ВВЕДЕНИЕ

Техническое задание

Спроектировать корпоративную сеть для Информационная система для лечебного учреждения (больницы). Предусматривается наличие филиала в данном городе, для которого обеспечивается удаленный доступ к сети, и удаленного филиала в другом городе.

* Четыре двухэтажных здания - 20х10
* Расстояние между зданиями 400м.

1. СХЕМА ИНФОРМАЦИОННЫХ ПОТОКОВ НА ПРЕДПРИЯТИИ И РАСЧЕТ ОБЪЕМА ПОТОКОВ МЕЖДУ ОТДЕЛАМИ
   1. Организационный анализ структуры предприятия.

Имеется несколько отделов для лечебного учреждения (больницы), расположенных в нескольких зданиях и на нескольких этажах. Необходимо соединить их в общую локальную сеть, учитывая, что каждый сотрудник центра имеет рабочее место с ПК.

Лечебного учреждение (больница) состоит из следующих отделов:

1. Администрация
2. Бухгалтерия
3. Отдел охраны
4. IT отдел
5. Отдел кадров
6. Регистратура
7. Врачебный отдел
8. Отдел хирургии
9. Отдел лаборатории
10. Научно-исследовательский отдел

В нее так же входят два филиала:

1. Филиал в городе
2. Филиал в другом городе.

Виды информации, передаваемой по сети:

* Текстовая (приказы, документация, отчеты)
* Графическая (схемы, диаграммы, чертежи, фото, рисунки)
* Видеонаблюдение
* Информация баз данных
* IP-телефония
* Датчики.
  1. Расчет объема потоков между отделами

В таблице 1.1. показан средний объём информации за один рабочий день (8 часов) в Мбайт, отправляемый и принимаемый подразделениями больницы, а также между отделами центра и филиалами.

Таблица 1.1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Ф1 | Ф2 | ΣИСХ. ИНФ |
| 1 | 15 | 25 | 15 | 10 | 15 | 5 | 15 | 15 | 10 | 25 | 20 | 20 | 190 |
| 2 | 25 | 35 | 10 | 5 | 15 | - | - | - | - | - | - | - | 90 |
| 3 | 15 | 10 | 15 | 5 | 5 | 5 | 5 | 15 | 20 | 20 | 15 | 15 | 145 |
| 4 | 15 | 5 | 5 | 20 | 5 | 10 | 5 | 5 | 15 | 15 | 10 | 10 | 120 |
| 5 | 20 | 5 | 5 | 5 | 20 | - | 5 | 5 | 5 | - | 10 | 10 | 90 |
| 6 | - | - | 10 | 5 | 5 | 10 | 15 | 15 | 10 | - | - | - | 70 |
| 7 | 5 | - | 10 | 5 | - | - | 15 | 20 | 20 | 15 | 10 | 10 | 110 |
| 8 | 5 | - | 10 | 5 | - | - | 20 | 15 | 20 | 15 | 10 | 10 | 110 |
| 9 | 10 | - | 15 | 5 | - | 15 | 20 | 20 | 40 | 40 | 30 | 25 | 220 |
| 10 | 10 | - | 20 | 5 | - | - | 15 | 15 | 40 | 40 | 35 | 30 | 210 |
| Филиал1 | 15 | - | 10 | 10 | 5 | - | 10 | 15 | 25 | 30 | - | 40 | 160 |
| Филиал2 | 15 | - | 10 | 10 | 5 | - | 15 | 10 | 20 | 30 | 40 | - | 155 |
| ΣВХОД. ИНФ. | 150 | 80 | 135 | 90 | 75 | 45 | 140 | 150 | 225 | 230 | 180 | 170 |  |
| Вход+исход | 340 | 170 | 280 | 210 | 165 | 115 | 250 | 260 | 445 | 440 | 340 | 325 |  |

Суммарная информационная нагрузка всех организационных связей центра в среднем составляет ИНΣmax=2458971 бит/сек.

Необходимо учитывать, что нагрузка в сети возрастает в определенные часы в течение дня, т. к. в утреннее время, в начале рабочего дня, происходит активный обмен информацией, ее загрузка и др., в середине рабочего дня, в обеденное время, сохранение данных и их загрузка, и в вечернее время, под конец рабочего дня, происходит активное сохранение информации.

Общая пропускная способность Ср сети определяется по формуле:

 (1.1)

где 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.

Тогда для нашей информационной системы имеем общую пропускную способность сети:

Коэффициент нагрузки неструктурированной локальной вычислительной сети определяется по формуле:

 (1.2)

где Смакс – максимальная пропускная способность базовой технологии сети (для Fast Ethernet Смакс = 100 Мбит/сек).

Коэффициент нагрузки исходной сети составляет:

Проверка выполнения условия допустимой нагрузки ЛВС (домена коллизий):

 (1.3)

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

Имеем:

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

1. Схема информационных потоков с учетом серверов.
   1. Логические сервера

Файл-сервер – необходим для обработки потоков информации между отделами, для организации внутреннего документооборота.

Proxy-сервер – необходим для организации доступа в Internet. Все запросы к настоящему серверу в действительности поступают сначала на Proxy-сервер, который таким образом получает возможность отвергнуть нежелательные запросы, предотвращая непосредственный доступ на сервер и к его данным. Обычно Proxy-сервер размещается с внутренней стороны межсетевого экрана, между браузером и реальным сервером, перехватывая Internet-запросы, передаваемые от клиентов, в силу чего последние не могут напрямую взаимодействовать с Internet.

Web-сервер – необходим для хранения Web-страниц.

Print-сервер – для печати любых документов необходим доступ сотрудников к принтеру. В каждом подразделении будет хотя бы один сетевой принтер подключенный через Print-сервер.

Сервер приложений – для удобства работы «медленных» клиентов (филиала например) с БД.

VoIP сервер – предназначен для выполнения основных управляющих функций в системе, таких как управление установлением телефонных и видео соединений, и обеспечение дополнительных функций для абонентов корпоративной сети IP-телефонии.

E-mail сервер – сервер электронной почты.

Антивирусный сервер – это необходимая часть любой сети. Антивирусный сервер выполняет проверку передаваемой по сети информации от вредоносных программ

DHCP – сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер».

PDC и BDC – главный и резервный контроллеры домена – хранит данные о пользователях и компьютерах в домене и позволяет централизованно управлять ими.

DNS (внутренний и внешний) – предназначен для автоматического поиска IP-адреса по известному символьному имени узла. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.

* 1. Физические сервера.

Сервер БД 1 – информация о сотрудниках и пациентах больницы, содержащий информацию о расписании и записи на прием.

Сервер БД 2 – БД бухгалтерского учета.

Сервер БД 3 – БД лабораторных результатов и исследований.

Сервер БД 4 – БД НИ отдела, содержит информацию о текущих разработках.

Сервер БД 5 – внутренний сервер БД, содержащий архивную информацию больницы.

* 1. Разбиение выбранных логических серверов по физическим серверам. Схема информационных потоков между отделами и серверами.

Сгруппируем выделенные логические сервера и распределим группы по физическим серверам, а также выделим связи информационных потоков между физическими серверами.

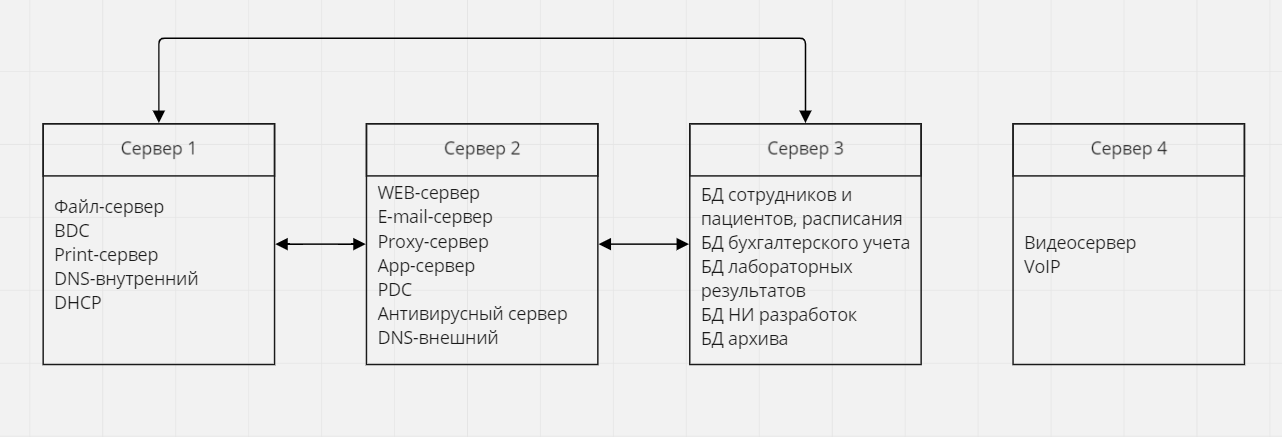


Рисунок 2.1 – Связь между серверами

Схема информационных потоков между отделами и серверами представлена в таблице 2.1.

Таблица 2.1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Сервер 1 | Сервер 2 | Сервер 3 | Сервер 4 |
| Администрация | + | + | + | + |
| Бухгалтерия | + | + | + | + |
| Отдел охраны | + |  |  | + |
| IT отдел | + | + | + | + |
| Отдел кадров | + | + | + | + |
| Регистратура | + |  | + | + |
| Врачебный отдел | + |  | + | + |
| Отдел хирургии | + |  |  | + |
| Отдел лаборатории | + |  | + | + |
| НИ отдел | + |  | + | + |
| Филиал 1 |  | + | + |  |
| Филиал 2 |  | + | + |  |

* 1. Распределение трафика к серверам

В таблице 2.2 показано процентное распределение информационных потоков к серверам от филиалов, отделов и серверов.

Таблица 2.2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Отделы | Серверы | | | |
| 1 | 2 | 3 | 4 |
| Администрация | 30 | 30 | 20 | 20 |
| Бухгалтерия | 50 | 25 | 10 | 15 |
| Отдел охраны | 10 | - | - | 90 |
| IT отдел | 20 | 20 | 5 | 55 |
| Отдел кадров | 50 | 10 | 30 | 10 |
| Регистратура | 40 | - | 20 | 40 |
| Врачебный отдел | 50 | - | 20 | 30 |
| Отдел хирургии | 60 | - | - | 40 |
| Отдел лаборатории | 60 | - | 10 | 30 |
| НИ отдел | 55 | - | 20 | 25 |
| Архив | - | 80 | 20 | - |
| Филиал 1 | - | 70 | 30 | - |
| Филиал 2 | - | 65 | 35 | - |
| Сервер 1 | 70 | - | 30 | - |
| Сервер 2 | 60 | 40 | - | - |
| Сервер 3 | 30 | 30 | 20 | 20 |

1. Проектирование структурной схемы корпоративной сети.

Расположение отделов и количество компьютеров в корпоративной сети зданий:

Здание – 1, Этаж – 1:

1. Охрана – 2 компьютера.
2. Архив – 4 компьютера.
3. IT-отдел – 4 компьютера, 4 сервера.
4. НИ отдел – 5 компьютеров.

На этаже имеются две камеры видеонаблюдения.

Здание – 1, Этаж – 2:

1. Администрация – 3 компьютера.
2. Бухгалтерия – 9 компьютеров.
3. Отдел кадров – 5 компьютеров.

На этаже имеется две камеры видеонаблюдения.

Здание – 2, Этаж – 1:

1. Охрана – 2 компьютера.
2. Регистратура – 3 компьютера.
3. Врачебный отдел – 4 компьютера.

На этаже имеется одна камера – на вход в больничный корпус.

Здание – 2, Этаж – 2:

1. Отдел лаборатории – 6 компьютеров.
2. Отдел хирургии – 2 компьютера.

На этаже имеется две камеры видеонаблюдения.

Связь между зданиями больницы осуществляется через маршрутизаторы R1 в здании 1 и R2 в здании 2, соединенных через оптоволоконный кабель.

Структурная схема корпоративной сети больницы приведена в приложении А.

1. Разработка защиты сети от несанкционированного доступа.

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

* Политику пользователей для защиты на внутреннем уровне.
* Использование межсетевого экрана для защиты локальной сети от внешних несанкционированных воздействий.
  1. Методы защиты внутри сети.

Access Control List.

Access Control List или ACL – список управления доступом, который определяет, кто или что может получать доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту (пользователю, группе пользователей).

В системе с моделью безопасности, основанной на ACL, когда субъект запрашивает выполнение операции над объектом, система сначала проверяет список разрешённых для этого субъекта операций, и только после этого даёт (или не даёт) доступ к запрошенному действию.

Использующие ACL системы могут быть разделены на две категории: дискреционные (англ. discretionary) и мандатные (англ. mandatory). Систему можно назвать построенной на дискреционном контроле доступа, если создатель или владелец объекта может полностью управлять доступом к объекту, включая и список тех, кому разрешено изменять права доступа к объекту. Систему можно назвать обладающей мандатным контролем доступа, если заданные пользователем ACL перекрываются системными ограничениями.

При централизованном хранении списков контроля доступа можно говорить о матрице доступа, в которой по осям размещены объекты и субъекты, а в ячейках – соответствующие права. Однако в большом количестве систем списки контроля доступа к объектам хранятся отдельно для каждого объекта, зачастую - непосредственно с самим объектом.

Традиционные ACL системы назначают права индивидуальным пользователям, и со временем и ростом числа пользователей в системе списки доступа могут стать громоздкими. Вариантом решения этой проблемы является назначение прав группам пользователей, а не персонально. Другим вариантом решения этой проблемы является «Управление доступом на основе ролей», где функциональные подмножества прав к ряду объектов объединяются в «роли», и эти роли назначаются пользователям. Однако, в первом варианте группы пользователей также часто называются ролями.

В сетях ACL представляют список правил, определяющих порты служб или имена доменов, доступных на узле или другом устройстве третьего уровня OSI, каждый со списком узлов и/или сетей, которым разрешен доступ к сервису. Сетевые ACL могут быть настроены как на обычном сервере, так и на маршрутизаторе и могут управлять как входящим, так и исходящим трафиком, в качестве межсетевого экрана.

* 1. Виртуальные локальные сети.

Современные сети предприятий представляют собой распределенные системы, состоящие из большого количества устройств разного назначения. Ситуация вынуждает разделять такие большие сети на автономные подсети, в итоге логические структуры сети отличаются от физических топологий. Подобные системы создаются с помощью технологии **VLAN (Virtual Local Area Network** – виртуальная локальная сеть), которая позволяет разделить одну локальную сеть на отдельные сегменты.

Технология VLAN обеспечивает:

* Гибкое построение сети – VLAN позволяет произвести сегментацию локальной сети на подсети по функциональному признаку независимо от территориального расположения устройств. То есть устройства одной подсети VLAN могут быть подключены к разным коммутаторам, удаленным друг от друга. И наоборот, к одному коммутатору могут быть подключены устройства, относящиеся к разным подсетям VLAN
* Увеличение производительности – VLAN разделяет подсеть на отдельные широковещательные домены. Это означает, что широковещательные сообщения будут получать только устройства, находящиеся в одной VLAN-подсети. Построение системы с использованием технологии VLAN позволяет уменьшить широковещательный трафик внутри сети, тем самым снижается нагрузка на сетевые устройства и улучшается производительность системы в целом.
* Улучшение безопасности – устройства из разных подсетей VLAN не могут общаться друг с другом, что уменьшает шансы произвести несанкционированный доступ к устройствам системы. Связь между разными подсетями возможна только через маршрутизатор. Кроме того, использование маршрутизатора позволяет настроить политики безопасности, которые могут быть применены сразу ко всей группе устройств, принадлежащей одной подсети.

У каждой VLAN-подсети есть свой идентификатор, по которому определяется принадлежность той или иной подсети. Информация об идентификаторе содержится в теге, который добавляется в тело Ethernet-фрейма сети, в которой внедрено разделение на подсети VLAN.

Самый распространенный стандарт, описывающий процедуру тегирования трафика, – это открытый стандарт 802.1 Q. Кроме него есть проприетарные протоколы, но они менее популярны.

Формат Ethernet – фрейма после тегирования:

Тег размером 4 байта состоит из нескольких полей:

* TPID (Tag Protocol Identifier) – Идентификатор протокола тегирования. Для стандарта 802.1Q значение TPID - 0x8100
* Р-тег – Определяет приоритет пакета. Используется при работе стандарта 802.1p для определения очередности обработки пакетов
* CFI (Canonical Format Indicator) – Идентификатор формата МАС-адреса, который использовался для совместимости между сетями Ethernet и Token Ring. В настоящее время поле CFI не используется в связи с отказом от сетей Token Ring
* VLAN ID – Идентификатор VLAN. Определяет, какой подсети VLAN принадлежит пакет

Именно по тегу сетевое оборудование определяет принадлежность пакета той или иной сети VLAN, осуществляет фильтрацию пакетов и определяет дальнейшие действия с ними: снять тег и передать на конечное оборудование, отбросить пакет, переслать следующему получателю с сохранением тега. Правила, определяющие действия с пакетом на основе тега, зависят от режима работы порта сетевого оборудования. В свою очередь, режим работы выбирается в соответствии с характеристиками подключаемого оборудования. В системе может присутствовать как оборудование с поддержкой технологии VLAN, так и без нее.

* 1. Политика пользователей для защиты на внутреннем уровне.

Распределим права доступа отделений к серверам больницы. Для каждого отделения будут созданы группы учетных записей (субдомены) с определенными ограничениями прав доступа, которые выдаются главным контроллером домена. Также отметим права некоторых серверов на доступ к другим серверам.

Для предотвращения НСД к сети извне необходимо поместить коммутационное оборудование внутри кабинетов здания или, при необходимости, в коридорах здания в специальных шкафах, закрывающихся на ключ. Все сетевые провода следует монтировать в специальных коробах на высоте не ниже 2 метров от пола.

Защиту от порчи данных сотрудниками внутри корпоративной сети будем осуществлять с помощью внутреннего DNS-сервера, а также политики учётных записей и прав пользователей. Внутренний DNS-сервер служит для скрытия от пользователей внутри сети информации об IP-адресах соседних машин и структуре корпоративной сети. Сеть будет принадлежать к одному домену, в который включены поддомены всех отделов фирмы. При этом каждый компьютер имеет своё сетевое имя.

Разграничение доступа отделов к информационным ресурсам данной сети приведено в таблицах 4.1 и 4.2

Таблица 4.1

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Отдел | С1 | | | | С2 | | | | | | |
| Файл-сервер | BDC | DNS внутр. | DHCP | Proxy | AppServ | PDC | WEB | E-mail | Antivirus serv | DNS внешний |
| Администрация | RW | + | R | + | + | + | + | + | + | + | + |
| Бухгалтерия | RW | + | R | + | + | + | + | + | + | + | + |
| Отдел охраны | - | + | R | + | - | - | + | - | - | - | + |
| IT отдел | RWE | RWE | RWE | RWE | RWE | RWE | RWE | RWE | RWE | RWE | RWE |
| Отдел кадров | RW | + | R | + | + | + | + | + | + | + | + |
| Регистратура | RW | + | R | + | - | + | + | + | + | + | + |
| Врачебный отдел | R | + | R | + | - | - | + | - | + | + | + |
| Отдел хирургии | R | + | R | + | - | - | + | - | + | + | + |
| Отдел лаборатории | R | + | R | + | - | - | + | - | + | + | + |
| НИ отдел | R | + | R | + | - | - | + | + | + | + | + |
| Web-server | - | - | - | - | - | - | - | - | - | - | + |
| DNS внутренний | - | + | - | + | - | - | + | - | - | - | + |
| AppServer | - | - | - | - | - | - | - | - | - | - | - |
| BDC | - | - | + | - | - | - | + | - | - | - | - |

Зададим короткое обозначение каждой из баз данных на сервере 3. Где БД 1 – Сотрудников, пациентов, расписания. БД 2 – бухгалтерского учета. БД 3 – Лабораторных результатов. БД 4 – Научно-исследовательских разработок. БД 5 – Архив.

Таблица 4.2

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Отдел | C3 | | | | | C4 | |
| БД 1 | БД 2 | БД 3 | БД 4 | БД 5 | Видеосервер | VoIP |
| Администрация | R | R | - | R | RW | R | + |
| Бухгалтерия | R | RW | - | - | R | - | + |
| Отдел охраны | - | - | - | - | - | RW | + |
| IT отдел | RWE | RWE | RWE | RWE | RWE | RWE | RWE |
| Отдел кадров | RW | R | - | - | R | - | + |
| Регистратура | RW | - | - | - | R | - | + |
| Врачебный отдел | R | - | R | - | R | - | + |
| Отдел хирургии | R | - | R | - | R | - | + |
| Отдел лаборатории | - | - | RW | - | R | - | + |
| НИ отдел | - | - | R | RW | RW | R | + |
| Web-server | R | - | - | R | R | - | - |
| DNS внутренний | - | - | - | - | - | - | - |
| AppServer | R | R | R | R | R | - | - |
| BDC | - | - | - | - | - | - | - |

* 1. Организация VLAN.

Для корпоративной сети больницы выделим VLAN-зоны и перечислим отделы и оборудование, которые к ним относятся:

VLAN 10: SW1 (Администрация), SW2 (Бухгалтерия), SW3 (Отдел кадров), SW4 (IT-отдел), SW13, R1.

VLAN 20: C1,C2,C3,C4, R3.

VLAN 30: SW5(Охрана), SW6(Архив), SW7(НИ отдел).

VLAN 40: SW8(Отдел лаборатории), SW9(Отдел хирургии).

VLAN 50: SW14, SW10(Охрана), SW11(Регистратура), SW12(Врачебный отжел), R2.

VLAN 60 (видеонаблюдение): SW13, SW1(Администрация), SW5(Охрана), C4(Видеосервер), R1, R2, SW14, SW10(Охрана), все IP-камеры больничного комплекса.

VLAN 70 (VoIP): все коммутаторы больничного комплекса, R1, R2, IP-телефон в каждом отделе.

VLAN 80(Датчики): SW13, R1, R2, SW14, все датчики.

VLAN 90(Wi-Fi): SW13, R1, R2, SW14, два Wi-Fi роутера (по одному в каждом здании).

* 1. Защита сети от внешнего НСД.
     1. Шифрование информации.

Шифрование – обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма.

Пользователи являются авторизованными, если они обладают определённым аутентичным ключом. Вся сложность и, собственно, задача шифрования состоит в том, как именно реализован этот процесс.

С помощью шифрования обеспечиваются три состояния безопасности информации:

* Конфиденциальность – шифрование используется для скрытия информации от неавторизованных пользователей при передаче или при хранении.
* Целостность – шифрование используется для предотвращения изменения информации при передаче или хранении.
* Идентифицируемость – шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

Для того, чтобы прочитать зашифрованную информацию, принимающей стороне необходимы ключ и дешифратор (устройство, реализующее алгоритм расшифровывания). Идея шифрования состоит в том, что злоумышленник, перехватив зашифрованные данные и не имея к ним ключа, не может ни прочитать, ни изменить передаваемую информацию. Кроме того, в современных криптосистемах (с открытым ключом) для шифрования, расшифрования данных могут использоваться разные ключи. Однако, с развитием криптоанализа, появились методики, позволяющие дешифровать закрытый текст без ключа. Они основаны на математическом анализе переданных данных.

Основными методами шифрования информации являются симметричный и асимметричный.

В **симметричной** методологии и для шифрования, и для расшифровки отправителем и получателем применяется один и тот же ключ, об использовании которого они договорились до начала взаимодействия. Если ключ не был скомпрометирован, то при расшифровке автоматически выполняется аутентификация отправителя, так как только отправитель имеет ключ, с помощью которого можно зашифровать информацию, и только получатель имеет ключ, с помощью которого можно расшифровать информацию. Так как отправитель и получатель - единственные люди, которые знают этот симметричный ключ, при компрометации ключа будет скомпрометировано только взаимодействие этих двух пользователей. Проблемой, которая будет актуальна и для других криптосистем, является вопрос о том, как безопасно распространять симметричные (секретные) ключи.



Рисунок 4.2 – Симметричное шифрование.

Алгоритмы симметричного шифрования используют ключи не очень большой длины и могут быстро шифровать большие объемы данных.

Порядок использования систем с симметричными ключами:

1. Безопасно создается, распространяется и сохраняется симметричный секретный ключ.
2. Отправитель создает электронную подпись с помощью расчета хэш-функции для текста и присоединения полученной строки к тексту
3. Отправитель использует быстрый симметричный алгоритм шифрования-расшифровки вместе с секретным симметричным ключом к полученному пакету (тексту вместе с присоединенной электронной подписью) для получения зашифрованного текста. Неявно таким образом производится аутентификация, так как только отправитель знает симметричный секретный ключ и может зашифровать этот пакет. Только получатель знает симметричный секретный ключ и может расшифровать этот пакет.
4. Отправитель передает зашифрованный текст. Симметричный секретный ключ никогда не передается по незащищенным каналам связи.
5. Получатель использует тот же самый симметричный алгоритм шифрования-расшифровки вместе с тем же самым симметричным ключом (который уже есть у получателя) к зашифрованному тексту для восстановления исходного текста и электронной подписи. Его успешное восстановление аутентифицирует кого-то, кто знает секретный ключ.
6. Получатель отделяет электронную подпись от текста.
7. Получатель создает другую электронную подпись с помощью расчета хэш-функции для полученного текста.
8. Получатель сравнивает две этих электронных подписи для проверки целостности сообщения (отсутствия его искажения)

**Асимметричное шифрование** – это метод шифрования данных, предполагающий использование двух ключей – открытого и закрытого. Открытый (публичный) ключ применяется для шифрования информации и может передаваться по незащищенным каналам. Закрытый (приватный) ключ применяется для расшифровки данных, зашифрованных открытым ключом. Открытый и закрытый ключи — это очень большие числа, связанные друг с другом определенной функцией, но так, что, зная одно, крайне сложно вычислить второе.

Асимметричное шифрование используется для защиты информации при ее передаче, также на его принципах построена работа электронных подписей.

Схема передачи данных между двумя субъектами (А и Б) с использованием открытого ключа выглядит следующим образом:

1. Субъект А генерирует пару ключей, открытый и закрытый (публичный и приватный).
2. Субъект А передает открытый ключ субъекту Б. Передача может осуществляться по незащищенным каналам.
3. Субъект Б шифрует пакет данных при помощи полученного открытого ключа и передает его А. Передача может осуществляться по незащищенным каналам.
4. Субъект А расшифровывает полученную от Б информацию при помощи секретного, закрытого ключа.

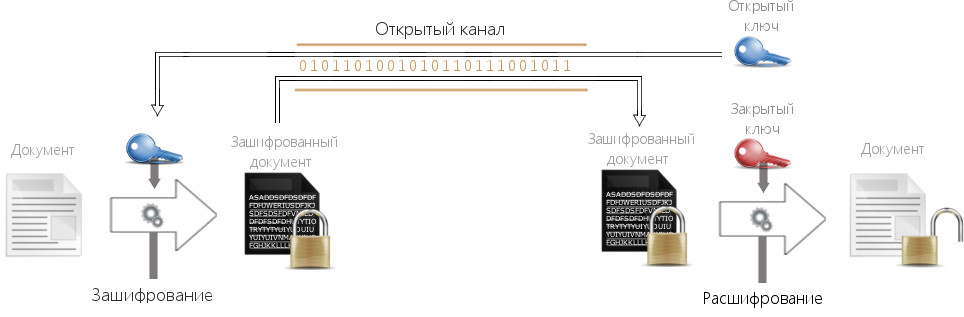


Рисунок 4.3 – Ассиметричное шифрование.

В такой схеме перехват любых данных, передаваемых по незащищенным каналам, не имеет смысла, поскольку восстановить исходную информацию возможно только при помощи закрытого ключа, известного лишь получателю и не требующего передачи.

Асимметричное шифрование решает главную проблему симметричного метода, при котором для кодирования и восстановления данных используется один и тот же ключ. Если передавать этот ключ по незащищенным каналам, его могут перехватить и получить доступ к зашифрованным данным. С другой стороны, асимметричные алгоритмы гораздо медленнее симметричных, поэтому во многих криптосистемах применяются и те и другие. Например, стандарты SSL и TLS используют асимметричный алгоритм на стадии установки соединения (рукопожатия): с его помощью кодируют и передают ключ от симметричного шифра, которым и пользуются в ходе дальнейшей передачи данных.

Также асимметричные алгоритмы применяются для создания электронных подписей для подтверждения авторства и (или) целостности данных. При этом подпись генерируется с помощью закрытого ключа, а проверяется с помощью открытого.

Наиболее распространенные алгоритмы асимметричного шифрования:

* RSA (аббревиатура от Rivest, Shamir и Adelman, фамилий создателей алгоритма) – алгоритм, в основе которого лежит вычислительная сложность факторизации (разложения на множители) больших чисел. Применяется в защищенных протоколах SSL и TLS, стандартах шифрования, например в PGP и S/MIME, и так далее. Используется и для шифрования данных, и для создания цифровых подписей.
* DSA (Digital Signature Algorithm, «алгоритм цифровой подписи») – алгоритм, основанный на сложности вычисления дискретных логарифмов. Используется для генерации цифровых подписей. Является частью стандарта DSS (Digital Signature Standard, «стандарт цифровой подписи»).
* Схема Эль-Гамаля – алгоритм, основанный на сложности вычисления дискретных логарифмов. Лежит в основе DSA и устаревшего российского стандарта ГОСТ 34.10–94. Применяется как для шифрования, так и для создания цифровых подписей.
* ECDSA (Elliptic Curve Digital Signature Algorithm) – алгоритм, основанный на сложности вычисления дискретного логарифма в группе точек эллиптической кривой. Применяется для генерации цифровых подписей, в частности для подтверждения транзакций в криптовалюте Ripple.
  + 1. Межсетевой экран.

Эффективным решением для защиты от внешнего несанкционированного доступа к информационным ресурсам внутри сети являются **межсетевые экраны (МСЭ)**, или **файерволы**. Это программное обеспечение или аппаратно-программные продукты, предназначенные для блокировки нежелательного трафика.

Разрешение или запрет доступа межсетевым экраном осуществляется на основе заданных администратором параметров. В том числе могут использоваться следующие параметры и их комбинации:

* IP-адреса. При помощи Firewall можно предоставить или запретить получение пакетов с определенного адреса или задать перечень запрещенных и разрешенных IP-адресов.
* Доменные имена. Возможность установки запрета на пропуск трафика с определенных веб-сайтов.
* Порты. Задание перечня запрещенных и разрешенных портов позволяет регулировать доступ к определенным сервисам и приложениям. Например, заблокировав порт 80, можно запретить доступ пользователей к веб-сайтам.
* Протоколы. МСЭ может быть настроен таким образом, чтобы блокировать доступ трафика определенных протоколов.

Для защиты локальных сетей от нежелательного трафика и несанкционированного доступа применяются различные виды межсетевых экранов. В зависимости от способа реализации, они могут быть программными или программно-аппаратными.

Программный Firewall – это специальный софт, который устанавливается на компьютер и обеспечивает защиту сети от внешних угроз. Это удобное и недорогое решение для частных ПК, а также для небольших локальных сетей – домашних или малого офиса. Они могут применяться на корпоративных компьютерах, используемых за пределами офиса.

Для защиты более крупных сетей используются программные комплексы, под которые приходится выделять специальный компьютер. При этом требования по техническим характеристикам к таким ПК являются довольно высокими. Использование мощных компьютеров только под решение задач МСЭ нельзя назвать рациональным. Да и производительность файервола часто оставляет желать лучшего.

Поэтому в крупных компаниях и организациях обычно применяют аппаратно-программные комплексы (security appliance). Это специальные устройства, которые, как правило, работают на основе операционных систем FreeBSD или Linux.

Функционал таких устройств строго ограничивается задачами межсетевого экрана, что делает их применение экономически оправданным. Также security appliance могут быть реализованы в виде специального модуля в штатном сетевом оборудовании — коммутаторе, маршрутизаторе и т. д.

Применение программно-аппаратных комплексов характеризуется следующими преимуществами:

* Повышенная производительность за счет того, что операционная система работает целенаправленно на выполнение одной функции.
* Простота в управлении. Контролировать работу security appliance можно через любой протокол, в том числе стандартный (SNMP, Telnet) или защищенный (SSH, SSL).
* Повышенная надежность защиты за счет высокой отказоустойчивости программно-аппаратных комплексов.
  + 1. Организация ДМЗ.

Название происходит от военного термина «демилитаризованная зона» – территория между враждующими государствами, на которой не допускаются военные операции. Иными словами, доступ в ДМЗ открыт для обеих сторон при условии, что посетитель не имеет злого умысла. По аналогии, концепция ДМЗ (например, при построении шлюза в публичный Интернет) состоит в том, что в локальной сети выделяется область, которая не безопасна как оставшаяся часть сети (внутренняя) и не опасна как публичная (внешняя).

Системы, открытые для прямого доступа из внешних сетей, как правило, являются главными целями злоумышленников и потенциально подвержены проявлению угроз. Как следствие, эти системы не могут пользоваться полным доверием. Поэтому необходимо ограничить доступ этих систем к компьютерам, расположенным внутри сети.

Предоставляя защиту от внешних атак, ДМЗ, как правило, не имеет никакого отношения к атакам внутренним, таким как перехват трафика.

Разделение сегментов и контроль трафика между ними, как правило, реализуются специализированными устройствами — межсетевыми экранами. Основными задачами такого устройства являются:

* контроль доступа из внешней сети в ДМЗ;
* контроль доступа из внутренней сети в ДМЗ;
* разрешение (или контроль) доступа из внутренней сети во внешнюю;
* запрет доступа из внешней сети во внутреннюю.

В некоторых случаях для организации ДМЗ достаточно средств маршрутизатора или даже прокси-сервера.

Серверы в ДМЗ при необходимости могут иметь ограниченную возможность соединиться с отдельными узлами во внутренней сети. Связь в ДМЗ между серверами и с внешней сетью также ограничивается, чтобы сделать ДМЗ более безопасной для размещения определённых сервисов, чем Интернет. На серверах в ДМЗ должны выполняться лишь необходимые программы, ненужные отключаются или вообще удаляются.

Существует множество различных вариантов архитектуры сети с DMZ. Два основных – с одним межсетевым экраном и с двумя межсетевыми экранами. На базе этих методов можно создавать как упрощенные, так и очень сложные конфигурации, соответствующие возможностям используемого оборудования и требованиям к безопасности в конкретной сети.

Для создания сети с ДМЗ может быть использован один межсетевой экран, имеющий минимум три сетевых интерфейса: один – для соединения с провайдером (WAN), второй – с внутренней сетью (LAN), третий – с ДМЗ. Подобная схема проста в реализации, однако предъявляет повышенные требования к оборудованию и администрированию: межсетевой экран должен обрабатывать весь трафик, идущий как в ДМЗ, так и во внутреннюю сеть. При этом он становится единой точкой отказа, а в случае его взлома (или ошибки в настройках) внутренняя сеть окажется уязвимой напрямую из внешней.

Реализуем ДМЗ с МЭ на роутере. Филиалы имеют доступ к двум серверам больницы (веб-серверу С2 и серверу баз данных С3). Данные сервера будут находится в ДМЗ. Роутер, связывающий филиалы с больницей, выберем далее.

* + 1. Организация VPN.

VPN (Virtual Private Network) – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети, например Интернет.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности:

* шифрования (с использование инфраструктуры криптосистем) на выделенных шлюзах (шлюз обеспечивает обмен данными между вычислительными сетями, функционирующими по разным протоколам);
* экранирования (с использованием межсетевых экранов);
* туннелирования;

На все компьютеры, имеющие выход в Интернет (вместо Интернета может быть и любая другая сеть общего пользования), устанавливаются VPN-агенты, которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям. Перед отправкой IP-пакета VPN-агентом выполняются следующие операции:

1. анализируется IP-адрес получателя пакета, в зависимости от этого адреса выбирается алгоритм защиты данного пакета (VPN-агенты могут поддерживать одновременно несколько алгоритмов шифрования и контроля целостности), кроме того, пакет может и вовсе быть отброшен, если в настройках VPN-агента такой получатель не значится;
2. вычисляется и добавляется в пакет его имитоприставка, обеспечивающая контроль целостности передаваемых данных;
3. пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию);
4. формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента (эта процедура называется инкапсуляцией пакета).

В результате этого обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для внешней атаки информация, например внутренние IP-адреса сети, в этом случае недоступна. При получении IP-пакета выполняются обратные действия.

Для передачи данных VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами. Такой канал называется туннелем, а технология его создания называется туннелированием. Вся информация передается по туннелю в зашифрованном виде, т. е. в пакетах, которые идут в открытой сети, в качестве адресов фигурируют только адреса «черных ящиков». Кроме того, туннелирование предполагает, что внутри локальных сетей трафик передается в открытом виде, а его защита осуществляется только тогда, когда он попадает в «туннель».

Одной из обязательных функций VPN-агентов является фильтрация пакетов. Она реализуется в соответствии с настройками VPN-агента, совокупность которых образует политику безопасности виртуальной частной сети. Для повышения защищенности виртуальных частных сетей на концах туннелей целесообразно располагать межсетевые экраны.

В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

VPN призвана решать следующие задачи:

* обеспечивать защиту (конфиденциальность, целостность, подлинность) передаваемой по сетям информации. Данная задача решается применением криптографического метода защиты передаваемой информации;
* выполнять защиту внутренних сегментов сети от НСД извне. Решение задачи возможно благодаря встроенным в VPN-системы функциям межсетевого экранирования, а также криптографическим механизмам, запрещающим незашифрованный сетевой трафик;
* обеспечивать идентификацию и аутентификацию пользователей. Данная задача возникает вследствие того, что, как сказано в определении VPN, в сети должны взаимодействовать лишь доверенные узлы, доверие к которым возможно после прохождения процедур идентификации и аутентификации.
* экономия финансовых ресурсов организации, когда для обеспечения защищенной связи с филиалами применяются не защищенные выделенные каналы связи, а Интернет.

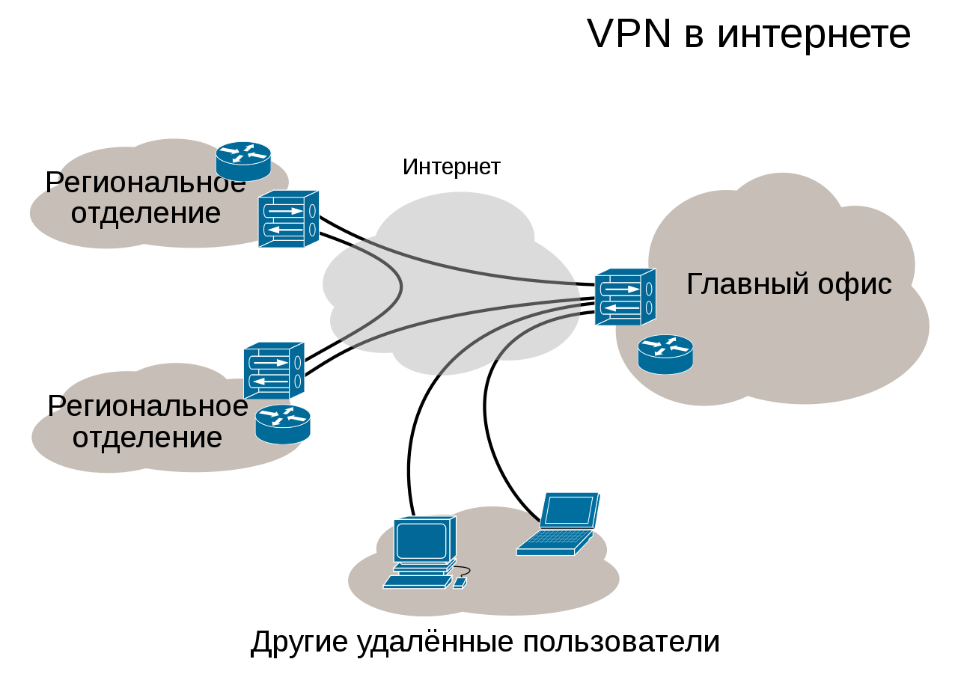


Рисунок 4.4 – Соединение с помощью VPN филиалов и удаленных пользователей.

Шифрование информации в виртуальной частной сети осуществляется протоколами, такими как SSH и SSL.

**SSH (Secure Shell)** – это протокол удаленного администрирования, разработанный для осуществления удаленного управления операционными системами и туннелирования TCP-соединения. Использование этого протокола допускает использование разных алгоритмов шифрования, что позволяет безопасно работать практически в любой незащищенной среде: работать с ПК через командную оболочку, передавать по шифрованному каналу любой тип данных (например, видео- и аудиофайлы).

SSH это протокол, использующий клиент-серверную модель для аутентификации удаленных систем и обеспечения шифрования данных, обмен которыми происходит в рамках удаленного доступа. По умолчанию для работы протокола используется TCP-22 порт: на нем сервер (хост) ожидает входящее подключение и, после получения команды и проведения аутентификации, организует запуск клиента, открывая выбранную пользователем оболочку. При необходимости пользователь может менять используемый порт.

Для создания SSH подключения клиент должен инициировать соединение с сервером, обеспечив защищенное соединение и подтвердив свой идентификатор (проверяются соответствие идентификатора с предыдущими записями, хранящимися в RSA-файле, и личные данные пользователя, необходимые для аутентификации).

Протокол **SSL (Secure Sockets Layer – уровень защищённых сокетов)** обеспечивает защищенный обмен данными за счет сочетания двух следующих элементов:

1. Цифровой сертификат привязан к конкретному домену сети Интернет, а центр сертификации проводит проверки, подтверждающие подлинность организации, а уже затем создает и подписывает цифровой сертификат для этой организации. Такой сертификат может быть установлен только на тот домен web-сервера, для которого он прошел аутентификацию, что и дает пользователям сети Интернет необходимые гарантии.
2. Шифрование – это процесс преобразования информации в нечитаемый для всех вид, кроме конкретного получателя.

Также возможно получить дополнительную информацию о степени защищенности конкретного SSL сеанса. Когда вы устанавливаете сетевое соединение с защищенным web-сервером, сервер должен вначале сам аутентифицировать клиентский web-браузер, что осуществляется с помощью цифрового сертификата, после чего устанавливается защищенное соединение.

В ходе этой процедуры web-браузер проверяет, чтобы:

* доменное имя в сертификате соответствовало тому домену, от которого идет запрос на защищенное соединение
* сертификат не был просрочен
* сертификат, подписавший сертификат домена, входил в число доверенных вашего web-браузера

Этапы этой процедуры проходят без пауз, так что пользователь «не чувствует» этой внутренней работы. Сертификат служит электронным документом, независимым образом заверяемым третьей стороной, такой как компания thawte, которая гарантирует, что домен принадлежит именно этой реально существующей компании. Действующий сертификат дает пользователю гарантию конфиденциальности при передаче прошедшему аутентификацию узлу Интернет. Передача информации осуществляется защищенным образом.

Когда происходит запрос сертификата для домена организации, то происходит запуск на сервере процесса генерации пары ключей – открытого и секретного. Секретный ключ устанавливается на сервере и при этом очень важно, чтобы никто кроме Вас не имел доступа к нему. На основе секретного ключа создается цифровая подпись, которая является своеобразной электронной печатью Вашей компании. Если Вы потеряете секретный ключ, то больше не сможете использовать свой сертификат. Необходимо создавать резервные копии секретного ключа, что является неотъемлемым элементом управления безопасностью информации.

Парный открытый ключ устанавливается на web-сервер и является частью цифрового сертификата. Открытый и секретный ключи связаны математической закономерностью, но не идентичны. Желающий установить с Вами защищенный сеанс (при помощи SSL протокола) клиент обращается к открытому ключу вашего сертификата и с помощью открытого ключа шифрует посылаемую Вам информацию. Этот процесс происходит мгновенно и незаметно для пользователя. Расшифровать информацию можно только с помощью секретного ключа сервера. Это дает гарантию клиенту, что никакая третья сторона не получит доступ к его информации.

Рассмотрев принцип работы VPN и протоколы шифрования информации, реализуем свою VPN.

В качестве VPN клиента будем использовать свободно распространяемое программное решение **OpenVPN**, которое установим на сервер. OpenVPN – свободная реализация технологии виртуальной частной сети (VPN) с открытым исходным кодом для создания зашифрованных каналoв типа точка-точка или сервер-клиенты между компьютерами. Она позволяет устанавливать соединения между компьютерами, находящимися за NAT и сетевым экраном, без необходимости изменения их настроек. Для обеспечения безопасности управляющего канала и потока данных OpenVPN использует библиотеку OpenSSL, использующую протоколы шифрования **SSL/TLS**.

В качестве алгоритма шифрования выберем один из самых используемых алгоритмов асимметричного шифрования – **RSA**. Его криптостойкость основывается на сложности разложения на множители больших чисел, а именно - на исключительной трудности задачи определить секретный ключ на основании открытого, так как для этого потребуется решить задачу о существовании делителей целого числа. Наиболее криптостойкие системы используют 1024-битовые и большие числа.

1. Организация связи с филиалами.
   1. Описание технологии связи.

В качестве технологии связи с филиалом в этом же городе была выбрана технология VDSL.

Цифровая абонентская линия (DSL) – это технология высокоскоростного Интернета, которая позволяет передавать цифровые данные по проводам телефонной сети.

DSL представляет собой технологию, которая исключает необходимость преобразования сигнала из аналоговой формы в цифровую форму и наоборот. Цифровые данные передаются на компьютер именно как цифровые данные, что позволяет использовать гораздо более широкую полосу частот телефонной линии. Для использования полосы более высоких частот, чем спектр речевого сигнала, оборудование xDSL должно быть установлено на обоих концах линии, а сама физическая линия должна обеспечивать возможность передачи сигнала в необходимой полосе частот. Еще одна особенность DSL-технологии – на скорость передачи данных влияет удаленность клиента от телефонной станции. Вполне приемлемое качество передачи данных обеспечивают до семи километров кабеля. Кроме того, на скорость передачи также влияет качество телефонной разводки внутри дома и тип самого телефонного кабеля (коаксиальный, витая пара и др.). Так что далеко не всегда можно заранее сказать, какая именно скорость будет у конкретного DSL-соединения. Но если соединение установилось, то даже в худшем случае скорость передачи данных через DSL-модемы составляет несколько сотен килобайт в секунду. DSL-модем не только передает данные, но также выполняет роль маршрутизатора. Существенно важно, что DSL-соединение является постоянным, а не коммутируемым.

VDSL (англ. Very high speed Digital Subscriber Line, сверхвысокоскоростная цифровая абонентская линия) — принадлежит к семейству технологий xDSL. Ее главное применение — цифровые абонентские линии, в которых требуется очень высокая скорость передачи от абонента в сеть. В решениях, основанных на VDSL, центральной точкой системы является специализированная, коммутирующая система, принимающая транслированные данные из источника (например, из оптико-волоконного кабеля), и, следовательно, используя классические, медные кабели, передающая данные целевому получателю. Правило работы технологии VDSL 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 м, 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 (на практике используются сегменты, не превышающие 200 м;

25 Мбит/с на дистанции 300—900 м;

10 Мбит/с на дистанции до 1500 м.

После превышения длины кабеля в 1500 м, 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 (практически не превышает 200 м);

100 Мбит/с на дистанции 500 м;

50 Мбит/с на дистанции до 1000 м.

На дистанции от 1500 м и выше возможная пропускная способность близка к той, что доступна по технологии ADSL, и удерживается на данном уровне на дистанции до 4-5 км.

* + 1. Выбор оборудования.

В качестве оборудования выберем гигабитный роутер TP-Link TD-W9977 N300 Wi-Fi с VDSL/ADSL модемом, обеспечивающий скорость широкополосного подключения до 100 Мбит/с по VDSL2.



Рисунок 5.1 – Роутер TP-Link TD-W9977 N300 Wi-Fi.

* 1. Организация связи с филиалом, расположенным в другом городе.

В качестве технологии связи с филиалом в другом городе была выбрана спутниковая связь. Спутниковая связь — это технология связи, которая использует спутник в космосе для передачи данных между удаленными местами на земле. Она может использоваться в случаях, когда другие технологии связи, такие как VDSL, не могут обеспечить достаточно высокой скорости передачи данных или надежности связи.

В качестве технологии используется TCP/IP для передачи данных в спутниковой связи.

TCP/IP - это сетевая модель, состоящая из двух протоколов: TCP (Transmission Control Protocol) и IP (Internet Protocol). Она определяет способ передачи данных между устройствами в компьютерных сетях. Протокол IP отвечает за маршрутизацию пакетов данных, тогда как TCP обеспечивает контроль за передачей данных и обеспечивает надежную доставку данных между устройствами.

Модель TCP/IP используется для передачи данных в Интернете и других компьютерных сетях. Она состоит из 4 уровней:

Уровень доступа к сети (Network Access Layer) - определяет физические и логические аспекты сетевой связи и обеспечивает доступ к среде передачи данных.

Транспортный уровень (Transport Layer) - отвечает за управление передачей данных между устройствами и обеспечивает надежность передачи данных при помощи протокола TCP.

Сетевой уровень (Internet Layer) - обеспечивает маршрутизацию данных между сетями при помощи протокола IP.

Прикладной уровень (Application Layer) - определяет протоколы приложений, которые используются для передачи данных между приложениями на устройствах в сети.

* + 1. Выбор оборудования.

В качестве оборудования, поддерживающего TCP/IP и спутниковое подключение, можно выбрать спутниковый модем Hughes 9202M. Этот модем предоставляет быстрое и надежное подключение к Интернету, используя глобальную спутниковую сеть Inmarsat BGAN. Он поддерживает протокол TCP/IP, который обеспечивает передачу данных в сети Интернет. Благодаря своим компактным размерам и портативности, Hughes 9202M может быть использован для связи с Интернетом в любом месте на земле, где есть доступ к спутниковой сети.

1. Распределение адресов рабочих станций с учетом структурной схемы.

Разделим сеть на несколько подсетей, исходя из структурной схемы сети. Выделим подсети I и II, соответствующие двум зданиям, которые занимает больница; подсеть III, состоящую из маршрутизаторов, связывающих здания (R1, R2); подсеть IV, объединяющую маршрутизатор R1 и сервер с возможностью маршрутизации C4; подсеть V, объединяющую сервера C1 и С4; подсеть VI, объединяющую R3 и DMZ; подсеть VII, объединяющую R3 и C4.

Определим IP-адреса для подсетей, серверов, ПК, IP-камер, IP-телефонов, датчиков и принтеров. Для распределения адресов будем использовать внеклассовую модель. Сетевой адрес состоит из адреса сети, адреса подсети и адреса хоста. Поскольку сеть разбита на пять подсетей, то для номера подсети зарезервируем 3 бита. Адрес подсети определяется младшим битом 3го байта сетевого адреса и двумя старшими битами 4го байта. Адрес сети определяется старшими 23 битами первых двух байт сетевого адреса. Адрес хоста определяется шестью младшими битами 4го байта сетевого адреса.

Количество компьютеров - 42. Количество серверов - 4. Соответственно, всего машин 46. Чтобы не записывать все IP адреса вручную, будем использовать протокол DHCP, который автоматизирует назначение IP- адресов.

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

Таблица 5.1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Подсеть | Адрес подсети | Кол-во у-ств | Отделы | IP-адрес |
| I | 10.10.1.0/25 | 6 | Администрация (телефон, датчик, принтер) | 10.10.1.1-10.10.1.6 |
| 9 | Отдел кадров (датчик, телефон, камера) | 10.10.1.7-10.10.1.15 |
| 13 | Бухгалтерия (3 датчика, телефон) | 10.10.1.16-10.10.1.28 |
| 3 | Охрана (телефон) | 10.10.1.29-10.10.1.31 |
| 8 | IT-отдел (телефон, 2 датчика, камера) | 10.10.1.32-10.10.1.39 |
| 6 | Архив (датчик, телефон) | 10.10.1.40-10.10.1.45 |
| 11 | НИ отдел (4 датчика, камера, телефон) | 10.10.1.46-10.10.1.56 |
| 1 | Маршрутизатор R3 | 10.10.1.57 |
| II | 10.10.1.128/25 | 5 | Регистратура (камера, телефон) | 10.10.1.129-10.10.1.133 |
| 3 | Охрана (телефон) | 10.10.1.134-10.10.1.136 |
| 13 | Врачебный отдел (телефон, 8 датчиков) | 10.10.1.137-10.10.1.149 |
| 9 | Отдел лаборатории (камера, датчик, телефон) | 10.10.1.150-10.10.1.158 |
| 13 | Отдел хирургии | 10.10.1.159-10.10.1.171 |
| 1 | Маршрутизатор R2 | 10.10.1.172 |
| III | 10.10.2.0/30 | 2 порта | Маршрутизаторы между зданиями | 10.10.2.1-10.10.2.2 |
| IV | 10.10.2.4/30 | 2 порта | C4 и R1 | 10.10.2.5-10.10.2.6 |
| V | 10.10.2.8/30 | 2 порта | C4 и C1 | 10.10.2.9-10.10.2.10 |
| VI | 10.10.2.12/29 | 3 порта | Маршрутизатор (DMZ) + 2 сервера в DMZ | 10.10.2.13-10.10.2.15 |
| VII | 10.10.2.16/30 | 2 порта | R3, C4 (сервер-маршрутизатор) | 10.10.2.17-10.10.2.18 |

1. Выбор сетевых протоколов.

В качестве стека сетевых протоколов выберем TCP/IP — это промышленный стандарт стека протоколов, разработанный для глобальных сетей.

Лидирующая роль стека TCP/IP объясняется следующими его свойствами:

* Это наиболее завершенный стандартный и в то же время популярный стек сетевых протоколов, имеющий многолетнюю историю.
* Почти все большие сети передают основную часть своего трафика с помощью протокола TCP/IP.
* Это метод получения доступа к сети Internet.
* Этот стек служит основой для создания intranet – корпоративной сети, использующей транспортные услуги Internet и гипертекстовую технологию WWW, разработанную в Internet.
* Все современные операционные системы поддерживают стек TCP/IP.
* Это гибкая технология для соединения разнородных систем как на уровне транспортных подсистем, так и на уровне прикладных сервисов.
* Это устойчивая масштабируемая межплатформенная среда для приложений клиент-сервер.

В стеке TCP/IP определены четыре уровня. Каждый из них несет на себе некоторую долю нагрузки по решению основной задачи - организации надежной и производительной работы составной сети, части которой построены на основе разных сетевых технологий.

Самый нижний соответствует физическому и канальному уровням модели OSI. Этот уровень в протоколах TCP/IP не регламентируется, но поддерживает вес популярные стандарты физического и канального уровня: для локальных сетей это Ethernet, Token Ring, FDDI, Fast Ethernet, 1 OOVG-AnyLAN, для глобальных сетей – протоколы соединений "точка-точка" SLIP и РРР, протоколы территориальных сетей с коммутацией пакетов Х.25, frame relay.

Стержнем всей архитектуры является уровень **межсетевого взаимодействия**, или сетевой уровень, который реализует концепцию передачи пакетов в режиме без установления соединений, то есть дейтаграммным способом. Именно этот уровень обеспечивает возможность перемещения пакетов по сети, используя тот маршрут, который в данный момент является наиболее рациональным. Этот уровень также называют уровнем internet, указывая, тем самым, на основную его функцию - передачу данных через составную сеть.

Основным протоколом уровня (в терминологии модели OSI) в стеке TCP/IP является протокол IP. Этот протокол изначально проектировался как протокол передачи пакетов в составных сетях, состоящих из большого количества локальных сетей, объединенных как локальными, так глобальными связями. Поэтому протокол IP хорошо работает в сетях со множеством топологий, рационально используя наличие в них подсистем и экономно расходуя пропускную способность низкоскоростных линий связи. Так как протокол IP является дейтаграммным протоколом, он не гарантирует доставку пакетов до узла назначения, но старается это сделать.

К уровню межсетевого взаимодействия относятся все протоколы, связанные с состоянием и модификацией таблиц маршрутизации, такие как протоколы сбора маршрутной информации RIP и OSPF, а также протокол межсетевых управляющих сообщений ICMP. Последний протокол предназначен для обмена информацией об ошибках между маршрутизаторами сети и удаленным источником пакета. С помощью специальных пакетов ICMP сообщает о невозможности доставки пакета, о превышении времени жизни или продолжительности сборки пакета из фрагментов, об аномальных величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т. п.

Помимо протокола ICMP, на данном уровне пригодится протокол ARP, позволяющий узнать MAC адрес устройства по его IP адресу.

На **основном** уровне функционируют протокол управления передачей TCP и протокол дейтаграмм пользователя UDP. Протокол TCP обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования виртуальных соединений. Протокол UDP обеспечивает передачу прикладных пакетов дейтаграммным способом, как и IP, и выполняет только функции связующего звена между сетевым протоколом и многочисленными прикладными процессами.

**Прикладной** уровень объединяет все службы, представляемые системой пользовательским приложениям. Прикладной уровень реализуется программными системами, построенными в архитектуре клиент-сервер, базирующейся на протоколах нижних уровней.

В отличие от протоколов остальных трех уровней, протоколы прикладного уровня занимаются деталями конкретного приложения и "не интересуются" способами передачи данных по сети. Этот уровень постоянно расширяется за счет присоединения к старым, прошедшим многолетнюю эксплуатацию сетевым службам типа Telnet, FTP, TFTP, DNS, SNMP, сравнительно новых служб, таких, например, как протокол передачи гипертекстовой информации HTTP.

Для получения информации о доменах корпоративной сети будем использовать протокол DNS. Также будем использовать протокол DHCP для осуществления динамической адресации.

Для организации зашифрованного VPN соединения с филиалами будем использовать протокол шифрования SSL.

1. Выбор топологии сети, среды передачи, метода доступа, активного и пассивного оборудования корпоративной сети.
   1. Виды используемых кабелей.

Для передачи информации используются коаксиальные, оптоволоконные кабели и витая пара.

**Коаксиальный кабель** представляет собой электрический кабель, состоящий из центрального провода и металлической оплетки, разделенных между собой слоем диэлектрика (внутренней изоляции) и помещенных в общую внешнюю оболочку. К нему труднее механически подключиться для несанкционированного прослушивания сети, он также дает заметно меньше электромагнитных излучений вовне. Однако монтаж и ремонт коаксиального кабеля существенно сложнее, чем витой пары, а стоимость его выше (он дороже примерно в 1,5-3 раза по сравнению с кабелем на основе витых пар). Сложнее и установка разъемов на концах кабеля. Поэтому его сейчас применяют реже, чем витую пару.

**Волоконно-оптический кабел**ь состоит из тонких (5-60 микрон) волокон, по которым распространяются световые сигналы. Это наиболее качественный тип кабеля - он обеспечивает передачу данных с очень высокой скоростью (до 10 Гбит/с и выше) и к тому же лучше других типов передающей среды обеспечивает защиту данных от внешних помех.

Волоконно-оптические кабели состоят из центрального проводника света (сердцевины) - стеклянного волокна, окруженного другим слоем стекла - оболочкой, обладающей меньшим показателем преломления, чем сердцевина. Распространяясь по сердцевине, лучи света не выходят за ее пределы, отражаясь от покрывающего слоя оболочки. В зависимости от распределения показателя преломления и от величины диаметра сердечника различают:

1). Многомодовое волокно со ступенчатым изменением показателя преломления;

2). Многомодовое волокно с плавным изменением показателя преломления;

3). Одномодовое волокно.

Понятие «мода» описывает режим распространения световых лучей во внутреннем сердечнике кабеля. В одномодовом кабеле (Single Mode Fiber, SMF) используется центральный проводник очень малого диаметра, соизмеримого с длиной волны света - от 5 до 10 мкм. При этом практически все лучи света распространяются вдоль оптической оси световода, не отражаясь от внешнего проводника. Полоса пропускания одномодового кабеля очень широкая - до сотен гигагерц на километр. Изготовление тонких качественных волокон для одномодового кабеля представляет сложный технологический процесс, что делает одномодовый кабель достаточно дорогим. Кроме того, в волокно такого маленького диаметра достаточно сложно направить пучок света, не потеряв при этом значительную часть его энергии.

В многомодовых кабелях (Multi Mode Fiber, MMF) используются более широкие внутренние сердечники, которые легче изготовить технологически. В стандартах определены два наиболее употребительных многомодовых кабеля: 62,5/125 мкм и 50/125 мкм, где 62,5 мкм или 50 мкм - это диаметр центрального проводника, а 125 мкм - диаметр внешнего проводника.

Многомодовые кабели имеют более узкую полосу пропускания - от 500 до 800 МГц/км. Сужение полосы происходит из-за потерь световой энергии при отражениях, а также из-за интерференции лучей разных мод.

В качестве источников излучения света в волоконно-оптических кабелях применяются светодиоды и полупроводниковые лазеры.

Для осуществления скоростной передачи данных между двумя корпусами больницы, а также для повышенной безопасности проведем многомодовый оптоволоконный кабель. Для исключения влияния внешних факторов на передающую среду, проложим оптоволокно через колодец.

* 1. Выбор коммутаторов.

Коммутаторы (Switch) - это:

1). Многопортовое устройство, обеспечивающее высокоскоростную коммутацию пакетов между портами;

2). В сети с коммутацией пакетов - устройство, направляющее пакеты, обычно на один из узлов магистральной сети. Такое устройство называется также коммутатором данных.

Коммутатор предоставляет каждому устройству (серверу, ПК или концентратору), подключенному к одному из его портов, всю полосу пропускания сети. Это повышает производительность и уменьшает время отклика сети за счет сокращения числа пользователей на сегмент. Как и двухскоростные концентраторы, новейшие коммутаторы часто конструируются для поддержки 10 или 100 Мбит/с, в зависимости от максимальной скорости подключаемого устройства. Если они оснащаются средствами автоматического опознавания скорости передачи, то могут сами настраиваться на оптимальную скорость - изменять конфигурацию вручную не требуется.

Коммутаторы передают пакеты только целевому устройству (адресату), так как знают MAC-адрес (Media Access Control) каждого подключенного устройства. В результате уменьшается трафик и повышается общая пропускная способность, а эти два фактора являются критическими с учетом растущих требований к полосе пропускания сети современных сложных бизнес приложений.

Коммутация завоевывает популярность, как простой, недорогой метод повышения доступной полосы пропускания сети. Современные коммутаторы нередко поддерживают такие средства, как назначение приоритетов трафика (что особенно важно при передаче в сети речи или видео), функции управления сетью и управление многоадресной рассылкой.

Для выбора коммутаторов предварительно необходимо вычислить минимальное количество портов у каждого из них. На каждом коммутаторе необходимо предусмотреть запасные порты, чтобы в случае отказа одного из используемых, можно было в кратчайшие сроки устранить неполадку и задействовать один из резервных портов. Такой подход имеет смысл для портов под UTP-кабель. Для оптических портов это неактуально, так как они отказывают крайне редко.

Вычислим количество портов необходимых для каждого коммутатора по формуле:

N = 1.5\*Nk+1,

где: N – требуемое количество портов; Nk – количество занятых портов.

Таблица 8.1

|  |  |  |
| --- | --- | --- |
| Коммутатор | Кол-во подключенных устройств | MIN кол-во портов |
| SW1 | 8 | 13 |
| SW2 | 16 | 25 |
| SW3 | 11 | 18 |
| SW4 | 10 | 16 |
| SW5 | 6 | 10 |
| SW6 | 9 | 15 |
| SW7 | 13 | 21 |
| SW8 | 17 | 27 |
| SW9 | 8 | 13 |
| SW10 | 8 | 13 |
| SW11 | 7 | 12 |
| SW12 | 12 | 19 |
| SW13 | 8 | 13 |
| SW14 | 6 | 10 |

В соответствии с полученными данными, делаем вывод, что требуется 7 коммутаторов на 16 портов, 5 коммутаторов на 24 порта и 2 коммутатора на 48 портов.

В качестве коммутаторов на 24 и 48 портов возьмем устройства **Cisco Switch WS-C2960S-24PD-L** и **Cisco Switch WS-C2960S-48LPD-L** из одной серии. Коммутатор работает под управлением операционной системы Cisco IOS, предусматривая функции безопасного централизованного управления через SSH, RADUIS, авторизации посредством 802.1X, поддерживает механизмы обеспечения безопасности доступа к сети, алгоритмы предотвращения атак, вторжений на уровне 2, таких как PortSecurity, Dynamic ARP Inspection, IP source guard, Port-based ACL. Поддерживает протоколы качества обслуживания QoS, обеспечивая маркировку пакетов и выстраивание очереди на основе меток CoS для совместной работы корпоративных приложений и приложений IP телефонии в единой сети. Коммутатор поддерживает протоколы транков, VLAN, обеспечивая возможность виртуализации локальной сети, возможность роста и масштабирования сети. Имеет расширенные функции QoS, расширенные функции контроля и сетевой безопасности Network Admission Control (NAC), базирующиеся на пользователе, порте или MAC адресе подключения. Коммутатор поддерживает маршрутизацию на уровне 3 и создание до 16 статических маршрутов.

В качестве коммутатора с 16 портами возьмем **C1000-16T-2G-L Cisco Catalyst**. Данный коммутатор обеспечивает:

* Высокую надежность благодаря более высокому среднему времени наработки на отказ (MTBF) и расширенной поддержке ограниченного срока службы (E-LLW);
* Управление через командную строку или веб-интерфейс;
* Мониторинг сети через выборочный поток (sFlow);
* Безопасность с поддержкой 802.1X для подключенных устройств, анализатор коммутируемых портов (SPAN) и защита данных протокола моста (BPDU);
* Поддержка управления устройством с помощью беспроводного доступа через Bluetooth, простой протокол управления сетью (SNMP), доступ к консоли через RJ-45 или USB.
  1. Выбор сетевых адаптеров.

Сетевые адаптеры служат для взаимодействия с другими устройствами в локальной сети. Существует целый спектр сетевых плат для различных ПК, имеющих определенные требования требованиям к производительности. Характеризуются по скорости передачи данных и способах подключения к сети.

Если рассматривать просто способ приема и передачи данных на подключенных к сети ПК, то современные сетевые платы (сетевые адаптеры) играют активную роль в повышении производительности, назначении приоритетов для ответственного трафика (передаваемой/принимаемой информации) и мониторинге трафика в сети. Кроме того, они поддерживают такие функции, как удаленная активизация с центральной рабочей станции или удаленное изменение конфигурации, что значительно экономит время и силы администраторов постоянно растущих сетей.

Сетевые адаптеры встраиваются в компьютеры, поэтому выбор сетевых адаптеров не требуется.

* 1. Выбор маршрутизаторов.

Для связи между корпусами больницы будем использовать маршрутизаторы **Cisco C921-4P** - это маршрутизаторs с интегрированными сервисами фиксированной конфигурации, обеспечивающий качественную и надёжную передачу голоса и данных, необходимую для предприятий малого размера или домашнего офиса

Особенности Cisco C921-4P:

* Высокая доступность и непрерывность бизнеса
* Высокий уровень сетевой безопасности
* 4-портовый управляемый коммутатор
* Бесшумность за счёт отсутствия вентиляторов охлаждения
* Унифицированное управление проводными и беспроводными сетями из общей консоли для упрощения операций
* Удаленное конфигурирование и управление, чтобы поддерживать местный ИТ-персонал

Для DMZ используем маршрутизатор **Cisco RV260-K8-RU** - это доступный VPN-маршрутизатор с продвинутыми функциями бизнес-класса, среди которых Gigabit Ethernet, QoS, поддержка IPv6 и расширенная безопасность.

Роутер имеет двухъядерный процессор, который обеспечивает производительность, обычно встречающуюся только в более дорогих решениях. WAN-порт малого форм-фактора (SFP) обеспечивает гибкое подключение и защиту инвестиций. RV260 включает в себя стандартные функции, такие как брандмауэр Stateful Packet Inspection (SPI) бизнес-класса, VPN-безопасность (IP Security [IPsec], протокол туннелирования «точка-точка» [PPTP] и OpenVPN), фильтрация содержимого и мастера устройств для упрощения настройки.

* 1. Выбор конфигурации серверов и рабочих станций.

Для надежного хранения данных и резервирования сервер баз данных реализуем на технологии RAID.

Сервер 3 (БД):

Сервер R2208WFTZS (2 PS):

* Процессор: 2 x Intel® Xeon® Scalable 4216 Silver 16 Core 2.10G 22M 100W
* HDD: SAS 2,5” 8 дисков по 900 Gb с возможностью горячей замены
* 4 NVMe диска с возможностью горячей замены
* Оперативная память: 96Gb DDR4 ECC Reg
* RAID-контроллер LSI MegaRAID SAS 9361-8i (8port SAS3, 1GB)
* 8 слотов PCI-E
* Два блока питания 1300 Вт
* Сетевой адаптер: 2 порта 10Gbase-T Ethernet

Intel Server System R2208WFTZS предназначена для построения серверных систем для работы в облачных средах, выполнения базовых операций с файлами, обработки больших массивов данных. Платформа разработана на базе материнской платы S2600WFT с чипсетом Intel® C624 и поддерживает возможность расширения регистровой оперативной памяти DDR4 до 1536 ГБ. Максимальное количество модулей оперативной памяти для данной модели составляет 24 шт.

В серверной платформе R2208WFTZS имеется 8 отсеков для дисков горячего подключения малого форм-фактора 2.5 дюйма позволяя создавать RAID структуру.

В качестве видеосервера возьмем сборку:

* процессор: Intel Core i7-10600;
* оперативная память: DDR4 16GB
* SSD: 60Gb
* HDD: 8x2000 Gb
* Сетевой адаптер: 2 порта по1000Mb

Конфигурация серверов 2 и 3 выглядит следующим образом:

* Процессор: Intel Xeon X3440 Quad-Core
* Память: 4\*HP 4GB 2Rx8 PC3-10600 -9 Kit
* Максимальный объем памяти: 16GB
* Жесткий диск: HP 1TB 6G SAS 7.2K rpm LFF (3.5-inch) Dual Port Midline 1yr Warranty Hard Drive
  1. Выбор IP-камер, IP-телефонов и датчиков.

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

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

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

В качестве IP-телефона будем использовать **D-LINK-DPH-150S.**

Сетевые интерфейсы:

* 2 порта Ethernet с разъемом RJ-45;
* 1 порт для подключения к ПК.

Сигнальные, медиа и сетевые протоколы

* SIP RFC 3261
* SDP RFC 3266
* RTP RFC 1889

Назначение IP-адреса: DHCP, статический IP-адрес и PPPoE.

Голосовые кодеки:

* G.711 a/u (64 кбит/с)
* G.729A/B (8 кбит/с)
* G.723.1 (опционально)

1. Выбор сетевой операционной системы и клиентской операционной системы, сетевое прикладное обеспечение.
   1. Выбор сетевой ОС.

В качестве сетевой ОС была выбрана **Microsoft Windows Server 2016** **–** серверная операционная система на базе Windows 10.

Характеристики:

* Поддержка контейнеров
* Вложенная виртуализация
* Последовательное обновление ОС кластера
* Горячее добавление сетевых карт и памяти
* Локальные дисковые пространства
* Реплика хранилища
* Унифицированное управление пакетами
* Безопасная загрузка Linux
* Полноценный Storage Quality of Service (QoS) — возможность динамического отслеживания производительности хранилищ и горячая миграция виртуальных машин при превышении этими хранилищами пороговых значений (IOPS).
  1. Выбор хостовой ОС.

В качестве хостовой ОС была выбрана **Windows 10 Enterprise** – специальная редакция Windows 10, предназначенная для крупных предприятий и организаций среднего бизнеса.

Windows 10 Enterprise предоставляет следующие возможности:

* Расширенная защита от современных угроз безопасности
* Гибкие процедуры развертывания и обновления, а также расширенная техническая поддержка
* Комплексное управление устройствами и приложениями
  1. Выбор сетевого ПО.

В качестве Web-сервера будем использовать решение компании Microsoft **IIS (Internet Information Services)** – проприетарный набор серверов для нескольких служб Интернета. Основным компонентом IIS является веб-сервер, который позволяет размещать в Интернете сайты. IIS поддерживает протоколы HTTP, HTTPS, FTP, POP3, SMTP, NNTP.

DNS-сервер и DHCP-сервер, а также файл-сервер поддерживаются сетевой ОС Windows Server 2016.

В качестве внешнего DNS-сервера и МЭ воспользуемся встроенными службами оборудования, отвечающего за связь с филиалами.

Для организации работы с базами данных архива предполагается использование СУБД **PostgreSQL**. PostgreSQL является решением для малых и средних приложений. Обычно PostgreSQL используется в качестве сервера, к которому обращаются локальные или удалённые клиенты, однако в дистрибутив входит библиотека внутреннего сервера, позволяющая включать PostgreSQL в автономные программы. В PostgreSQL значительно расширена функциональность, которая ставит PostgreSQL в один ряд с коммерческими СУБД.

Работу базы данных бухгалтерии предполагается организовать под управлением ПО **1С Бухгалтерия 8.0**.

В качестве E-mail-сервера воспользуемся **Microsoft Exchange Server 2016**. Гибкие средства электронных коммуникаций, которые бы оправдывали затраты на их приобретение, сейчас нужны организациям больше, чем когда либо. Microsoft Exchange Server 2016 позволяет достичь новых уровней надежности и производительности, предоставляя возможности, которые упрощают администрирование, помогают защитить передаваемую информацию и радуют пользователей, предоставляя им большую мобильность. В роли клиента данного сервера будет использоваться **Microsoft Outlook 2016**.

Для обеспечения безопасности установим антивирусную систему **Microsoft Security Essentials (MSE)** – бесплатный пакет антивирусных приложений от компании Microsoft, предназначенный для борьбы с различными вирусами, шпионскими программами, руткитами и троянскими программами.

1. Разработка модели сети.

Проведем моделирование разрабатываемой сети в программе Cisco Packet Tracer. Для моделирования будем использовать упрощенную структурную схему. Для упрощения моделирования примем за все оборудование отдела один хост, соответственно трафик от всех рабочих станций отдела и прочего оборудования будет суммировано исходить с этого хоста. Также некоторые сервера представим как один сервер. Для доступа к серверам C1 и C4 добавим дополнительный роутер R4.

Модель корпоративной сети в программе представлена на рисунке