МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное образовательное бюджетное учреждение высшего образования
«Вологодский государственный университет»
(ВоГУ)

СЕТИ И ТЕЛЕКОММУНИКАЦИИ

КУРСОВОЙ ПРОЕКТ:

“РАЗРАБОТКА ПРОЕКТА КОРПОРАТИВНОЙ СЕТИ АВТОМАТИЗАЦИИ ДОКУМЕНТООБОРОТА ПОДСИСТЕМЫ СБЫТА ПРОИЗВОДСТВЕННОГО ПРЕДПРИЯТИЯ”

Направление подготовки: 09.03.04 Программная инженерия

Направленность (профиль): Разработка программно-информационных систем

Форма обучения: очная

Институт: Математики, естественных и компьютерных наук

Кафедра: Автоматики и вычислительной техники

Группа: ВМ-41

Студент: Пчелкина О.С.

Руководитель: Суконщиков А.А.

Вологда
2022 г.

Оглавление

ВВЕДЕНИЕ

В 20 веке наука и промышленность стремительно развивались, причем это было обусловлено социально-экономическим соперничеством двух систем - капиталистической (во главе с США) и социалистической (во главе с СССР). Это соперничество привело к неустанному росту объемов поступающей информации, а также к созданию целой индустрии по ее переработке, передаче и распределению. Рост объемов информации и успехи в области микроэлектроники привели к появлению сверхбыстрых процессоров, которые сегодня являются основным средством переработки и управления информацией. В современном обществе информационные ресурсы играют гораздо большую роль, чем материальные, и эти ресурсы имеют свои законы, правила и закономерности. Они становятся необходимым элементом материального производства.

Если на заре информационного взрыва, в 60–70-х годах прошлого столетия, в области информационных технологий доминировали инженеры и программисты, то сегодня пользователи ЭВМ являются доминирующей группой в различных областях человеческой деятельности. Это особенно актуально на производственных предприятиях, где ежедневно поступает множество запросов на организацию работы всех сотрудников. Для предотвращения коллизий и корректной организации рабочего процесса необходима корпоративная сеть, которая не только обеспечивает правильную работу, но и служит главным хранилищем всей информации предприятия.

Данная работа посвящена разработке такой корпоративной сети, которая прошла основные этапы проектирования, анализа и корректировки реальной сети.

1. СХЕМА ИНФОРМАЦИОННЫХ ПОТОКОВ НА ПРЕДПРИЯТИИ И РАСЧЕТ ОБЪЕМА ПОТОКОВ МЕЖДУ ОТДЕЛАМИ

По техническому заданию предприятие располагается в двух семиэтажных зданиях площадью 10х150 м и занимает 4 этажа в каждом здании. Расстояние между зданиями – 150 м.

Имеется несколько отделов производственного предприятия, расположенных в нескольких зданиях и на нескольких этажах.

Производственное предприятие состоит из следующих отделов:

1. Администрация
2. Бухгалтерия
3. IT отдел
4. Технологический отдел
5. Отдел кадров
6. Отдел охраны
7. Производственный отдел
8. Отдел снабжения
9. Отдел сбыта
10. Транспортный отдел
11. Филиал в городе
12. Филиал в другом городе

Виды информации, передаваемой по сети:

1. Текстовая (приказы, документация, отчеты);
2. Графическая (схемы, диаграммы, чертежи, фото, рисунки);
3. Видеонаблюдение;
4. Информация баз данных;
5. IP-телефония;
6. Датчики.

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

Таблица 1

	1	2	3	4	5	6	7	8	9	10	Ф1	Ф2	$\Sigma_{\text{ИСХ. ИНФ}}$
1	15	25	15	5	15	25	5	10	10	5	20	20	170
2	25	35	10	-	15	-	-	-	-	-	-	-	85
3	15	10	15	5	5	10	5	5	5	5	15	15	110
4	15	-	5	20	-	10	20	15	15	-	10	10	120
5	20	15	5	-	20	-	-	-	-	-	10	10	80

6	15	10	10	5	5	10	20	25	25	25	15	15	180
7	5	-	5	20	-	10	20	15	15	-	-	-	90
8	10	-	5	15	-	15	15	30	10	20	10	10	140
9	10	-	5	15	-	15	15	10	30	20	10	10	140
10	5	-	5	-	-	15	-	20	20	25	35	35	160
Филиал1	20	-	15	10	10	15	-	10	10	35	-	40	165
Филиал2	20	-	15	10	10	15	-	10	10	35	40	-	165
$\Sigma_{\text{ВХОД. ИНФ.}}$	175	95	110	105	80	140	100	150	150	170	165	165	
Вход+исход	345	265	280	275	250	310	270	320	320	340	335	335	

Суммарная информационная нагрузка всех организационных связей центра в среднем составляет $ИН_{\Sigma max}$=1542000 $\frac{\text{бит}}{\text{сек}}$

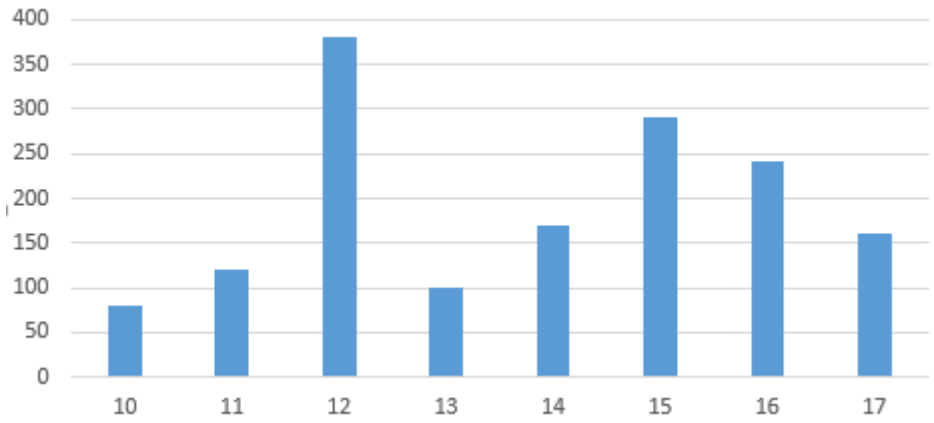


Рис. 1 – гистограмма информационной нагрузки по часам

Общая пропускная способность Ср сети определяется по формуле:

$C_р = k_1 * k_2 * ИН_{\sum max}$

k1=(1,1÷1,5) – коэффициент учета протокольной избыточности стека протоколов, измеренного в практикуемой сети; для стека TCP/IP k1≈1,3;

k2 – коэффициент запаса производительности для будущего расширения сети, обычно k2≈2.

$C_р = 1{,}3 * 2 * 1542000 = 40009200$

Определение коэффициента нагрузки неструктурированной локальной вычислительной сети:

$$p_н = \frac{C_p}{C_{max}} \frac{\text{бит}}{\text{сек}}$$

Смакс – максимальная пропускная способность базовой технологии сети.

$p_н = \ 0{,}038$

Проверка выполнения условия допустимой нагрузки ЛВС (домена коллизий):

$p_н \ \leq p_{доп} \ = 0{,}35$

$p_н$ коэффициент нагрузки неструктурированной сети или домена коллизий – логического сегмента ЛВС.

$0{,}038 \leq p_{доп} = 0{,}35$

Условие выполняется, следовательно, в качестве сетевой технологии используем Fast Ethernet.

2. СХЕМА ИНФОРМАЦИОННЫХ ПОТОКОВ С УЧЕТОМ СЕРВЕРОВ

Для полноценного функционирования сети необходимы сервера. Для их определения необходимо провести тщательный анализ работы предприятия (в данном случае, документооборота производственного предприятия).

Во-первых, для обработки между отделами потоков информации, как, например, поступление новых экспонатов между филиалами, необходим файл-сервер.

- Файл-сервер

Во-вторых, для организации доступа в интернет необходим прокси-сервер.

- Прокси-сервер

В-третьих, для возможности использования функционала внешней и внутренней (между начальниками и заместителями) электронной почты, должны присутствовать web-сервер, Exchange-сервер и Mail-сервер.

В-четвёртых, для печати любых документов необходим принтер. Доступ к принтерам в отдалении осуществляется через Print-сервер.

В-пятых, должен быть сервер баз данных для хранения информации о всех созданных организационно-распорядительных документах предприятия.

Кроме того, для защиты и нормального функционирования сети необходимы межсетевой экран, антивирусный сервер, главный и резервный контроллеры домена, DNS-сервера, менеджер IP-телефонии и видео - сервер для записи видео с камер наблюдения.

На рисунке 3 показана получившаяся схема информационных потоков:

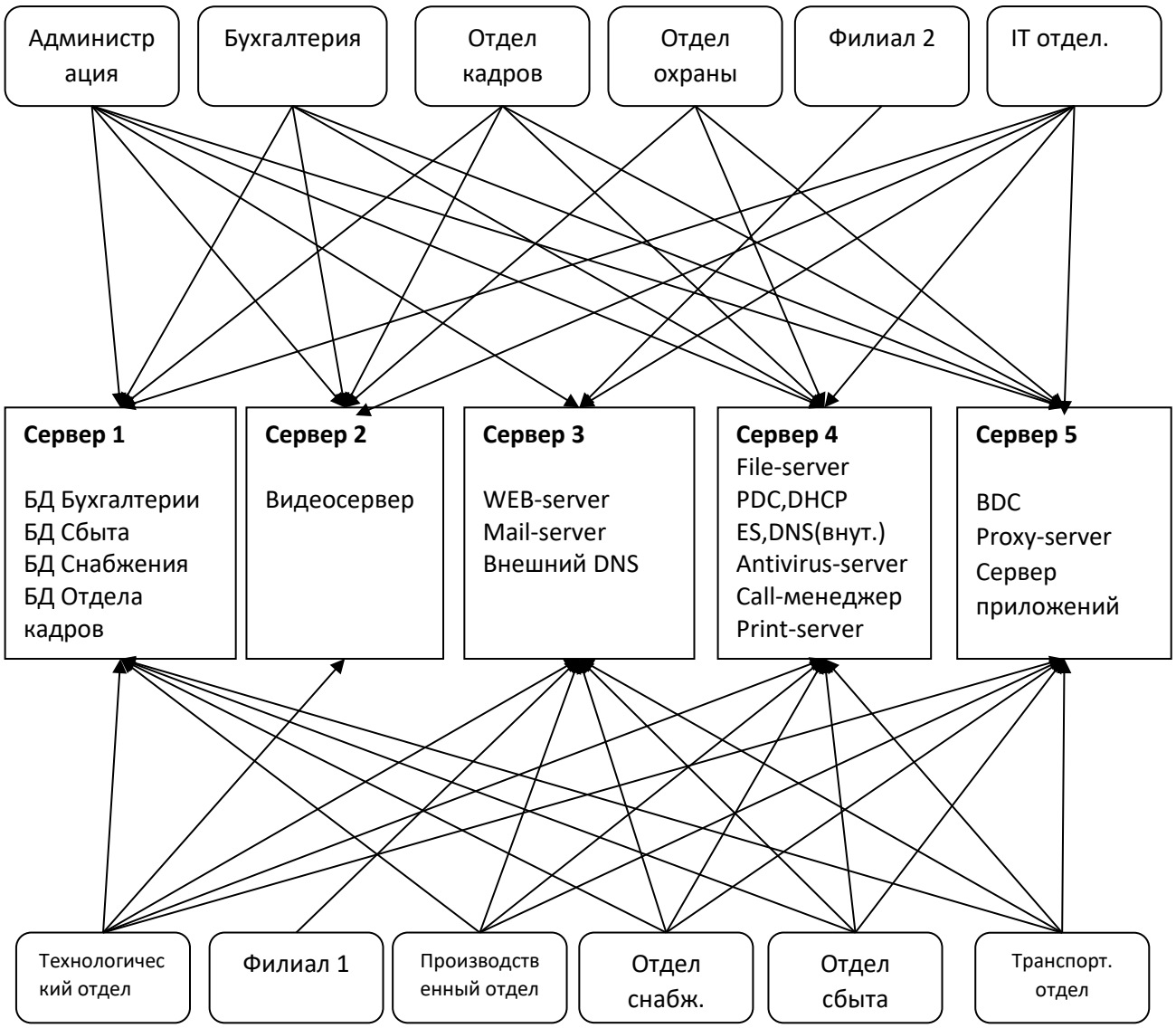


Рис2. Схема информационных потоков с учетом серверов.

3. СТРУКТУРНАЯ СХЕМА КОРПОРАТИВНОЙ СЕТИ

Расположение отделов и количество компьютеров в корпоративной сети

зданий:

Здание 1:

1 этаж:

- Администрация: 5 компьютеров (камера наблюдения - на входе в отдел)
- Бухгалтерия: 7 компьютеров (камера наблюдения - на входе в отдел)
- Отдел охраны: 2 компьютера (камера наблюдения - на входе в отдел)

7 этаж:

- IT отдел: 10 компьютеров (камера наблюдения - на входе в отдел)
- Технологический отдел: 12 компьютеров (камера наблюдения - на входе в отдел)
- Отдел кадров: 5 компьютеров (камера наблюдения - на входе в отдел)

Здание 2:

1 этаж:

- Производственный отдел: 15 компьютеров (камера наблюдения - на входе в отдел)

7 этаж:

- Отдел снабжения: 10 компьютеров (камера наблюдения - на входе в отдел)
- Отдел сбыта: 8 компьютеров (камера наблюдения - на входе в отдел)
- Транспортный отдел: 5 компьютера (камера наблюдения - на входе в отдел)

Исходя из схемы информационных потоков, разделения этих потоков, и схемы информационной потоков с учетом серверов, также зная расположение зданий и их габариты составим структурную схему корпоративной сети (Приложение А).

4. РАЗРАБОТКА ЗАЩИТЫ СЕТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Подключение компьютеров к сети позволяет упростить процесс обмена информацией, обеспечить доступ к общим ресурсам и увеличить эффективность работы. Однако, вместе с этим, возникает необходимость в обеспечении безопасности и защите от несанкционированного доступа.

Политика доступа к сетевым сервисам должна быть составлена в соответствии с общей политикой организации по защите информационных ресурсов. Для обеспечения эффективной защиты, необходимо установить реалистичную политику доступа пользователей к сетевым сервисам, которая будет учитывать не только риски, но и потребности пользователей.

Ограничения на доступ к определенным сервисам Интернета и методам доступа к ним также должны быть определены согласно установленной политике доступа. Для обеспечения безопасной работы, необходимо использовать межсетевой экран и другие компоненты программной среды.

Для защиты на внутреннем уровне необходимо определить, какие группы пользователей имеют доступ к каким ресурсам, а также установить права доступа для каждой группы пользователей. Для защиты на внешнем уровне, необходимо настроить межсетевой экран для внешних пользователей.

Важно отметить, что требования по безопасности данных в БД и СУБД схожи с требованиями к безопасности данных в компьютерных системах. Контроль доступа, криптозащита, проверка целостности и протоколирование являются основными требованиями по безопасности данных.

Таким образом, для обеспечения безопасной работы в локальной сети необходимо разработать и реализовать политику доступа и разграничения доступа к информационным ресурсам сети на административном уровне.

4.1. 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 также 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:

Сервер1: базы данных

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.

Таблица 2

Отд	С1				С3			С4								С5			С2
	БД бух	БД сбыт	БД снаб	БД ОК	Web-server	Mail-server	DNS внеш	File-server	PDC	DNCP	DNS внут	Print-server	Anyivirus-server	ES	Call	BDC	Proxy-server	AS	Видео
АДМ	R	R	R	R	+	+	+	+	R	R	R	R	R	+	+	R	R	+	R
БУХ	RW	R	R	R	-	-	-	+	R	R	R	R	R	+	+	R	R	+	R
ОК	-	-	-	RW	-	-	-	+	R	R	R	R	R	+	+	R	R	+	R
ОХР	-	-	-	-	-	-	-	+	R	R	R	R	R	+	+	R	R	+	R
ИТ	ME	ME	ME	ME	+	+	+	+	+	+	+	+	+	+	+	R ME	R ME	R ME	+
ТЕХ О	-	-	-	-	+	+	+	+	R	R	R	R	R	+	+	R	R	+	-
ПР О	-	R	R	-	+	+	+	+	R	R	R	R	R	+	+	R	R	+	-
СНАБ	-	RW	R	-	+	+	+	+	R	R	R	R	R	+	+	R	R	+	-
СБЫТ	-	R	RW	-	+	+	+	+	R	R	R	R	R	+	+	R	R	+	-
ТР О	-	R	R	-	+	+	+	+	R	R	R	R	R	+	+	R	R	+	-
AS	+	+	+	-	-	-	R	-	-	-	-	-	-	-	-	-	-	+	-

DNS	-	-	-	-	-	-	+	RW	+	+	-	RW	-	RW	-	RW	-	-	-
Call	-	-	-	-	-	-	-	-	-	-	-	RW	-	-	-	RW	-	-	RW
WEB	-	-	-	-	-	-	R	-	-	-	-	-	-	-	-	-	-	-	-
PDC	-	-	-	-	-	-	R	-	-	-	RW	R	-	-	-	-	-	-	-

Типы доступа определяются следующим образом:

* R (Read) – доступ на чтение данных

* W (Write) – доступ на изменение и удаление данных

* E (Execution) – доступ на исполнение исходного кода

* M (Modification) – доступ на изменение исходного кода

* F (Full) – доступ ко всем вышеперечисленным привилегиям.

4.2. 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.

Имеем следующее распределение объектов по VLAN:

VLAN 1 - Администрация (здание 1)

5 компьютеров

Камера наблюдения на входе в отдел

VLAN 2 - Бухгалтерия (здание 1)

7 компьютеров

Камера наблюдения на входе в отдел

VLAN 3 - Отдел охраны (здание 1)

2 компьютера

Камера наблюдения на входе в отдел

VLAN 4 - IT отдел (здание 1)

10 компьютеров

Камера наблюдения на входе в отдел

VLAN 5 - Технологический отдел (здание 1)

12 компьютера

Камера наблюдения на входе в отдел

VLAN 6 - Отдел кадров (здание 1)

5 компьютеров

Камера наблюдения на входе в отдел

VLAN 7 - Производственный отдел (здание 2)

15 компьютеров

Камера наблюдения на входе в отдел

VLAN 8 - Отдел снабжения (здание 2)

10 компьютеров

Камера наблюдения на входе в отдел

VLAN 9 - Отдел сбыта (здание 2)

8 компьютеров

Камера наблюдения на входе в отдел

VLAN 10 – Транспортный отдел (здание 2)

5 компьютеров

Камера наблюдения на входе в отдел

VLAN 11 – Сервера

4.3. Организация защиты от внешнего НСД.

Абсолютно любая компьютерная корпоративная сеть уязвима для хакерских атак извне. Для сохранности ценной информации и исключения доступа к ней посторонних лиц необходимо разработать систему защиты от внешнего несанкционированного доступа. Под внешним НСД понимается удаленный взлом и, вследствие этого, несанкционированный доступ к данным предприятия извне. Защита от таких прецедентов достигается путем установки межсетевого экрана (МСЭ) или, как его называют по-другому, прокси-сервера. Прокси-сервер является своего рода представителем web-сервера в интернете, является посредником при передаче данных и служит для фильтрации ненужных пакетов данных, поступающих на сервер, что может быть использовано как защита от внешнего НСД.

Вполне возможно, что КС предприятия может быть подвержена DoS или DDoS атакам, вследствие чего вся сеть не будет в рабочем состоянии. Защита от этого организуется наличием и необходимыми настройками МСЭ как на аппаратном, так и на уровне приложений.

При каких-либо ошибках работы сети, например, как нахождение ошибки в заголовках IP-пакетов или отсутствие маршрута к адресату при отправке пакета данных, маршрутизаторы генерируют ICMP-сообщения.

Внешний НСД подразумевает собой доступ к КС через интернет. Легальный доступ к КС имеют филиалы, гости, зарегистрированные клиенты и мобильные сотрудники. Для остальных доступ должен быть ограничен.

Разграничение доступа к сети в зависимости от пользователя.

Таблица 3

Пользователи	WEB	MAIL	AS	DNS внеш
Ф1	R	RW	RW	+
Ф2	R	RW	RW	+
Гости	R	R	-	-
МС	RW	RW	RW	+
Клиент	R	R	R	+

4.4. Защита передаваемой информации через интернет от НСД

Связь головного офиса с филиалами будет осуществляться через интернет.

В целях обеспечения безопасности процесса передачи и изоляции от внешней глобальной сети пакетов данных, канал связи будет проходить через туннель, созданный при помощи организации виртуальной приватной сети (VPN) между головным офисом и филиалами. VPN позволяет настроить сетевое соединение поверх интернета, данные в котором проходят в инкапсулированном состоянии, благодаря чему, их нельзя перехватить. Данные в сети должны проходить по протоколу ESP + IKE.

ESP (Encapsulating Security Payload) – один из протоколов передачи данных из набора IPsec. Позволяет осуществлять подтверждение подлинности, проверку целостности и шифрование IP-пакетов. Протокол ESP использует 50 порт соединения через IPsec.

Схожую с ESP структуру имеет протокол AH.

AH (Authentication Header) – схожий с ESP протокол безопасности передачи данных. Использует 51 порт IPsec. Так же, как и ESP, используется для аутентификации, то есть для подтверждения того, что мы связываемся именно с тем, с кем предполагаем, и что данные, которые мы получаем, не искажены при передаче

Также необходимо использовать при передаче данных через VPN IKE.

IKE (Internet Key Exchange) – протокол, связывающий все компоненты IPsec в работающее целое. В частности, IKE обеспечивает первоначальную аутентификацию сторон, а также их обмен общими секретными ключами. Существует и более новая версия IKE протокола – IKEv2 – но мы остановимся на первой в соответствии с техническим заданием. Используется преимущественно для организации VPN-туннелей. Процесс работы IKE разбивается на две фазы:

1) IKE создает безопасный канал между двумя узлами. При этом два узла согласуют сессионный ключ по алгоритму Диффи-Хеллмана. Первая фаза может проходить в одном из двух режимов: основной или агрессивный. Последний характеризуется тем, что обходится меньшим количеством обменов, в первом сообщении помещается практически вся нужная информация для установления соединения. В связи с этим агрессивный режим слабее с точки зрения безопасности, так как участники начинают обмениваться информацией до установления безопасного канала, поэтому возможен несанкционированный перехват данных. Однако, этот режим быстрее, чем основной.

2) Во второй фазе IKE существует только один, быстрый, режим. Быстрый режим выполняется только после создания безопасного канала в ходе первой фазы. Он согласует общую политику IPsec, получает общие секретные ключи для алгоритмов протоколов IPsec (AH или ESP), устанавливает IPsec-соединение. Использование последовательных номеров обеспечивает защиту от атак повторной передачи.

Протокол ESP используется, в основном, для организации VPN-туннелей. Кроме того, настраивая политики безопасности определенным образом, протокол можно использовать для создания межсетевого экрана. Устанавливается набор правил, и экран просматривает все проходящие через него пакеты. Если передаваемые пакеты попадают под действие этих правил, межсетевой экран обрабатывает их соответствующим образом. Например, он может отклонять определенные пакеты, тем самым прерывая небезопасные соединения. Настроив политику безопасности соответствующим образом, можно, например, запретить веб-трафик. Для этого достаточно запретить отсылку пакетов, в которые вкладываются сообщения протоколов HTTP и HTTPS. ESP+IKE можно применять и для защиты серверов — для этого отбрасываются все пакеты, кроме пакетов, необходимых для корректного выполнения функций сервера.

5. ОРГАНИЗАЦИЯ СВЯЗИ С ФИЛИАЛАМИ

Связь с филиалами осуществляется с помощью двух технологий: 5G и спутниковая связь.

5.1. Краткий обзор 5G.

5G - это пятый поколение мобильной связи, которое обеспечивает более высокую скорость передачи данных, более надежную связь и большую емкость сети, чем предыдущие поколения. Он работает на более высоких частотах, чем 4G, что позволяет передавать данные на большие расстояния и с большей скоростью.

Сети 5G имеют меньшую задержку и большую пропускную способность, что делает их идеальным выбором для приложений, которые требуют высокой скорости и надежной связи, таких как автономные автомобили, виртуальная реальность и интернет вещей. Кроме того, 5G позволяет подключать большое количество устройств к одной сети, что облегчает управление большим количеством устройств в промышленности и других сферах.

Однако, внедрение 5G требует больших инвестиций в новую инфраструктуру, такую как более высокие башни и оборудование, а также создание новых стандартов и протоколов связи. Кроме того, из-за использования более высоких частот, сети 5G имеют более ограниченное покрытие, чем предыдущие поколения, и могут быть подвержены более высокой помехам от физических препятствий, таких как стены зданий.

В целом, 5G обещает революционизировать способ, которым мы используем мобильную связь и интернет, открывая новые возможности для инноваций и развития новых технологий. Однако, полный переход на 5G может занять много времени и потребовать больших инвестиций, как со стороны провайдеров связи, так и со стороны пользователей.

Преимущества 5G-технологии, которые могут быть полезны в данной работе:

- Высокая скорость передачи данных
- Низкая задержка (лаг)
- Широкий диапазон частот для более надежной связи и большей пропускной способности
- Беспроводная технология, что позволит избежать необходимости прокладывать кабели между зданиями

Минусы 5G-технологии:

- Стоимость может быть высокой в сравнении со стандартными проводными технологиями связи

- Наличие препятствий, таких как деревья или здания, может снизить качество сигнала и привести к потере связи
- Некоторые устройства могут не поддерживать 5G, что может привести к ограничению доступа к сети.

5.2. Краткий обзор спутниковой связи.

Спутниковая связь представляет собой систему, которая обеспечивает передачу информации через спутники, находящиеся в орбите Земли. Эта технология используется для связи на больших расстояниях, где использование проводных линий связи неэффективно или невозможно.

Основным преимуществом спутниковой связи является возможность связи в любой точке на Земле, даже в отдаленных и труднодоступных местах. Это особенно важно для коммуникации в местах, где нет других средств связи, например, в морских путешествиях или экспедициях в отдаленные регионы. Также спутниковая связь может использоваться для организации дистанционного управления и мониторинга различных процессов, например, в геологии, метеорологии и спутниковой навигации.

Спутниковая связь также имеет некоторые недостатки. Один из них - это высокая стоимость оборудования и эксплуатации системы, особенно для небольших компаний и отдельных пользователей. Кроме того, из-за большого расстояния, которое сигнал должен преодолеть, скорость передачи данных через спутник может быть медленнее, чем при использовании проводных средств связи.

Несмотря на эти ограничения, спутниковая связь продолжает развиваться и находить новые применения, такие как глобальный доступ к интернету и дистанционное управление беспилотными летательными аппаратами. Спутниковая связь также играет важную роль в системах обеспечения безопасности и спасения, обеспечивая связь на местах стихийных бедствий и катастроф.

Плюсы спутниковой связи:

- Покрытие: Спутники обеспечивают глобальное покрытие земной поверхности, что позволяет обеспечить доступ к связи в любой точке планеты, даже в удаленных или труднодоступных местах.
- Надежность: Спутниковая связь обеспечивает высокую степень надежности и устойчивости в случае аварий или катастроф, когда обычные средства связи могут быть недоступны.
- Безопасность: Спутниковая связь может обеспечить высокую степень безопасности для передачи данных, так как передача происходит через защищенные каналы связи.

- Масштабируемость: Спутниковые системы могут легко масштабироваться для обеспечения связи между большим числом устройств, таких как мобильные телефоны, планшеты и компьютеры.
- Мобильность: Спутниковая связь может быть использована в подвижных объектах, таких как самолеты и корабли, что позволяет обеспечить надежную связь в любой точке мира.

Минусы спутниковой связи:

- Задержки: Спутниковая связь обычно имеет задержки в передаче данных, связанные с временем, которое требуется для передачи сигнала на спутник и обратно.
- Стоимость: Спутниковые системы обычно дороже, чем проводные или беспроводные системы связи, что может быть проблемой для небольших предприятий и потребителей.
- Ограничения пропускной способности: Пропускная способность спутниковой связи может быть ограничена в зависимости от числа пользователей, использующих систему, и скорости передачи данных.
- Влияние погоды: Погода может повлиять на качество связи, так как дождь, снег, туман и облачность могут ослабить сигнал и повлиять на скорость передачи данных.
- Негативное воздействие на окружающую среду: Спутниковые системы могут иметь негативное воздействие на окружающую среду из-за потребления энергии и выбросов при производстве и утилизации.

6. РАСПРЕДЕЛЕНИЕ АДРЕСОВ РАБОЧЕЙ СТАНЦИИ С УЧЕТОМ 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.

Для нашей сети можно создать несколько подсетей, чтобы управлять трафиком более эффективно и снизить нагрузку на сеть. Определим следующие подсети:

Подсеть для здания 1:

- Администрация: 192.168.1.0/28 (адреса: 192.168.1.1-192.168.1.14)
- Бухгалтерия: 192.168.1.16/28 (адреса: 192.168.1.17-192.168.1.30)
- Отдел охраны: 192.168.1.32/29 (адреса: 192.168.1.33-192.168.1.38)
- IT отдел: 192.168.1.64/27 (адреса: 192.168.1.65-192.168.1.94)
- Технологический отдел: 192.168.1.96/27 (адреса: 192.168.1.97-192.168.1.126)
- Отдел кадров: 192.168.1.128/29 (адреса: 192.168.1.129-192.168.1.134)

Подсеть для здания 2:

- Производственный отдел: 192.168.2.0/28 (адреса: 192.168.2.1-192.168.2.17)
- Отдел снабжения: 192.168.2.16/28 (адреса: 192.168.2.18-192.168.2.30)
- Отдел сбыта: 192.168.2.32/29 (адреса: 192.168.2.65-192.168.2.94)
- Транспортный отдел: 192.168.2.64/29 (адреса: 192.168.2.97-192.168.2.126)

Для серверов можно выделить отдельную подсеть, чтобы обеспечить им более высокую скорость и безопасность передачи данных:

Подсеть для серверов:

- Сервер1: 10.0.0.1/24
- Сервер2: 10.0.0.2/24
- Сервер3: 10.0.0.3/24
- Сервер4: 10.0.0.4/24
- Сервер5: 10.0.0.5/24

Маска подсети для всех подсетей - 255.255.255.0, широковещательный адрес для каждой подсети вычисляется путем установки всех битов маски в 1 и применения операции "ИЛИ" к адресу подсети.

Таким образом, широковещательный адрес и маска подсети для каждой подсети выглядят следующим образом:

Подсеть для здания 1:

- Администрация: Broadcast - 192.168.1.15, Маска - 255.255.255.240
- Бухгалтерия: Broadcast - 192.168.1.31, Маска - 255.255.255.240
- Отдел охраны: Broadcast - 192.168.1.39, Маска - 255.255.255.248
- IT отдел: Broadcast - 192.168.1.95, Маска - 255.255.255.224
- Технологический отдел: Broadcast - 192.168.2.127, Маска - 255.255.255.224
- Отдел кадров: Broadcast - 192.168.1.143, Маска - 255.255.255.240

Подсеть для здания 2:

- Производственный отдел: Broadcast - 192.168.2.18, Маска - 255.255.255.240
- Отдел снабжения: Broadcast - 192.168.2.31, Маска - 255.255.255.248
- Отдел сбыта: Broadcast - 192.168.2.95, Маска - 255.255.255.248
- Транспортный отдел: Broadcast - 192.168.2.127, Маска - 255.255.255.248

Широковещательный адрес - это последний адрес в диапазоне IP-адресов подсети, который никому не присваивается и используется только для передачи широковещательных сообщений в сети.

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 ТОПОЛОГИИ СЕТИ, СРЕДЫ ПЕРЕДАЧИ, МЕТОДА ДОСТУПА, АКТИВНОГО И ПАССИВНОГО ОБОРУДОВАНИЯ КОРПАРАТИВНОЙ СЕТИ

8.1. Выбор проводов для передачи данных.

Для данной сети рекомендуется использовать витую пару категории 6 (Cat6) для соединения всех компьютеров и серверов в каждом здании. Для соединения серверов между зданиями рекомендуется использовать оптоволоконный кабель многомодовый OM3 или OM4.

Для подключения камер наблюдения рекомендуется использовать коаксиальный кабель RG-59/U или RG-6/U, а также усилитель сигнала, если расстояние от камеры до системы мониторинга более 100 метров.

Для соединения сетевых устройств с беспроводной сетью можно использовать Wi-Fi точки доступа, поддерживающие протоколы 802.11ac или 802.11ax. Рекомендуется использовать точки доступа, поддерживающие функцию балансировки нагрузки, чтобы обеспечить равномерное распределение трафика между точками доступа.

Для защиты сети от перенаправления трафика и других сетевых атак рекомендуется использовать межсетевой экран (firewall) и систему обнаружения вторжений (IDS/IPS).

Рекомендуется также установить систему резервного питания (UPS) для серверов и сетевых устройств, чтобы обеспечить бесперебойную работу сети в случае отключения электропитания.

8.2. Выбор типов кабелей для сети.

Необходимо выбрать методы доступа к сетям множества машин.

Для Ethernet-сетей и оптической сети была выбрана CSMA/CD – технология множественного доступа к общей передающей среде в локальной компьютерной сети с контролем коллизий. Относится к децентрализованным случайным методам. Он используется как в обычных сетях типа Ethernet, так и в высокоскоростных сетях (Fast Ethernet, Gigabit Ethernet). Работает на канальном уровне в модели OSI.

Для беспроводных сетей была выбрана CSMA/CA – класс протоколов доступа к среде передачи данных в беспроводных сетях. На канальном уровне перед передачей данных в эфир, станция отправляет специальный фрейм RTS, который извещает остальных о том, что узел готов передать данные. Узел назначения отвечает фреймом CTS, сообщая о готовности к приему.

8.3. Выбор коммутаторов.

Если в каждой локальной подсети имеется N количество рабочих станций, столько же IP-телефонов, по одной камере, одному датчику и одному принтеру, вычислим минимальное количество портов в коммутаторе для каждого отдела по формуле:

$$P = 1.5 * (N_{\text{р.ст}} + N_{VoiceIP} + 3)$$

Для данной сети можно выбрать следующие коммутаторы:

Администрация: коммутатор с минимум 8 портами - Cisco Catalyst 2960-X с 24 портами + 2 порта SFP (WS-C2960X-24PS-L)

Бухгалтерия: коммутатор с минимум 8 портами - Cisco Catalyst 2960-X с 24 портами + 2 порта SFP (WS-C2960X-24PS-L)

Отдел охраны: коммутатор с минимум 4 портами - Cisco Catalyst 2960-X с 24 портами + 2 порта SFP (WS-C2960X-24PS-L)

IT отдел: коммутатор с минимум 16 портами - Cisco Catalyst 2960-X с 48 портами + 2 порта SFP (WS-C2960X-48TS-L)

Технологический отдел: коммутатор с минимум 16 портами - Cisco Catalyst 2960-X с 48 портами + 2 порта SFP (WS-C2960X-48TS-L)

Отдел кадров: коммутатор с минимум 8 портами - Cisco Catalyst 2960-X с 24 портами + 2 порта SFP (WS-C2960X-24PS-L)

Производственный отдел: коммутатор с минимум 20 портами - Cisco Catalyst 2960-X с 48 портами + 2 порта SFP (WS-C2960X-48TS-L)

Отдел снабжения: коммутатор с минимум 12 портами - Cisco Catalyst 2960-X с 24 портами + 2 порта SFP (WS-C2960X-24PS-L)

Отдел сбыта: коммутатор с минимум 10 портами - Cisco Catalyst 2960-X с 24 портами + 2 порта SFP (WS-C2960X-24PS-L)

Транспортный отдел: коммутатор с минимум 8 портами - Cisco Catalyst 2960-X с 24 портами + 2 порта SFP (WS-C2960X-24PS-L)

Сервер 1: базы данных

- Cisco Catalyst 2960X-48FPD-L

Сервер 2: видеосервер

- Netgear ProSAFE M4300-28G (GSM4328S)

Сервер 3: Внешний DNS, WEB-сервер, mail-server

- Dell Networking N2024P

Сервер 4: File-server, PDC, DHCP, DNS внутренний, антивирусный сервер, Call-manager, Exchange-manager, PRINT

- Cisco Catalyst 2960X-48FPD-L

Сервер 5: Сервер приложений, BDC, PROXY

- TP-Link JetStream T2600G-28TS

8.4. Выбор сетевых адаптеров.

Администрация: 5 компьютеров - Intel Wi-Fi 6E AX210

Бухгалтерия: 7 компьютеров - ASUS PCE-AX58BT

Отдел охраны: 2 компьютера - TP-Link Archer TX3000E

IT отдел: 10 компьютеров - Netgear Nighthawk AX12 12-Stream Wi-Fi 6E Router

Технологический отдел: 12 компьютеров - ASUS ROG Rapture GT-AX11000

Отдел кадров: 5 компьютеров - ASUS PCE-AX58BT

Производственный отдел: 15 компьютеров - Netgear Nighthawk AX12 12-Stream Wi-Fi 6E Router

Отдел снабжения: 10 компьютеров - ASUS PCE-AX58BT

Отдел сбыта: 8 компьютеров - TP-Link Archer TX3000E

Транспортный отдел: 5 компьютеров - Netgear Nighthawk AX12 12-Stream Wi-Fi 6E Router

Сервер 1: базы данных - Intel Wi-Fi 6E AX210

Сервер2: видеосервер - ASUS PCE-AX58BT

Сервер 3: Внешний DNS, WEB-сервер, mail-server - Netgear Nighthawk AX12 12-Stream Wi-Fi 6E Router

Сервер 4: File-server, PDC, DHCP, DNS внутренний, антивирусный сервер, Call-manager, Exchange-manager, PRINT - ASUS ROG Rapture GT-AX11000

Сервер 5: Сервер приложений, BDC, PROXY - TP-Link Archer TX3000E

8.5. Выбор конфигурации серверов и рабочих станций.

Сервер 1: базы данных -

- Процессор: Intel Xeon Gold 6240
- Оперативная память: 64 ГБ
- Жесткий диск: 2 x 1 ТБ SSD в RAID 1
- Сетевой адаптер: Intel Wi-Fi 6E AX210

Сервер 2: видеосервер -

- Процессор: Intel Core i7-11700K
- Оперативная память: 32 ГБ
- Жесткий диск: 4 x 4 ТБ HDD в RAID 10
- Сетевой адаптер: ASUS PCE-AX58BT

Сервер 3: Внешний DNS, WEB-сервер, mail-server -

- Процессор: AMD EPYC 7302P
- Оперативная память: 128 ГБ
- Жесткий диск: 2 x 2 ТБ SSD в RAID 1
- Сетевой адаптер: Netgear Nighthawk AX12 12-Stream Wi-Fi 6E Router

Сервер 4: File-server, PDC, DHCP, DNS внутренний, антивирусный сервер, Call-manager, Exchange-manager, PRINT -

- Процессор: Intel Xeon Silver 4210
- Оперативная память: 128 ГБ
- Жесткий диск: 2 x 2 ТБ SSD в RAID 1 + 4 x 6 ТБ HDD в RAID 10
- Сетевой адаптер: ASUS ROG Rapture GT-AX11000

Сервер 5: Сервер приложений, BDC, PROXY -

- Процессор: AMD Ryzen 9 5950X
- Оперативная память: 64 ГБ
- Жесткий диск: 2 x 1 ТБ SSD в RAID 1
- Сетевой адаптер: TP-Link Archer TX3000E

Конфигурации рабочих станций:

- Администрация: 5 компьютеров - Intel Wi-Fi 6E AX210, процессор Intel Core i7, 16 ГБ оперативной памяти, жесткий диск 1 ТБ.
- Бухгалтерия: 7 компьютеров - ASUS PCE-AX58BT, процессор Intel Core i5, 8 ГБ оперативной памяти, жесткий диск 500 ГБ.
- Отдел охраны: 2 компьютера - TP-Link Archer TX3000E, процессор Intel Core i5, 8 ГБ оперативной памяти, жесткий диск 500 ГБ.
- IT отдел: 10 компьютеров - Netgear Nighthawk AX12 12-Stream Wi-Fi 6E Router, процессор Intel Core i7, 16 ГБ оперативной памяти, твердотельный накопитель 1 ТБ.
- Технологический отдел: 12 компьютеров - ASUS ROG Rapture GT-AX11000, процессор Intel Core i7, 16 ГБ оперативной памяти, твердотельный накопитель 1 ТБ.
- Отдел кадров: 5 компьютеров - ASUS PCE-AX58BT, процессор Intel Core i5, 8 ГБ оперативной памяти, жесткий диск 500 ГБ.
- Производственный отдел: 15 компьютеров - Netgear Nighthawk AX12 12-Stream Wi-Fi 6E Router, процессор Intel Core i7, 16 ГБ оперативной памяти, твердотельный накопитель 1 ТБ.

- Отдел снабжения: 10 компьютеров - ASUS PCE-AX58BT, процессор Intel Core i7, 16 ГБ оперативной памяти, твердотельный накопитель 1 ТБ.
- Отдел сбыта: 8 компьютеров - TP-Link Archer TX3000E, процессор Intel Core i7, 16 ГБ оперативной памяти, твердотельный накопитель 1 ТБ.
- Транспортный отдел: 15 компьютеров - Netgear Nighthawk AX12 12-Stream Wi-Fi 6E Router, процессор Intel Core i5, 8 ГБ оперативной памяти, твердотельный накопитель 512 ГБ.

9. ВЫБОР СЕТЕВОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ И КЛИЕНТСКОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ, СЕТЕВОЕ ПРИКЛАДНОЕ ОБЕСПЕЧЕНИЕ

В данном разделе необходимо выбрать операционную систему для персональных компьютеров и серверов.

Для ПК была выбрана Windows 10 Professional, ввиду дружелюбности интерфейса и удобности в работе. А для серверов была выбрана ОС Ubuntu, так как она легка и проста в настройке.

9.1. Выбор СУБД

Выбираем СУБД Oracle Database 11g.

Oracle Database 11g Standard Edition One характеризуется беспрецедентной простотой эксплуатации, мощью и выгодным соотношением цены и производительности для приложений масштаба рабочих групп, отдельных подразделений или приложений, работающих в среде интернет/интранет. Работая в различных средах, начиная от односерверных конфигураций для малого бизнеса и заканчивая распределенными средами крупных филиалов, Oracle Database 11g Standard Edition One обладает всеми функциональными возможностями для обеспечения работы критических для бизнеса приложений.

Особенности Oracle Database 11g:

1) Oracle 11G самостоятельно распределяет дисковое пространство для хранения данных, а администраторы могут просто назначать новые диски, которые автоматически в режиме реального времени разбиваются системой. 11G также осуществляет настройку ввода/вывода.

2) В области управления производительностью Oracle 11G обладает встроенным представлением текущей производительности системы в виде диаграммы, а также имеет средства управления настройкой SQL, помимо этого, он собирает и обрабатывает статистическую информацию. Это служит громадным подспорьем в диагностике системы, чего нет в DB2 и SQL.

3) Менеджер автоматической диагностики базы данных интуитивно чувствует появляющиеся трудности и так же автоматизировано разрешает проблемные ситуации. Он тщательно анализирует сотни тысяч строк SQL выражений с целью обнаружения неверных корреляций, таким образом, помогая правильному отображению данных. Это очень полезно при работе с комплексными приложениями от PeopleSoft, SAP или Siebel.

4) 10G Application Server заметно облегчает выполнение приложений и табличные вычисления. ПО имеет повышенную интеграцию и возможности сетевых сервисов, которые помогают пользователям на лету обрабатывать изменения в бизнес среде.

5) Новый подход к управлению рабочей нагрузкой основан на политике контроля доступа, которая позволяет сотрудникам эффективно открывать доступ к своим ресурсам по мере надобности.

На базе Oracle 11g реализуем следующие логические базы данных: архив баз данных, базы данных бухгалтерии, IT-отдела, хозяйственного отдела, отдела кадров, организационно-методического отдела и датчиков.

9.2. Выбор сервера приложений

В качестве сервера приложений выберем Oracle Application Server 10g версии 10.1.3.1. Oracle Application Server 10g идеально дополняет собой новую флагманскую СУБД Oracle Database 10g и позволяет максимально эффективно использовать преимущества распределенных вычислений для работы современных приложений уровня предприятия.

Oracle Application Server 10g 10.1.3.1 —сервер приложений, позволяющий упростить управление приложениями, выполняемыми в распределенной вычислительной среде.

Oracle Application Server 10g 10.1.3.1 — это основанная на стандартах интегрированная программная платформа, позволяющая организациям любого масштаба оперативнее реагировать на меняющиеся требования рынка. Oracle Application Server 10g 10.1.3.1 обеспечивает полную поддержку технологии J2EE и распределенных вычислений, включает встроенное ПО для корпоративных порталов, высокоскоростного Web-кэширования, бизнес-анализа, быстрого внедрения приложений, интеграции бизнес-приложений, поддержки беспроводных технологий, Web-сервисов — и все это в одном продукте. Поскольку платформа Oracle Application Server 10g 10.1.3.1 оптимизирована для Grid Computing, она позволяет повысить степень готовности IT-систем и снизить расходы на приобретение аппаратных средств и администрирование.

Oracle Application Server 10g 10.1.3.1 обладает рядом ключевых возможностей:

1) Улучшенная управляемость. Новые средства управления рабочей нагрузкой, предоставляемые Oracle Application Server 10g 10.1.3.1, упрощают оптимизацию вычислительной мощности путем перераспределения имеющихся ресурсов между приложениями.

2) Повышенная надежность. Oracle Application Server 10g 10.1.3.1 обладает новыми средствами повышения надежности корпоративных приложений, выполняемых на кластерах и в сети распределенных вычислений предприятия. Новые функции включают усовершенствованную архитектуру быстрого запуска при устранении отказа Fast Start Fault Recovery Architecture и функцию оповещения об ошибках Failure Notification (FaN).

3) Интеграция приложений. Oracle Application Server 10g 10.1.3.1 обладает усовершенствованными возможностями интеграции, которые позволяют использовать один программный продукт для различных типов интеграции приложений. В результате появляется

возможность создания в масштабе всей компании единой модели данных, выступающей в роли информационного ядра, что позволяет обеспечить экономию при реализации будущих интеграционных проектов.

4) Новые возможности для Web-сервисов. В Oracle Application Server 10g 10.1.3.1 усовершенствована функциональность Web-сервисов. Распределенная модель вычислений позволяет оптимизировать процесс наращивания и распределения вычислительной мощности, в то время как Web-сервисы облегчают повторное использование и интеграцию приложений.

5) Работа сервера приложений. Oracle Grid Control позволяет управлять всеми компонентами сервера приложений (Web-кэшем, инфраструктурой, J2EE, EJB и т.д.) Сервер приложений тесно связан с узлами сервера БД и при выходе из строя узла сервера БД, сервер приложения тут же узнает об этом и переключается на оставшиеся узлы.

9.3. Выбор МСЭ и mail-сервера

Воспользуемся прокси-сервером WinGate 9.2, его же будем использовать в качестве почтового сервера для внешней почты.

WinGate – прокси-сервер для Windows, позволяющий организовать прозрачный доступ в Интернет через один компьютер для всех пользователей корпоративной сети. Поддержка VPN позволяет соединять друг с другом удаленные сегменты сети так же просто, как если бы они находились в одной локальной сети. Кроме того, в состав WinGate входит полнофункциональный почтовый SMTP/POP сервер, который поддерживает многочисленные домены, сетевые псевдонимы и другие функции, необходимые для обработки электронной почты.

9.4. Выбор антивирусного сервера

NOD32 Enterprise Edition – многоуровневая легкая в управлении система безопасности для рабочих мест, серверов и почтовых шлюзов. Проактивная защита от угроз, обладающая настолько высокой производительностью, что вы забудете о существовании вирусов.

Пакет NOD32 Enterprise Edition был разработан для крупных и средних компьютерных сетей предприятий. Это уникальный пакет, включающий в себя лицензии на NOD32 для рабочих станций и файловых серверов Windows, Novell, Linux и BSD, а также мощную консоль удаленного администрирования (NOD32 Remote Administrator Console). Это идеальный выбор для средних и крупных организаций, имеющих несколько файловых серверов и удаленных офисов. Это решение можно также с легкостью использовать и на малых предприятиях с парком машин от пяти компьютеров.

NOD32 Enterprise Edition обеспечивает защиту клиентским рабочим станциям и файловым серверам в организациях любого размера и доступен для покупки на 1 или 2 года. Программа

поставляется с расширенной консолью администрирования, установки, настройки политик безопасности, централизованного обновления вирусных баз.

9.5. Exchange Server

Выбираем Microsoft Exchange Server.

На базе Microsoft Exchange может быть построена система информационного обмена в организации любого масштаба, начиная от небольшого офиса - до территориально распределенной корпорации. При этом встроенные механизмы обеспечат надежное тиражирование данных между серверами, а администратор сможет конфигурировать и управлять всей системой из единого места.

С одной стороны, Microsoft Exchange предоставляет в распоряжение пользователей законченное и готовое к употреблению решение, включающее в свой состав следующие компоненты:

- полнофункциональную электронную почту;
- средства группового планирования;
- средства организации доступа к совместно используемой информации (общие папки);
- средства поддержки коллективных дискуссий;
- шлюзы, обеспечивающие пользователям централизованный доступ к глобальным системам электронной почты, в первую очередь, Интернет.

С другой стороны, Microsoft Exchange может рассматриваться как среда для создания самых разнообразных приложений, в том числе:

- комплексных приложений для автоматизации групповой работы и WorkFlow-приложений;
- комплексных систем сбора и обработки корпоративной информации;
- приложений, обеспечивающих доступ пользователей к различным инородным системам передачи информации, таким, как факс-служба, голосовая почта и прочее;
- систем автоматизации документооборота предприятия.

Выпуск Exchange 2016 предназначен для крупных организаций и позволяет создавать несколько групп хранения и несколько баз данных. Выпуск Exchange 2016 предоставляет хранилище сообщений емкостью 8 ТБ, что позволяет расширить рамки ограничений на объем данных, хранимых на одном сервере. Выпуск Exchange 2016 предоставляет следующие средства и возможности:

- Все средства и компоненты, входящие в Exchange 2016 Standard Edition.
- Размер базы данных ограничен только возможностями оборудования
- Возможность размещения нескольких баз данных на одном сервере.
- Возможность работы с мобильных устройств, что удобно не только для мобильных, но и для стационарных работников.

9.6. Выбор Web-сервера

В качестве Web-сервера будем использовать NGINX 1.14.0.

это HTTP-сервер и обратный прокси-сервер, почтовый прокси-сервер, а также TCP/UDP прокси-сервер общего назначения. Уже длительное время он обслуживает серверы многих высоконагруженных российских сайтов, таких как Яндекс, Mail.Ru, ВКонтакте и Рамблер. Согласно статистике, Netcraft nginx обслуживал или проксировал 25.45% самых нагруженных сайтов в сентябре 2018 года.

Основная функциональность HTTP-сервера:

- Обслуживание статических запросов, индексных файлов, автоматическое создание списка файлов, кэш дескрипторов открытых файлов;
- Акселерированное обратное проксирование с кэшированием, распределение нагрузки и отказоустойчивость;
- Акселерированная поддержка FastCGI, uwsgi, SCGI и memcached серверов с кэшированием, распределение нагрузки и отказоустойчивость;
- Модульность, фильтры, в том числе сжатие (gzip), byte-ranges (докачка), chunked ответы, XSLT-фильтр, SSI-фильтр, преобразование изображений; несколько подзапросов на одной странице, обрабатываемые в SSI-фильтре через прокси или FastCGI/uwsgi/SCGI, выполняются параллельно;
- Поддержка SSL и расширения TLS SNI;
- Поддержка HTTP/2 с приоритетизацией на основе весов и зависимостей.

9.7. Выбор остального программного обеспечения

Call-менеджер: Office Communications Server 2016

ПО для видеонаблюдения: Milestone XProtect Enterprise 5.0

ПО для рабочих станций: Microsoft Office Корпоративный 2016

Для реализации файл-сервера, DNS, DHCP, PDC и BDC и Print-сервера воспользуемся встроенными службами серверной операционной системы.

10. РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ СЕТИ

Проведем моделирование разрабатываемой сети в программе Cisco Packet Tracer. Для моделирования будем использовать упрощенную структурную схему

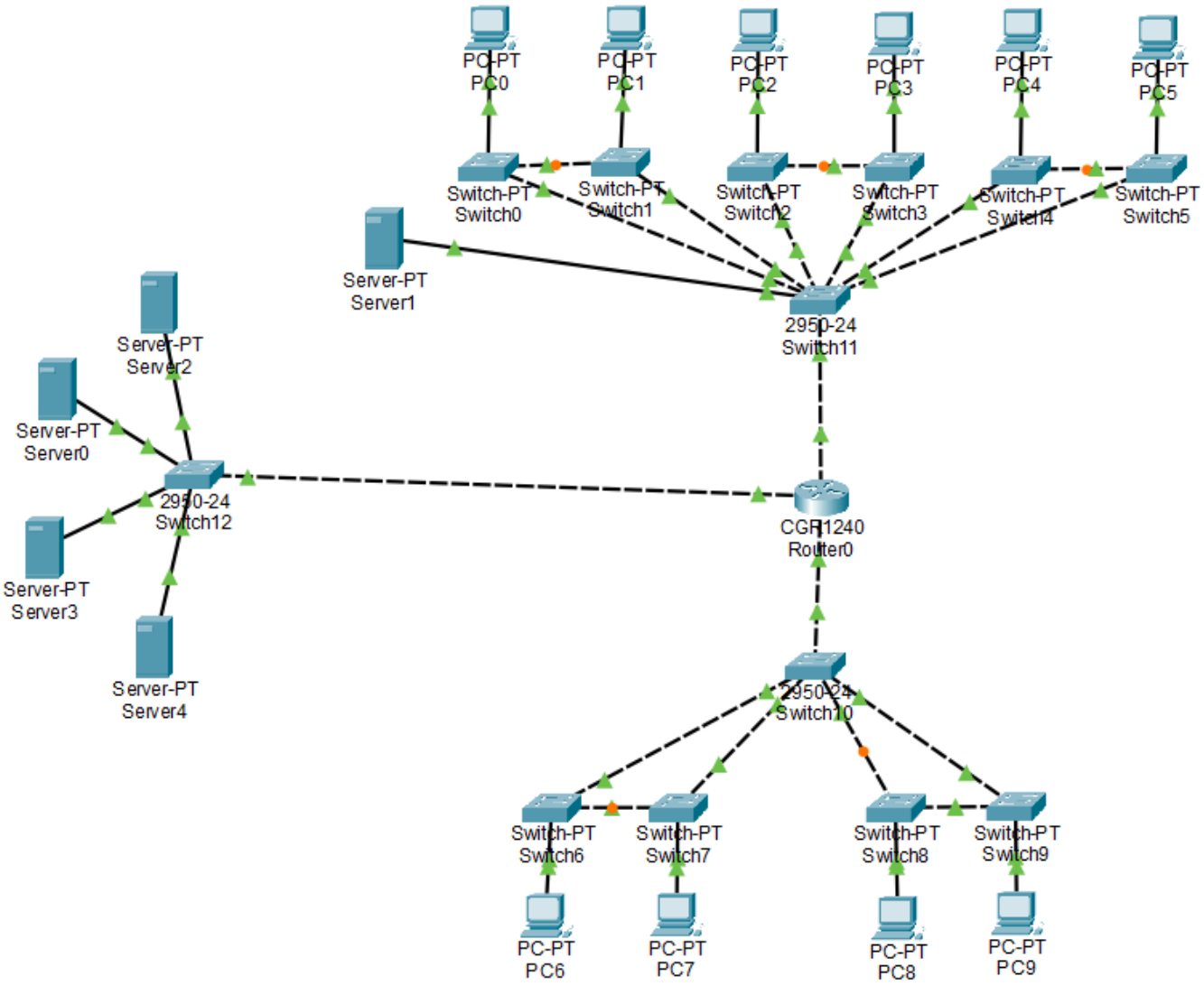


Рис. 3 – схема сети для моделирования

Моделирование производим исходя из нагрузки одной машины на один коммутатор, то есть, каждый отдел заменяется одним ПК. Каждый сервер в свою очередь также генерирует пакеты, но объем трафика от серверов мал, поэтому для упрощения имитационной программы его учитывать не будем.

В полученной модели мы можем пропинговать любое устройство сети с любого устройства, что говорит о том, что схема работоспособна.

11. РАЗРАБОТКА МОНТАЖНОЙ СХЕМЫ

Планирование - это отдельная, наиболее важная часть процесса создания всей сети. Необходимо знать точное расположение каждого абонентского отвода кабеля, при этом лучше, если оно будет отмечено на плане этажа, с тем, чтобы его можно было отследить во время прокладки сети. Через стены и потолки могут быть пропущены сотни идентичных кабелей, и если не будет соответствующей организации дела, то результатом явится беспорядок. План должен быть разработан с учетом требований протокола канального уровня, правил эксплуатации здания и пожарной безопасности для того, чтобы в дальнейшем не пришлось вытаскивать все кабели. Конечно, могут возникнуть сюрпризы, вызванные планировкой помещений и конструкцией здания, которые вынудят изменить план в середине его осуществления.

В курсовом проекте требуется разработать монтажную схему каждого этажа главного офиса организации.

Организация занимает четыре этажа (первый и последний) в двух семиэтажных зданиях, размерами 10х150 метров. Высота каждого этажа (а также подвала и чердака) равняется трём метрам.

С учетом всех требований, составим схемы:

1) Первого этажа первого здания

2) Седьмого этажа первого здания

3) Первого этажа второго здания

4) Седьмого этажа второго здания

Все вышеперечисленные монтажные схемы приведены в приложении Б.

Кабель будем прокладывать в коробах на высоте 2.5 метра от пола (высота этажей 3 метра). При прокладке постараемся как можно больше сократить количество используемого короба и кабеля. У рабочей станции кабель будет опущен по стене до уровня 0,5 метра от пола (т.е. длина вертикальной прокладки составит 2 метра), и там будет вмонтирована розетка. Отметим также, что в коридорах для прокладки кабеля использованы фальш-потолки, что позволяет избежать сверления перекрытий, а также пропуска коробов по потолку. Расстояние от розетки до конечного оборудования в среднем возьмем 1 метр.

Таблица 4 – расчет длины проводов в зданиях

Здание	Этаж	Длина,м
Витая пара		
1	1,7	2026
2	1,7	2049
Коаксиальный кабель		
1,2	Чердак, крыша	38

12. СМЕТА РАЗРАБОТКИ ПРОЕКТА

Сервер 1:

Процессор: Intel Xeon Gold 6240 - $4800

Оперативная память: 64 ГБ - $400

Жесткий диск: 2 x 1 ТБ SSD в RAID 1 - $400

Сетевой адаптер: Intel Wi-Fi 6E AX210 - $50

Итого: $5650

Сервер 2:

Процессор: Intel Core i7-11700K - $400

Оперативная память: 32 ГБ - $200

Жесткий диск: 4 x 4 ТБ HDD в RAID 10- $800

Сетевой адаптер: ASUS PCE-AX58BT- $60

Итого: $1460

Сервер 3:

Процессор: AMD EPYC 7302P- $2000

Оперативная память: 128 ГБ - $800

Жесткий диск: 2 x 2 ТБ SSD в RAID 1- $400

Сетевой адаптер: Netgear Nighthawk AX12 12-Stream Wi-Fi 6E Router - $600

Итого: $3800

Сервер 4:

Процессор: Intel Xeon Silver 4210 - $1700

Оперативная память: 128 ГБ - $1200

Жесткий диск: 2 x 2 ТБ SSD в RAID 1 - $500

4 x 6 ТБ HDD в RAID 10 - $1200

Сетевой адаптер: ASUS ROG Rapture GT-AX11000 - $450

Итого: $5050

Сервер 5:

Процессор: AMD Ryzen 9 5950X - $850

Оперативная память: 64 ГБ - $600

Жесткий диск: 2 x 1 ТБ SSD в RAID 1 - $200

Сетевой адаптер: TP-Link Archer TX3000E - $60

Итого: $1710

Администрация: 5 компьютеров - Intel Wi-Fi 6E AX210 ($40/шт) + процессор Intel Core i7 ($320/шт) + 16 ГБ оперативной памяти ($80/шт) + жесткий диск 1 ТБ ($100/шт) = $2700

Бухгалтерия: 7 компьютеров - ASUS PCE-AX58BT ($50/шт) + процессор Intel Core i5 ($200/шт) + 8 ГБ оперативной памяти ($40/шт) + жесткий диск 500 ГБ ($30/шт) = $2240

Отдел охраны: 2 компьютера - TP-Link Archer TX3000E ($60/шт) + процессор Intel Core i5 ($200/шт) + 8 ГБ оперативной памяти ($40/шт) + жесткий диск 500 ГБ ($30/шт) = $660

IT отдел: 10 компьютеров - Netgear Nighthawk AX12 12-Stream Wi-Fi 6E Router ($600/шт) + процессор Intel Core i7 ($320/шт) + 16 ГБ оперативной памяти ($80/шт) + твердотельный накопитель 1 ТБ ($100/шт) = $11000

Технологический отдел: 12 компьютеров - ASUS ROG Rapture GT-AX11000 ($700/шт) + процессор Intel Core i7 ($320/шт) + 16 ГБ оперативной памяти ($80/шт) + твердотельный накопитель 1 ТБ ($100/шт) = $14400

Отдел кадров: 5 компьютеров - ASUS PCE-AX58BT ($50/шт) + процессор Intel Core i5 ($200/шт) + 8 ГБ оперативной памяти ($40/шт) + жесткий диск 500 ГБ ($30/шт) = $1600

Производственный отдел: 15 компьютеров - Netgear Nighthawk AX12 12-Stream Wi-Fi 6E Router ($600/шт) + процессор Intel Core i7 ($320/шт) + 16 ГБ оперативной памяти ($80/шт) + твердотельный накопитель 1 ТБ ($100/шт) = $16500

Отдел снабжения: 10 компьютеров - ASUS PCE-AX58BT ($50/шт) + процессор Intel Core i7 ($320/шт) + 16 ГБ оперативной памяти ($80/шт) + твердотельный накопитель 1 ТБ ($100/шт) = $5500

Отдел сбыта: 8 компьютеров - TP-Link Archer TX3000E ($100/шт) + процессор Intel Core i7 ($320/шт) + 16 ГБ оперативной памяти ($80/шт) + твердотельный накопитель 1 ТБ ($100/шт) = $4800

Транспортный отдел: 15 компьютеров - Netgear Nighthawk AX12 12-Stream Wi-Fi 6E Router ($500/шт) + процессор Intel Core i5 ($250/шт) + 8 ГБ оперативной памяти ($40/шт) + твердотельный накопитель 500 ГБ ($30/шт) = $12300

Cisco Catalyst 2960-X с 24 портами + 2 порта SFP (WS-C2960X-24PS-L): 7 шт. - $1 200/шт = $8400

Cisco Catalyst 2960-X с 48 портами + 2 порта SFP (WS-C2960X-48TS-L): 3 шт. - $2 800/шт = $8400

Cisco Catalyst 2960X-48FPD-L: 2 шт. - $5 000/шт = $10000

Netgear ProSAFE M4300-28G (GSM4328S) - $1 200/шт = $1200

Dell Networking N2024P - $1 500/шт = $1500

TP-Link JetStream T2600G-28TS - $300/шт = $300

ЗАКЛЮЧЕНИЕ

В ходе данной курсовой лабораторной работы был разработан проект корпоративной сети предприятия. В частности, были сформированы схем информационных потоков на предприятии, спроектирована структурная схема вычислительно сети, разработана защита от несанкционированного доступа, организованы связи с филиалами, также были распределены рабочие станции с учетом структурной схемы, выбрана топология сети и был разработан план монтажной прокладки соединений и расположения сетевого оборудования. В итоге получилась полноценная работоспособная корпоративная сеть для документооборота на производственном предприятии.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

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.

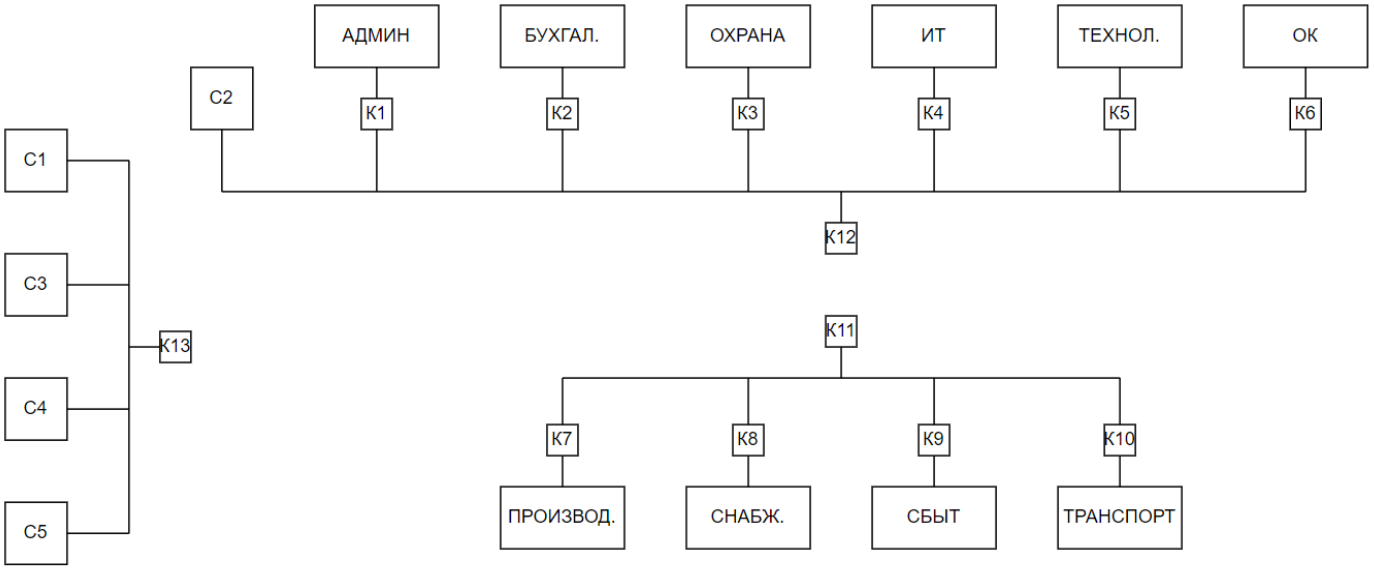
3) Советов Б. Я., Яковлев С. А. Моделирование систем: Учеб. для вузов – 3-е изд, перераб и доп. – М.: Высш. шк., 2001. – 343 с.

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.

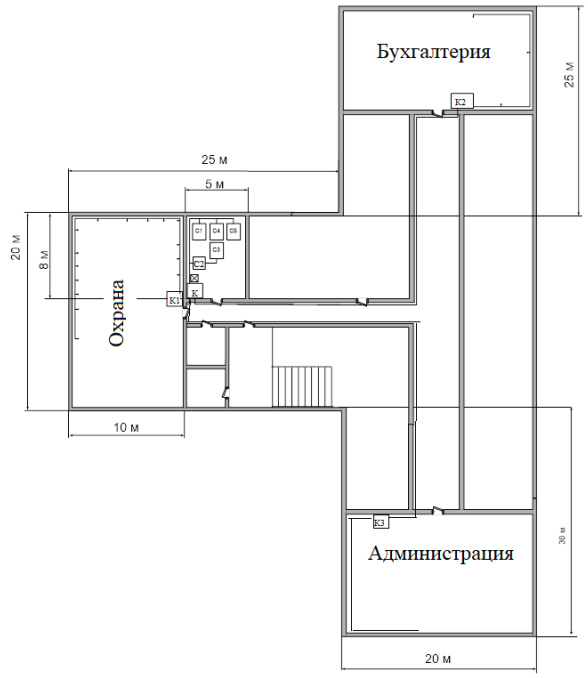
6) Алексеев В. GSM/GPRS Терминалы ведущих мировых производителей - "Компоненты и технологии" № 1, 2005

ПРИЛОЖЕНИЕ А



ПРИЛОЖЕНИЕ Б

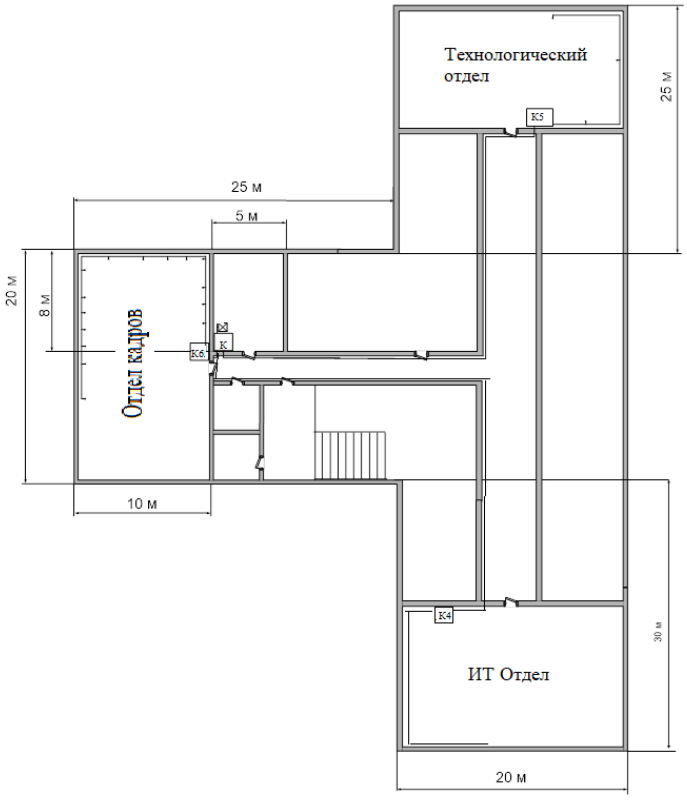
Первое здание (1 этаж):



К1 К2 К3 - Коммутаторы;

- Шахта для оптоволокна;

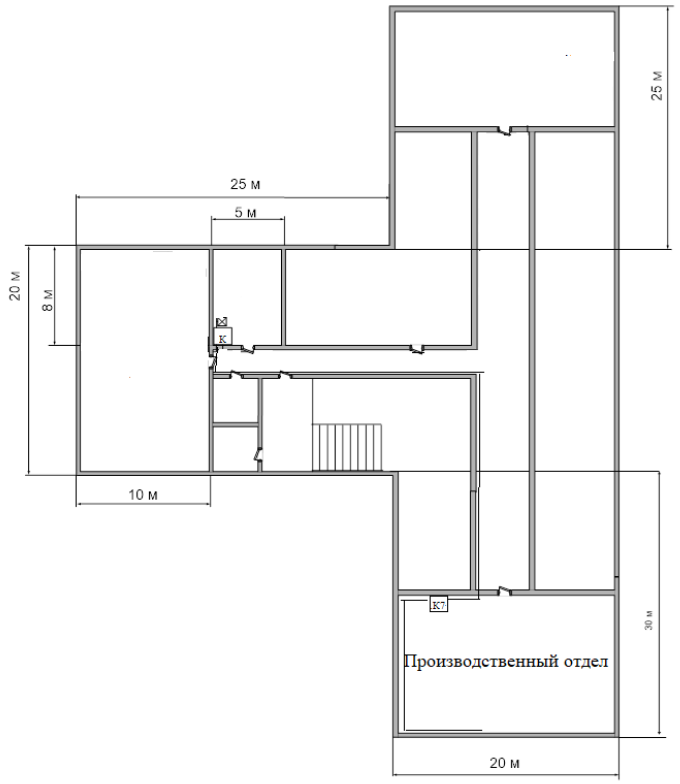
Первое здание (7 этаж):



К4 К5 К6 - Коммутаторы;

- Шахта для оптоволокна;

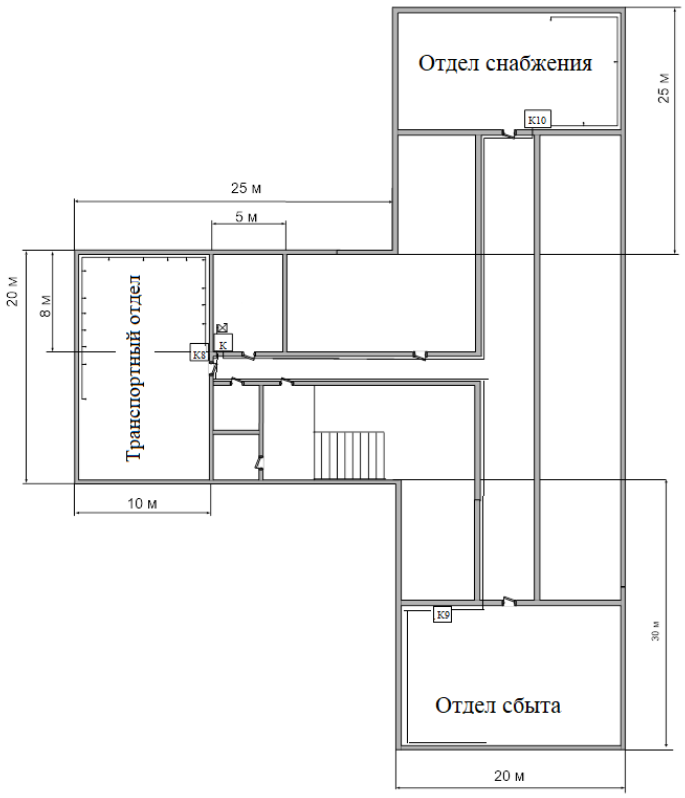
Второе здание (1 этаж):



К7 - Коммутаторы;

- Шахта для оптоволокна;

Второе здание (7 этаж):



К8 К9 К10 - Коммутаторы;

- Шахта для оптоволокна;