**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**федеральное государственное образовательное бюджетное учреждение высшего образования**

**«Вологодский государственный университет»**

**(ВоГУ)**

**Сети и телекоммуникации**

* + 1. **КУРСОВОЙ ПРОЕКТ:**
    2. **“РАЗРАБОТКА ПРОЕКТА КОРПОРАТИВНОЙ СЕТИ АВТОМАТИЗАЦИИ ОРГАНИЗАЦИОННО-  
       РАСПОРЯДИТЕЛЬНОГО ДОКУМЕНТООБОРОТА 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: РПС-41**

**Студент: Алиев Т.С.,**

**Руководитель: Суконщиков А.А.**

Вологда

2022 г.

**Оглавление**

[1. СХЕМА ИНФОРМАЦИОННЫХ ПОТОКОВ НА ПРЕДПРИЯТИИ И РАСЧЕТ ОБЪЕМА ПОТОКОВ МЕЖДУ ОТДЕЛАМИ 4](#_Toc121086101)

[1.1. Организационный анализ структуры предприятия 4](#_Toc121086102)

[1.2. Схема информационных потоков с учетом серверов 5](#_Toc121086103)

[2. СТРУКТУРНАЯ СХЕМА КОРПОРАТИВНОЙ СЕТИ 7](#_Toc121086104)

[3. РАЗРАБОТКА ЗАЩИТЫ СЕТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА 8](#_Toc121086105)

[3.1. Разработка защиты от внутреннего НСД 8](#_Toc121086106)

[3.4. Разработка VLAN 13](#_Toc121086107)

[4. РАСПРЕДЕЛЕНИЕ IP-АДРЕСОВ 15](#_Toc121086108)

[5. ОРГАНИЗАЦИЯ СВЯЗИ С ФИЛИАЛАМИ 17](#_Toc121086109)

[6. ВЫБОР СЕТЕВЫХ ПРОТОКОЛОВ 19](#_Toc121086110)

[7. ВЫБОР ТОПОЛОГИИ СЕТИ 22](#_Toc121086111)

[8. ВЫБОР СРЕДЫ ПЕРЕДАЧИ 24](#_Toc121086112)

[9. ВЫБОР СЕТЕВОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ 27](#_Toc121086113)

[10. ВЫБОР СЕТЕВОГО ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 28](#_Toc121086114)

[10.1. Выбор СУБД 28](#_Toc121086115)

[10.2. Выбор сервера приложений 28](#_Toc121086116)

[10.3. Выбор МСЭ и mail-сервера 30](#_Toc121086117)

[10.4. Выбор антивирусного сервера 30](#_Toc121086118)

[10.5. Exchange Server 30](#_Toc121086119)

[10.6. Выбор Web-сервера 31](#_Toc121086120)

[10.7. Выбор остального программного обеспечения 32](#_Toc121086121)

[11. РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ СЕТИ 33](#_Toc121086122)

[12. РАЗРАБОТКА МОНТАЖНОЙ СХЕМЫ 33](#_Toc121086123)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 36](#_Toc121086124)

[ПРИЛОЖЕНИЕ 1 37](#_Toc121086125)

[ПРИЛОЖЕНИЕ 2 38](#_Toc121086126)

ВВЕДЕНИЕ

Бурное развитие науки и промышленности в 20 веке, обусловленное социально-экономическим соревнование двух систем: капиталистической во главе с США и социалистической в главе с СССР, породило неудержимый рост объемов поступающей информации. Возникла целая индустрия по переработке, передаче и распределения информации. Рост информационных объемов и достижения в области микроэлектроники привели к созданию сверхскоростных процессоров, являющихся сегодня основным средством переработки и управления информацией. Информационные ресурсы стали играть в современном обществе большую роль чем материальные, что накладывает свои законы, правила и закономерности. Эти закономерности и правила становятся необходимым элементом материального производства. Если на заре информационного взрыва, в 60–70е годы прошлого столетия в области информационных технологий доминировали инженеры и программисты, то сейчас пользователи ЭВМ в самых различных областях человеческой деятельности являются доминирующей группой в самых различных областях

На производственном предприятия это как никогда актуально, ведь каждый день поступает несколько десятков запросов, а может и даже сотней, и для организации слаженной работы всех сотрудников во избежание различного рода коллизий должна быть разработана корпоративная сеть, позволяющая не только корректно организовать рабочий процесс, но и стать главным хранилищем все информации предприятия.

В данной работе будет разработана такая КС, будут пройдены 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 трех четырехэтажных зданиях площадью 24х200 м и занимает первый и последний этажи в каждом здании. Расстояние между зданиями – 80 м.

1.1. Организационный анализ структуры предприятия

На начальном этапе проектирования корпоративной сети предприятия необходимо выделить:

* Отделы
* Операции в отделах
* Необходимую операцию для отделов
* Виды информации, передаваемой между отделами
* Предварительные объемы передаваемой информации

Если рассматривать сеть документооборота производственного предприятия, то она имеет следующую структуру:

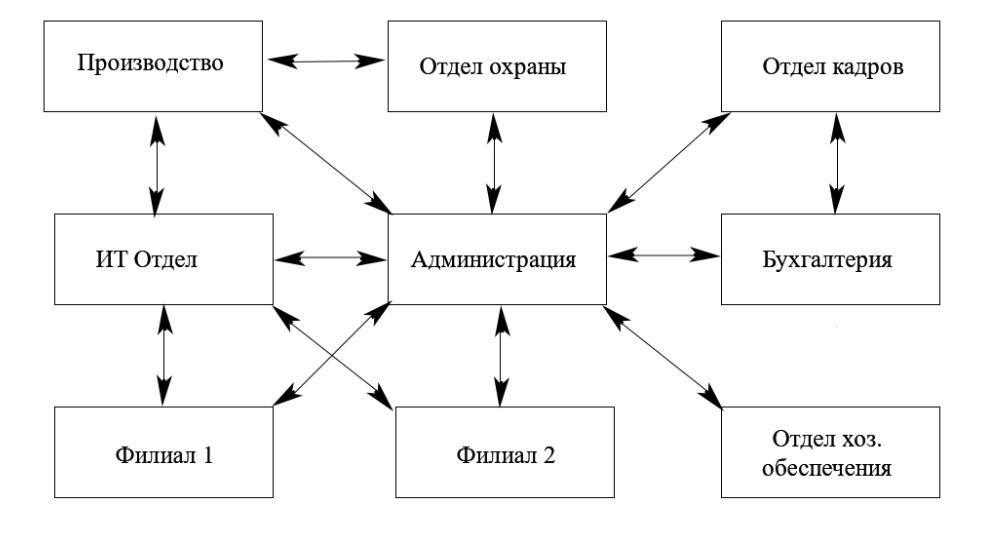


Рис. 1 – структура здания

Определим распределение трафика между отделами. В таблице 1.1 показан средний объём информации, передаваемый между отделами и филиалами за один рабочий день в мегабайтах. Трафик складывается из рабочей информации плюс 10% служебной информации, также учитываем, что при передаче по сети информации она увеличивается в 1,7 раза за счет помехоустойчивого кодирования.

Таблица 1.1

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | АДМ | ИТ | ОХР | ПР | ОК | БУХ | ХОЗ | ФИЛ1 | ФИЛ2 | Σ |
| АДМ | - | 50 | 20 | 40 | 70 | - | 70 | 55 | 60 | 325 |
| ИТ | 90 | - | - | 58 | - | - | 40 | 80 | 50 | 260 |
| ОХР | 40 | - | - | - | - | - | - | - | - | 40 |
| ПР | 50 | 90 | - | - | - | - | - | 82 | 65 | 287 |
| ОК | 60 | - | - | - | - | - | - | - | - | 60 |
| БУХ | 30 | - | - | - | - | - | 50 | 25 | 70 | 185 |
| ХОЗ | 25 | 40 | - | 51 | - | 60 | - | 45 | 25 | 195 |
| ФИЛ1 | 50 | 35 | - | 73 | - | 30 | 40 | - | 10 | 165 |
| ФИЛ2 | 60 | 24 | - | 54 | - | 60 | 35 | 65 | - | 244 |
| Σ | 385 | 239 | 20 | 276 | 70 | 150 | 235 | 352 | 280 |  |

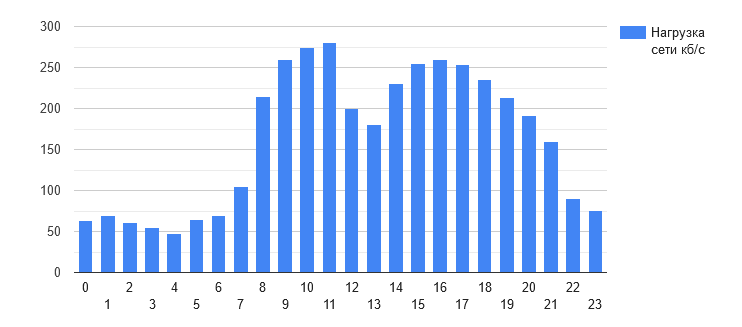


Рис. 2 – гистограмма информационной нагрузки по часам

1.2. 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:

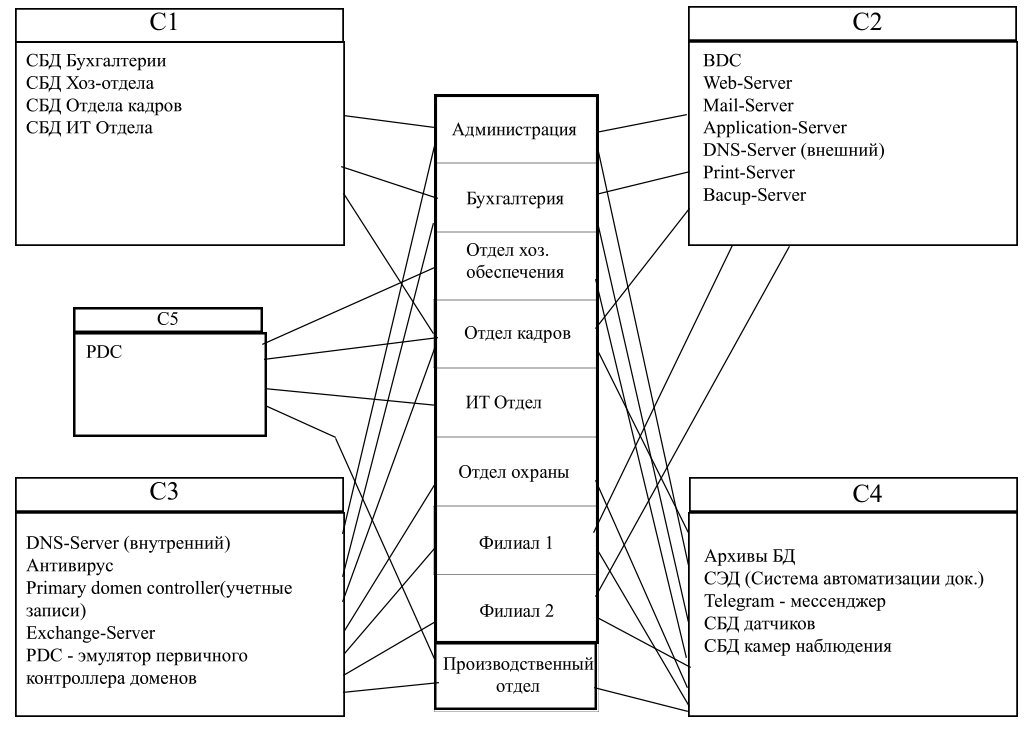


Рис. 3 – схема информационных потоков с учетом серверов

2. СТРУКТУРНАЯ СХЕМА КОРПОРАТИВНОЙ СЕТИ

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 1).

3. РАЗРАБОТКА ЗАЩИТЫ СЕТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Подключение компьютеров к сети позволяет организовать общий доступ к файлам и принтерам на других компьютерах, подключение к базам данных, а также обмен электронной почтой.

Политика доступа к сетевым сервисам должна быть уточнением общей политики организации в отношении защиты информационных ресурсов в организации. Для того чтобы межсетевой экран успешно защищал ресурсы организации, политика доступа пользователей к сетевым сервисам должна быть реалистичной. Таковой считается политика, при которой найден гармоничный баланс между защитой сети организации от известных рисков и необходимостью доступа пользователей к сетевым сервисам. В соответствии с принятой политикой доступа к сетевым сервисам определяется список сервисов Интернета, к которым пользователи должны иметь ограниченный доступ. Задаются также ограничения на методы доступа, необходимые для того, чтобы пользователи не могли обращаться к запрещенным сервисам Интернета обходными путями.

Для обеспечения безопасной работы и защиты от несанкционированного доступа необходимо иметь:

1. Политику пользователей для защиты на внутреннем уровне.

2. Использование межсетевого экрана для защиты локальной сети от внешних несанкционированных воздействий.

Контроль прав доступа производится разными компонентами программной среды - ядром операционной системы, дополнительными средствами безопасности, системой управления базами данных, посредническим программным обеспечением (таким как монитор транзакций) и т.д.

Основные требования по безопасности данных, предъявляемые к БД и СУБД, во многом совпадают с требованиями, предъявляемыми к безопасности данных в компьютерных системах – контроль доступа, криптозащита, проверка целостности, протоколирование и т.д. Большинство современных СУБД имеют встроенные средства, позволяющие администратору системы определять права пользователей по доступу к различным частям БД, вплоть до конкретного элемента.

Для организации защиты на внутреннем уровне необходимо определить какие группы пользователей к каким ресурсам имеют тот или иной вид доступа.

Для организации защиты на внешнем уровне необходимо настроить межсетевой экран для внешних пользователей.

Таким образом, для нашей локальной сети необходимо на административном уровне разработать политику доступа и разграничения доступа к информационным ресурсам данной сети.

3.1. Разработка защиты от внутреннего НСД

Организация защиты от НСД на внутреннем уровне реализуется путем ограничения доступа различных отделов к различным серверам. Например, бухгалтерия имеет доступ к своей базе данных для занесения хранимой информации, например, о поставках различных отделов и о квитанциях на выплату зарплаты сотрудникам. Также бухгалтерии необходимо иметь доступ на чтение данных баз данных других отделов для сбора информации о вышеупомянутых поставках. Для каждого отдела должен быть определен уровень привилегий доступа к необходимым для слаженной работы серверам. Для этого построим таблицу типов доступа (табл. 2) для всех отделов производственного предприятия.

Таблица 2

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Отд | С1 | | | |  | | С2 | | | | | | С3 | | | С4 | | | | | | C5 |
| СБД бух | СБД хоз | СБД ОК | СБД ИТ |  | Print | | Web | МСЭ BU | DNS внеш. | BDC | Mail | | ES | DNS внут. |  | Арх БД | VS | TG | СБД дат | СЭД | P | |
| АДМ | R | R | R | R |  | RW | | RW | R R | R | - | RW | | RW | R |  | RW | R | RW | R RW | | RW | |
| ИТ | ME | ME | ME | ME |  | F | | F | F ME | RW | - | RW | | RW | RW |  | RW | - | RW | RW ME | | RW | |
| ОХР | - | R | - | - |  | RW | | - | - - | - | - | - | | RW | R |  | R | - | RW | - R | | RW | |
| ПР | - | - | - | - |  | RW | | - | - - | - | - | - | | RW | R |  | R | - | RW | - R | | RW | |
| ОК | ME | ME | ME | ME |  | F | | F | F - | ME | ME | F | | F | F |  | ME | ME | F | ME R | | F | |
| БУХ | RW | - | - | - |  | RW | | - | - R | - | - | - | | RW | R |  | RW | - | RW | - RW | | - | |
| ХОЗ | - | R | - | - |  | RW | | - | - - | - | - | - | | RW | R |  | R | RW | RW | RW R | | RW | |
| ФИЛ1 | R | R | R | R |  | RW | | - | - - | - | - | - | | RW | R |  | R | - | RW | * R | | - | |
| ФИЛ2 | R | R | R | R |  | RW | | - | - - | - | - | - | | RW | R |  | R | - | RW | - R | | - | |
| AS | RW | RW | RW | RW |  | - | | - | - - | R | - | - | | RW | - |  | RW | RW | - | - - | | - | |
| DNS | - | - | - | - |  | RW | | - | - - | - | RW | - | | RW | E |  | R | R | - | - - | | RW | |
| Call | - | - | - | - |  | - | | - | - - | - | RW | - | | - | RW |  | - | - | - | - - | | RW | |
| Арх | R | R | R | R |  | - | | - | - - | - | W | - | | - | - |  | - | R | - | - - | | W | |
| PDC | - | - | - | - |  | R | | - | - - | R | - | - | | - | RW |  | R | R | R | R 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

Такие типы доступа, как RW или ME, являются разного рода комбинациями вышеперечисленных основных типов доступа и сочетают в себе все привилегии, взятые для каждого из них по-отдельности.

3.2. 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.

Для начала определим отделы, имеющие доступ к интернету и филиалам. Данные представлены в таблице 3.

Таблица 3

|  |  |  |  |
| --- | --- | --- | --- |
| Отдел | Интернет | Ф1 | Ф2 |
| АДМ | + | + | + |
| ИТ | + | - | - |
| ОХР | - | - | - |
| ПР | - | - | - |
| ОК | - | - | - |
| БУХ | + | - | - |
| ХОЗ | - | - | - |
| ФИЛ1 | - | - | - |
| ФИЛ2 | - | - | - |
| AS | - | + | + |
| DNS | + | + | + |
| Арх | - | - | - |
| Mail | + | + | + |

Теперь определим уровень доступа к серверам из интернета. Данные сведены в таблице 4.

Таблица 4

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Отдел | C2 | | | С2' | | |
| AS | МСЭ | AVS | Web | Mail | DNS (внеш) |
| Ф1 | RW | + | R | R | RW | R |
| Ф2 | RW | + | R | R | RW | R |
| Гости | - | - | - | R | - | - |
| МС | RW | + | R | R | RW | R |
| Клиент | R | - | - | R | RW | R |

3.3. 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.

Протокол ESP имеет следующую структуру:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Байт | № | 0 | | | | | | | | 1 | | | | | | | | 2 | | | | | | | | 3 | | | | | | | |
| № | Бит | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 0 | Индекс параметров безопасности | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | 32 | Порядковый номер | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8 | 64 | Данные | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| … | … |  | | | | | | | | Дополнение (0-255 байтов) | | | | | | | | | | | | | | | | | | | | | | | |
| … | … |  | | | | | | | | | | | | | | | | Длина дополнения | | | | | | | | Тип данных | | | | | | | |
| … | … | Контрольная сумма | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Первый байт – индекс параметров безопасности. Значение этого поля вместе с IP-адресом получателя однозначно определяет защищенное виртуальное соединение для данного пакета.

Второй – порядковый номер. Служит для защиты от повторной передачи. Поле содержит монотонно возрастающее значение параметра. Несмотря на то, что получатель может отказаться от услуги по защите от повторной передачи пакета, оно всегда присутствует в ESP-заголовке. Отправитель (передающий IPsec-модуль) должен всегда использовать это поле, но получатель к этому не обязан.

Последующие байты используются для передачи данных в соответствии с полем «Тип данных». Если используемый для шифрования этого поля алгоритм требует данных для синхронизации крипто процессов, то это поле может содержать эти данные в явном виде.

После байтов данных следует дополнение. Необходимо, например, для алгоритмов, которые требуют, чтобы открытый текст был кратен некоторому числу байтов), например, размеру блока для блочного шифра. Последние два байта дополнения используются для хранения его размера и типа данных.

Каждый пакет завершается одним байтом контрольной суммы, служащей для аутентификации и проверки целостности пакета

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. Имеет следующую структуру:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Байт | № | 0 | | | | | | | | 1 | | | | | | | | 2 | | | | | | | | 3 | | | | | | | |
| № | Бит | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 0 | Тип заголовка | | | | | | | | Длина | | | | | | | | Зарезервировано | | | | | | | | | | | | | | | |
| 4 | 32 | Индекс параметров безопасности | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8 | 64 | Порядковый номер | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 12 | 96 | Данные аутентификации | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| … | … |

Первый байт – тип следующего заголовка, идущего после заголовка AH. По этому полю приёмный IPsec-модуль узнает о защищаемом протоколе верхнего уровня. В этом же байте содержатся длина содержимого и два зарезервированных байта, заполняемых нулями.

Далее следуют индекс параметров безопасности и порядковый номер, как в ESP, а затем следуют данные аутентификации – цифровой подписи, содержащей в себе контрольную сумму, используемую для проверки целостности пакета.

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.

3.4. Разработка VLAN

VLAN (Virtual Local Area Network) - виртуальная локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным членам группироваться вместе, даже если они не находятся в одной физической сети.

В процессе разработки такой виртуальной сети для каждого отдела и сервера требуется прописать название такой сети, подключаемые устройства, коммутаторы, связывающие их, и сервер, к которому обращаются эти устройства.

Для сетей всех устройств сети будут прописываться таким образом:

VLAN 10 VoiceIP;

(T1-T12; K1-K14; C4(Call-manager))

VLAN 20 Датчики

(D1-D12; K1-K14; C4(СБД датчиков))

VLAN 30 Камеры

(VC1-VC12; K1-K14; C4(VS))

VLAN 40 Принтеры

(P1-P12; K1-K14; C1(Print-Server))

VLAN 50 Администрация

(PC1-PC9; K1, K13; C1(Все), С2(Все), С3(Все), С4(VS, СБД датчиков, Call-Manager, Архив БД))

VLAN 60 Отдел кадров

(PC10-PC19; K2, K13; C1(СБД ОК, Print-server), С2(AS, AVS), С3(Все), С4(Call-Manager, Архив БД))

VLAN 70 Бухгалтерия

(PC20-PC27; K3, K13; C1(Все), С2(Все), С3(Все), С4(Call-Manager, Архив БД))

VLAN 80 Хозяйственный отдел

(PC28-PC37; K4, K13; C1(СБД хоз, Print-server), С2(AS, AVS), С3(Все), С4(Call-Manager, Архив БД))

VLAN 90 ИТ-отдел

(PC38-PC57; K5, K13-14; C1(Все), С2(Все), С3(Все), С4(Все), C5(PDC))

VLAN 100 Охрана

(PC58-PC60; K6, K13; C1(Print-server), С2(AS, AVS), С3(Все), С4(Call-Manager, Архив БД, VS, СБД датчиков))

VLAN 110 Орг. отдел

(PC61-PC70; K7, K13-14; C1(СБД орг, Print-server), С2(AS, AVS), С3(ES, DNS внут.), С4(Call-Manager, Архив БД), С5(PDC))

VLAN 120 Хирургическое отделение

(PC71-PC80; K8, K13-14; C1(СБД орг, Print-server), С2(AS, AVS), С3(ES, DNS внут.), С4(Call-Manager, Архив БД), С5(PDC))

VLAN 130 Терапевтическое отделение

(PC81-PC100; K9, K13-14; C1(СБД орг, Print-server), С2(AS, AVS), С3(ES, DNS внут.), С4(Call-Manager, Архив БД), С5(PDC))

VLAN 140 Травмпункт

(PC101-PC106; K10, K13-14; C1(СБД орг, Print-server), С2(AS, AVS), С3(ES, DNS внут.), С4(Call-Manager, Архив БД), С5(PDC))

VLAN 150 Приёмное отделение

(PC107-PC118; K11, K13-14; C1(СБД орг, Print-server), С2(AS, AVS), С3(ES, DNS внут.), С4(Call-Manager, Архив БД), С5(PDC))

VLAN 160 Главная медсестра

(PC119-PC130; K12, K13-14; C1(СБД орг, Print-server), С2(AS, AVS), С3(ES, DNS внут.), С4(Call-Manager, Архив БД), С5(PDC))

4. РАСПРЕДЕЛЕНИЕ IP-АДРЕСОВ

Теперь необходимо разделить сеть на подсети исходя из структурной схемы сети. Для каждой подсети определяются IP-адреса, маска и широковещательный адрес.

В разработке подсети необходимо учитывать различного рода датчики, телефоны, камеры и другие устройства, имеющие IP-адрес в сети.

Таким образом, первая подсеть первого здания включает в себя 98 устройств, из чего следует, что маска подсети будет равна 255.255.255.128. Результаты дальнейших подсчетов сведены в таблицу 5.

Таблица 5

|  |  |  |  |
| --- | --- | --- | --- |
| Сеть | Кол-во устройств | Маска | Кол-во адресов |
| Net1 | 86 | 255.255.255.128 | 128 |
| Net2 | 78 | 255.255.255.128 | 128 |
| Net3 | 13 | 255.255.255.248 | 16 |
| Net4 | 13 | 255.255.255.252 | 16 |
| Net5 | 13 | 255.255.255.252 | 16 |
| Net6 | 13 | 255.255.255.252 | 16 |

Распределение адресов по машинам будет происходить следующим образом:

* Нулевой адрес становится адресом подсети
* Первая группа адресов будет распределена на персональные компьютеры
* Вторая - на датчики
* Третья - на телефоны
* Четвертая - на принтеры
* Пятая - на камеры
* Шестая - на коммутаторы
* Седьмая - на серверы и входы роутера
* Восьмая – свободные адреса
* Последний адрес будет считаться широковещательным

Распределим таким образом адреса и получим для первой подсети:

1) Адрес сети: 192.168.19.0;

2) Адреса ПК: 192.168.19.1 – 192.168.19.60;

3) Адреса датчиков: 192.168.19.61 – 192.168.19.66;

4) Адреса телефонов: 192.168.19.67 – 192.168.19.72;

5) Адреса принтеров: 192.168.19.73 – 192.168.19.78;

6) Адреса видеокамер: 192.168.19.79 – 192.168.19.84;

7) Адреса коммутаторов: 192.168.19.85 – 192.168.19.97;

8) Адрес Wi-Fi: 192.168.19.98;

9) Свободные адреса: 192.168.19.99 – 192.168.19.126;

10) ША: 192.168.19.127;

Вторая подсеть:

1) Адрес сети: 192.168.19.128;

2) Адреса ПК: 192.168.19.129 – 192.168.19.198;

3) Адреса датчиков: 192.168.19.199 – 192.168.19.204;

4) Адреса телефонов: 192.168.19.205 – 192.168.19.211;

5) Адреса принтеров: 192.168.19.212 – 192.168.19.217;

6) Адреса видеокамер: 192.168.19.218 – 192.168.19.223;

7) Адреса коммутаторов: 192.168.19.224 – 192.168.19.229;

8) Адрес Wi-Fi: 192.168.19.230;

9) Адрес С5: 192.168.19.231;

9) Свободные адреса: 192.168.19.232 – 192.168.19.254;

10) ША: 192.168.19.255;

Третья подсеть:

1) Адрес сети: 192.168.20.0;

2) Адрес коммутатора: К13 = 192.168.20.1;

3) Адреса серверов:

С1 = 192.168.20.2; С2 = 192.168.20.3; С3 = 192.168.20.4; С4 = 192.168.20.5;

4) Свободный адрес: 192.168.20.6;

10) ША: 192.168.20.7;

Четвертая подсеть:

1) Адрес сети: 192.168.20.8;

2) Адреса коммутаторов:

К13 = 192.168.20.9; К14 = 192.168.20.10;

10) ША: 192.168.20.11;

Пятая подсеть:

1) Адрес сети: 192.168.20.12;

2) Адреса роутера и сервера:

R = 192.168.20.13; C2 = 192.168.20.14;

10) ША: 192.168.20.15;

Шестая подсеть:

1) Адрес сети: 192.168.20.16;

2) Адреса роутера и сервера:

R2 = 192.168.20.17; C2` = 192.168.20.18; R3 = 192.168.20.20

10) ША: 192.168.20.19;

5. ОРГАНИЗАЦИЯ СВЯЗИ С ФИЛИАЛАМИ

В этом разделе необходимо описать выданный преподавателем тип связи с филиалами по следующим разделам: теоретическое описание выданного метода, аппаратура, которая позволяет организовать данную связь на приемной и передающей стороне.

По техническому заданию связь с филиалами должна осуществляться по VDSL-линии и по спутниковой связи.

VDSL – сверхвысокоскоростная цифровая абонентская линия. Принадлежит к семейству технологий xDSL. Ее главное применение - цифровые абонентские петли, в которых требуется очень высокая скорость трансмиссии. В решениях, основанных на VDSL, центральной точкой системы является специализированная, коммутирующая система, принимающая транслированные данные из источника (напр. из оптико-волоконного кабеля), и, следовательно, используя классические, медные кабели, передающая данные целенаправленному получателю. Правило работы технологии ADSL опирается на использовании широкого диапазона частот сигналов, посылаемых в медных кабелях, и четвертного умножения используемых диапазонов, с целью отделить частотные каналы. Нижней, предельной частотой является 300 кГц (на практике принимается 350 кГц) в ситуации отсутствия необходимости передачи сигналов аналоговой телефонии. Верхний предел зависит от длины сегмента кабелей и может составлять от 30 МГц для кабеля, не превышающего 300 метров и до 10 МГц при 500-метровом кабеле.

Такие технические решения позволяют получить очень высокую пропускную способность, однако на относительно коротких отрезках кабелей:

• 56 Мбит/с на дистанции до 300 метров.

• 25 Мбит/с на дистанции 300 - 900 м.

• 10 Мбит/с на дистанции до 1500 м.

После превышения длины кабеля в 1500 метров, пропускная способность, доступная по технологии VDSL, становится ниже, чем в случае использования технологии ADSL. По этой причине, на больших дистанциях решения, основанные на VDSL, не используются.

Расширением VDSL является технология, называемая VDSL2, в которой принято мультиплексирование вместе с делением частоты сигнала, и взят за основу полный диапазон до 30 МГц. Решение этого типа позволяет значительно умножить возможную пропускную способность, однако, подобно тому как в случае предшественника, на коротких дистанциях:

• 200 Мбит/с на дистанции, не превышающей 300 м.

• 100 Мбит/с на дистанции 500 м.

• 50 Мбит/с на дистанции до 1000 м.

На дистанции от 1500 метров и выше возможная пропускная способность близка к той, что доступна по технологии ADSL, и удерживается на данном уровне на дистанции до 4 - 5 км. Считается, что в будущем VDSL2 вытеснит ADSL из рынка. Однако, наибольшим недостатком VDSL2 является необходимость использовать кабели высшей категории, с точно определенными, физическими параметрами, особенно на кратчайших, двухсотметровых сегментах. Такие требования отчетливо повышают общую стоимость реализации VDSL2, и в небольших применениях ее экономическая значимость становится дискуссионной.

В данной работе будем использовать технологию VDSL2 из-за её высокой пропускной способности. Расстояние между зданиями составляет 130 м, что позволяет использовать VDSL2 на максимальной скорости – 200 Мбит/с.

6. ВЫБОР СЕТЕВЫХ ПРОТОКОЛОВ

В данном разделе необходимо выбрать сетевые протоколы для каждого уровня сетевой модели сети, которые будут использоваться в разработанной сети и какие функции на основе данных протоколов будут выполняться.

В соответствии с техническим заданием, в данной корпоративной сети на сетевом уровне будут использоваться протоколы EIGRP и OSPF.

EIGRP (англ. Enhanced Interior Gateway Routing Protocol) — протокол маршрутизации, разработанный фирмой Cisco на основе протокола IGRP той же фирмы.

* Протокол IGRP (англ. Interior Gateway Routing Protocol) — протокол маршрутизации, разработанный фирмой Cisco, для своих многопротокольных маршрутизаторов в середине 1980-х годов для маршрутизации в пределах автономной системы (AS), имеющей сложную топологию и разные характеристики полосы пропускания и задержки. IGRP является протоколом внутренних роутеров (IGP) с вектором расстояния.

EIGRP — переработанный и улучшенный вариант IGRP, свободный от основного недостатка дистанционно-векторных протоколов — особых ситуаций с зацикливанием маршрутов — благодаря специальному алгоритму распространения информации об изменениях в топологии сети. EIGRP более прост в реализации и менее требователен к вычислительным ресурсам маршрутизатора чем OSPF. Также EIGRP имеет более продвинутый алгоритм вычисления метрики DUAL (Diffusing Update ALgorithm), который может использовать 5 различных компонентов для расчета:

* Bandwidth (Пропускная способность). Минимальная пропускная способность для данного маршрута (а не сумма цен (cost) в отличие от OSPF).
* Delay (Задержка). Суммарная задержка на всём пути маршрута.
* Reliability (Надежность). Наихудший показатель надёжности на всём пути маршрута, основанный на keepalive.
* Loading (Загруженность). Наихудший показатель загруженности интерфейса на всём пути маршрута, основанный на количестве трафика, проходящего через интерфейс и настроенном на нём параметре bandwidth.
* MTU. Минимальный размер MTU на всём пути маршрута.

По умолчанию, EIGRP использует только первые два компонента, так как надежность и загруженность — динамические величины, которые могут изменяться до нескольких раз в секунду. Соответственно, каждое изменение вызывает перерасчет метрики для маршрутов и использование процессорной мощности маршрутизатора до 100 %. MTU не является динамической величиной, но не используется по причине слабого влияния на метрику маршрута.

Ещё одно преимущество протокола EIGRP в том, что он способен производить суммаризацию на любом маршрутизаторе на пути, поскольку является протоколом класса «вектор расстояния» (Distance Vector), информация передается от соседа к соседу, где каждый следующий выбирает только лучший маршрут, отдаваемый соседу.

Единственным недостатком протокола EIGRP на данный момент является его ограниченность в использовании оборудования только компании Cisco. Хотя в феврале 2013 года Cisco открыла EIGRP, его внедрение в маршрутизаторы других производителей официально не объявлено.

OSPF (англ. Open Shortest Path First) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала. OSPF имеет следующие преимущества:

* Высокая скорость сходимости по сравнению с дистанционно-векторными протоколами маршрутизации;
* Поддержка сетевых масок переменной длины (VLSM);
* Оптимальное использование пропускной способности с построением дерева кратчайших путей.

OSPF поддерживает широковещательные сети со множественным доступом, использующие интерфейс Ethernet.

Кроме этого, на сетевом уровне будут применяться протоколы IPv4, ARP, ICMP

На канальном уровне будут использоваться протоколы HDLC и ARP.

HDLC – High-Level Data Link Control – бит-ориентированный протокол канального уровня сетевой модели OSI, разработанный для использования в соединениях с множественным доступом.

ARP – Address Resolution Protocol - протокол в компьютерных сетях, предназначенный для определения MAC-адреса, имея IP-адрес другого компьютера. По этому протоколу компьютер, желающий отправить пакет данных, отправляет широковещательный запрос, адресованный всем компьютерам в одном с ним широковещательном домене. Суть запроса: «компьютер с IP-адресом 10.22.22.2, сообщите свой MAC-адрес компьютеру с МАС-адресом (напр. a0:ea:d1:11:f1:01)». Сеть Ethernet доставляет этот запрос всем устройствам в том же сегменте Ethernet, в том числе и необходимому компьютеру. Тот, в свою очередь, отвечает первому компьютеру на запрос и сообщает свой MAC-адрес (напр. 00:ea:d1:11:f1:11) Теперь, получив MAC-адрес целевого компьютера, отправитель может передавать ему любые данные через сеть Ethernet.

На транспортном уровне будут использоваться протоколы TCP и UDP.

UDP будет использоваться для передачи данных с камер наблюдения, для совершения звонков по IP-телефонам и для передачи данных с датчиков дыма.

TCP будет использоваться для остальных операций, как, например, запись данных в БД, чтение данных из архива БД, отправка документа на сетевой принтер и т. д.

На прикладном уровне определяются функции доступа к сетевым службам. На серверах будут использоваться следующие протоколы:

СБД: NFS;

Print-сервер: FTP;

Exchange-сервер: SMTP, IMAP;

DNS-серверы: DNS;

PDC: NFS;

Web-сервер: HTTP,

Proxy-сервер: SNMP;

AS: NFS;

Mail-сервер: SMTP, IMAP;

Video-сервер: FTP,

VoiceIP: RTP;

7. ВЫБОР ТОПОЛОГИИ СЕТИ

Для определения принципа размещения и подключения машин и обеспечения стабильной работы сети необходимо выбрать её топологию. Топология сети – схема расположения и соединения сетевых устройств и способ описания конфигурации сети. Среди простейших видов топологий выделяют шинную, звезду, кольцо, ячеистую и возможные их комбинации:

1. Шинная топология сети — топология, при которой все компьютеры сети подключаются к одному кабелю, который используется совместно всеми рабочими станциями. При такой топологии выход из строя одной машины не влияет на работу всей сети в целом. Недостаток же заключается в том, что при выходе из строя или обрыве шины нарушается работа всей сети.
2. Топология сети «Звезда» — топология, при которой все рабочие станции имеют непосредственное подключение к серверу, являющемуся центром "звезды". При такой схеме подключения, запрос от любого сетевого устройства направляется прямиком к серверу, где он обрабатывается с различной скоростью, зависящей от аппаратных возможностей центральной машины. Выход из строя центральной машины приводит к остановке всей сети. Выход же из строя любой другой машины на работу сети не влияет.
3. Кольцевая топология сети — схема, при которой все узлы соединены каналами связи в неразрывное кольцо (необязательно окружность), по которому передаются данные. Выход одного ПК соединяется с входом другого. Начав движение из одной точки, данные, в конечном счете, попадают на его начало. Такая топология сети не требует установки дополнительного оборудования (сервера или хаба), но при выходе из строя одного компьютера останавливается и работа всей сети.
4. Ячеистая топология сети — топология, при которой каждая рабочая станция соединяется со всеми другими рабочими станциями этой же сети. Каждый компьютер имеет множество возможных путей соединения с другими компьютерами. Поэтому обрыв кабеля не приведет к потере соединения между двумя компьютерами. Эта топология сети допускает соединение большого количества компьютеров и характерна, как правило, для крупных сетей.

В нашей корпоративной сети мы будем использовать комбинацию шинной и звездной топологий, называемую «звездно-шинной»:

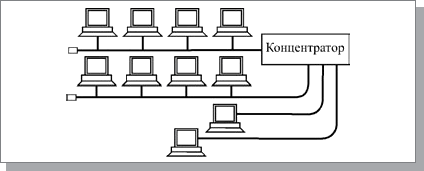


Рис. 4 – звездно-шинная топология сети

В звездно-шинной топологии используется комбинация шины и пассивной звезды. К концентратору подключаются как отдельные компьютеры, так и целые шинные сегменты. На самом деле реализуется физическая топология шина, включающая все компьютеры сети. В данной топологии может использоваться и несколько концентраторов, соединенных между собой и образующих так называемую магистральную, опорную шину. К каждому из концентраторов при этом подключаются отдельные компьютеры или шинные сегменты. В результате получается звездно-шинное дерево. Таким образом, пользователь может гибко комбинировать преимущества шинной и звездной топологий, а также легко изменять количество компьютеров, подключенных к сети. С точки зрения распространения информации данная топология равноценна классической шине.

8. ВЫБОР СРЕДЫ ПЕРЕДАЧИ

8.1. Выбор проводов для передачи данных.

В соответствии с техническим заданием необходимо использовать спутниковую связь между зданиями. Для осуществления обмена данными через спутник необходимы: спутниковая антенна, конвертер, провод для передачи данных и спутниковый приёмник.

В самих же зданиях используем витую пару для передачи данных на расстояния не больше 100 метров между рабочими станциями и серверами. Для нашей сети отлично подойдет широкораспространенный провод UTP, 4 пары, кат. 5е.

8.2. Метод доступа

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. Активное оборудование

Активным оборудованием считаются коммутаторы, концентраторы, адаптеры, маршрутизаторы, принт-серверы и многое другое. Активное оборудование обеспечивает передачу данных, независимо от канала и техники, и отвечает за то, чтобы вся информация была сортирована в пакеты, а также все пакеты строго разделялись по нужным каналам.

В нашей КС в понятие активного оборудования включаются: сетевые видеокамеры, коммутаторы, роутеры, сетевые принтеры, веб-камеры, датчики дыма и телефоны.

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:

Сведем результаты в таблицу 6:

Таблица 6

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Отдел | Количество машин | Телефоны | Камеры | Датчики | Принтеры | Порты |
| Администрация | 12 | 12 | 1 | 1 | 1 | 32 |
| Бухгалтерия | 8 | 8 | 1 | 1 | 1 | 29 |
| Отдел кадров | 17 | 17 | 2 | 2 | 2 | 35 |
| ИТ-отдел | 20 | 20 | 1 | 1 | 1 | 65 |
| Хозяйственный отдел | 10 | 10 | 3 | 3 | 3 | 35 |
| Производство | 24 | 24 | 4 | 4 | 4 | 35 |
| Охрана | 6 | 6 | 2 | 2 | 2 | 16 |
| Роутер-коммутатор 1 | 10 | 0 | 0 | 0 | 0 | 12 |
| Роутер-коммутатор 2 | 12 | 0 | 0 | 0 | 0 | 15 |
| Роутер-коммутатор 3 | 10 | 0 | 0 | 0 | 0 | 15 |

Оборудование было выбрано следующее:

Коммутаторы:

Таблица 7

|  |  |  |  |
| --- | --- | --- | --- |
| Отдел | Номер | Модель | Порты |
| Администрация | К1 | ZYXEL GS2210-24 | 32 |
| Отдел кадров | К2,К10 | Nortel Networks BayStack 5510-48Т | 48 |
| Бухгалтерия | К3 | ZYXEL GS2210-24 | 32 |
| Хозяйственный отдел | К4,К11 | Nortel Networks BayStack 5510-48Т | 48 |
| ИТ-отдел | К5 | 3Com SuperStack 3 Switch 4400 (3) | 72 |
| Охрана | К6,К12 | Ubiquiti TS-16-CARRIER | 16 |
| Производство | К7,8,9 | Nortel Networks BayStack 5510-48Т | 48 |
| Роутер-коммутатор 1 | К13 | Ubiquiti TS-16-CARRIER | 16 |
| Роутер-коммутатор 2 | К14 | Ubiquiti TS-16-CARRIER | 16 |
| Роутер-коммутатор 3 | К15 | Ubiquiti TS-16-CARRIER | 16 |  |  | 15 |

Сетевая видеокамера: ActiveCam AC-D8111IR2;

Роутер: TP-LINK AC1200 Archer VR400;

Принтер: Samsung SL-C430W;

Веб-камера: A4Tech PK-910H;

Датчик дыма: Xiaomi Mijia Honeywell;

Телефон: IP телефон GRANDSTREAM GXP-1610;

Спутниковый ресивер: GI HD Micro Plus;

8.4. Пассивное оборудование

Пассивное оборудование – оборудование, не получающее питание от электрической сети и выполняющее функции распределения или снижения уровня сигналов. Например, кабели, розетки и т. д.

В нашей сети в качестве пассивного оборудования нужно выбрать провода передачи данных в зданиях, сетевые карты для персональных рабочих станций и серверов, конвертер сигналов для спутникового интернета, спутниковую антенну.

В качестве проводов уже были выбраны: кабель витая пара UTP, 4 пары, кат. 5е для передачи данных в здании.

Сетевые карты выберем следующие:

Для ПК: Сетевая карта D-Link DFE-551FX с пропускной способностью 10/100/200 Мбит/с, что подходит к выбранной скорости передачи данных в ЛКС.

Для серверов: Сетевая карта SNR-E1G42ET с пропускной способностью до 1 Гбит/с, что также нам подходит.

Спутниковое оборудование:

1) Спутниковая антенна WISI Orbit OA13A;

2) Конвертер LUMAX LU-40SCIR

3) Коаксиальный кабель CAVEL DG 113PEM

9. ВЫБОР СЕТЕВОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ

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.

10. ВЫБОР СЕТЕВОГО ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

10.1. 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.

10.2. 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.

10.3. 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.

10.4. 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.

10.5. 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.

10.6. 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.

10.7. 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.

11. РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ СЕТИ

Проведем моделирование разрабатываемой сети в программе Cisco Packet Tracer. Для моделирования будем использовать упрощенную структурную схему (рис. 11.1)

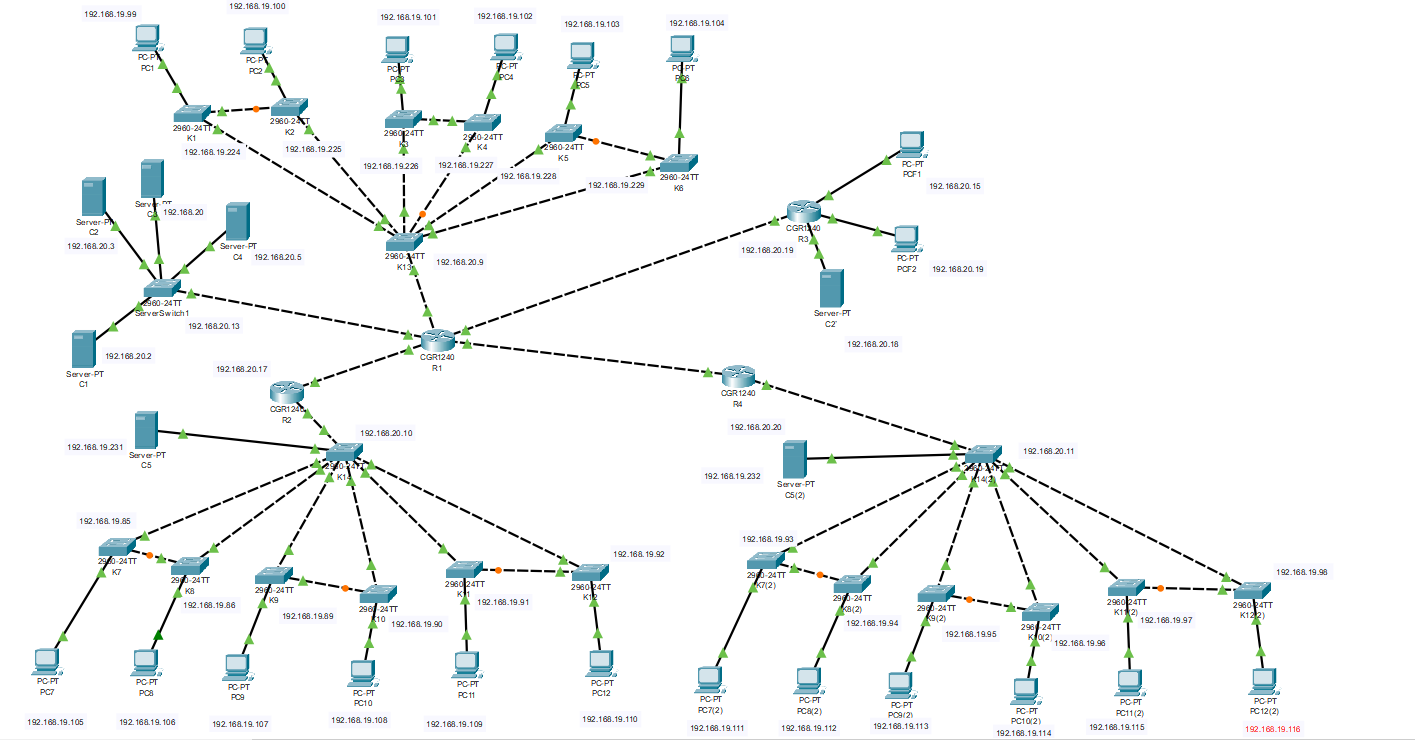


Рис. 11.1 – схема сети для моделирования

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.

12. 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 трёх четырёхэтажных зданиях, размерами 24х200 метров. Высота каждого этажа (а также подвала и чердака) равняется трём метрам.

С учетом всех требований, составим схемы:

1) Первого этажа первого здания

2) Последнего этажа первого здания

3) Первого этажа второго здания

4) Последнего этажа второго здания

5) Первого этажа третьего здания

6) Последнего этажа третьего здания

7) Установки спутникового оборудования

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 12.1 – расчет длины проводов в зданиях

|  |  |  |
| --- | --- | --- |
| Здание | Этаж | Длина,м |
| Витая пара | | |
| 1 | 1,4 | 2026 |
| 2 | 1,4 | 2049 |
| 3 | 1,4 | 2030 |
| Коаксиальный кабель | | |
| 1,2,3 | Чердак, крыша | 38 |

# 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. Статья «Коммутаторы Fast/Gigabit Ethernet для большой сети». – Режим доступа:  
   <http://citforum.ru/nets/lvs/fast_gigabit/>
2. Пособие «Как подключить спутниковый интернет» – Режим доступа:  
   <http://www.starblazer.ru/article/kak_podklyuchit_sputnikovyj_internet/>
3. Интернет-магазин спутникового оборудования. – Режим доступа:  
   <http://www.1dvb.ru/product/gi-hd-micro-plus-sputnikovyj-resiver/>
4. Спектр ТВ, телевизионные антенны. – Режим доступа  
   <http://www.spektr-tv.ru/anten_stv/wisi.php>
5. Автоматизация документооборота на предприятии. – Режим доступа  
   https://www.cleverence.ru/articles/bukhgalteriya/avtomatizatsiya-dokumentooborota-na-predpriyatii-avtomatizirovannye-sistemy-upravleniya-dokumentami-/?ysclid=lb943w7zcp489346176

ПРИЛОЖЕНИЕ 1

**Структурная схема корпоративной сети**

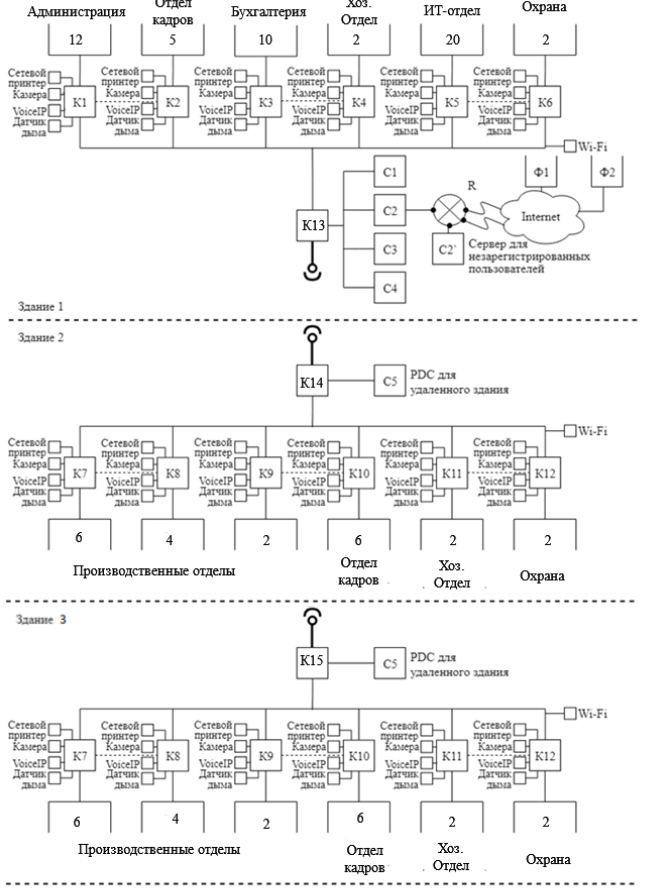
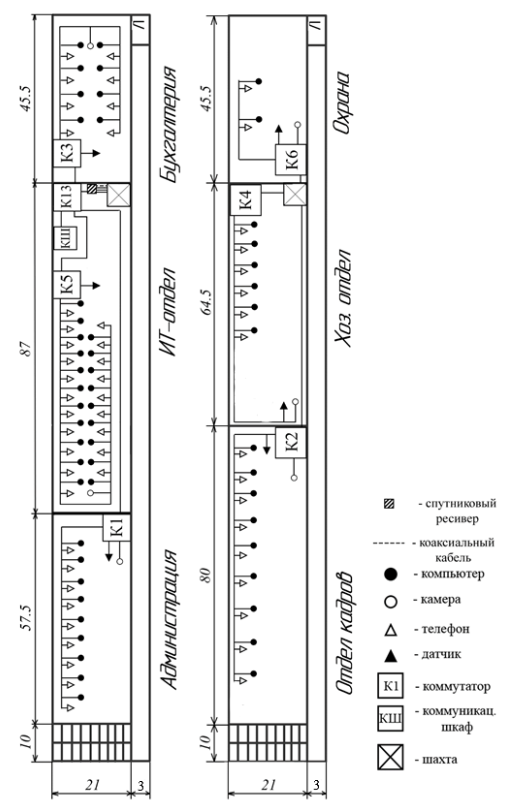


Рис. А1 – структурная схема корпоративной сети

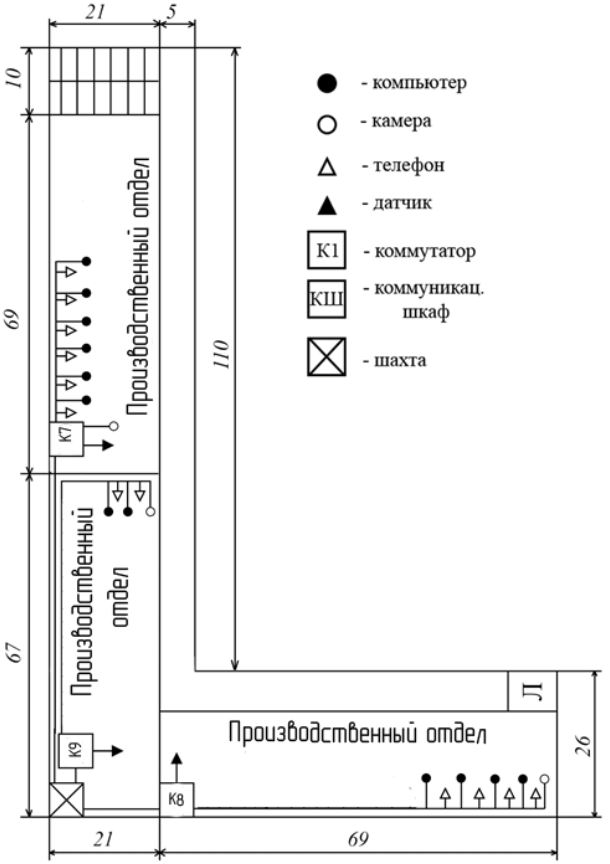
ПРИЛОЖЕНИЕ 2

**Монтажные схемы зданий производственного предприятия**

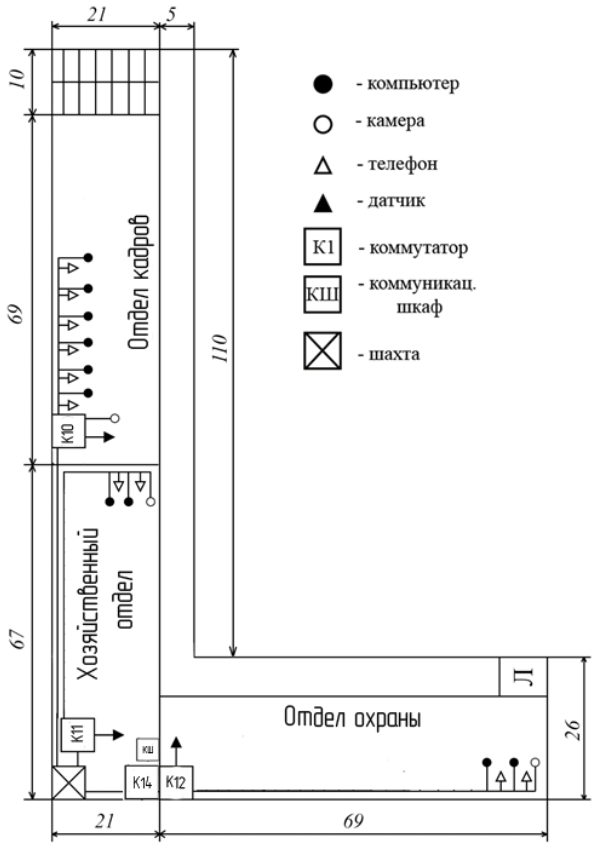
Первое здание (1,4 этажи):



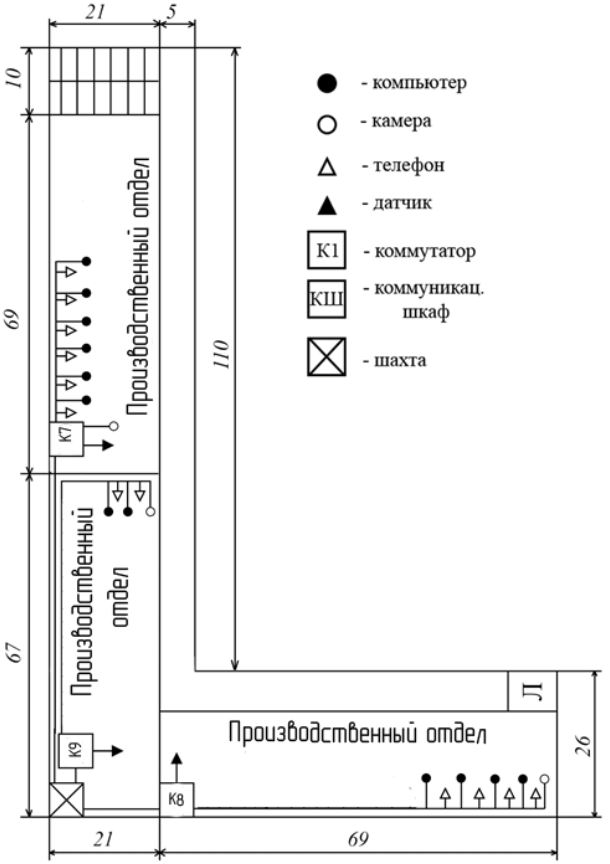
Второе здание (1 этаж):



Второе здание (4 этаж):



Третье здание (1 этаж):



Третье здание (4 этаж):

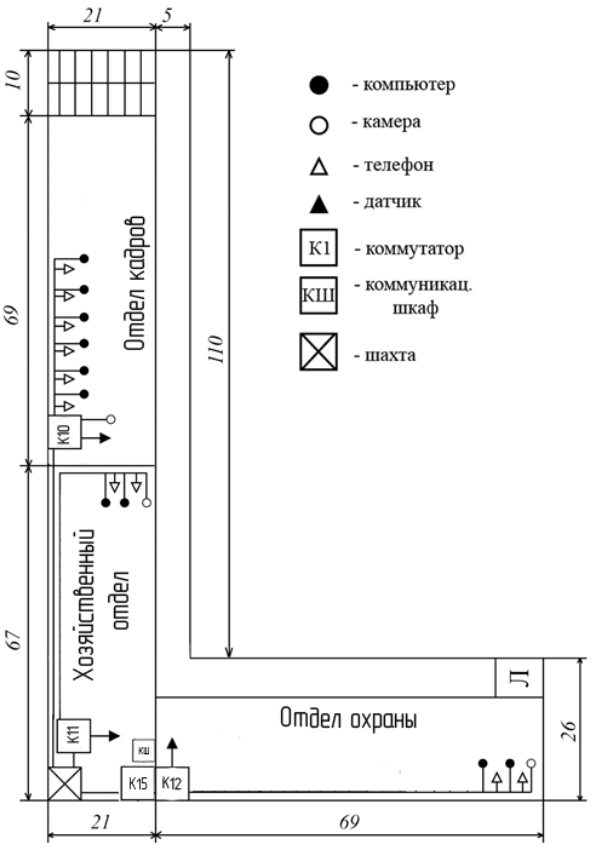


Схема установки спутникового оборудования:

