisted pair)
* фольгированная экранированная витая пара (SFTP — Shielded Foiled twisted pair)

Существует несколько категорий кабеля витая пара, которые нумеруются от CAT1 до CAT7 и определяют эффективный пропускаемый частотный диапазон. Кабель более высокой категории обычно содержит больше пар проводов и каждая пара имеет больше витков на единицу длины. Категории неэкранированной витой пары описываются в стандарте EIA/TIA 568.

В настоящее время наиболее распространенным является кабель категории 5. Кабели этой категории могут работать до частот в 100 Мгц, волновое сопротивление 100 Ом, можно установить и минимальное количество скручиваний на 1 фут длины – 8 скручиваний. Кабель категории 5 стандартизирован для технологии Fast Ethernet и является недорогим решением построения локальных сетей.

Для прокладки сети в зданиях воспользуемся витой парой UTP категории 5e.

## 8.1.2. Волоконно-оптический кабель

*Оптическое волокно* – нить из оптически прозрачного материала (стекло, пластик), используемая для переноса света внутри себя посредством полного внутреннего отражения.

Оптическое волокно имеет круглое сечение и состоит из двух частей — сердцевины и оболочки. Для обеспечения полного внутреннего отражения абсолютный показатель преломления сердцевины несколько выше показателя преломления оболочки. Например, если показатель преломления оболочки равен 1,474, то показатель преломления сердцевины — 1,479.

Луч света, направленный в сердцевину, будет распространяться по ней, испытывая многократные переотражения от границы раздела «сердцевина — оболочка».

Все оптические волокна, используемые в телекоммуникациях, имеют диаметр 125±1 микрон. Диаметр сердцевины может отличаться в зависимости от типа волокна и национальных стандартов.

Характеристики:

* Кабели предназначены для эксплуатации в диапазоне температур от **минус 40 °С до 50 °С**.
* Допустимое растягивающее усилие **2,7 кН**.
* Допустимое раздавливающее усилие не менее **0,5 кН/см**.
* Количество оптических волокон в кабеле - от **2 до 24**.
* Стойкость к раздавливанию **не менее 0,5 кН/см**.
* Стойкость к однократному удару с начальной энергией **5 Дж**.

Для объединения подсетей воспользуемся многомодовым оптоволокном.

Многомодовое волокно широко используется в локальных сетях организаций, когда расстояние между зданиями составляет не более двух километров.

В Европе и России широкое распространение получил стандарт многомодового волокна 50/125, принятый позже и также поддерживаемый спецификациями ISO/IEC 11801 (общая укладка кабеля на территории заказчика).

На скоростях передачи до 622 Мбит/с (STM-4) многомодовое волокно может использоваться совместно со светодиодами (LED). На больших скоростях необходимо использовать лазеры, так как инертные по своей природе светодиоды не способны переключаться достаточно быстро.

Выберем оптический кабель LANmark-OF TBW+ LSZH. Волоконно-оптический кабель Nexans LANmark-OF TBW+ LSZH был разработан специально для того, чтобы соответствовать требованиям к прокладке кабеля как внутри, так и вне зданий. Имеет уникальные характеристики, обеспечивающие выполнение норм пожаробезопасности для внутриобъектового использования и высокую степень влагостойкости для прокладки снаружи. Одновременно с этим кабель TBW+ ориентирован на наиболее экономически эффективную технологию оконцовки – прямую оконцовку волокна на оптическую вилку. Кабели имеют полностью диэлектрическую конструкцию и доступны в оболочке не поддерживающей горение (LSZH-FR). Волокна кабеля в количестве от 2 до 24 внешним диаметром 900 мкм дополнительно защищены кевларовыми нитями. Монтаж кабеля должен быть выполнен в кабелепроводе.

## 8.2. Выбор коммутаторов

*Сетевой коммутатор (switch — переключатель)* — устройство, предназначенное для соединения нескольких [узлов](http://ru.wikipedia.org/wiki/%D0%A3%D0%B7%D0%B5%D0%BB_%D1%81%D0%B5%D1%82%D0%B8) [компьютерной сети](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) в пределах одного или нескольких [сегментов сети](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D0%B3%D0%BC%D0%B5%D0%BD%D1%82_%D1%81%D0%B5%D1%82%D0%B8). Коммутатор работает на [канальном (2) уровне](http://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C) [модели OSI](http://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI) и потому в общем случае может только объединять узлы одной сети по их [MAC-адресам](http://ru.wikipedia.org/wiki/MAC-%D0%B0%D0%B4%D1%80%D0%B5%D1%81).

Рассматривались следующие коммутаторы:

**Коммутатор DES-1008D/PRO на 8 портов:**

**Количество портов**   
 8 портов 10/100 Мбит/с

**Протокол**   
 CSMA/CD

**Сетевые кабели**

* 10BASE-T:

UTP категорий 3, 4, 5 (до 100 м)   
EIA/TIA-568 150 Ом STP (до 100 м)

* 100BASE-TX:   
  UTP категорий 5 (до 100 м)   
  EIA/TIA-568B 150 Ом STP (до 100 м)

**Потребляемая мощность**   
 3.37 Вт

**Коммутатор DGS-1210-24** на 24 порта

**Количество портов**   
24 порта 10/100/1000 Мбит/с, 4 комбо-порта 10/100/1000BASE-T/SFP\

**Сетевые кабели**   
+ UTP категории. 5, 5e (макс. 100 м)   
+ EIA/TIA-568 100 Ом STP (макс. 100 м)

**VLAN**  
+ 802.1Q  
+ Группы VLAN   
- Макс. 256 статических групп VLAN   
- Макс. 4094 VID  
+ Управляющий VLAN  
+ Asymmetric VLAN  
+ Auto Voice VLAN  
- Макс. 10 пользователей определенных OUI  
- Макс. 8 по умолчанию определенных OUI  
**QoS (Quality of Service)**+ 802.1p Quality of Service  
+ 4 очереди на порт  
+ Обработка очередей  
- Strict  
- Weighted Round Robin (WRR)  
+ CoS на основе  
- Очередей приоритетов 802.1p  
- DSCP  
+ Управление полосой пропускания  
- На основе порта (Входящее/исходящее, с шагом до 64 Кб/с)

**Безопасность**  
+ 802.1X  
+ Безопасность порта  
- Поддержка до 64 MAC-адресов на порт   
+ Управление широковещательным /многоадресным /одноадресным штормом  
+ Статический MAC-адрес  
+ D-Link Safeguard Engine  
+ Функция DHCP Server Screening\*  
+ Предотвращение атак ARP Spoofing\*  
- Макс. 64 записи  
+ SSL\*  
- Поддержка v1/v2/v3  
- Поддержка IPv4

**Потребляемая мощность**  
24.1 Вт

**Коммутатор на 16 портов DES-3200-18**

**Количество портов**

16 портов 10/100BASE-T  
+ 1 порт 100/1000 SFP  
+ 1 комбо-порт 10/100/1000BASE-T/ 100/1000 SFP  
  
  
**VLAN**  
+ 802.1Q Tagged VLAN  
+ Группы VLAN:  
  -  Макс. 4K VLAN  
+ VLAN на основе порта  
+ VLAN на основе МАС-адресов  
+ GVRP:  
  - Макс. 255 динамических VLAN  
+ 802.1v VLAN на основе протокола  
+ VLAN Trunking  
+ Asymmetric VLAN3  
+ Double  VLAN (Q-in-Q):  
  - Q-in-Q на основе порта  
  - Selective Q-in-Q  
+ ISM VLAN  
+ VLAN Translation  
+ Voice VLAN4

**Качество обслуживания (QoS)**  
+ Управление полосой пропускания:  
  - На основе порта (входящее/исходящее, с шагом до 62,5кбит/с)  
  - На основе потока (входящее, с шагом до 62,5кбит/с)  
+ 4 очереди на порт  
+ 802.1p  
+ Обработка очередей:  
  - Strict Priority  
  - Weighted Round Robin (WRR)  
+ CoS на основе:  
  - Порта коммутатора  
  - VLAN ID  
  - Очереди приоритетов 802.1p  
  - МАС-адреса  
  - Ether Type  
  - IP-адреса  
  - TOS  
  - DSCP  
  - Типа протокола  
  - Порта TCP/UDP  
  - Содержимого пакета, определяемого пользователем    
+ QoS на основе времени  
+ Поддержка следующих действий для потоков:  
  - Установка тегов приоритетов 802.1p

**Безопасность**  
+ SSH v2  
+ SSL v1/v2/v3  
+ Безопасность порта  
  До 64 МАС-адресов на порт  
+ Управление широковещательным/многоадресным/одноадресным штормом  
+ Traffic Segmentation  
+ IP-MAC-Port Binding (IMPB):  
  - Поддержка D-Link IMPB v3.3  
  - Проверка пакетов ARP  
  - DHCP Snooping  
  - Поддержка до 500 адресных записей на устройство  
+ D-Link Safeguard Engine    
+ Предотвращение атак DoS    
+ Предотвращение ARP Spoofng\*    
+ Предотвращение атак BPDU\*

**Потребляемая мощность**  
 10,7 Вт

Исходя из обзора коммутаторов, сделаем выводы в виде таблицы:

Таблица 8.2.1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Отдел | Свитч | Число занятых портов | Минимальное число портов | Название свитча |
| Администрация | SW1 | 5 | 8 | DES-3200-18 |
| Бухгалтерия | SW2 | 9 | 15 | DES-3200-18 |
| Отдел охраны | SW3 | 7 | 12 | DES-3200-18 |
| Тренерский отдел | SW4 | 15 | 23 | DGS-1210-24 |
| Отдел кадров | SW5 | 7 | 12 | DES-3200-18 |
| Отдел тех.осбслуж. | SW6 | 12 | 19 | DGS-1210-24 |
| Кассы оплаты услуг | SW7 | 4 | 7 | DES-1008D/PRO |
| Отдел физвоспитания | SW8 | 4 | 7 | DES-1008D/PRO |
| Отдел маркетинга | SW9 | 15 | 23 | DGS-1210-24 |
| От.по пров.спор.мероп. | SW14 | 4 | 7 | DES-1008D/PRO |

Также, имеются свитчи, соединяющие здания между собой:

Таблица 8.2.2.

|  |  |  |  |
| --- | --- | --- | --- |
| свитч | Число занятых портов | Минимальное число портов | Название свитча |
| SW10 | 7 | 11 | DES-3200-18 |
| SW11 | 5 | 9 | DES-3200-18 |
| SW12 | 9 | 15 | DES-3200-18 |
| SW13 | 4 | 7 | DES-3200-18 |

## 8.3. Выбор сетевых адаптеров

*Сетевой адаптер*, также известный как сетевая карта, сетевая плата, Ethernet-адаптер, NIC (network interface card) — периферийное устройство, позволяющее [компьютеру](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80) взаимодействовать с другими устройствами [сети](http://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C).

**DGE-528T** -  высокопроизводительный PCI- адаптер Gigabit Ethernet с медным портом 10/100/1000Mбит/с для настольных компьютеров. Устанавливаемый в персональный компьютер и снабженный PCI-слотами расширения, этот адаптер позволяет подключить персональный компьютер к рабочим станциям Gigabit Ethernet или серверам, работающим на скорости 2000Мбит/с в режиме полного дуплекса.

Сетевой адаптер поддерживает фильтрацию тегированных Ethernet-кадров VLAN, позволяя настраивать ПК совместно с коммутатором, поддерживающим VLAN. Компьютер может быть частью виртуальной сети VLAN, изолированной от остальной сети для повышения безопасности и производительности. Адаптер поддерживает функцию управления потоком и независимую очередь FIFO, обеспечивая средства защиты данных во время их передачи по сети. При подключении к гигабитному коммутатору, поддерживающему управление потоком, адаптер, во время пиковых нагрузок, получает от него сигналы о переполнении буфера. После этого адаптер задерживает передачу данных до тех пор, пока не получит сигнал от коммутатора, что он готов к приему данных.

**Протокол**

CSMA/CD

**Скорость передачи данных**

* Ethernet:   
  10Мбит/с (полудуплекс)   
  20Мбит/с (полный дуплекс)
* Fast Ethernet:   
  100Мбит/с s (полудуплекс)   
  200Мбит/с (полный дуплекс)
* Gigabit Ethernet:   
  2000Мбит/с (полный дуплекс)

**Сетевые кабели**

* 10BASE-T:   
  UTP Cat. 3, 4, 5 (100 м макс.)   
  EIA/TIA-586 100-Ом STP (100 м макс.)
* 100BASE-TX, 1000BASE-T:   
  UTP Cat. 5 (100 м макс.)   
  EIA/TIA-568 100- Ом STP (100 м макс.)

## 8.4. Выбор маршрутизатора

*DI-808HV* – это высокопроизводительный широкополосный маршрутизатор с функциями безопасной передачи данных, спроектированный специально для применения в связках центральный офис – отделение. Предлагая эффективное решения для подключения удаленных офисов во всем мире к центральному через Интернет, устройство составляет серьезную конкуренцию подключениям типа точка-точка по дорогим выделенным каналам. Маршрутизатор поддерживает IPSec для обеспечения безопасности соединений, связывая небольшие сети удаленных офисов в единую сеть или позволяя удаленно получать дополнительные сервисы вашим доверенным партнерам.

**Аппаратное ускорение**  
Маршрутизатор использует специально разработанные микросхемы ASIC для выполнения шифрования и дешифрации. Благодаря аппаратному ускорению это снижает нагрузку на процессор.

**Защита межсетевым экраном**  
DI-808HV обеспечивает защиту межсетевым экраном при помощи проверки состояния пакета SPI, ведет протокол попыток хакерских атак типа отказ в обслуживании – DoS. Перед передачей данных во внутреннюю сеть, SPI проверяет содержимое заголовков всех входящих пакетов. Фильтры могут быть настроены на основе МАС-адресов, IP-адресов, URL и/или доменных имен.

**Поддержка DMZ и виртуального сервера**  
Маршрутизатор блокирует и перенаправляет определенные порты, ограничивая сервисы во внутренней сети, к которым внешние пользователи могут получить доступ. Виртуальный сервер используется для перенаправления сервисов на несколько серверов. Маршрутизатор может быть настроен таким образом, что отдельные FTP, Web и игровые серверы смогут совместно использовать один, видимый извне IP адрес, и в тоже время, останутся защищенными от атак хакеров.  
Любой из портов встроенного коммутатора может функционировать в качестве порта DMZ. Установки DMZ применяются для единичного клиента (например, WEB-сервера), находящегося за маршрутизатором для полного доступа к нему из Интернет и гарантии полной совместимости приложений Интернет, даже если определенный порт неизвестен. Это позволяет поддерживать Web-сервер и использовать средства электронной коммерции, обеспечивая безопасность локальной офисной сети.

**8 портовый коммутатор для подключения LAN**  
DI-808HV оснащен 8-ми портовым коммутатором 10/100 Мбит/с, с автоматическим определением скорости и полярности MDI/MDIX, обеспечивая готовое решение для подключения серверов и рабочих станций. Это избавляет от необходимости приобретать отдельный коммутатор и от проблем с его установкой.

**UpnP расширяет совместимость устройств**  
Маршрутизатор спроектирован с учетом совместного использования с гетерогенными устройствами и обеспечивает простоту и надежность подключения к другому оборудованию. Компьютеры могут напрямую работать с маршрутизатором для автоматического открывания и закрытия UDP/TCP портов для использования всех преимуществ безопасности без принесения в жертву работоспособности он-лайновых приложений.

## 8.5. Выбор конфигурации серверов

Сервер1 и Сервер 2:

**HP ProLiant ML310 G5p**

Технические характеристики:

Процессор: Dual-Core Intel® Core™2 duo processor E8400 (3.00 GHz, 6MB L2 Cache, 65 Watts, 1333MHz FSB)

Память: 2\*2GB PC2-6400 UB ECC (DDR2-800MHz)

Максимальный объем памяти: 8GB

Жесткий диск: 2\*HP 1TB 3G SATA 7.2K 3.5" MDL HDD

Сервер 3, 4, 5:

**HP ProLiant DL120 G6**

Технические характеристики:

Процессор: Intel Xeon X3440 Quad-Core

Память: 4\*HP 4GB 2Rx8 PC3-10600 -9 Kit

Максимальный объем памяти: 16GB

Жесткий диск: HP 1TB 6G SAS 7.2K rpm LFF (3.5-inch) Dual Port Midline 1yr Warranty Hard Drive

В качестве рабочих станций используются модели **HP Z210**:

Процессор:Intel Core i7 2.5

Обьем оперативной памяти:4 Гб

Жёсткие диски:Твердотельные диски 160 ГБ

## 8.6. Выбор IP-телефонии

В качестве IP-телефона выбираем **D-LINK-DPH-150S**

Характеристики:

Сетевые интерфейсы:

* 2 порта Ethernet с разъемом RJ-45:
* 1 порт для подключения к кабельному / DSL-модему, удаленному маршрутизатору или коммутатору Ethernet/Gigabit
* 1 порт для подключения к ПК
* Сигнальные, медиа и сетевые протоколы
* SIP RFC 3261
* SDP RFC 3266
* RTP RFC 1889
* Назначение IP-адреса: DHCP, статический IP-адрjavascript:openEditor(document.catForm.behav)ес и PPPoE
* STUN, UPnP и static port mapping
* SNTP
* DNS и DNS SRV
* TFTP/FTP/HTTP
* IP/TCP/UDP/ARP/ICMP  
    
  Голосовые кодеки:
* G.711 a/u (64 кбит/с)
* G.729A/B (8 кбит/с)
* G.723.1 (опционально)  
    
  Расширенные функции QoS:
* Подавление пауз
* Акустическое подавление эха (G.167)
* Определение голосовой активности (VAD)
* Обнаружение/генерация DTMF
* Генерация комфортного шума (CNG)
* Jitter-буфер
* Передатчик DTMF (SIP info, Transparent, RTP 2833 Relay)
* Packet Lost Concealment (PLC)Клавиатура
* Меню
* Телефонная книга
* 4 навигационные клавиши для навигации в настройках, настройка уровня громкости звонка, громкоговорителя и телефонной трубки
* MWI
* Конференция
* Выключение микрофона MUTE
* Function (интегрирована с Mute)
* Transfer
* Redial
* Hold
* Speaker
* 12 цифровых клавиш, включая клавиши \* и #

## 8.7. Выбор IP-камер

Для организации видеонаблюдений потребуются видеокамеры. Выбираем Мегапиксельная IP-камера видеонаблюдения STC-IPM3096A «день-ночь» с MPEG-4, 1280х960 пикс. и 0.06 лк

Некоторые характеристики камеры таковы: чувствительный элемент 1/3” Sony ExViewHAD CCD с прогрессивной разверткой . Стандарт сжатия: MPEG-4/M-JPEG.Подключение IP-камеры к сети: Ethernet 10/100Base-T, RJ-45. Веб-браузер: Internet Explorer 6.0 или выше

Видеокамера поддерживает следующие протоколы: TCP/IP, UDP/IP, HTTP, SMTP, DNS, DHCP, NTP, FTP, RTP.

Для видеоконференций выберем Level One FCS-1010. Ее характеристики:

Поддержка 10/100 Ethernet Auto-MDIX, Поддержка DDNS для динамических IP-адресов, Моторизованный поворот объектива в двух плоскостях, 4-кратное цифровое увеличение, Разрешение от 176x120 до 704x576 , Скорость от 10 до 30 кадров в секунду, 1/4" CCD сенсор, электронный затвор со скоростью до 1/100 000 секунды, Встроенный микрофон 20 Гц - 20 КГц, (сигнал/шум 58 дБ), Встроенный аудио кодек 24 Кбит/с

## 8.8. Выбор датчиков температуры и дыма.

Для контроля помещений будем использовать датчик дыма и температуры THERMASGARD ASTF

|  |  |
| --- | --- |
| **Диапазон измерения температуры** | - 30 ...+75 °C |
| **Чувствительные элементы** | Pt100, Pt1000, Ni1000, NTC, KTY81, LМ235Z |
| **Тип подключения** | по двухпроводной схеме (опционально – трех- или четырехпроводная) |
| **Степень защиты** | IP 30 |
| **Монтаж ⁄ подключение** | при помощи винтов |

# 9.Выбор программного обеспечения.

## 9.1. Выбор сетевой операционной системы

В своей работе в качестве сетевой ОС была выбрана Windows Server 2008 R2, производимая компанией Microsoft.

*Сетевая операционная система* — [операционная система](http://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) со встроенными возможностями для работы в [компьютерных сетях](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C). К таким возможностям можно отнести:

* поддержка сетевого оборудования
* поддержка сетевых протоколов
* поддержка протоколов маршрутизации
* поддержка фильтрации сетевого трафика
* поддержка доступа к удалённым ресурсам, таким как принтеры, диски и т. п. по сети
* поддержка сетевых протоколов авторизации
* наличие в системе сетевых служб, позволяющих удалённым пользователям использовать ресурсы компьютера

## 9.2. Операционная система на рабочих станциях

На рабочих станциях установлена Windows 7 Enterprise.

Windows 7 Enterprise — это выпуск Windows 7, в котором реализованы уникальные технологии, ориентированные на нужды корпоративных клиентов. Помимо функций Windows 7 Professional, заказчики Windows 7 Enterprise получают дополнительные инструменты призванные обеспечить пользователю плодотворную работу в офисе и за его пределами, улучшить безопасность, повысить контроль и сделать администрирование ПК более простым и гибким.

## 9.3. Система управления базами данных

В качестве СУБД используется OracleEnterprise Edition 11g.

Данная СУБД обеспечивает эффективное, надежное и безопасное управление данными таких критически важных для бизнеса приложений, как онлайновые среды, выполняющие масштабную обработку транзакций (OLTP), хранилища данных с высокой интенсивностью потока запросов, а также ресурсоемкие интернет-приложения. Редакция Oracle Database Enterprise Edition предоставляет инструментальные средства и функции, обеспечивающие соответствие требованиям современных корпоративных приложений в области доступности и масштабируемости. Эта редакция содержит все компоненты Oracle Database, а также допускает расширение посредством приобретения дополнительных модулей и приложений.

## 9.4. E-Mail – сервер

В качестве e-mail – сервера используется Microsoft Exchange Server 2010.

Гибкие средства электронных коммуникаций, которые бы оправдывали затраты на их приобретение, сейчас нужны организациям больше, чем когда либо. Microsoft Exchange Server 2010 позволяет достичь новых уровней надежности и производительности, предоставляя возможности, которые упрощают администрирование, помогают защитить передаваемую информацию и радуют пользователей, предоставляя им большую мобильность.

Microsoft Exchange Server, краеугольный камень Объединенных коммуникаций Microsoft – это гибкая и надежная платформа для обмена сообщениями, которая помогает сократить затраты на 50-80%, повысить продуктивность пользователей с помощью повсеместного доступа к электронным коммуникациям и снизить риски с помощью средств контроля и защиты информации.

## 9.5. Web – сервер

В качестве e-mail – сервера используется Apache.

Apache - сервер — [свободный](http://ru.wikipedia.org/wiki/%D0%A1%D0%B2%D0%BE%D0%B1%D0%BE%D0%B4%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) [веб-сервер](http://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80).

Apache является [кроссплатформенным ПО](http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%BE%D1%81%D1%81%D0%BF%D0%BB%D0%B0%D1%82%D1%84%D0%BE%D1%80%D0%BC%D0%B5%D0%BD%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5), поддерживает операционные системы [Linux](http://ru.wikipedia.org/wiki/Linux), [BSD](http://ru.wikipedia.org/wiki/BSD), [Mac OS](http://ru.wikipedia.org/wiki/Mac_OS), [Microsoft Windows](http://ru.wikipedia.org/wiki/Microsoft_Windows), [Novell NetWare](http://ru.wikipedia.org/wiki/Novell_NetWare),[BeOS](http://ru.wikipedia.org/wiki/BeOS).

Основными достоинствами Apache считаются надёжность и гибкость конфигурации. Он позволяет подключать внешние модули для предоставления данных, использовать [СУБД](http://ru.wikipedia.org/wiki/%D0%A1%D0%A3%D0%91%D0%94) для [аутентификации](http://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) пользователей, модифицировать сообщения об ошибках и т. д. Поддерживает [IPv6](http://ru.wikipedia.org/wiki/IPv6).

Существует множество модулей, добавляющих к Apache поддержку различных [языков программирования](http://ru.wikipedia.org/wiki/%D0%AF%D0%B7%D1%8B%D0%BA_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F) и систем разработки. Кроме того, Apache поддерживает механизмы [CGI](http://ru.wikipedia.org/wiki/CGI) и [FastCGI](http://ru.wikipedia.org/wiki/FastCGI" \o "FastCGI), что позволяет исполнять программы на практически всех языках программирования, в том числе [C](http://ru.wikipedia.org/wiki/%D0%A1%D0%B8_(%D1%8F%D0%B7%D1%8B%D0%BA_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F)), [C++](http://ru.wikipedia.org/wiki/C%2B%2B), [sh](http://ru.wikipedia.org/wiki/Sh" \o "Sh), [Java](http://ru.wikipedia.org/wiki/Java).

Apache имеет различные механизмы обеспечения безопасности и разграничения доступа к данным. Основными являются:

* Ограничение доступа к определённым директориям или файлам.
* Механизм [авторизации](http://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) пользователей для доступа к директории по методу HTTP-Авторизации (mod\_auth\_basic) и digest-авторизации (mod\_auth\_digest).
* Ограничение доступа к определённым директориям или всему серверу, основанное на [IP-адресах](http://ru.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81) пользователей.
* Запрет доступа к определённым типам файлов для всех или части пользователей, например, запрет доступа к конфигурационным файлам и файлам баз данных.
* Существуют модули, реализующие авторизацию через [СУБД](http://ru.wikipedia.org/wiki/%D0%A1%D0%A3%D0%91%D0%94) или [PAM](http://ru.wikipedia.org/wiki/PAM).

## 9.6. Антивирусный сервер

Антивирус Касперского для Windows Servers Enterprise Edition защищает данные на серверах под управлением Microsoft Windows Server. Продукт разработан специально для высокопроизводительных корпоративных серверов.

Преимущества продукта:

* Высокая производительность.   
  Новое антивирусное ядро, регулируемое использование ресурсов сервера, технологии оптимизации антивирусного сканирования и гибкая система исключений из проверки повышают производительность продукта и уменьшают нагрузку на сервер.
* Поддержка Windows Server 2008 R2.   
  Продукт поддерживает актуальные версии Microsoft Windows Server, в том числе Windows Server 2008 R2 (включая режим Server Core и редакцию Microsoft Hyper-V Server 2008 R2).
* Защита сложной сетевой инфраструктуры.   
  Продукт защищает терминальные серверы Citrix и Microsoft Terminal, а также кластеры серверов, что позволяет использовать его в крупных компаниях со сложной сетевой инфраструктурой.
* Поддержка виртуализированных сред.   
  Продукт имеет сертификат VMware Ready, подтверждающий его эффективную работу в виртуализированных средах.
* Защита файловых систем со сложной иерархией.   
  Продукт совместим с системами иерархического управления запоминающими устройствами (HSM), что обеспечивает более эффективное управление защитой.
* Удобное управление и гибкая система отчетов.   
  Простые в использовании средства управления продуктом, интуитивно понятный интерфейс, подробная информация о статусе защиты сервера, гибкие настройки сканирования и формирования отчетов позволяют эффективно управлять безопасностью файловых серверов.
* Надежность.   
  Автоматический перезапуск продукта в случае принудительного завершения его работы или программного сбоя обеспечивает стабильность системы защиты, в то время как система диагностики позволяет установить причину сбоя.
* Совместимость с другим серверным ПО.   
  Продукт совместим с решениями сторонних производителей (программами резервного копирования, системами HSM и др.)

# 10.Разработка имитационной модели.

Моделирование корпоративной сети произведем в системе моделирования GPSS/PC, использующей для описания модели сети язык GPSS. Основываясь на принципах перехода сообщений от устройства к устройству, она наиболее подходит для моделирования потоков пакетов.

Каждый отдел представим в виде одного компьютера. Расчет параметров модели сети будем вести с учетом средней длинны пакета: Vп=1000 байт. В модели используем следующие события:

* Рабочие станции посылают сообщения серверам с подтверждением;
* Некоторые сервера(указано в таблице доступа) общаются между собой;

## 10.1. Расчет задержки в каналах.

Задержке в канале рассчитывается по формуле:



где - скорость среды передачи;

 - размер пакета.

Расчет задержек в каналах приведен в таблице 10.1.

Таблица 10.1.

|  |  |  |  |
| --- | --- | --- | --- |
| **Тип линии** | **Объем пакета (Vпакета),байты** | **Скорость среды , байт/с** | **Задержка L , с** |
| Витая пара | 1000 | 12500000 | 0,000080 |
| Оптоволокно | 1000 | 125000000 | 0,000008 |

## 10.2. Расчет задержки в коммутаторах.

Расчет задержки посчитаем по формуле:

 , где

 - объем пакета;

 - скорость передачи;

N – количество портов

Расчет задержек на коммутаторах приведен в таблице 12.2.

Таблица 10.2.

|  |  |  |
| --- | --- | --- |
| **Номер свитча на схеме.** | **Число портов** | **Время задержки, с** |
| 1 | 24 | 0,00192 |
| 2 | 8 | 0,00064 |
| 3 | 24 | 0,00192 |
| 4 | 24 | 0,00192 |
| 5 | 24 | 0,00192 |
| 6 | 16 | 0,00128 |
| 7 | 16 | 0,00128 |
| 8 | 16 | 0,00128 |
| 9 | 24 | 0,00192 |
| 10 | 16 | 0,00128 |
| 11 | 8 | 0,00064 |
| 12 | 8 | 0,00064 |
| 13 | 8 | 0,00064 |
| 14 | 16 | 0,00013 |

## 10.3. Расчет задержки на серверах и компьютерах.

В задержку времени обработки сервером одного сообщения входит обращение к НМЖД плюс время обработки процессором:



,где  - время доступа к НМЖД,

- частота процессора сервера,

- разрядность процессора.

Время доступа к НМЖД составляет примерно в два раза больше времени обработки процессором:



Задержки на сервере:

,



В итоге, получаем следующее:

|  |  |
| --- | --- |
| Сервер | Задержка (в с) |
| Сервер1, сервер 2 |  |
| Сервер3, сервер4, сервер5 |  |

Задержка на рабочих станциях:



## 10.4. Расчет времени генерации.

Произведем корректировку объема информации по формуле:

;

Период генерации пакетов одним отделом:

;

Период генерации пакетов рабочими станциями:

Таблица 10.4.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Отдел** | **Максимальный поток (V), Мбайт/час** | **Макс. Поток(V’), байт/с** | **Время генерации**  **одним компьютером(G), с** |
| 1 | Администрация | 233 | 64722,22 | 0,030901 |
| 2 | Отдел кадров | 118 | 32777,78 | 0,061017 |
| 3 | Бухгалтерия | 366 | 101666,7 | 0,019672 |
| 4 | Отдел охраны | 128 | 35555,56 | 0,05625 |
| 5 | Отдел тех.обслуж. | 131 | 36388,89 | 0,054962 |
| 6 | Отдел физвоспит. | 81 | 22500 | 0,088889 |
| 7 | От. по провед. спорт. мероприятий | 301 | 83611,11 | 0,02392 |
| 8 | Кассы оплаты | 136 | 37777,78 | 0,052941 |
| 9 | Тренерский отдел | 106 | 29444,44 | 0,067925 |
| 10 | Отдел маркетинга | 106 | 29444,44 | 0,067925 |
| 11 | Филиал1 | 119 | 33055,56 | 0,060504 |
| 12 | Филиал2 | 149 | 41388,89 | 0,048322 |

## 10.5. Результат и анализ моделирования.

В результате моделирования работы сети необходимо определить в течении какого времени она может стабильно функционировать. С каждым годом нагрузка сети повышается на 25%. В нашем случае необходимо увеличивать нагрузку сети за счет уменьшения времени генерации в 1,25 раза с каждым годом до тех пор пока сеть не выйдет из строя. Значения задержек для каждого года приведены в таблице 10.7.

Расчет времени генерации по годам. Таблица 10.7.

|  |  |  |  |
| --- | --- | --- | --- |
| Администрация | 30901,29 | 24721 | 19776,82 |
| Отдел кадров | 61016,95 | 48814 | 39050,85 |
| Бухгалтерия | 19672,13 | 15738 | 12590,16 |
| Отдел охраны | 56250 | 45000 | 36000 |
| Отдел технич. обслуживания | 54961,83 | 43969 | 35175,57 |
| Отдел физвоспитания | 88888,89 | 71111 | 56888,89 |
| Отдел по провед. спортивных мероприятий | 23920,27 | 19136 | 15308,97 |
| Кассы оплаты услуг | 52941,18 | 42353 | 33882,35 |
| Тренерский отдел | 67924,53 | 54340 | 43471,7 |
| Отдел маркетинга | 67924,53 | 54340 | 43471,7 |
| Филиал1 | 60504,2 | 48403 | 38722,69 |
| Филиал2 | 48322,15 | 38658 | 30926,17 |

Листинг модели для языка GPSS, составленного для первого года эксплуатации представлен в приложении 3. Фрагменты отчетов по нечетным годам от начала эксплуатации сети, составленные программой GPSSREPT, представлены в приложении В. В 5-й год нагрузка больше на 25%, в 7-й ещё на 25% больше.

Степень загруженности коммутаторов(%). Таблица 10.8.

|  |  |  |  |
| --- | --- | --- | --- |
| Устройство | Год эксплуатации | | |
| 1 | 5 | 7 |
| sw1 | 9,7 | 12,3 | 15,9 |
| sw2 | 1,7 | 3 | 3,8 |
| sw3 | 0,4 | 0,6 | 0,8 |
| sw4 | 15,3 | 18,7 | 21,2 |
| sw5 | 4,9 | 10,5 | 13,3 |
| sw6 | 3,3 | 6,6 | 8,4 |
| sw7 | 30,8 | 31,2 | 33,4 |
| sw8 | 2,3 | 3,8 | 4,3 |
| sw9 | 10,5 | 11,2 | 12,8 |
| sw10 | 59,5 | 64,3 | 69,6 |
| sw11 | 2,1 | 3,6 | 5 |
| sw12 | 1,6 | 2,3 | 3,6 |
| sw13 | 1,6 | 2,3 | 3,6 |
| sw14 | 0,4 | 0,6 | 0,8 |

По результатам отчета мы видим, что нагрузка на сеть после 5 лет использования вцелом возрасла незначительно. Коммутаторы по-прежнему используются не больше, чем на 1%. Нагрузка на сервера и каналы стала незначительно больше, но тоже не превышает предельных значений. Из всего этого мы можем сделать вывод, что на первоначальном этапе сервера в четвертом здании мы можем объединить в один, что позволит значительно сэкономить ресурсы.

Из результатов отчета по 7-му году эксплуатации видно, что нагрузка на сеть возросла, но сеть с ней нормально справляется. Сервера и коммутаторы также справляюся с нагрузкой. Таким образом, из результатов моделирования видно, что в течение 7 лет сеть будет работать стабильно. Также имеется резерв для расширения сети.

Разработанная мною программа является модельной и может оличаться от работы реальной сети, но из результатов моделирования видно, что разарботанная сеть имеет резерв для расширения и может выдержать более сильные нагрузки, поэтому данную сеть можно внедрить в работу культурно-спортивного центра.

# 11.Разработка плана монтажной прокладки соединений сети и расположения сетевого оборудования в зданиях организации и разработка кабельных трасс между зданиями

План монтажной прокладки приведён в приложении Г.

Линии в зданиях прокладываются по стандарту *TIA/EIA*, который определяет:

* минимально необходимые требования для телекоммуникационной проводки в офисных и промышленных помещениях;
* рекомендованную топологию и длины для кабельной сети;
* параметры сред, определяющие качество систем;
* назначение и раскладку коннекторов и контактов для гарантии их взаимозаменяемости;
* возможность использования телекоммуникационных кабельных систем по истечении десяти лет.

Внутри зданий используется кабель витая пара. Между зданиями через подземные коммуникации на глубине 3 метров прокладывается оптоволоконный кабель.

В таблице 11.1 указано необходимое для построения сети количество кабеля.

Таблица 11.1

|  |  |
| --- | --- |
| **Тип кабеля** | **Общая длина** |
| Витая пара | 825 м |
| Оптоволоконный кабель | 1. м |

# 12.Смета разработки проекта сети

Таблица 12.1

|  |  |  |
| --- | --- | --- |
| **Наименование** | **Модель/Версия** | **Количество** |
| Кабели | | |
| Витая пара | LAN-5EUTP | 3 катушки (по 305 м) |
| Оптоволоконный кабель | LANmark-OF TBW+ LSZH | 2200 м |
| Сетевое оборудование | | |
| Коммутатор | D-Link DES-108D/PRO | 3 шт. |
| Коммутатор | D-Link DES-3200-18 | 8 шт. |
| Коммутатор | D-Link DGS-1210-24 | 3 шт. |
| Сетевая плата | D-Link DGE-528T | 80 шт. |
| Маршрутизатор | D-Link DI-808HV | 1 шт. |
| IP-камера | STC-IPM3096A | 12 шт. |
| IP-телефон | D-Link DPH-150S | 2 шт. |
| IP-датчик огня и дыма | THERMASGARD ASTF | 12 шт. |
| Рабочие станции/серверы | | |
| Сервер модель 1 | HP ProLiant ML310G5p | 2 шт. |
| Сервер модель 2 | HP ProLiant DL120G6 | 3 шт. |
| Рабочая станция | HP Z210 | 72 шт. |
| Программное обеспечение | | |
| Операционная система | Windows Server 2008 R2 | на 5 серверов |
| Операционная система | Windows 7 Enterprise | на 72 рабочих мест |
| СУБД | Oracle Enterprise Edition 11g | на 1 сервер |
| Веб-сервер | Apache 2.3 | на 1 сервер |
| Антивирусный сервер | Антивирус Касперского  для Windows Servers Enterprise Edition | на 1 сервер |
| E-Mail - сервер | Microsoft Exchange Server 2010 | на 1 сервер |

# ЗАКЛЮЧЕНИЕ.

В данном курсовом проекте была разработана корпоративная сеть для культурно-спортивного центра. Для более достоверного расчёта необходимы реальные данные и более глубокие знания в данной области, дальнейшее изучение позволит подробнее разобраться и применять знания для проектировки сетей.

В ходе разработки проекта были определены информационные потоки между отделами, с учетом которых были выбраны сервера и построена схема информационных потоков с учетом серверов. Далее в ходе курсового проекта было выбрано активное и пассивное сетевое оборудование, сетевая и клиентские операционные системы и сетевое прикладное обеспечение, разработана защита сети от несанкционированного внутреннего и внешнего доступа. Составлен план монтажной прокладки соединений сети и расположения сетевого оборудования. Так же составлена смета разработки проекта сети, произведено моделирование сети на языке имитационного моделирования GPSS. В завершение проекта составлена смета разработки проекта сети.

# 

# Приложение А

# 

# Приложение Б

Листинг программы GPSS на начало эксплуатации сети.

1 AD1 FUNCTION RN3,D4

0.1,1/0.5,2/0.9,3/1,4

2 ADRPC1 FUNCTION RN3,D5

0.13,11/0.37,12/0.59,13/0.8,14/1,15

3 ADRPC2 FUNCTION RN3,D5

0.08,11/0.42,12/0.59,13/0.67,14/1,15

4 ADRPC3 FUNCTION RN3,D5

0.03,11/0.3,12/0.51,13/0.78,14/1,15

5 ADRPC4 FUNCTION RN3,D5

0.08,11/0.55,12/0.78,13/0.79,14/1,15

6 ADRPC5 FUNCTION RN3,D5

0.08,11/0.53,12/0.73,13/0.93,14/1,15

7 ADRPC6 FUNCTION RN3,D5

0.12,11/0.8,12/0.88,13/0.94,14/1,15

8 ADRPC7 FUNCTION RN3,D5

0.03,11/0.53,12/0.76,13/0.77,14/1,15

9 ADRPC8 FUNCTION RN3,D5

0.07,11/0.51,12/0.7,13/0.85,14/1,15

10 ADRPC9 FUNCTION RN3,D5

0.09,11/0.66,12/0.8,13/0.94,14/1,15

11 ADRPC10 FUNCTION RN3,D5

0.09,11/0.66,12/0.76,13/0.86,14/1,1520 GENERATE 30901,5000

30 SEIZE PC1

40 ASSIGN 1,1

50 ASSIGN 2,FN$ADRPC1

60 ASSIGN 3,FN$AD1

70 ASSIGN 4,0

80 ADVANCE 36,18

90 RELEASE PC1

100 SEIZE KAN1

110 ADVANCE 80,40

120 RELEASE KAN1

130 TRANSFER ,SW\_I

140 GENERATE 30901,5000

150 SEIZE PCF1

160 ADVANCE 36,18

170 RELEASE PCF1

180 TRANSFER ,LKF1P

190 GENERATE 30901,5000

200 SEIZE PCF2

210 ADVANCE 36,18

220 RELEASE PCF2

230 TRANSFER ,LKF2P

240 GENERATE 61016,5000

250 SEIZE PC2

260 ASSIGN 1,2

270 ASSIGN 2,FN$ADRPC2

280 ASSIGN 3,FN$AD1

290 ASSIGN 4,0

300 ADVANCE 36,18

310 RELEASE PC2

320 SEIZE KAN2

330 ADVANCE 80,40

340 RELEASE KAN2

350 TRANSFER ,SW\_II

360 GENERATE 19675,5000

370 SEIZE PC3

380 ASSIGN 1,3

390 ASSIGN 2,FN$ADRPC3

400 ASSIGN 3,FN$AD1

410 ASSIGN 4,0

420 ADVANCE 36,18

430 RELEASE PC3

440 SEIZE KAN3

450 ADVANCE 80,40

460 RELEASE KAN3

470 TRANSFER ,SW\_IV

480 GENERATE 56250,5000

490 SEIZE PC4

500 ASSIGN 1,4

510 ASSIGN 2,FN$ADRPC4

520 ASSIGN 3,FN$AD1

530 ASSIGN 4,0

540 ADVANCE 36,18

550 RELEASE PC4

560 SEIZE KAN4

570 ADVANCE 80,40

580 RELEASE KAN4

590 TRANSFER ,SW\_V

600 GENERATE 54961,5000

610 SEIZE PC5

620 ASSIGN 1,5

630 ASSIGN 2,FN$ADRPC5

640 ASSIGN 3,FN$AD1

650 ASSIGN 4,0

660 ADVANCE 36,18

670 RELEASE PC5

680 SEIZE KAN5

690 ADVANCE 80,40

700 RELEASE KAN5

710 TRANSFER ,SW\_VI

720 GENERATE 88888,5000

730 SEIZE PC6

740 ASSIGN 1,6

750 ASSIGN 2,FN$ADRPC6

760 ASSIGN 3,FN$AD1

770 ASSIGN 4,0

780 ADVANCE 36,18

790 RELEASE PC6

800 SEIZE KAN6

810 ADVANCE 80,40

820 RELEASE KAN6

830 TRANSFER ,SW\_VIII

840 GENERATE 29920,5000

850 SEIZE PC7

860 ASSIGN 1,7

870 ASSIGN 2,FN$ADRPC7

880 ASSIGN 3,FN$AD1

890 ASSIGN 4,0

900 ADVANCE 36,18

910 RELEASE PC7

920 SEIZE KAN7

930 ADVANCE 80,40

940 RELEASE KAN7

950 TRANSFER ,SW\_IX

960 GENERATE 52941,5000

970 SEIZE PC8

980 ASSIGN 1,8

990 ASSIGN 2,FN$ADRPC8

1000 ASSIGN 3,FN$AD1

1010 ASSIGN 4,0

1020 ADVANCE 36,18

1030 RELEASE PC8

1040 SEIZE KAN8

1050 ADVANCE 80,40

1060 RELEASE KAN8

1070 TRANSFER ,SW\_XI

1080 GENERATE 67924,5000

1090 SEIZE PC9

1100 ASSIGN 1,9

1110 ASSIGN 2,FN$ADRPC9

1120 ASSIGN 3,FN$AD1

1130 ASSIGN 4,0

1140 ADVANCE 36,18

1150 RELEASE PC9

1160 SEIZE KAN9

1170 ADVANCE 80,40

1180 RELEASE KAN9

1190 TRANSFER ,SW\_XII

1200 GENERATE 67924,5000

1210 SEIZE PC10

1220 ASSIGN 1,10

1230 ASSIGN 2,FN$ADRPC10

1240 ASSIGN 3,FN$AD1

1250 ASSIGN 4,0

1260 ADVANCE 36,18

1270 RELEASE PC10

1280 SEIZE KAN10

1290 ADVANCE 80,40

1300 RELEASE KAN10

1310 TRANSFER ,SW\_XIII

1320 GENERATE 60000,5000

1330 SEIZE FS4

1340 ASSIGN 1,14

1350 ASSIGN 2,13

1360 ASSIGN 3,FN$AD1

1370 ASSIGN 4,0

1380 ADVANCE 36,18

1390 RELEASE FS4

1400 SEIZE KAN28

1410 ADVANCE 80,40

1420 RELEASE KAN28

1430 TRANSFER ,SW\_X

1440 GENERATE 60000,5000

1450 SEIZE FS1

1460 ASSIGN 1,11

1470 ASSIGN 2,15

1480 ASSIGN 3,FN$AD1

1490 ASSIGN 4,0

1500 ADVANCE 36,18

1510 RELEASE FS1

1520 SEIZE KAN25

1530 ADVANCE 80,40

1540 RELEASE KAN25

1550 TRANSFER ,SW\_X

1560 LK1 SEIZE KAN1

1570 ADVANCE 80,40

1580 RELEASE KAN1

1590 SEIZE PC1

1600 ADVANCE 72,36

1610 RELEASE PC1

1620 TERMINATE

1630 LK2 SEIZE KAN2

1640 ADVANCE 80,40

1650 RELEASE KAN2

1660 SEIZE PC2

1670 ADVANCE 72,36

1680 RELEASE PC2

1690 TERMINATE

1700 LK3 SEIZE KAN3

1710 ADVANCE 80,40

1720 RELEASE KAN3

1730 SEIZE PC3

1740 ADVANCE 72,36

1750 RELEASE PC3

1760 TERMINATE

1770 LK4 SEIZE KAN4

1780 ADVANCE 80,40

1790 RELEASE KAN4

1800 SEIZE PC4

1810 ADVANCE 72,36

1820 RELEASE PC4

1830 TERMINATE

1840 LK5 SEIZE KAN5

1850 ADVANCE 80,40

1860 RELEASE KAN5

1870 SEIZE PC5

1880 ADVANCE 72,36

1890 RELEASE PC5

1900 TERMINATE

1910 LK6 SEIZE KAN6

1920 ADVANCE 80,40

1930 RELEASE KAN6

1940 SEIZE PC6

1950 ADVANCE 72,36

1960 RELEASE PC6

1970 TERMINATE

1980 LK7 SEIZE KAN7

1990 ADVANCE 80,40

2000 RELEASE KAN7

2010 SEIZE PC7

2020 ADVANCE 72,36

2030 RELEASE PC7

2040 TERMINATE

2050 LK8 SEIZE KAN8

2060 ADVANCE 80,40

2070 RELEASE KAN8

2080 SEIZE PC8

2090 ADVANCE 72,36

2100 RELEASE PC8

2110 TERMINATE

2120 LK9 SEIZE KAN9

2130 ADVANCE 80,40

2140 RELEASE KAN9

2150 SEIZE PC9

2160 ADVANCE 72,36

2170 RELEASE PC9

2180 TERMINATE

2190 LK10 SEIZE KAN10

2200 ADVANCE 80,40

2210 RELEASE KAN10

2220 SEIZE PC10

2230 ADVANCE 72,36

2240 RELEASE PC10

2250 TERMINATE

2260 SW\_I SEIZE SW1

2270 ADVANCE 1920,900

2280 RELEASE SW1

2290 TEST NE p3 1 d11

2300 TEST NE p3 2 d12

2310 TEST NE p3 3 d13

2320 TEST NE p3 4 d14

2330 ff1 TEST NE P2 1 LK1

2340 TRANSFER ,LK1S

2350 LK1S SEIZE KAN11

2360 ADVANCE 80,40

2370 RELEASE KAN11

2380 TRANSFER ,SW\_III

2390 SW\_II SEIZE SW2

2400 ADVANCE 640,320

2410 RELEASE SW2

2420 TEST NE p3 1 d21

2430 TEST NE p3 2 d22

2440 TEST NE p3 3 d23

2450 TEST NE p3 4 d24

2460 ff2 TEST NE P2 2 LK2

2470 TRANSFER ,LK2S

2480 LK2S SEIZE KAN12

2490 ADVANCE 80,40

2500 RELEASE KAN12

2510 TRANSFER ,SW\_III

2520 SW\_III SEIZE SW3

2530 ADVANCE 64,5

2540 RELEASE SW3

2550 TEST NE p3 1 d31

2560 TEST NE p3 2 d32

2570 TEST NE p3 3 d33

2580 TEST NE p3 4 d34

2590 ff3 TEST NE P2 2 LK2P

2600 TEST NE P2 1 LK1P

2610 TRANSFER ,LK13S

2620 LK13S SEIZE KAN13

2630 ADVANCE 80,40

2640 RELEASE KAN13

2650 TRANSFER ,SW\_X

2660 LK1P SEIZE KAN11

2670 ADVANCE 80,40

2680 RELEASE KAN11

2690 TRANSFER ,SW\_I

2700 LK2P SEIZE KAN12

2710 ADVANCE 80,40

2720 RELEASE KAN12

2730 TRANSFER ,SW\_II

2740 SW\_IV SEIZE SW4 ;

2750 ADVANCE 1920,900

2760 RELEASE SW4

2770 TEST NE p3 1 d41

2780 TEST NE p3 2 d42

2790 TEST NE p3 3 d43

2800 TEST NE p3 4 d44

2810 ff4 TEST NE P2 3 LK3

2820 TRANSFER ,LK4S

2830 LK4S SEIZE KAN14

2840 ADVANCE 80,40

2850 RELEASE KAN14

2860 TRANSFER ,SW\_VII

2870 SW\_V SEIZE SW5

2880 ADVANCE 1920,900

2890 RELEASE SW5

2900 TEST NE p3 1 d51

2910 TEST NE p3 2 d52

2920 TEST NE p3 3 d53

2930 TEST NE p3 4 d54

2940 ff5 TEST NE P2 4 LK4

2950 TRANSFER ,LK5S

2960 LK5S SEIZE KAN15

2970 ADVANCE 80,40

2980 RELEASE KAN15

2990 TRANSFER ,SW\_VII

3000 SW\_VI SEIZE SW6

3010 ADVANCE 1280,640

3020 RELEASE SW6

3030 TEST NE p3 1 d61

3040 TEST NE p3 2 d62

3050 TEST NE p3 3 d63

3060 TEST NE p3 4 d64

3070 ff6 TEST NE P2 5 LK5

3080 TRANSFER ,LK6S

3090 LK6S SEIZE KAN16

3100 ADVANCE 80,40

3110 RELEASE KAN16

3120 TRANSFER ,SW\_VII

3130 SW\_VII SEIZE SW7

3140 ADVANCE 64,5

3150 RELEASE SW7

3160 TEST NE p3 1 d71

3170 TEST NE p3 2 d72

3180 TEST NE p3 3 d73

3190 TEST NE p3 4 d74

3200 ff7 TEST NE P2 3 LK4P

3210 TEST NE P2 4 LK5P

3220 TEST NE P2 5 LK6P

3230 TRANSFER ,LK17S

3240 LK17S SEIZE KAN17

3250 ADVANCE 80,40

3260 RELEASE KAN17

3270 TRANSFER ,SW\_X

3280 LK4P SEIZE KAN14

3290 ADVANCE 80,40

3300 RELEASE KAN14

3310 TRANSFER ,SW\_IV

3320 LK5P SEIZE KAN15

3330 ADVANCE 80,40

3340 RELEASE KAN15

3350 TRANSFER ,SW\_V

3360 LK6P SEIZE KAN16

3370 ADVANCE 80,40

3380 RELEASE KAN16

3390 TRANSFER ,SW\_VI

3400 SW\_VIII SEIZE SW8

3410 ADVANCE 1280,640

3420 RELEASE SW8

3430 TEST NE p3 1 d81

3440 TEST NE p3 2 d82

3450 TEST NE p3 3 d83

3460 TEST NE p3 4 d84

3470 ff8 TEST NE P2 6 LK6

3480 TRANSFER ,LK8S

3490 LK8S SEIZE KAN18

3500 ADVANCE 80,40

3510 RELEASE KAN18

3520 TRANSFER ,SW\_X

3530 SW\_IX SEIZE SW9

3540 ADVANCE 1920,900

3550 RELEASE SW9

3560 TEST NE p3 1 d91

3570 TEST NE p3 2 d92

3580 TEST NE p3 3 d93

3590 TEST NE p3 4 d94

3600 ff9 TEST NE P2 7 LK7

3610 TRANSFER ,LK9S

3620 LK9S SEIZE KAN19

3630 ADVANCE 80,40

3640 RELEASE KAN19

3650 TRANSFER ,SW\_X

3660 SW\_X SEIZE SW10

3670 ADVANCE 120,5

3680 RELEASE SW10

3690 TEST NE p3 1 d101

3700 TEST NE p3 2 d102

3710 TEST NE p3 3 d103

3720 TEST NE p3 4 d104

3730 ff10 TEST NE P2 1 LK13P

3740 TEST NE P2 2 LK13P

3750 TEST NE P2 3 LK17P

3760 TEST NE P2 4 LK17P

3770 TEST NE P2 5 LK17P

3780 TEST NE P2 6 LK8P

3790 TEST NE P2 7 LK9P

3800 TEST NE P2 8 LK20P

3810 TEST NE P2 9 LK20P

3820 TEST NE P2 10 LK20P

3830 TEST NE P2 11 LK25S

3840 TEST NE P2 12 LK26S

3850 TEST NE P2 13 LK27S

3860 TEST NE P2 14 LK28S

3870 TEST NE P2 15 LK29S

3880 LK20S SEIZE KAN20

3890 ADVANCE 8,4

3900 RELEASE KAN20

3910 TRANSFER ,SW\_X

3920 LK8P SEIZE KAN18

3930 ADVANCE 80,40

3940 RELEASE KAN18

3950 TRANSFER ,SW\_VIII

3960 LK9P SEIZE KAN19

3970 ADVANCE 80,40

3980 RELEASE KAN19

3990 TRANSFER ,SW\_IX

4000 SW\_XI SEIZE SW11

4010 ADVANCE 720,360

4020 RELEASE SW11

4030 TEST NE p3 1 d111

4040 TEST NE p3 2 d112

4050 TEST NE p3 3 d113

4060 TEST NE p3 4 d114

4070 ff11 TEST NE P2 8 LK8

4080 TRANSFER ,LK11S

4090 LK11S SEIZE KAN21

4100 ADVANCE 8,4

4110 RELEASE KAN21

4120 TRANSFER ,SW\_XIV

4130 SW\_XII SEIZE SW12

4140 ADVANCE 720,360

4150 RELEASE SW12

4160 TEST NE p3 1 d121

4170 TEST NE p3 2 d122

4180 TEST NE p3 3 d123

4190 TEST NE p3 4 d124

4200 ff12 TEST NE P2 9 LK9

4210 TRANSFER ,LK22S

4220 LK22S SEIZE KAN22

4230 ADVANCE 8,4

4240 RELEASE KAN22

4250 TRANSFER ,SW\_XIV

4260 SW\_XIII SEIZE SW13

4270 ADVANCE 720,360

4280 RELEASE SW13

4290 TEST NE p3 1 d131

4300 TEST NE p3 2 d132

4310 TEST NE p3 3 d133

4320 TEST NE p3 4 d134

4330 ff13 TEST NE P2 10 LK1

4340 TRANSFER ,LK23S

4350 LK23S SEIZE KAN23

4360 ADVANCE 8,4

4370 RELEASE KAN23

4380 TRANSFER ,SW\_XIV

4390 SW\_XIV SEIZE SW14

4400 ADVANCE 64,5

4410 RELEASE SW14

4420 TEST NE p3 1 d141

4430 TEST NE p3 2 d142

4440 TEST NE p3 3 d143

4450 TEST NE p3 4 d144

4460 ff14 TEST NE P2 8 LK21P

4470 TEST NE P2 9 LK22P

4480 TEST NE P2 10 LK23P

4490 TRANSFER ,LK20S

4500 LK13P SEIZE KAN13

4510 ADVANCE 80,40

4520 RELEASE KAN13

4530 TRANSFER ,SW\_III

4540 LK17P SEIZE KAN17

4550 ADVANCE 80,40

4560 RELEASE KAN17

4570 TRANSFER ,SW\_VII

4580 LK20P SEIZE KAN20

4590 ADVANCE 8,40

4600 RELEASE KAN20

4610 TRANSFER ,SW\_XIV

4620 LK21P SEIZE KAN21

4630 ADVANCE 8,4

4640 RELEASE KAN21

4650 TRANSFER ,SW\_XI

4660 LK22P SEIZE KAN22

4670 ADVANCE 8,4

4680 RELEASE KAN22

4690 TRANSFER ,SW\_XII

4700 LK23P SEIZE KAN23

4710 ADVANCE 8,4

4720 RELEASE KAN23

4730 TRANSFER ,SW\_XIII

4740 LK25S SEIZE KAN25

4750 ADVANCE 8,4

4760 RELEASE KAN25

4770 SEIZE FS1

4780 ADVANCE 36,18

4790 ASSIGN 2 P1

4800 RELEASE FS1

4810 test ne p4 1 stop

4820 ASSIGN 2 P1

4830 ASSIGN 4 0

4840 SEIZE KAN25

4850 ADVANCE 8,4

4860 RELEASE KAN25

4870 TRANSFER ,SW\_X

4880 LK26S SEIZE KAN26

4890 ADVANCE 8,4

4900 RELEASE KAN26

4910 SEIZE FS2

4920 ADVANCE 36,18

4930 ASSIGN 2 P1

4940 RELEASE FS2

4950 test ne p4 1 stop

4960 ASSIGN 2 P1

4970 ASSIGN 4 0

4980 SEIZE KAN26

4990 ADVANCE 8,4

5000 RELEASE KAN26

5010 TRANSFER ,SW\_X

5020 LK27S SEIZE KAN27

5030 ADVANCE 8,4

5040 RELEASE KAN27

5050 SEIZE FS3

5060 ADVANCE 36,18

5070 ASSIGN 2 P1

5080 RELEASE FS3

5090 test ne p4 1 stop

5100 ASSIGN 2 P1

5110 ASSIGN 4 0

5120 SEIZE KAN27

5130 ADVANCE 8,4

5140 RELEASE KAN27

5150 TRANSFER ,SW\_X

5160 LKF1P SEIZE KANF1

5170 ADVANCE 4000,40

5180 RELEASE KANF1

5190 SEIZE FS4

5200 ADVANCE 36,18

5210 RELEASE FS4

5220 SEIZE KANF1

5230 ADVANCE 4000,40

5240 RELEASE KANF1

5250 TRANSFER ,LKF1S

5260 LKF1S SEIZE PCF1

5270 ADVANCE 36,18

5280 RELEASE PCF1

5290 TERMINATE

5300 LKF2P SEIZE KANF2

5310 ADVANCE 80,40

5320 RELEASE KANF2

5330 SEIZE FS4

5340 ADVANCE 36,18

5350 RELEASE FS4

5360 SEIZE KANF2

5370 ADVANCE 80,40

5380 RELEASE KANF2

5390 TRANSFER ,LKF2S

5400 LKF2S SEIZE PCF2

5410 ADVANCE 36,18

5420 RELEASE PCF2

5430 TERMINATE

5440 LK28S SEIZE KAN28

5450 ADVANCE 80,40

5460 RELEASE KAN28

5470 SEIZE FS4

5480 ADVANCE 36,18

5490 ASSIGN 2 P1

5500 RELEASE FS4

5510 test ne p4 1 stop

5520 ASSIGN 2 P1

5530 ASSIGN 4 0

5540 SEIZE KAN28

5550 ADVANCE 80,40

5560 RELEASE KAN28

5570 TRANSFER ,SW\_X

5580 LK29S SEIZE KAN29

5590 ADVANCE 80,40

5600 RELEASE KAN29

5610 SEIZE FS5

5620 ADVANCE 36,18

5630 RELEASE FS5

5640 test ne p4 1 stop

5650 ASSIGN 2 P1

5660 ASSIGN 4 0

5670 SEIZE KAN29

5680 ADVANCE 80,40

5690 RELEASE KAN29

5700 TRANSFER ,SW\_X

5710 stop TERMINATE

5720 d11 link l11,FIFO

5730 d12 link l12,FIFO

5740 d13 link l13,FIFO

5750 d14 link l14,FIFO

5760 d21 link l21,FIFO

5770 d22 link l22,FIFO

5780 d23 link l23,FIFO

5790 d24 link l24,FIFO

5800 d31 link l31,FIFO

5810 d32 link l32,FIFO

5820 d33 link l33,FIFO

5830 d34 link l34,FIFO

5840 d41 link l41,FIFO

5850 d42 link l42,FIFO

5860 d43 link l43,FIFO

5870 d44 link l44,FIFO

5880 d51 link l51,FIFO

5890 d52 link l52,FIFO

5900 d53 link l53,FIFO

5910 d54 link l54,FIFO

5920 d61 link l61,FIFO

5930 d62 link l62,FIFO

5940 d63 link l63,FIFO

5950 d64 link l64,FIFO

5960 d71 link l71,FIFO

5970 d72 link l72,FIFO

5980 d73 link l73,FIFO

5990 d74 link l74,FIFO

6000 d81 link l81,FIFO

6010 d82 link l82,FIFO

6020 d83 link l83,FIFO

6030 d84 link l84,FIFO

6040 d91 link l91,FIFO

6050 d92 link l92,FIFO

6060 d93 link l93,FIFO

6070 d94 link l94,FIFO

6080 d101 link l101,FIFO

6090 d102 link l102,FIFO

6100 d103 link l103,FIFO

6110 d104 link l104,FIFO

6120 d111 link l111,FIFO

6130 d112 link l112,FIFO

6140 d113 link l113,FIFO

6150 d114 link l114,FIFO

6160 d121 link l121,FIFO

6170 d122 link l122,FIFO

6180 d123 link l123,FIFO

6190 d124 link l124,FIFO

6200 d131 link l131,FIFO

6210 d132 link l132,FIFO

6220 d133 link l133,FIFO

6230 d134 link l134,FIFO

6240 d141 link l141,FIFO

6250 d142 link l142,FIFO

6260 d143 link l143,FIFO

6270 d144 link l144,FIFO

6280 generate 10000

6290 test ne CH$l11,0,dd11

6300 unlink l11 ff1

6310 terminate

6320 dd11 test ne CH$l12,0,dd12

6330 unlink l12 ff1

6340 terminate

6350 dd12 test ne CH$l13,0,dd13

6360 unlink l13 ff1

6370 terminate

6380 dd13 test ne CH$l14,0,dd14

6390 unlink l14 ff1

6400 terminate

6410 dd14 terminate

6420 generate 10000

6430 test ne CH$l21,0,dd21

6440 unlink l21 ff2

6450 terminate

6460 dd21 test ne CH$l22,0,dd22

6470 unlink l22 ff2

6480 terminate

6490 dd22 test ne CH$l23,0,dd23

6500 unlink l23 ff2

6510 terminate

6520 dd23 test ne CH$l24,0,dd24

6530 unlink l24 ff2

6540 terminate

6550 dd24 terminate

6560 generate 10000

6570 test ne CH$l31,0,dd31

6580 unlink l31 ff3

6590 terminate

6600 dd31 test ne CH$l32,0,dd32

6610 unlink l32 ff3

6620 terminate

6630 dd32 test ne CH$l33,0,dd33

6640 unlink l33 ff3

6650 terminate

6660 dd33 test ne CH$l34,0,dd34

6670 unlink l34 ff3

6680 terminate

6690 dd34 terminate

6700 generate 10000

6710 test ne CH$l41,0,dd41

6720 unlink l41 ff4

6730 terminate

6740 dd41 test ne CH$l42,0,dd42

6750 unlink l42 ff4

6760 terminate

6770 dd42 test ne CH$l43,0,dd43

6780 unlink l43 ff4

6790 terminate

6800 dd43 test ne CH$l44,0,dd44

6810 unlink l44 ff4

6820 terminate

6830 dd44 terminate

6840 generate 10000

6850 test ne CH$l51,0,dd51

6860 unlink l51 ff5

6870 terminate

6880 dd51 test ne CH$l52,0,dd52

6890 unlink l52 ff5

6900 terminate

6910 dd52 test ne CH$l53,0,dd53

6920 unlink l53 ff5

6930 terminate

6940 dd53 test ne CH$l54,0,dd54

6950 unlink l54 ff5

6960 terminate

6970 dd54 terminate

6980 generate 10000

6990 test ne CH$l61,0,dd61

7000 unlink l61 ff6

7010 terminate

7020 dd61 test ne CH$l62,0,dd62

7030 unlink l62 ff6

7040 terminate

7050 dd62 test ne CH$l63,0,dd63

7060 unlink l63 ff6

7070 terminate

7080 dd63 test ne CH$l64,0,dd64

7090 unlink l64 ff6

7100 terminate

7110 dd64 terminate

7120 generate 10000

7130 test ne CH$l71,0,dd71

7140 unlink l71 ff7

7150 terminate

7160 dd71 test ne CH$l72,0,dd72

7170 unlink l72 ff7

7180 terminate

7190 dd72 test ne CH$l73,0,dd73

7200 unlink l73 ff7

7210 terminate

7220 dd73 test ne CH$l74,0,dd74

7230 unlink l74 ff7

7240 terminate

7250 dd74 terminate

7260 generate 10000

7270 test ne CH$l81,0,dd81

7280 unlink l81 ff8

7290 terminate

7300 dd81 test ne CH$l82,0,dd82

7310 unlink l82 ff8

7320 terminate

7330 dd82 test ne CH$l83,0,dd83

7340 unlink l83 ff8

7350 terminate

7360 dd83 test ne CH$l84,0,dd84

7370 unlink l84 ff8

7380 terminate

7390 dd84 terminate

7400 generate 10000

7410 test ne CH$l91,0,dd91

7420 unlink l91 ff9

7430 terminate

7440 dd91 test ne CH$l92,0,dd92

7450 unlink l92 ff9

7460 terminate

7470 dd92 test ne CH$l93,0,dd93

7480 unlink l93 ff9

7490 terminate

7500 dd93 test ne CH$l94,0,dd94

7510 unlink l94 ff9

7520 terminate

7530 dd94 terminate

7540 generate 10000

7550 test ne CH$l101,0,dd101

7560 unlink l101 ff10

7570 terminate

7580 dd101 test ne CH$l102,0,dd102

7590 unlink l102 ff10

7600 terminate

7610 dd102 test ne CH$l103,0,dd103

7620 unlink l103 ff10

7630 terminate

7640 dd103 test ne CH$l104,0,dd104

7650 unlink l104 ff10

7660 terminate

7670 dd104 terminate

7680 generate 10000

7690 test ne CH$l111,0,dd111

7700 unlink l111 ff11

7710 terminate

7720 dd111 test ne CH$l112,0,dd112

7730 unlink l112 ff11

7740 terminate

7750 dd112 test ne CH$l113,0,dd113

7760 unlink l113 ff11

7770 terminate

7780 dd113 test ne CH$l114,0,dd114

7790 unlink l114 ff11

7800 terminate

7810 dd114 terminate

7820 generate 10000

7830 test ne CH$l121,0,dd121

7840 unlink l121 ff12

7850 terminate

7860 dd121 test ne CH$l122,0,dd122

7870 unlink l122 ff12

7880 terminate

7890 dd122 test ne CH$l123,0,dd123

7900 unlink l123 ff12

7910 terminate

7920 dd123 test ne CH$l124,0,dd124

7930 unlink l124 ff12

7940 terminate

7950 dd124 terminate

7960 generate 10000

7970 test ne CH$l131,0,dd131

7980 unlink l131 ff13

7990 terminate

8000 dd131 test ne CH$l132,0,dd132

8010 unlink l132 ff13

8020 terminate

8030 dd132 test ne CH$l133,0,dd133

8040 unlink l133 ff13

8050 terminate

8060 dd133 test ne CH$l134,0,dd134

8070 unlink l134 ff13

8080 terminate

8090 dd134 terminate

8100 generate 10000

8110 test ne CH$l141,0,dd141

8120 unlink l141 ff14

8130 terminate

8140 dd141 test ne CH$l142,0,dd142

8150 unlink l142 ff14

8160 terminate

8170 dd142 test ne CH$l143,0,dd143

8180 unlink l143 ff14

8190 terminate

8200 dd143 test ne CH$l144,0,dd144

8210 unlink l144 ff14

8220 terminate

8230 dd144 terminate

8240 GENERATE 6000000

8250 TERMINATE 1

8260 START 1

# Приложение В

Фрагмент отчета по 1-ому году эксплуатации сети.

FACILITY ENTRIES UTIL. AVE.\_TIME AVAILABLE OWNER PEND INTER RETRY DELAY

PC1 153 0.002 50.09 1 0 0 0 0 0

KAN1 153 0.004 80.84 1 0 0 0 0 0

PCF1 96 0.001 36.39 1 0 0 0 0 0

PCF2 122 0.001 37.42 1 0 0 0 0 0

PC2 80 0.001 50.27 1 0 0 0 0 0

KAN2 80 0.002 80.21 1 0 0 0 0 0

PC3 238 0.003 49.66 1 0 0 0 0 0

KAN3 238 0.006 80.79 1 0 0 0 0 0

PC4 81 0.001 48.88 1 0 0 0 0 0

KAN4 81 0.002 81.51 1 0 0 0 0 0

PC5 82 0.001 48.00 1 0 0 0 0 0

KAN5 82 0.002 81.96 1 0 0 0 0 0

PC6 56 0.000 51.73 1 0 0 0 0 0

KAN6 56 0.001 81.04 1 0 0 0 0 0

PC7 167 0.002 50.25 1 0 0 0 0 0

KAN7 167 0.004 79.49 1 0 0 0 0 0

PC8 88 0.001 47.24 1 0 0 0 0 0

KAN8 88 0.002 81.58 1 0 0 0 0 0

PC9 70 0.001 48.39 1 0 0 0 0 0

KAN9 70 0.001 81.23 1 0 0 0 0 0

PC10 68 0.001 51.46 1 0 0 0 0 0

KAN10 68 0.001 80.44 1 0 0 0 0 0

FS4 18454 0.221 35.94 1 254 0 0 0 0

KAN28 36638 0.676 79.92 1 783 0 0 0 3

FS1 80720 0.669 36.03 1 129 0 0 0 3

KAN25 161393 0.431 8.02 1 0 0 0 0 0

SW1 153 0.097 1908.40 1 0 0 0 0 0

KAN11 152 0.004 82.20 1 0 0 0 0 0

SW2 80 0.017 649.27 1 0 0 0 0 0

KAN12 79 0.002 79.73 1 0 0 0 0 0

SW3 231 0.004 63.81 1 0 0 0 0 0

KAN13 231 0.006 82.61 1 0 0 0 0 0

SW4 238 0.152 1927.30 1 0 0 0 0 0

KAN14 237 0.006 81.49 1 0 0 0 0 0

SW5 81 0.049 1823.01 1 0 0 0 0 0

KAN15 81 0.002 88.40 1 0 0 0 0 0

SW6 82 0.033 1234.44 1 0 0 0 0 0

KAN16 82 0.002 74.96 1 0 0 0 0 0

SW7 400 0.008 63.89 1 0 0 0 0 0

KAN17 399 0.010 80.89 1 0 0 0 0 0

SW8 56 0.023 1246.05 1 0 0 0 0 0

KAN18 56 0.001 77.41 1 0 0 0 0 0

SW9 167 0.105 1897.66 1 183 0 0 0 0

KAN19 166 0.004 80.53 1 0 0 0 0 0

SW10 273397 0.595 5.00 1 0 0 0 0 0

KAN20 173305 0.462 8.00 1 0 0 0 0 0 SW11 88 0.021 720.43 1 0 0 0 0 0

KAN21 88 0.004 7.82 1 0 0 0 0 0

SW12 70 0.016 702.44 1 0 0 0 0 0

KAN22 70 0.000 8.01 1 0 0 0 0 0

SW13 68 0.016 715.09 1 0 0 0 0 0

KAN23 68 0.000 7.81 1 0 0 0 0 0

SW14 226 0.004 64.12 1 0 0 0 0 0

KAN26 534 0.011 7.86 1 0 0 0 0 0

FS2 267 0.003 36.77 1 0 0 0 0 0

KAN27 304 0.002 7.88 1 0 0 0 0 0

FS3 152 0.021 35.01 1 0 0 0 0 0

KANF1 96 0.127 3999.60 1 0 0 0 0 0

KANF2 122 0.003 78.50 1 0 0 0 0 0

KAN29 326 0.008 79.92 1 0 0 0 0 0

FS5 163 0.021 35.61 1 0 0 0 0 0

USER\_CHAIN CHAIN\_SIZE RETRY AVE.CONT ENTRIES MAX AVE.TIME

L11 0 0 0.02 8 1 6338.25

L12 0 0 0.17 80 3 6422.26

L13 1 0 0.14 54 3 7939.61

L14 0 0 0.03 11 1 7184.09

L21 0 0 0.02 8 1 7669.12

L22 1 0 0.11 46 2 7470.52

L23 0 0 0.04 21 1 5283.48

L24 0 0 0.01 5 1 5325.60

L31 0 0 0.05 16 1 9688.50

L32 0 0 0.42 125 4 10114.72

L33 0 0 0.35 74 5 14328.74

L34 0 0 0.08 16 2 14153.12

L41 0 0 0.05 24 1 6556.04

L42 0 0 0.24 121 4 5966.59

L43 1 0 0.17 72 3 6989.89

L44 0 0 0.07 21 3 10262.81

L51 0 0 0.01 2 1 8966.00

L52 0 0 0.08 40 2 6214.45

L53 0 0 0.07 34 2 6420.53

L54 0 0 0.01 5 1 5130.60

L61 0 0 0.03 13 1 6120.54

L62 0 0 0.07 33 3 6061.55

L63 0 0 0.07 35 2 6282.03

L64 0 0 0.00 1 1 3893.00

L71 0 0 0.12 39 2 9605.18

L72 0 0 0.68 194 7 10588.87

L73 0 0 1.03 140 6 22110.09

L74 0 0 0.46 27 4 51524.11

L81 0 0 0.00 2 1 5577.00

L82 0 0 0.09 39 2 6716.97

L83 0 0 0.03 15 1 6045.20

L84 0 0 0.00 4 0 3243.11

L91 0 0 0.06 30 1 6319.27

L92 0 0 0.17 76 5 6660.66

L93 0 0 0.09 50 3 5414.28

L94 0 0 0.02 10 1 5790.20

L101 0 0 0.32 7299 4 8.73

L102 0 0 1.32 8638 72 353.04

L103 1 0 3.44 4326 246 51423.89

L104 1 0 4.77 3134 162 54658.66

L111 0 0 0.03 12 1 8298.17

L112 0 0 0.10 43 2 6976.65

L113 0 0 0.04 25 3 4986.72

L114 0 0 0.01 8 1 4284.87

L121 0 0 0.02 6 1 7960.67

L122 0 0 0.07 30 2 7277.27

L123 0 0 0.06 29 1 5858.45

L124 0 0 0.01 5 1 6591.00

L131 0 0 0.03 12 1 7897.58

L132 0 0 0.07 26 2 7693.46

L133 0 0 0.05 25 1 5693.48

L134 0 0 0.01 5 1 6458.00

L141 0 0 0.10 30 2 9786.40

L142 0 0 0.33 99 5 10066.48

L143 0 0 0.45 79 7 17181.62

L144 0 0 0.11 18 1 18199.94

XACT\_GROUP GROUP\_SIZE RETRY

POSITION 0 0

Фрагмент отчета по 5-му году эксплуатации сети.

FACILITY ENTRIES UTIL. AVE.\_TIME AVAILABLE OWNER PEND INTER RETRY DELAY

PC1 153 0.004 51.04 1 0 0 0 0 0

KAN1 153 0.005 80.84 1 0 0 0 0 0

PCF1 96 0.002 36.39 1 0 0 0 0 0

PCF2 122 0.002 37.42 1 0 0 0 0 0

PC2 80 0.002 50.27 1 0 0 0 0 0

KAN2 80 0.001 80.21 1 0 0 0 0 0

PC3 238 0.004 49.66 1 0 0 0 0 0

KAN3 238 0.007 80.79 1 0 0 0 0 0

PC4 81 0.002 48.88 1 0 0 0 0 0

KAN4 81 0.003 81.51 1 0 0 0 0 0

PC5 82 0.002 48.00 1 0 0 0 0 0

KAN5 82 0.003 81.96 1 0 0 0 0 0

PC6 56 0.001 51.73 1 0 0 0 0 0

KAN6 56 0.002 81.04 1 0 0 0 0 0

PC7 167 0.003 50.25 1 0 0 0 0 0

KAN7 167 0.005 79.49 1 0 0 0 0 0

PC8 88 0.002 47.24 1 0 0 0 0 0

KAN8 88 0.003 81.58 1 0 0 0 0 0

PC9 70 0.002 48.39 1 0 0 0 0 0

KAN9 70 0.002 81.23 1 0 0 0 0 0

PC10 68 0.002 51.46 1 0 0 0 0 0

KAN10 68 0.002 80.44 1 0 0 0 0 0

FS4 18454 0.222 35.94 1 254 0 0 0 0

KAN28 36638 0.677 79.92 1 783 0 0 0 3

FS1 80720 0.679 36.03 1 129 0 0 0 3

KAN25 161393 0.434 8.02 1 0 0 0 0 0

SW1 153 0.123 1908.40 1 0 0 0 0 0

KAN11 152 0.004 82.20 1 0 0 0 0 0

SW2 80 0.031 649.27 1 0 0 0 0 0

KAN12 79 0.003 79.73 1 0 0 0 0 0

SW3 231 0.006 63.81 1 0 0 0 0 0

KAN13 231 0.007 82.61 1 0 0 0 0 0

SW4 238 0.187 1927.30 1 0 0 0 0 0

KAN14 237 0.007 81.49 1 0 0 0 0 0

SW5 81 0.105 1823.01 1 0 0 0 0 0

KAN15 81 0.003 88.40 1 0 0 0 0 0

SW6 82 0.066 1234.44 1 0 0 0 0 0

KAN16 82 0.003 74.96 1 0 0 0 0 0

SW7 400 0.012 63.89 1 0 0 0 0 0

KAN17 399 0.010 80.89 1 0 0 0 0 0

SW8 56 0.038 1246.05 1 0 0 0 0 0

KAN18 56 0.001 77.41 1 0 0 0 0 0

SW9 167 0.112 1897.66 1 183 0 0 0 0

KAN19 166 0.004 80.53 1 0 0 0 0 0

SW10 273397 0.643 5.00 1 0 0 0 0 0

KAN20 173305 0.462 8.00 1 0 0 0 0 0

SW11 88 0.036 720.43 1 0 0 0 0 0

KAN21 88 0.001 7.82 1 0 0 0 0 0

SW12 70 0.023 702.44 1 0 0 0 0 0

KAN22 70 0.001 8.01 1 0 0 0 0 0

SW13 68 0.023 715.09 1 0 0 0 0 0

KAN23 68 0.001 7.81 1 0 0 0 0 0

SW14 226 0.006 64.12 1 0 0 0 0 0

KAN26 534 0.012 7.86 1 0 0 0 0 0

FS2 267 0.004 36.77 1 0 0 0 0 0

KAN27 304 0.001 7.88 1 0 0 0 0 0

FS3 152 0.022 35.01 1 0 0 0 0 0

KANF1 96 0.129 3999.60 1 0 0 0 0 0

KANF2 122 0.003 78.50 1 0 0 0 0 0

KAN29 326 0.009 79.92 1 0 0 0 0 0

FS5 163 0.021 35.61 1 0 0 0 0 0

USER\_CHAIN CHAIN\_SIZE RETRY AVE.CONT ENTRIES MAX AVE.TIME

L11 0 0 0.04 17 1 6851.59

L12 0 0 0.22 96 4 6765.01

L13 0 0 0.16 78 6 6202.47

L14 0 0 0.04 14 1 7680.64

L21 0 0 0.03 12 1 7541.92

L22 0 0 0.13 58 3 6838.93

L23 0 0 0.07 37 11 5773.14

L24 0 0 0.01 3 1 5848.67

L31 0 0 0.09 29 1 9646.17

L32 0 0 0.47 154 7 9236.10

L33 0 0 0.77 115 30 20088.74

L34 0 0 0.11 17 2 19450.71

L41 0 0 0.08 37 2 6705.14

L42 1 0 0.32 156 5 6180.83

L43 0 0 0.31 106 6 8868.26

L44 0 0 0.14 21 4 20037.52

L51 0 0 0.06 26 1 6545.15

L52 0 0 0.13 58 3 6897.33

L53 0 0 0.06 31 6 6281.94

L54 0 0 0.01 6 1 2671.50

L61 0 0 0.03 13 1 7110.54

L62 0 0 0.08 41 2 6111.95

L63 0 0 0.10 53 8 5713.87

L64 0 0 0.00 3 1 3447.67

L71 0 0 0.24 75 2 9675.01

L72 0 0 1.07 255 14 12545.16

L73 0 0 2.75 190 55 43350.30

L74 0 0 0.99 30 8 98818.57

L81 0 0 0.02 8 1 5957.87

L82 0 0 0.07 34 2 6198.74

L83 0 0 0.06 31 4 5694.94

L84 0 0 0.00 2 1 3488.00

USER\_CHAIN CHAIN\_SIZE RETRY AVE.CONT ENTRIES MAX AVE.TIME

L91 0 0 0.05 28 2 5842.43

L92 0 0 0.23 112 5 6047.29

L93 0 0 0.25 121 7 6168.14

L94 0 0 0.04 17 2 7244.00

L101 0 0 0.42 5991 4 8.69

L102 1 0 1.67 2799 69 778.40

L103 1 0 3.26 1611 259 5041.84

L104 1 0 5.69 2159 85 29907.23

L111 0 0 0.03 12 1 7409.42

L112 0 0 0.11 52 4 6455.94

L113 0 0 0.10 50 13 5739.18

L114 0 0 0.01 9 1 3098.78

L121 0 0 0.03 12 1 7375.00

L122 0 0 0.10 43 3 6913.12

L123 0 0 0.07 37 10 5490.46

L124 0 0 0.01 6 1 3032.67

L131 0 0 0.04 16 1 7084.19

L132 0 0 0.11 46 2 7305.30

L133 0 0 0.09 39 13 6575.97

L134 0 0 0.01 5 1 6391.80

L141 0 0 0.13 40 2 9776.77

L142 0 0 0.51 141 7 10886.94

L143 0 0 1.02 126 40 24280.55

L144 0 0 0.15 20 2 23066.55

Фрагмент отчета по 7-ому году эксплуатации сети.

FACILITY ENTRIES UTIL. AVE.\_TIME AVAILABLE OWNER PEND INTER RETRY DELAY

PC1 153 0.005 51.04 1 0 0 0 0 0

KAN1 153 0.006 80.84 1 0 0 0 0 0

PCF1 96 0.003 36.39 1 0 0 0 0 0

PCF2 122 0.003 37.42 1 0 0 0 0 0

PC2 80 0.002 50.27 1 0 0 0 0 0

KAN2 80 0.002 80.21 1 0 0 0 0 0

PC3 238 0.005 49.66 1 0 0 0 0 0

KAN3 238 0.007 80.79 1 0 0 0 0 0

PC4 81 0.003 48.88 1 0 0 0 0 0

KAN4 81 0.003 81.51 1 0 0 0 0 0

PC5 82 0.003 48.00 1 0 0 0 0 0

KAN5 82 0.004 81.96 1 0 0 0 0 0

PC6 56 0.002 51.73 1 0 0 0 0 0

KAN6 56 0.002 81.04 1 0 0 0 0 0

PC7 167 0.004 50.25 1 0 0 0 0 0

KAN7 167 0.006 79.49 1 0 0 0 0 0

PC8 88 0.004 47.24 1 0 0 0 0 0

KAN8 88 0.004 81.58 1 0 0 0 0 0

PC9 70 0.002 48.39 1 0 0 0 0 0

KAN9 70 0.003 81.23 1 0 0 0 0 0

PC10 68 0.003 51.46 1 0 0 0 0 0

KAN10 68 0.003 80.44 1 0 0 0 0 0

FS4 18454 0.234 35.94 1 254 0 0 0 0

KAN28 36638 0.684 79.92 1 783 0 0 0 3

FS1 80720 0.694 36.03 1 129 0 0 0 3

KAN25 161393 0.454 8.02 1 0 0 0 0 0

SW1 153 0.159 1908.40 1 0 0 0 0 0

KAN11 152 0.004 82.20 1 0 0 0 0 0

SW2 80 0.038 649.27 1 0 0 0 0 0

KAN12 79 0.003 79.73 1 0 0 0 0 0

SW3 231 0.008 63.81 1 0 0 0 0 0

KAN13 231 0.007 82.61 1 0 0 0 0 0

SW4 238 0.212 1927.30 1 0 0 0 0 0

KAN14 237 0.007 81.49 1 0 0 0 0 0

SW5 81 0.133 1823.01 1 0 0 0 0 0

KAN15 81 0.003 88.40 1 0 0 0 0 0

SW6 82 0.084 1234.44 1 0 0 0 0 0

KAN16 82 0.003 74.96 1 0 0 0 0 0

SW7 400 0.019 63.89 1 0 0 0 0 0

KAN17 399 0.010 80.89 1 0 0 0 0 0

SW8 56 0.043 1246.05 1 0 0 0 0 0

KAN18 56 0.001 77.41 1 0 0 0 0 0

SW9 167 0.128 1897.66 1 183 0 0 0 0

KAN19 166 0.004 80.53 1 0 0 0 0 0

SW10 273397 0.696 5.00 1 0 0 0 0 0

KAN20 173305 0.462 8.00 1 0 0 0 0 0 SW11 88 0.051 720.43 1 0 0 0 0 0

KAN21 88 0.001 7.82 1 0 0 0 0 0

SW12 70 0.036 702.44 1 0 0 0 0 0

KAN22 70 0.001 8.01 1 0 0 0 0 0

SW13 68 0.036 715.09 1 0 0 0 0 0

KAN23 68 0.001 7.81 1 0 0 0 0 0

SW14 226 0.008 64.12 1 0 0 0 0 0

KAN26 534 0.013 7.86 1 0 0 0 0 0

FS2 267 0.005 36.77 1 0 0 0 0 0

KAN27 304 0.002 7.88 1 0 0 0 0 0

FS3 152 0.023 35.01 1 0 0 0 0 0

KANF1 96 0.131 3999.60 1 0 0 0 0 0

KANF2 122 0.004 78.50 1 0 0 0 0 0

KAN29 326 0.011 79.92 1 0 0 0 0 0

FS5 163 0.021 35.61 1 0 0 0 0 0

USER\_CHAIN CHAIN\_SIZE RETRY AVE.CONT ENTRIES MAX AVE.TIME

L11 0 0 0.08 38 2 6622.89

L12 0 0 0.25 121 5 6127.69

L13 0 0 0.11 52 2 6563.00

L14 0 0 0.05 16 1 9094.00

L21 0 0 0.03 12 1 7933.33

L22 0 0 0.18 74 9 7199.86

L23 0 0 0.05 28 2 5306.68

L24 0 0 0.01 6 1 7207.17

L31 0 0 0.16 50 2 9622.70

L32 0 0 0.76 195 19 11736.77

L33 1 0 0.39 80 2 14705.77

L34 0 0 0.13 22 2 17564.45

L41 0 0 0.13 58 2 6641.52

L42 0 0 0.34 169 6 6111.71

L43 0 0 0.37 102 4 10894.75

L44 0 0 0.11 21 2 15635.76

L51 0 0 0.03 12 1 6281.67

L52 0 0 0.12 56 5 6293.91

L53 1 0 0.09 41 1 6231.27

L54 0 0 0.01 6 1 4329.83

L61 0 0 0.01 5 1 7367.60

L62 0 0 0.13 60 4 6642.60

L63 0 0 0.07 34 1 6229.85

L64 0 0 0.02 11 1 5028.18

L71 0 0 0.24 75 2 9632.85

L72 0 0 1.28 285 23 13511.49

L73 1 0 1.42 176 7 24256.84

L74 1 0 1.19 37 7 96857.59

L81 0 0 0.03 14 1 6524.71

L82 0 0 0.07 29 3 7044.41

L83 0 0 0.04 24 1 5270.83

L84 0 0 0.01 6 1 3683.33

L91 0 0 0.11 50 2 6878.84

L92 1 0 0.30 151 5 6007.17

L93 0 0 0.18 66 3 8173.15

L94 0 0 0.10 28 2 10546.68

L101 3 0 0.99 8198 5 9.34

L102 0 0 2.57 2659 108 2538.68

L103 0 0 4.75 1046 465 5332.86

L104 1 0 7.63 1148 122 68136.85

L111 0 0 0.05 22 1 6987.82

L112 1 0 0.13 59 7 6704.42

L113 0 0 0.07 35 1 5911.09

L114 0 0 0.03 13 1 7307.38

L121 0 0 0.02 8 1 7637.00

L122 0 0 0.13 53 5 7152.60

L123 0 0 0.07 36 2 5793.78

L124 0 0 0.01 4 1 5831.75

L131 0 0 0.02 10 1 7304.80

L132 0 0 0.12 54 5 6693.93

L133 0 0 0.06 30 1 6157.23

L134 0 0 0.01 6 1 4381.83

L141 0 0 0.13 40 2 9847.75

L142 0 0 0.57 165 14 10429.13

L143 0 0 0.50 101 3 14900.25

L144 1 0 0.16 23 1 21222.83

# ПРИЛОЖЕНИЕ Г

План размещения оборудования и монтажных соединений сети

Здание 1, этаж 1



Здание 2, этаж 1



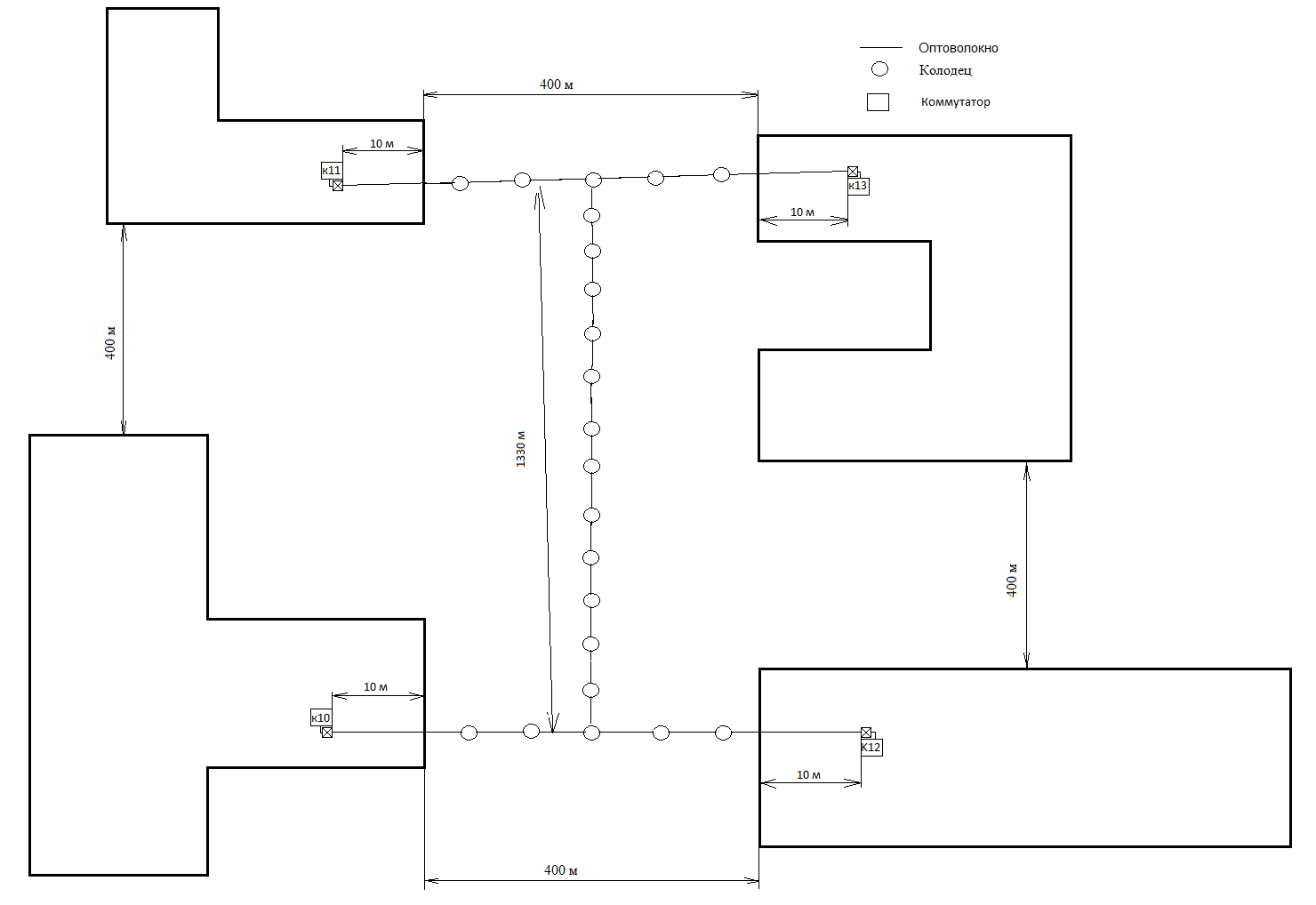
Здание 3, этаж 1



Здание 4, этаж 1



Кабель между зданиями



# СПИСОК ЛИТЕРАТУРЫ.

1) Головин Ю. А., Суконщиков А. А. Информационные сети и телекоммуникации. Часть 1: Учебное пособие, 2-е изд. – Вологда: ВоГТУ, 2003. – 151 с.

2) Филимонов А. Ю. Протоколы Интернета. – СПб.: БХВ-Петербург, 2003. – 528 с.

3) Советов Б. Я., Яковлев С. А. Моделирование систем: Учеб. для вузов – 3-е изд, перераб и доп. – М.: Высш. шк., 2001. – 343 с.

4) Советов Б. Я., Яковлев С. А. Моделирование систем. Практикум: Учеб. пособие для вузов – 2-е изд., перераб и доп. – М.: Высш. шк., 2003. – 295 с.

5) Ерофеев Д., Перепелкина М. **Корпоративные сети: формат на вырост *-*** "Свой бизнес", № 04 (21), апрель 2004 г.

6)Алексеев В. GSM/GPRS Терминалы ведущих мировых производителей - "Компоненты и технологии" № 1, 2005