

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

кафедра Компьютерных технологий

«Допущен к защите»
Заведующий кафедрой Куралбаев З.К.
профессор, к.фр.-м.н.
(Ф.И.О., ученая степень, звание)
« » 20 г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Построение компьютерно-коммуникационной сети предприятия на основе технологий NGN.

Специальность 5В070400 - ВТчПО

Выполнил (а) Акимбаев Ж.Ж. ВТ 12-4
(Фамилия и инициалы) группа

Научный руководитель Рахимжанова З.М., ст.преп.
(Фамилия и инициалы, ученая степень, звание)

Консультанты:

по экономической части:

Бекмусова А.У., к.э.н., доцент
(Фамилия и инициалы, ученая степень, звание)
А.У. « 12 » 05 2016 г.
(подпись)

по безопасности жизнедеятельности:

Тришадвер Н.Г., д.х.н., доцент
(Фамилия и инициалы, ученая степень, звание)
Н.Г. « 28 » 04 2016 г.
(подпись)

по применению вычислительной техники:

Рахимжанова З.М., ст.преп.
(Фамилия и инициалы, ученая степень, звание)
З.М. « 27 » 05 2016 г.
(подпись)

Нормоконтролер: Рахимжанова З.М., ст.преп.

З.М. (Фамилия и инициалы, ученая степень, звание)
« 30 » 05 2016 г.
(подпись)

Рецензент: Мурмалбеков М.Ж., докт. техн. наук

М.Ж. (Фамилия и инициалы, ученая степень, звание)
« » 2016 г.
(подпись)

Алматы 2016 г.

Перечень графического материала (с точным указанием обязательных чертежей)

- 10 рисунков в главе 2.
- 2 рисунка в главе 3.
- 1 рисунок в главе 4.

Рекомендуемая основная литература

- 1) Поголов А.В. Учебное пособие НЭИЗ Зарубежные и отечественные платформы сетей. - М.: Эко-Трендз, 2014 - 400 с.
- 2) Балланов И.Т. НЭИЗ. Приемы построения и организации - М.: Эко-Трендз, 2013 - 943 с.
- 3) Фришман Д. Волоконно-оптические системы связи - М.: Техносфера, 2013 - 543 с.

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант*	Сроки	Подпись
Экспертная часть	Белицкий А.С.	06.04-11.05.16	
БНР	Трихорько Н.П.	01.04-28.04.16	
Основная часть	Рахматжанова З.М.	15.03-10.04.16	
Расчетная часть	Рахматжанова З.М.	13.04-23.04.16	
Нормоконтроль	Рахматжанова З.М.	30.05.16	

Аннотация

В дипломном проекте было рассмотрено построение компьютерно-коммуникационной сети предприятия на основе технологии NGN.

Так же описаны основные преимущества и недостатки данной технологии, основы построения мультисервисных сетей NGN. В расчетной части описана информационная безопасность, построена виртуальная сеть предприятия на эмуляторе UNL. Рассмотрен план помещений и установка в нем нового оборудования для построения сети NGN.

В разделе безопасности жизнедеятельности проведен анализ условий труда в помещении и расчет кондиционирования.

Приведено технико-экономическое обоснование внедрения данного проекта и рассчитан бизнес-план.

Annotation

The thesis project was reviewed by the construction of the computer communication network of the enterprise on the basis of NGN technology.

The project examined the advantages and disadvantages, the basis of multiservice NGN networks. As part of the settlement describes the information security, based on the virtual network emulator UNL. Considered plan of the premises and installing new equipment in it for the NGN network.

In the health and safety section of the analysis of working conditions in the room and air conditioning.

Developed feasibility study for implementation of the project and business-plan.

Аңдатпа

Дипломдық жобада NGN технологиясы негізінде кәсіпорынның компьютерлік-коммуникациялық желісін құру қарастырлығын.

Сонымен қатар аталған технологияның артықшылықтары мен кемшіліктері, NGN мультисервистік желілерді құру негіздері сипатталған. Есептік бөлімінде ақпараттық қауіпсіздік сипатталып, UNL эмуляторында кәсіпорынның виртуалды құрылған. Ғимарат жобасы және онда желіні құруға арналған жабдықтарды орнату қарастырлығын.

Өміртіршілік қауіпсіздігі бөлімінде ғимараттағы еңбек шарттарына талдау жасалып, желдету есептелген.

Берілген жобаны енгізудің технико-экономикалық негіздемесі келтірілген және бизнес-жоспары есептелген.

Содержание

Введение.....	13
1 Основы Мультисервисных Сетей NGN	14
1.1 Основные понятия сети NGN	14
1.2 Архитектура сетей NGN.....	17
1.3 Трехуровневая модель NGN	19
1.4 Применение серверов в сетях NGN	22
1.5 Протоколы сетей NGN.....	27
1.6 Базовые протоколы стека TCP/IP	27
1.7 Сигнальные протоколы	29
2 Построение сети	33
2.1 Описание оборудования	33
2.1.1 Маршрутизатор серии Cisco 3700	33
2.1.2 Описание сервера Cisco UCS C420 M3.....	35
2.1.3 Коммутатор Cisco Catalyst серии 3850	38
2.2 Построение сети для предприятия.	40
2.2.1 Выбор топологии сети и методов доступа	41
2.2.2 Планирование IP адресации.....	42
2.2.3 Выбор сетевой операционной системы. Выбор программного обеспечения для защиты информации.....	42
2.3 Описание UNetLab	43
2.3.1 Построение сети на эмуляторе UNetLab	45
2.4 Обеспечение информационной безопасности	47
2.4.1 Оценка стоимости	48
2.4.2 Сетевое окружение	49
2.4.3 Разработка политики	53
2.4.4 Реализация политики безопасности	54
2.4.5 Проведение аудита.....	56
3 Безопасность жизнедеятельности.....	58
3.1 Анализ условий труда технического персонала	58

3.2 Выбор системы освещения рабочих мест. Расчет производственного освещения	60
3.2.1 Расчет естественного освещения.....	60
3.2.2 Расчет искусственного освещения	63
3.3 Расчет системы кондиционирования	65
4 Бизнес план сети NGN	70
4.1 Резюме.....	70
4.3 Компания и отрасль	71
4.4 Основные продукции (услуги).....	72
4.5 Анализ рынка сбыта. Изучение рынка услуг	72
4.6 Финансовый план	73
4.6.1 Трудоемкость.....	73
4.7 Расчет потребностей инвестиций	74
4.8 Эксплуатационные расходы.....	75
4.8.3 Расчет накладных расходов	77
Заключение	79
Список литературы	80

Введение

На данный момент всё большее и большее число пользователей в Казахстане ощущают либо нехватку, либо недостаточное качество услуг, предоставляемых операторами связи. Телефонная сеть общего пользования базируется на принципе коммутации каналов, который не может дать высокой пропускной способности линий связи. И вследствие того, что такие необходимые сейчас услуги, как передача голоса в хорошем качестве, передача видео в реальном времени, конференцсвязь требуют высокой пропускной способности, ТфОП реализовать их может только в случае установке дополнительного оборудования.

Кроме того, в настоящий момент у всех сетей связи существует один очень важный недостаток: узкая специализация, т.е. для каждого вида связи существует хотя бы одна самостоятельная сеть. При этом ресурсы одной сети не могут использоваться другой сетью по ряду причин (правовые, конкурентные, рыночные и др.). В результате, потребитель за отдельными услугами связи вынужден обращаться в разные компании, заключать много договоров, вести на своем предприятии разные виды учета.

Некоторые операторы реализуют одну или несколько услуг, например, высокоскоростной Интернет, но установка модема и сама услуга относительно дороги, а сопряжение оборудования с другим оператором, предоставляющим конференц-связь, весьма проблематична. Решением этой и других проблем, возникающих у пользователей, желающих иметь весь комплекс необходимых услуг, могла бы стать сеть, объединяющая все услуги, сеть нового поколения – Next Generation Network. Она бы преодолела архитектурные ограничения, свойственные традиционным фиксированным телефонным сетям за счёт реорганизации сетевой архитектуры, выделения нового уровня управления услугами, слияния телефонии и информационных технологий, и использования открытых протоколов.

1 Основы Мультисервисных Сетей NGN

1.1 Основные понятия сети NGN

В сети следующего поколения (NGN) представляет собой современный коммутации сетевых пакетов, узлы многопользовательский. SPP основана на технологии Gigabit Ethernet (ГКП) и MPLS (Multiprotocol коммутации по меткам) и обеспечивает связь со скоростью до 10 Гбит и имеет все возможности для обеспечения качества обслуживания (поддержка QoS, CoS) и предоставляет клиенту необходимые параметры составить набор необходимых услуг, а также для настройки параметров. На базе сети следующего поколения, мы можем предоставить клиенту полный спектр услуг от традиционной голосовой телефонии для высококачественной видеоконференцсвязи. Клиент, в дополнение к традиционному высокому качеству услуг, получает массу преимуществ, в том числе минимизации операционных затрат и поддержание сети достигается за счет создания единой универсальной среды мультисервисной, свести к минимуму затраты на управление этой инфраструктурой, возможность создания корпоративная сеть любого размера, адаптивное управление в качестве частной сети, и это дало ему ресурсы оператора, возможность организации единого веб-интерфейс для управления услугами.

Строительство сети NGN позволяет расширить спектр дополнительных услуг связи и предоставить клиентам широкий спектр средств массовой информации и информационных ресурсов.

Абоненты сети NGN открывает много возможностей для более чем 50 дополнительных услуг связи, в том числе административных услуг через измерения интернет-трафика и биллинга для группы бизнес-клиентов. Другими словами, сеть связи нового поколения позволяет независимой регулировки дополнительных услуг телефонии через Интернет, трафик вызовов, создавать группы абонентов и определить конкретный набор услуг, а также других. Абонент в этом случае она будет выступать в качестве администратора и воспользоваться дополнительными услугами единой информационной среды. Сеть NGN позволяет индивидуализировать услуги для конкретного пользователя и предложить спектр услуг, необходимых пользователю. Важным преимуществом нового поколения NGN сети к традиционной телефонии, в дополнение к широкому спектру услуг связи обеспечиваются высокая скорость передачи данных, мобильность (доступ пользователя к данным может осуществляться независимо от его местоположения), индивидуальность (услуга доступна в любое время в необходимом количестве и содержание форматов) доступность (умеренная цена, в сочетании с возможностью выбрать тип оборудования, используемого в сети NGN позволяет подключать другую сеть).

Сети следующего поколения (NGN - сети следующего поколения) - это результат эволюции всей системы электросвязи. Однако основой для реализации идеи телефонная сеть NGN, единственным существующим сетям, которые:

- обеспечивает диалоговые услуги самой группе абонентов;
- приносит оператору основные доходы.

Для сетевых характеристик NGN существенных особенностей, которые отличают его в новый класс телекоммуникационных систем. Обычно существует пять таких особенностей NGN:

- использование технологии пакетной передачи и коммутации для обмена всеми видами информации;
- применение систем коммутации с распределенной архитектурой, которые отличаются от функционально ориентированных телефонных станций;
- разделение функций, которые относятся к службам поддержки, коммутации и передачи;
- включение широкополосного доступа и мультисервисной службы движения вида "тройные услуги (голос, данные и видео);
- реализация оперативных функций управления (в том числе делегированные пользователи) за счет веб-технологий.

Передача информации в виде пакетов через сети NGN на основе протоколов IP (Интернет-протокол). Но идеология построения NGN является значительно отличаются от принципов, которые создали Интернет. Прежде всего, следует выделить поддержку предопределенных СПП показателей качества обслуживания (QoS - качество обслуживания). Эти показатели должны быть определены для обеспечения качественной связи через сети IP - услуг VoIP (голос поверх IP), более известный как IP-телефония.

Современный рынок связи находится на таком этапе, когда операторы имеют возможность обойти все трудности конвергенции, когда-сущие сетям прошлых лет, и перейти напрямую к сети следующего поколения технологии, которая получила рабочее название NGN на сети нового поколения". Для того, чтобы сделать рывок и вступить в ряды высокотехнологичных операторов требуются новые решения в области создания и обеспечения высокой производительности. Сети NGN - технология построения сети - предназначена для предоставления услуг передачи данных и голосовых услуг. Она снимает ряд ограничений и барьеров, которые существуют сейчас, и в этом заключается ее экономическая продуктивность.

К новым возможностям относятся:

- переход от принципа соединения "точка-точка" к принципу "каждый с каждым";
- используется универсальный характер обслуживания разных приложений;

– абстрагирование пользователей от технологий реализации услуг связи (принцип черного ящика) и беспрецедентная гибкость получения необходимого набора, объема и качества услуг;
Полная прозрачность взаимоотношений между продавцом и покупателем услуг.

В основу технологии положена концепция перестройки общества на принципах полноводности, когда информация становится общедоступной ресурсом в любой среде, они могут быть доставлены независимо от того, где находится человек. Появился зародыш концепции полноводности в Интернете, что и породило огромную популярность в сети. Пользователь, выходя в Интернет, получает доступ к миру.

NGN с точки зрения потребителя представляет собой облако или "черный ящик", потому что потребителю не интересно знать стеки, протоколы и т. д. Она позволяет предоставлять такие услуги, как широкополосный доступ к Интернет (100 Мбит / сек), пакетную телефонию, VPN, а также "видео по запросу" и выделенные широкополосные каналы.

Таким образом, сеть связи NGN является следующего поколения (следующий шаг поколения) является гетерогенной мультисервисной сети для передачи всех видов трафика мультимедиа и распределенных предоставление неограниченного спектра телекоммуникационных услуг с возможностью добавления, редактирования, распределенных зарядки. Сеть поддерживает передачу трафика с различными требованиями к качеству обслуживания и обеспечивает поддержку этих требований.

Пакетная обработка технологии позволяют предложить Пользователю в такой сети прозрачные автоматизированные принципы расчетов за приобретение вания, расчета входящих, исходящих, ввод платежей для посвя-alizatio, транзита и терминции трафика, трафик считать сигнал, выделяя составляющую трафика, пропущенного от стороннего оператора.

Эти особенности отличают сети NGN от обычных телефонных и IP-сетей, наиболее распространенные в мире телекоммуникаций. Сети NGN, будучи результатом слияния сети Интернет и телефонных сетей, объединения имеют лучшие характеристики. Сети NGN обладают следующими характеристика: спектакли:

– адаптивность к трафика любого вида, что можно сравнить с приспособляемостью Интернету, в отличие от отсутствия гибкости ТФОП при передаче данных (это особенно важно, учитывая, что передача данных в ближайшее время вырастет до 90% телекоммуникационного трафика);

– гарантированное качество голосовой связи и критически важных приложений передачи данных. В данном случае, в сеть NGN обладает надежностью ТСОП в отличие от негарантированного качества подключения к Интернету;

– низкая стоимость передачи в расчете на единицу объема информации приближается к стоимости передачи данных в Интернет, не ТФОП

(суммарный объем трафика данных и голосового трафика утраивается каждый год).

Одной из существенных особенностей NGN является перенос сроков реализации некоторых функций/услуг специализированных сетевых элементов. Таким образом, сервер получает часть задач, традиционных телефонных сетей (ТФОП) были проведены на станции (простой, сообщения, конференции). Наиболее строго специализированных сетей для генерации тональных сигналов необходимо иметь специальное устройство. Наверное, в самом деле, специализация не будет идти так далеко, как изменения в архитектуре влекут за собой определенную степень риска[1].

1.2 Архитектура сетей NGN

Существует множество вариантов построения мультисервисной сети. Один из них предусматривает строительство однородной инфраструктуры, полностью или частично, не ориентирована на сетевое подключение (например, на основе и коммутируемых ЛВС пакет региональных сетей), или подключение ориентированных сетей (например, банкомат). Ни одна из этих архитектур в отдельности, вряд ли смогут удовлетворить пользователей при построении мультисервисной сети из-за различий в экономических и функциональных требований для локальных сетей и региональных сетей. Мультисервисная сеть, распространяясь на большие-ди-ции, должны иметь ядра региональной сети связи, в окружении периферийных локальных сетей.

Существующие сети характеризуются вертикальной интеграции передачи, связи, маршрутизации и услуг: для предоставления различных услуг (телефонная связь, передача видео, данных) различных сетей. В отличие от обычных сетей, сетей следующего поколения (NGN) характеризуются открытой архитектурой и горизонтальные отношения на различных уровнях.

Общей инфраструктуры для сетей NGN, используемых для предоставления различных услуг, осуществляется на транспортном уровне на основе технологии пакетной передачи. Обмен информацией между источником и местом назначения находится на том же принципе, вне зависимости от типа подключения (телефонный звонок, сессия, Интернет, передача видео, игры по сети с несколькими игроками или перевод фильма).

Этот уровень является логически и физически отделены от транспортного уровня, который позволяет самостоятельно разрабатывать различные сегменты сети. В то время персональных услуг (телефония, электронная торговля, передача видео по запросу и т. д.) соответствуют разные сервера, отделившись от транспортного уровня. Для реализации новой услуги нужно всего лишь добавить новый сервер, который из-за уровня транспорт доступен для всех подключенных к сети пользователей.

Пользователи, которые подключены к сети NGN по интерфейсам осуществляется с различных диапазонов частот и пропускной способности, основанные на различных технологиях. Несмотря на то, что наиболее

подходит для подключения широкополосных интерфейсов NGN (>0.5 Мбит/с), все пользователи получают универсальный доступ к услугам независимо от оборудования.

Основные особенности и преимущества сети NGN:

- снижение операционных затрат (ОРЕХ);
- сети NGN дают возможность внедрять новые услуги, получать дополнительные доходы;
- масштабируемость;
- возможность предоставления пакетов услуг;
- снижение стоимости портов;
- открытые стандартные интерфейсы;
- возможность внедрения новых услуг, созданных сторонними поставщиками;
- простота установки и обслуживания сети;
- консолидация сетей.
- Услуги:
- VoIP телефонии;
- голосовой почты;
- Студенческий центр Centrex и IP-УАТС, управляемой;
- данных услуг;
- мультимедийные услуги;
- виртуальные частные сети;
- единая система обмена сообщениями;
- обмен мгновенными сообщениями;
- услуги системы интерактивного речевого ответа;
- услуги контакт-центра;
- интерактивные игры;
- распределенная виртуальная реальность;
- видеоконференции;
- домашний менеджер.

Некоторые застройщики предлагают такой вариант: NGN является универсальной многоцелевой сетью, предназначенную для передачи речи, изображений и данных с использованием технологии пакетной коммутации. По сути, он является результатом слияния Интернета и телефонных сетей, объединяя их лучшие черты. На практике это означает гарантированное качество голосовой связи и передачи данных в критически важных приложениях. Таким образом, сети NGN имеют степень надежности, характерную для ТФОП (в отличие от негарантированного качества связи через Интернет) и обеспечивают низкую стоимость передачи в расчете на единицу объема информации (близко к стоимости передачи данных по Интернету, не ТСОП).

Главной архитектурной особенностью NGN является передача и маршрутизация пакетов и основные элементы транспортной инфраструктуры (каналы, маршрутизаторы, коммутаторы, шлюзы) физически и логически отделены от устройств и механизмов для управления вызовами, а также услуги доступа.

Сети следующего поколения будут поддерживать единую платформу управления и имеют общее ядро и для мобильных и для стационарных сетей. В итоге абоненты будут получать единый набор услуг для ТСОП и IP-телефонии, так и для мобильной сети. И первое сохранении номера при переходе от одного оператора к другому.

1.3 Трехуровневая модель NGN

Архитектура сети NGN является трехуровневой и состоит из следующих уровней:

- транспортного уровня;
- уровень контроля коммутации и передачи информации;
- уровень услуг и управление сервисом.

Задача транспортного уровня являются коммутация и прозрачная передача информации пользователя.

Уровень управления услугами содержит функции управления логикой услуг и приложений и представляет собой распределенную вычислительную среду, обеспечение:

- предоставления инфокоммуникационных услуг;
- услуги по управлению;
- создание и внедрение новых услуг;
- взаимодействие различных служб.

Трехуровневая модель сети NGN представлена на рисунке 1.1.



Рисунок 1.1 – Трехуровневая модель сети NGN

Особенностью технологии являются открытые интерфейсы между СПП транспортного уровня и уровня управления коммутацией. По отношению к классической АТС это все равно, что делить оборудование на функциональные блоки, когда один реализует функции блока обработки сигнализации, маршрутизация вызовов, статические сбора информации, и др., и второй блок (или группу блоков) обеспечивает реальное включение несущие каналы. Взаимодействие между блоками осуществляется с использованием стандартных протоколов.

Транспортный слой NGN на основе технологий пакетной передачи информации. Технологий являются АТМ и IP.

Как правило, в основу транспортного уровня мультисервисной сети крепятся к существующей сети АТМ или IP, т. е. сеть NGN может быть сформирована накладывается на существующую транспортную сеть пакет.

Сети на основе технологии АТМ с помощью встроенных инструментов для обеспечения качества обслуживания.

В случае, если маршрутизатор или коммутатор АТМ/IP, который реализует функцию перехода под внешнее управление, то они должны реализовывать функцию управления от гибкого коммутатора с реализацией протоколов, как H.248/MGCP (IP) или ВСС (для банкоматов).

Уровень управления коммутацией и позвонить в сервис.

Задачей уровня управления коммутацией и передачей является Управление связи фрагмента сети NGN[2].

Функция установления соединения реализуется на уровне элементов транспортной сети под внешним управлением, оборудование гибких коммутирующих Торы. Исключение составляет АТС с функции MGC, которые сами устраивают на уровне элемента коммутации транспортной сети.

В случае использования гибкой сети нескольких коммутаторов, они взаимодействуют через межузловой протоколы (как правило, семья из SIP-T) и обеспечить совместное управление связи.

Задачи гибкого коммутатора:

- обработку всех видов сигнализации, применяемых в домене;
- хранения и управления данными подписчика пользователей, подключение обученный в своей области непосредственно или через оборудование шлюзов доступа;
- взаимодействие с серверами приложений для обеспечения расширенного перечня услуг пользователям сети.

При установлении сетевого оборудования гибкая переключатель обеспечивает обмен сигнала функциональными элементами уровня управления коммутацией. Такими элементами являются шлюзы, терминальное оборудование мультисервисной сети (устройства доступа (ОВР), терминалы SIP и H323), оборудование других гибких коммутаторов и АТС функциями контроллера транспортных шлюзов (MGC). Для передачи

сигнальной информации ТФОП через сеть пакетов используются специальные протоколы.

Так, для передачи сигнализации ОКС7 информации, полученной через шлюзы сигнала от ТФОП к оборудованию гибкого коммутатора, используется протокол MxUA технологии протокола sigtran (в то же время в ряде гибкую реализацию переключатель имеет прямого ввода сигнализации ОКС-7).

На основе анализа полученной информации и решения о последующей маршрутизации вызова оборудование гибкого коммутатора, используя соответствующие протоколы, осуществляет сигнальный обмен по установлению соединения с сетевым элементом и назначения элементов управления с помощью протокола H/248 (переключение IP) или ВСС (АТМ коммутатора) связи для передачи информации пользователя. Поток информации пользователя не проходит через гибкий переключатель, и закрылся на уровне транспортной сети.

Терминальное оборудование пакетной сети взаимодействует с оборудованием гибкого коммутатора с помощью протоколов SIP и H.323. Информация пользователя из терминального оборудования прибывает на уровне узла сети доступа пакета и далее направляется под контролем гибкого коммутатора.

Вся информация, связанная со статистикой работы мультисервисной сети, учетом стоимости и направлений, в том числе стоимости для пользователей, хранится и обрабатывается на уровне гибкого коммутатора для передачи в направлении соответствующих систем (ASR).

Уровня услуг и управления услугами.

Основной услугой, предоставляемой как в классическом сетей связи и мультисервисных сетей является передача информации между пользователями сети. Использование технологии пакетной транспортной сети позволяет обеспечить единые алгоритмы доставки информации для различных видов связи.

Помимо услуг доставки информации в мультисервисных сетях реализована возможность поддержки предоставления, расширенные списки услуг.

Что касается телефона, услуги точка-добавляемого гибкое коммутационное оборудование или оборудование, серверы приложений.

Для пользователей, использующих мультимедийный терминал (H323 в SIP), могут быть предоставлены различные типы мультимедийных услуг.

Логика реализации обслуживания вызовов к ограниченному числу точек сети, чтобы оптимизировать структуру доступа к интеллектуальной сети. Для этого уровня гибкий коммутатор выполняет функции сети NGN.

Использование пакетной технологии позволяет совместное предоставление дополнительных услуг, независимо от типа доступа, используемого пользователем.

Мультисервисной сети реализовать возможность предоставления аналогичных услуг с различными параметрами классов обслуживания (QoS).

Как правило, различные производители оборудования мультисервисных сетей предлагают свой спектр современных телекоммуникационных услуг, которые следует учитывать при выборе оборудования.

Следует отметить, что взаимодействие между гибкими серверами или услуг коммутатора недостаточно развиты международным стандартам, и, таким образом, возможной несовместимости различных производителей оборудования.

1.4 Применение серверов в сетях NGN

В сетях NGN серверов приложений, участвующих в предоставлении различных дополнительных коммуникационных и информационных услуг пользователям этих сетей и используются для контроля пользователем сервиса. Условно весь спектр возможных услуг можно разделить на четыре класса:

- услуги таких дополнительных услуг традиционной связи сети с коммутацией каналов (уведомление о входящем вызове, переадресация вызова, конференция и т.д.);
- услуги, такие услуги интеллектуальной сети связи (звонки для предоплаченных карт, телеголосование, вызов, бесплатно, и т.д.);
- услуги, которые являются специфическими для компьютерных сетей (интерактивного обмена сообщениями (мгновенных сообщений), онлайн мультиплеер, и т.д.);
- услуги специфичные для широкополосных сетей связи (видео по запросу, игры по запросу, интерактивное телевидение и т. д.).

Но это только условное деление: в реальности услуга в сетях NGN могут обеспечить любые комбинации из вышеперечисленных услуг или быть особо оговорены) в набор СПП. Следует отметить, что услуги могут быть применены к одному типу трафика (аудио, видео, данные) и любые их комбинации с необходимо синхронизации информационных потоков и необходимый класс обслуживания для каждого потока.

В дополнение к предоставлению услуг, сервер приложений отвечает за управление конфигурацией услуг от пользователя в интерактивном режиме. Учитывая, что современные пользовательские терминалы к сетям NGN имеют графический пользовательский интерфейс (SIP-телефоны) и что сервер приложений может связываться с любым компьютером терминал (ПК, КПК, смартфон и т.д.), сервер приложений должен быть иметь возможность взаимодействовать с пользователем с помощью графического интерфейса пользователя.

Взаимодействие пользователей с сервером приложений и сети NGN на основе модели "клиент-сервер", широко используется в компьютерных сетях. В соответствии с этой моделью приложения выполнен в ССВ файл (сетевые) вычислительной системы. Приложение разделено на клиентские и серверные

процессы. В сети, помимо серверов приложений, существуют также следующие типы серверов:

- файловых серверов - неорганизованные хранилища информации общая;
- информация или серверы баз данных - организованное хранилище информации с определенной логикой доступа;
- узкоспециализированные сервера выполнение определенных задач в сети, например связи (прокси), специализированных баз данных сетей (протокол DHCP, DNS и WINS) и взаимодействия (транзакции, сообщения, почта) и много других типов (для каждого сетевого протокола и технологии могут быть использованы на вашем сервере).

Сервер приложений предназначен для выполнения прикладных процессов. В данном случае функциональная логика находится на сервере, а логика обеспечения на клиенте. Основная задача сервера приложений является максимальное абстрагирование от клиента следующие вопросы:

- где и как хранится информация;
- где и как обрабатывается информация;
- где и между тем, что оборудование сетевое взаимодействие при запуске приложения.

В дополнение к этой проблеме, сервер приложений должен стремиться обеспечить максимальную доступность сервиса (Service). Он должен обеспечивать общий интерфейс для соединения с клиентом с учетом технических возможностей пользовательского терминала и канала связи. сервер приложений клиентов, в зависимости от функций делятся на "тонкие" и "толстый" (в терминах модели "клиент-сервер"). функциональность клиента определяется степенью обработки пользовательского ввода, степень обработки и правил, формирующих пользовательский интерфейс информации (или дисплей, предоставляющий информацию). Каждый из этих факторов, определяющих функциональные возможности клиента, можно разделить на несколько классов (реализации метода). Для удобства эти сорта будут предоставляться временное имя. Пользовательский ввод может быть обработан следующим образом:

- последовательно после каждого действия пользователя, сервер передает информацию о действии (например, какая клавиша была задействована, где находится курсор). Преимущество в том, что возможности клиентского терминала, должны отвечать минимальным требованиям, и недостатки, которые имеют повышенную чувствительность к сетевой задержки и нагрузки на сервер.
- группа образом - информация хранится до тех пор, пока пользователь выполняет специальные действия, чтобы отправить эту информацию на сервер приложения. Преимущество по сравнению с последовательным режимом является то, что последовательность действий может быть изменена или отменена, и создает меньшую нагрузку на сервер. Но многие требования

применяются к терминальному клиенту, как он должен уметь накапливать ввода и отображения его пользователю;

– изображения группы путем обработки накопленной информации при вводе и/или перед отправкой на сервер, обрабатывается, например, проверяется на корректность, непротиворечивость, соответствие последовательности ввода, а также могут быть сгруппированы, упакованы, конвертировать, и т. д. Преимущества-щество в сравнении с предыдущим режимом, что в данном случае создает более комфортные условия для ввода пользователя и обеспечивает минимальную нагрузку на сервер. Но для этого вам придется платить большую нагрузку на клиентский терминал и особые требования к его функциональности из-за того, что он должен реализовать дополнительную логику для обработки ввода.

Пользовательский ввод может быть акустической, символов (алфавитно-цифровой), координат (обработанные пространственных координат инструмента ввода) и смешанные. Также есть псевдо или ввод команды, которая получается только после обработки или преобразования в режиме реального пользовательского ввода.

Под лечением в данном случае речь идет о довольно сложных ресурсоемких операции, выполняемые над информацией (например, сортировки, выборки, математические вычисления и преобразования, преобразования в другой тип информации или других показателей, и др.). Такая обработка может быть сделано либо на клиенте, либо по запросу клиента на стороне сервера. Соответственно, где происходит лечение, есть большой функционал и потребности в ресурсах для оборудования. Объем передаваемой информации может увеличиться или уменьшиться в зависимости от вида обработки и типа информации. Поэтому, для оптимизации трафика, если это позволяет Тип клиентского терминала может использоваться и распределенной обработки между клиентом и сервером[3].

Функциональность клиента определяется сочетанием в другие группировки выше факторов. В соответствии с этой комбинацией клиент покупает определенные плюсы и минусы. Клиенты пробации по функциональности можно разделить на следующие основные типы:

– терминал для обработки последовательного метода ввода пользователя: пользовательский интерфейс создается с помощью физического отображения, а не обработки информационного контента на стороне клиента не возможен;

– Web-клиент - ввод пользователя обрабатывается группе изображения, формировании пользовательского интерфейса выполняется методом составления инструкций и обработки информации на стороне клиента не возможен;

– апплет для пользовательского ввода может быть использована групповая терапия способ способ или же метод с дополнительной обработкой; пользовательский интерфейс формируется методом компиляции на сервере. По степени обработки информации на стороне клиента ограничений нет. Это

обычно зависит от типа приложения, но общей практикой является использование ограниченной обработки на стороне клиента;

– программное обеспечение является ввод пользователя обрабатывается групповым методом с дополнительной обработкой. Создайте свой собственный пользовательский интерфейс выполнен по методике составления клиентом, информацию, Контент, как правило, подвергается значительной переработке.

– наиболее перспективных на сегодняшний день типов клиентов считаются веб - клиента и приложения, а также их переходных форм (например, "активный" Web - клиент пользователя интерфейс, который осуществляется при помощи апплетов). Их полезность определяется тем, что они универсальны и обеспечивают необходимую гибкость в создании и обслуживании, а также относительно высокие требования к ресурсам клиентского терминала компенсируется прогрессом в области аппаратного обеспечения.

Взаимодействие между клиентом и сервером приложений может быть реализована аппаратно с помощью любого стандартного протокола об обмене информацией в компьютерных сетях (протокол Telnet, протокол SNMP, LDAP, то по FTP, по http, RPC и т.д.) или специальный протокол транспортного уровня или сверху над стандартным протоколам, или по протоколам группы, а не одного протокола. Выбор протоколов определяется потребностями конкретного приложения, т. е. зависит от типа клиента, Тип Контента, медиа, технологии, используемые приложения, и т. д. Сегодня наиболее часто в качестве базового протокола связи используется http, так как он имеет достаточную функциональность для приложений "клиент-сервер" и обеспечивает прозрачную передачу трафика во всех сетях.

Логика взаимодействия между сервером и клиентом процессы применения обычно строится на базе модели "вызова удаленной процедуры" (НПК), так как это значительно облегчает процесс разработки приложений и упрощает логическое представление приложения в виде единого целого. он появляется в одной среде исполнения.

Логика взаимодействия между сервером и клиентом процессы применения обычно строится на базе модели "вызова удаленной процедуры" процедур (RPC), а это значительно облегчает процесс разработки приложений и упрощает логическое представление приложения в виде единого целого. он появляется в одной среде исполнения:

- COM/DCOM/OLE;
- COBRA;
- SOAP/XML/UDDI/WSDL.

Наиболее перспективным на сегодняшний день объектной технологии является SOAP/XML, поскольку он более универсальный, на основе международных стандартов и имеет широкую поддержку от различных производителей программного обеспечения. Данная технология наиболее часто используется для создания веб-служб, и организация их взаимодействия

с клиентом процесс. В качестве клиента в этом случае является апплет или "активный" Web-клиент.

В компьютерных сетях взаимодействие между клиентом и сервером происходит напрямую или через специализированные сервера. В сетях NGN, такое взаимодействие осуществляется с участием выключатель программного обеспечения. Переключатель программы в данном случае выполняет следующие функции:

- проверки подлинности и авторизации, клиенте и сервере приложений (как сервер приложений);
- проверки подлинности и авторизации, клиенте и сервере приложений (как сервер приложений);
- управления соединением между клиентом и сервером, а также других соединений, представленной логики приложения;
- управлять брандмауэры (брандмауэр - брандмауэр) при взаимодействии с другими сетями, например, когда сервер приложений и клиент находятся в разных сетях;
- управляющий шлюзы, например, когда сервер приложений взаимодействия с абонентом сети с коммутацией каналов. Такое взаимодействие возможно, если сервер приложений поддерживает акустический интерфейс, специальные символы или команды.

С помощью переключателя программ обычно только потоки управления и потоки, связанные с передачей информации контентные мимо него. Протокол взаимодействия между переключателем программы и сервера приложений, и между коммутатором и абонентом сети NGN считается наиболее перспективным использование протокола SIP и его расширение[4].

При предоставлении дополнительных услуг, связанных с подключением через выключатель программного обеспечения, возможны следующие сценарии взаимодействия с сервером приложений:

- сервер приложений обрабатывает запросы клиента и взаимодействует с сервером базы данных (БД), связанный с переключателем программы, вносит необходимые изменения в базу данных. Переключатель, в свою очередь, взаимодействует с сервером базы данных и клиентом с сетью запрашиваемой услуги с заданными параметрами. Недостатком этого сценария является то, что структура базы данных должна быть известна на обоих устройствах, то есть универсальность и гибкость взаимодействия;
- сервер приложений обрабатывает запросы клиента и взаимодействует с сервером базы данных, связанные с ним, вносит необходимые изменения в базу данных. Переключатель, в свою очередь, взаимодействуя с запросами сервера приложений, необходимую информацию от сервера приложений, и обеспечивает клиента с сетью запрашиваемой услуги с заданными параметрами. В этом случае роль сервера играет роль клиента. Этот сценарий лишенный недостатков первый сценарий, но он имеет свой недостаток, связанный с ненужной повышенной нагрузке на сервер приложений;

– сервер приложений обрабатывает запросы клиента и взаимодействия с переключателем программного обеспечения, вносит изменения в базы данных, расположенные на сервере баз данных, связанных с переключателем. Коммутатор, в свою очередь, взаимодействует с сервером базы данных и предоставляет клиенту сети запрашиваемую услугу с заданными параметрами. В этом случае сервер выполняет роль переключателя программного обеспечения, и исполняет роль приложений клиент-сервер. Этот сценарий лишена недостатков предыдущего сценария, но изменения программного обеспечения должны быть в состоянии выполнять роль сервера приложений, хотя и в ограниченных рамках;

– сервер приложений обрабатывает запросы клиента и управляет работой коммутатора в процессе оказания услуг. Это взаимодействие аналогично взаимодействию ssp и SCP в интеллектуальных сетях. В данном случае, в качестве протокола взаимодействия может быть использован по протоколу iNAP.

1.5 Протоколы сетей NGN

Сеть NGN можно рассматривать в качестве сетевых решений, сочетающих различные фрагменты существующих сетей (Интернет и PSTN) с использованием методов, характерных для этих сетей. Соответственно, в СПП применяются в качестве интернет-протоколов (например, IP, TCP, UDP, FTP, HTTP, SMTP и другие протоколы стека TCP / IP), и сообщает ТфОП (например, SS7, EDSS1, протоколы интерфейса V5) Кроме того, некоторые протоколы сетей нового поколения перспективны, прямо или косвенно затрагивающих принципы взаимодействия между Интернетом и PSTN сетей в рамках сети с множеством услуг. NGN протоколы с некоторой степенью условности можно классифицировать следующим образом:

- основные Интернет-протоколы: IP, ICMP, TCP, UDP;
- транспортные протоколы: RTP, RTCP;
- сигнальные протоколы: SIP, H.323 SIGTRAN, MEGACO/H.248, MGCP, RSVP, SCTP, ISUP, BICC, SCCP, INAP;
- протоколы маршрутизации: RIP, IGRP, OSPF, IS-IS, EGP, BGP, IDRP, TRIP;
- протоколы информационных служб и управления: SLP, OSP, LDAP, SNMP;
- протоколы услуг: FTP, SMTP, HTTP, кодеки G.xxx, H.xxx, факс T.37, T.38, IRP, NNTP.

1.6 Базовые протоколы стека TCP/IP

Протоколов Интернет может использоваться для передачи сообщений через любой набор объединенных сетей. Они одинаково пригодны для

подключения как локально, так и в глобальных сетях. Стек протоколов Интернета включает в себя не только спецификации низших уровней (например, TCP и IP), но также спецификации для таких распространенных приложений, как почта (SMTP), гипертекст приложение терминал (http) и передачи файлов(FTP).

Протокол IP.

Маршрутизация Интернет-протокола (IP) определяет Формат, обращаясь, и характер движения IP-дейтаграмм через межсеть (одну партию одновременно). В начале последовательностью дейтаграмм весь их маршрут не известен. Вместо этого, на каждом промежуточном узле вычисляется пунктом назначения путем проверки адреса назначения, содержащегося в дейтаграмме, с записью данных в таблицу маршрутизации текущего узла. Участие каждого узла в процесс маршрутизации состоит в продвижении пакетов, основываясь только на внутренней информации, независимо от того, насколько успешно осуществляется процесс, а дойдет или нет конечный пункт назначения пакета. Другими словами, IP не отправить к узлу - источнику сигналов неисправности, когда аномалии маршрутизации. Эта задача представил другой протокол Интернета, а именно Интернет-протокола управляющих Сообщений протокола ICMP - протокола ICMP).

Протокол ICMP.

Протокол ICMP выполняет ряд задач в рамках единой IP-сети. Помимо основной задачи, для которой он был создан (сообщение источнику об отказе маршрутизации), ICMP также предоставляет:

- способ для проверки способности узлов образовывать единую сеть Re-Эхо (сообщение и ICMP Эхо-ответ);
- стимулирования более эффективной маршрутизации (сообщение ICMP редирект - переадресация ICMP), которые;
- способ информирования источника о том, что дейтаграмма превысила назначенный срок службы в этой сети [в ICMP-сообщение истечения времени (время ожидания превышено)];
- способ передачи другие полезные сообщения.

Недавнее дополнение к ICMP обеспечивает для новых узлов вероятность найти маску подсети используется на промежуточной сети на данный момент. В общем, протокол ICMP является неотъемлемой частью всех IP реализаций, особенно тех, которые используются в маршрутизаторах.

Протокол TCP.

Протокол управления передачей (TCP) обеспечивает полностью гарантировано, с подтверждением и управления потоком данных, служба доставки для протоколов верхнего уровня. Он перемещает неструктурированные данные в непрерывном потоке байтов, которые идентифицируются порядковыми номерами. TCP также может поддерживать несколько одновременных разговоров более высокие уровни.

Протокол UDP.

Протокол UDP намного проще, чем TCP. Это полезно в ситуациях, когда мощные механизмы обеспечения надежности протокола TCP не требуется. Заголовок `udp` имеет всего четыре поля: поле порта источника (исходный порт) поле порт назначения (порт назначения) поле `length` (длина) и поле контрольной суммы (контрольной суммы UDP протокол UDP). Поля порт источника и порта назначения выполняют те же функции, как в заголовке TCP, поле длины указывает длину заголовка UDP и данных; поле контрольной суммы обеспечивает целостность пакета. Контрольной суммы UDP является дополнительным возможность.

Набор протоколов Интернета включает в себя большое количество протоколов более высокого уровня, представляющие различные приложения, включая управление сетью, передачей файлов, распределенных служб использование файлов, эмуляцию терминала и электронной почте.

1.7 Сигнальные протоколы

Протоколы SIP и H.323.

В настоящее время для создания мультимедийных вызовов по IP-сетям, созданных несколько протоколов, таких как SIP (Session Initiation Protocol) [RFC 2543] и H.323. Появление этих стандартов открывает возможность децентрализации предоставления услуг телефонии и услуги могут управляться пользователем.

Session Initiation Protocol (SIP) для организации, модификации и завершения мультимедийных сеансов или вызовов. Мультимедийные сессии включают в себя мультимедийные конференции, интернет-телефонии и других подобных приложений. SIP является одним из основных протоколов, используемых для реализации IP (передача голоса по IP - VoIP) сети для передачи голоса. Таким образом, протокол сигнализации SIP спокойно, имеющий широкое применение в интернет-телефонии.

SIP представляет собой простой протокол сигнализации для установления, изменения и разрушения голосовых и мультимедийных сеансов соединений в IP-телефонии (VoIP) и мультимедийных конференций. SIP является протоколом типа "клиент-сервер" и похож на протокол передачи гипертекста (протокол передачи гипертекста - HTTP) как синтаксической и семантической точки зрения. Он имеет текстовые запросы и ответы, которые содержат поля заголовка, которые передал информацию об услугах и характеристиках соединения.

Сигнализация управления основным транспортным протоколом является шлюзы MGCP и Megaco / H.248, а также основные протоколы, сигнализации взаимодействия между SoftSwitch выключателей T и SIP-BICC.

Протокол MGCP.

Протокол управления транспортным шлюзом (СМИ протокол управления шлюзом - пробкой раковины топления) используется между элементами распределенной мультимедийного шлюза. Распределенный

мультимедийный шлюз включает в себя вызов агента (вызов агента), который содержит "интеллект" в управление вызовами и транспортный шлюз, который содержит транспортные функции (например, преобразование речи канальный РСМ в VoIP).

Транспортные шлюзы содержат конечные точки, в сочетании с которой оператор может создавать, изменять и удалять соединения для создания и обработки сеанса связи с другими конечными точками. Кроме того, вызов агента можно поручить конечные точки выполнения функций обнаружения некоторых событий и генерировать особые сигналы. Конечные точки автоматически информировать вызов агента об изменении условий обслуживания. Кроме того, оператор может провести проверку качества конечных точек и связей между ними.

Базовый протокол пробкой раковины топления может быть расширен с дополнительными функциями определенными в так называемые пакеты (Package) - точно описывает расширения пробкой раковины топления. Например, можно упомянуть пакеты различного назначения под общим названием "пробкой раковины топления пакеты 2ВСК". Эти блоки расширения предназначены для работы с линиями связи, которая может быть использована система аварийная система телефона с многочастотный или импульсный набор, взаимодействует с корпоративной АТС, и т. д.

Протокол управления транспортным шлюзом Н.248/MEGACO.

Протокол управления транспортным шлюзом и Н. 248/MEGACO является дальнейшим развитием протокола mgcp и ряд других событий, как ietf и МСЭ-т протокол управления транспортным шлюзом и Н. 248/MEGACO используется в интерфейс между контроллером mgc и шлюзе мг, то есть между элементами физического распада медиа-шлюз по архитектуре определенными в рекомендации Н. 323. Управление транспортным шлюзом (мг) осуществляется специальным устройством управления транспортный шлюз или контроллер (МИК).

Пакет сетевой интерфейс может использовать IP и другие технологии atm. Интерфейс будет поддерживать большое количество сетевых систем сигнализации с коммутацией каналов, в том числе тон сигнализация ISDN сигнализация, ИСУП, QSIG и GSM.

Для переноса сигнальных Сообщений MEGACO/Н. 248 может использовать следующие протоколы транспортные протоколы: udpr, протокол TCP, протокол sctp (транспортный протокол управления потоком) и технологии atm. Udr-это требование для контроллера шлюза компанией mgc. TCP должен поддерживаться контроллер и шлюз. Поддержка протокола sctp, при котором и технологии ATM в обоих устройствах является обязательным. Сообщения протокола MEGACO/Н. 248 могут быть закодированы двумя способами. Комитет предложил текстовый ЦИГИ кодирования сигнальной информации, а для описания связи является протокол sdp. МСЭ-Т обеспечивает двоичный способ представления сигнальной информации по спецификации абстрактного синтаксиса ASN.1, а для описания сеансов связи

рекомендует специальный инструмент тег Формат Длина-значение (ПДК). Контроллер МИК должен поддерживать оба метода кодирования, и шлюз мг это всего лишь один из них[5].

Протокол MEGACO является внутренним протоколом, который проходит между функциональными блоками распределенного шлюза, а именно между и MGC мг. Принцип работы этого протокола является ведущий / ведомый, т. Е. ведущий / ведомый. Устройство управления Мастер и MGC транспортным шлюзом мг - раб, который выполняет команды, которые он получает от блока управления.

Протокол ВСС.

Протокол ВСС определяется рекомендацией Q. 1901 г., протокол управления вызовами, якобы между "обслуживающие узлы" (узлы порции - СН). Этот протокол называется "независимым носителем называть контролем или позвонить протокола контроля, независимые от услуг доставки информации. Управление транспортным возможностей между ЗП указана от других протоколов.

Определены три типа SN:

- интерфейс узла обслуживания (ПС) обеспечивает взаимодействие сетей с коммутацией каналов;
- транзитного узла (ТСН) - обеспечивает функциональность транзитом, справки по телефону и транспорта в сети с использованием протокола ВСС;
- узла шлюза (ГСН) обеспечивает функции между сетевым шлюзом транспортные вызова с использованием протокола ВСС.

Ethernet.

Наиболее эффективный способ подключения к Интернет-соединение с помощью кабеля Ethernet. Этот тип связи характерен для офисных зданий (бизнес-центров) и жилых домов: многоквартирных домов, а также компактные поселения. подключение к Ethernet состоит из кабельной сети, и установка Ethernet в вашей компьютерной сети Ethernet адаптера. К достоинствам можно отнести низкую стоимость установки и низкая стоимость ежемесячной арендной платы.

Эффективность, скорость и рентабельность с точки зрения стоимости и простоты, простоты использования и популярность технологии Ethernet является большим плюсом для нового подхода к построению городских сетей. Ethernet доступа, обеспечивая истинный широкополосный доступ, становятся все более экономически эффективное решение для телекоммуникационных компаний, обеспечивая большую пропускную способность.

Ethernet является единственной технологией, которая полностью поддерживает концепцию предоставления мульти-услуг. Концепция три-в-одном включает в себя осуществление услуг доступа в Интернет, IP-телефонии и видео по IP, как полный спектр услуг для индивидуальных абонентов в единую сетевую инфраструктуру, FSN (полная услуга сети).

IP МПЛС (Multiprotocol Label Switching).

Сеть IP MPLS (многопротокольной коммутации по меткам) - технология быстрой коммутации пакетов в многопротокольных сетях, а, основанный на использовании этикеток. MPLS сети разработаны и реализуются как способ построения высокоскоростных магистральных сетей, но сфера его применения не ограничивается протоколом, и распространяются на весь трафик направляется сетевому протоколу.

Традиционно, основные требования к магистральной сетевой технологии, имеют высокую пропускную способность, низкую латентность и хорошую масштабируемость. Тем не менее, современный рынок диктует новые приоритеты. Для того, чтобы удовлетворить потребности пользователей, чтобы получить доступ к интегрированным сетевым сервисам, виртуальной частной сети (VPN), а также других интеллектуальных услуг, разработана МАС архитектура, которая позволяет создавать магистральные сети с практически неограниченной масштабируемостью, высокоскоростного движения и беспрецедентную гибкость в терминах организации дополнительных услуг. Кроме того, технология MPLS позволяет интегрировать сети IP и ATM.

2 Построение сети

2.1 Описание оборудования

2.1.1 Маршрутизатор серии Cisco 3700



Рисунок 2.1 – Маршрутизатор серии Cisco 3700

Cisco 3700 Маршрутизаторы серии предназначены для удаленных офисов, которым требуется высокий уровень интеграции услуг. Cisco 3700 предлагает широкий спектр сетевых и голосовых интерфейсов в одном компактном устройстве и может значительно улучшить качество передачи голосового трафика и трафика данных. С помощью этой платформы пользователи, благодаря новым модулям расширения с высокой производительности (HDSM) и сервисных модулей (AIM), получить устройство, которое интегрирует маршрутизации высокопроизводительный / коммутации с поддержкой соединений WAN.

Cisco 3700 обеспечивает решение, которое может поддерживать большое количество традиционных устройств телефонии в сочетании с устройствами IP-телефонии. Использование 16- или 36-портовый EtherSwitch модули поддерживают встроенным источником питания, аналоговые и цифровые интерфейсы и голосовые функции Cisco IOS позволяет объединять отдельные сети PBX телефонии и передачи данных, объединяя их в единое целое. Значительная экономия средств достигается за счет финансирования решения, а не два параллельных, и, следовательно, за счет снижения затрат на развертывание, поддержку и обучение.

Особенности Cisco 3700.

– Модульные маршрутизаторы серии Cisco 3700 с помощью интерфейсных плат, которые совместимы с серией Cisco 1600, 1700, 2600, 3600, поддерживаемые возможностью обновления сетевых модулей.

– Интегрированная поддержка LAN / WAN, большое количество слотов для модулей и Н.М. HDSM, а также наличие AIM, WIC слотов расширения позволяют гибко изменять конфигурацию оборудования в соответствии с требованиями заказчика. Гибкая настройка стандартных и IP-телефонии, возможность постепенного перехода от традиционного к IP-телефонии, благодаря совместимости с более чем 90% от традиционной телефонной оборудования и TDM АТС и голосовые шлюзы поддерживают большое количество аналоговых и цифровых соединений [6].

– Система Операционная Cisco IOS используется в маршрутизаторах серии 3700, в соответствии с его способностью, близкой к изложенным в серии 2600 и 3600. Качество обслуживания, управление полосой пропускания, механизмы сетевой безопасности в сочетании с постоянными обновлениями для обеспечения Cisco IOS эффективной решение для компьютерных сетей.

Масштабируемость.

– Маршрутизаторы серии Cisco 3700 увеличилось количество мишени (2) и Вика (3) слотов. Специально встроенный слот расширения для дополнительных услуг по установке оборудования, резервного копирования и WAN-соединения для повышения производительности и реализовать более гибкое решение.

– Увеличение объема памяти и 32 Мб памяти Compact Flash и 128 Мб DRAM.

– Высокой плотности (HDSM) модули службы поддержки позволяет развертывать высокую производительность, и высокая плотность портов.

Отказоустойчивость.

– Поддержка дополнительного питания - резервный источник питания (внешний для Cisco 3725, Cisco 3745 интегрирована) - уменьшает нестабильную работу.

– Установка IP-телефонии звонки на маршрутизаторе (живучести удаленного сайта телефонии). Установка может использовать локальное соединение. Если вы потеряли связь с центральным офисом удаленных офисов с Cisco 3700.

– Горячий режим подкачки (3745) модули нм RPM, вентилятор может быть заменен в то время как маршрутизатор. Название модели должно быть функционально идентичны.

– Поддерживает обновление аппаратных средств материнской платы, материнские платы ввода / вывода платы, блок питания и вентилятор (3745 только) значительно увеличивает способность поддерживать.

Характеристики Cisco 3700.

– Cisco IOS Software min Cisco IOS realase - 12.2(8) T).

WAN модули:

- 4-х и 8-ми портовые синхронно/асинхронные интерфейсы;
- 16-ти и 32-х портовые асинхронные интерфейсы;
- 8-ми и 16-ти портовые аналоговые модемные модули;
- 1-но и 2-х портовый Channelized E1/PRI balanced/unbalanced модуль;
- 4-х и 8-ми портовый модуль ISDN BRI с NT1 или S/T интерфейсом;
- 2-х слотовый модуль для установки WIC карт.

Другие:

- 64 портовый модуль мониторинга и управления AIC (Alarm Interface Controller).

- Максимальное количество flash памяти.

- 32/128 Мб.

- Максимальное количество DRAM памяти.

- 32/256 Мб.

Габариты:

- Cisco 3725-3.5" x 17.25" x 14.7" (2 Rack Units).

- Cisco 3725-3.5" x 17.25" x 14.7" (3 Rack Units).

Электропитание:

- Cisco 3725 - поддерживает только один внутренний источник питания -48 В постоянного тока мощностью до 360 Вт, а также подключение карт расширения к источнику питания переменного тока; возможность подключения нескольких внешних источников питания.

2.1.2 Описание сервера Cisco UCS C420 M3



Рисунок 2.2 – Сервер Cisco UCS C420 M3

Решения UCS C420 высокой плотности м3, сервер 4-стойку высотой RU Размер 2 (2 стойки) предназначен для вычислений, ввода / вывода, хранения, а также для автономных приложений, интенсивно работающих с памятью. серверные решения UCS C420 M3 и расширяет возможности унифицированной вычислительной системы Cisco UCS за счет использования Intel Xeon серии e5-4600 многоядерных процессоров, чтобы обеспечить его работоспособность и эффективность. серверные решения UCS C420 M3 является частью единой унифицированной вычислительной системы Cisco, которая включает стойку и блейд-серверов с доступом к сети и доступа к памяти. С ее центральное единая система управления на основе

компьютерных моделей, решения UCS упрощает и ускоряет развертывание корпоративных приложений, работающих в среде "чистого оборудования, виртуализированных сред и облачных вычислительных средах.

Серверные решения и UCS C420 M3 предназначен для обеспечения производительности корпоративного класса и масштабируемость, а также сочетает в себе преимущества 4-сокета вычислений с использованием Intel Xeon семейства процессоров e5-4600 серии для требовательных средств виртуализации, баз данных и высокого уровня высокопроизводительных вычислений, Плотные и масштабируемые серверные решения UCS C420 M3 представляет собой сбалансированную высокопроизводительная платформа, которая добавляет к линии серверов Cisco UCS стоечных.

Высота 2 серверных решений UCS C420 M3 RU и поддерживает 48 слотов DIMM, 16 колес, 7 слотов расширения PCIe 4-портовый встроенный сетевой адаптер 1 Gigabit Ethernet. Он использует уникальную технологию интерфейсной платы, и позволяет получить доступ к той же администрации объектов решения UCS.

Серверные решения Интерфейсы UCS C420 M3 с системой Cisco UCS с использованием уникальной и инновационной карты виртуального интерфейса Cisco в CPM Виктория 1225. Cisco UCS Виктория 1225 - Улучшенная борту двухпортовый SFP + 10 Gigabit Ethernet PCI Courier стандарт Fiber Channel через Ethernet (FCoE), комбинированные, специально разработанные для работы с Cisco UCS стоечных серверов C-серии.

Он также использует Cisco конвергентной сетевой адаптер нового поколения, которая позволяет защитить ваши инвестиции в будущее.

Движущийся заряд создает серверную инфраструктуру на основе политик без запоминания состояния, которая поддерживает до 256 стандартных интерфейсов PCIe для узла, который может быть настроен как сетевой интерфейс карт или адаптеров. Кроме того, плата Циско ПСК Виктория 1225 поддерживает данные Cisco Центр виртуальной машины ткани расширитель (VM-fex), которая расширяет порты соединения с Cisco UCS на виртуальные машины, тем самым упрощая процесс развертывания виртуализации серверов.

Применение стоечного сервера Cisco UCS C420 M3.

Стойный сервер решений UCS C420 M3 и поддерживает ориентацию компании Cisco, чтобы обеспечить уникальные отличительные преимущества, матрица интеграции коммутации и простоту управления, которые являются уникальными в отрасли корпоративного класса для приложений, требовательных памяти:

- приложения совместной работы;
- базы данных;
- виртуализация и консолидация;
- приложения планирование ресурсов в масштабах предприятия (ERP) и управления взаимоотношениями с клиентами (CRM);
- высокопроизводительные облачные вычисления высокого класса.

Серверы Cisco UCS на изменение экономической политики центра обработки данных. ИТ-инфраструктура становится все более важным, поскольку организации стремятся получить полную инфраструктуру как услугу (IaaS), из "чистого железа", серверов виртуализации и облачных вычислений. Компания Cisco продолжает лидировать инновации для центров обработки данных с новейшими устройствами системы Cisco UCS и дополнить его исключительной простоте, гибкости и эффективности, включая такие инновации как стоечный сервер решений UCS C420 M3.

Компоненты системы Cisco UCS.

Компания Cisco инновации, как с помощью Cisco UCS и позволяют администраторам создавать модели программного обеспечения желаемого сервера (с помощью сервисных профилей и шаблонов Cisco), а затем реализовать этот сервер и подключения связывая модель физических ресурсов.

Этот подход существенно отличается от традиционных методов ручной настройки каждой отдельной системы ресурсов по отдельным распорядителям элементов.

В отличие от устройств других производителей, профили Cisco услуги могут быть легко перемещены из серверного шкафа в шкаф или Блейд-сервер, или между лезвием или стоечными серверами в разных шасси. Другими словами, компания Cisco Менеджер по UCS и профили сервиса не зависят от форм-фактора.

Кроме того, система Cisco UCS и состоит из дополнительные параметры сервера ввода-вывода и расширенные межсоединения решений UCS, которые повышают масштабируемость и упростить управление стойку и Блейд-систем в условиях "чистого железа". виртуализированных и облачных вычислительных средах.

Компания Cisco гарантирует, что инвестиции практически во все компоненты системы решений UCS были защищены, а сами компоненты были обратно совместимы. Например, расширители матрицы коммутации обновляются, используя те же соединения, и виртуальные карты интерфейс Cisco ПСК Виктория 1225.

Оборудование межсоединений могут быть обновлены независимо от матрицы расширителей и Блейд-шасси.

Cisco продолжает постоянно совершенствоваться во всех этих областях, делая это так, что более мощные стоечные серверы с большим объемом и скоростью памяти, оказывает благоприятное пропускную способность ввода/вывода и вычислительной мощности.

Компания Cisco выполняет эту задачу посредством непрерывных инноваций виртуальный интерфейс карты, специализированная интегральная схема (микросхема), расширитель матрицы коммутации, соединения, Блейд-серверов, Блейд-шасси и стойку серверных технологий и решений UCS Manager, который может быть использован независимо от форм-фактора и соединяет все эти компоненты в единую постоянно развивающуюся систему.

Серверных решений UCS C420 M3 является частью большого семейства стоечных серверов решений UCS C-серии стоечных серверов решений UCS серии C поддержка в различных средах, а также в рамках решений UCS и Cisco используют технологии для того, чтобы пользователи, чтобы иметь возможность справляться с самыми серьезными нагрузками.

С компанией Cisco UCS на сервер завершает единой системы связи на основе стандартов, благодаря поддержке виртуализации ЦОД Cisco VM-fex на Cisco UCS с менеджером, архитектура расширитель матрицы межсоединений и Cisco, а также расширенной памяти технологии Cisco Расширенная память Технология)[7].

Cisco является внедрение этих технологий. Благодаря архитектурному преимуществу системы Cisco UCS и обновления программного обеспечения, постоянные инновации и уникальный дизайн Blade-серверов и шасси, решений UCS-это первая по-настоящему единой площадке ЦОД.

Кроме того, компании Cisco UCS позволяет Вам превратить работу ИТ-подразделений по автоматизации на основе политик тесная интеграция и привычных инструментов системы управления и оркестрации.

Особенности и преимущества решений UCS C420 м3.

Сервер решений UCS C420 M3 и обеспечивает интегрированной точки входа для унифицированных вычислений. В следующей таблице перечислены характеристики и преимущества стоечных серверов решений UCS C420 м3.

2.1.3 Коммутатор Cisco Catalyst серии 3850



Рисунок 2.3 – Cisco Catalyst серии 3850

Cisco Catalyst 3850 Коммутаторы серии относится к следующему поколению корпоративного класса стекируемых коммутаторов, уровня доступа, обеспечивая полную конвергенцию проводных и беспроводных сетей на единой платформе. Коммутатор основан на новой специализированной интегральной схемы Unified Access Data Plane (UADP) ASIC, обеспечение соблюдения единой политики в области беспроводных и проводных сетей, мониторинга, гибкости и оптимизации приложений.

Основные преимущества:

– Модели с 24 и 48 10/100/1000 Mbps портами PoE+ и Cisco UPoE или модели с 24 и 48 100Mbps/1/2.5/5/10 Gbps портами Cisco UPoE.

- Модели с 12 и 24 1 Gb Ethernet SFP портами или 12,24 и 48 1/10 Gb Ethernet SFP+ портами.
- Опционально пять Uplink модулей с 4xGE, 2x10GE, 4x10GE, 8x10GE или 2x40GE QSFP+ портами.
- Технология Cisco StackWise-480, позволяющая объединять коммутаторы в стек с пропускной способностью 480 Gbps.
- Технология Cisco StackPower, позволяющая объединять коммутаторы в стек по питанию.
- Возможность установки двух блоков питания.
- Встроенный контроллер беспроводных точек доступа – поддержка до 50 точек доступа и 2000 беспроводных клиентов для каждого объекта коммутации (коммутатор или стек).
- Пропускная способность передачи данных беспроводной сети - до 40 Гб (48-портовые модели)
- Поддержка протокола Flexible NetFlow (FNF) для получения данных по трафику на всех портах коммутатора.
- Доступно три вида программного обеспечения: LAN Base (Enterprise Access Layer 2 Switching), IP Base (Enterprise Access Layer 3 Switching), IP Services (Advanced Layer 3 Switching (IPv4 и IPv6)).

Таблица 2.1 – Техническая характеристика коммутатора

Технические характеристики	Коммутатор Cisco Catalyst серии 3850
Общее кол-во портов 10/100/1000 Mbps Ethernet	24 48 24 PoE+ 48 PoE+ 24 UPoE 48 UPoE
Общее кол-во портов 100Mbps/1/2.5/5/10 Gbps Ethernet	24 UPoE 48 UPoE
Общее кол-во портов 1 GE SFP или 10 GE SFP+	12 SFP 24 SFP 12 SFP+ 24 SFP+ 48 SFP+
Блок питания	350W 715W 750W 1100W

Поддержка PoE	<p style="text-align: center;">— 435W — 800W/ 580W/630W (в зависимости от модели)</p>
---------------	---

2.2 Построение сети для предприятия.

Логическая схема (ТТВ) потоки данных показали, что внешние по отношению к системе источники и стоки (адресаты) данных, идентифицирует логические функции (процессы) и группы элементов данных, связывающие одну функцию с другой (потоки), а также идентифицирует хранилища (хранение) данных, к которым обращаются. Структуры потоков данных и определения их компонентов сохраняются и анализируются в словаре данных. Потоки используются для моделирования информации о передачи данных (или физические компоненты) от одной к другой части системы [8].

Распределение компьютеров по этажам.

- 1) Центр обслуживания абонентов – 2 компьютеров.
- 2) Информационная служба – 2 компьютеров.
- 3) Коммерческий отдел – 12 компьютеров.
- 4) It-отдел-2 компьютера.
- 5) Бухгалтерия – 5 компьютеров.
- 6) Менеджеры – 5 компьютеров.
- 7) Зам. глав. менеджера – 1 компьютер.
- 8) Главный менеджер– 1 компьютер.

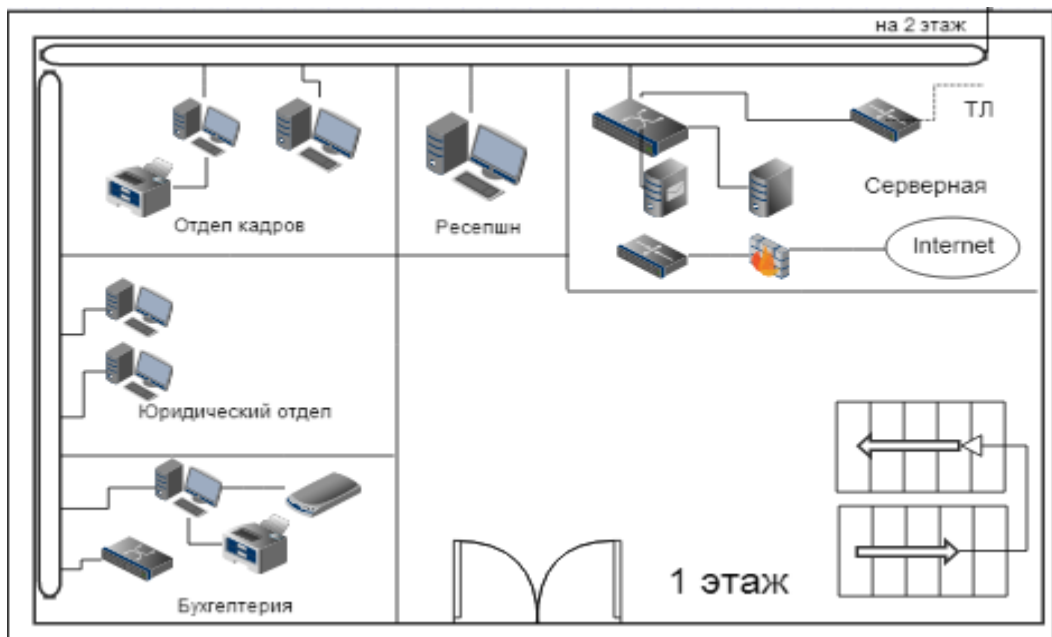


Рисунок 2.4 – Планирование сети на 1 этаже

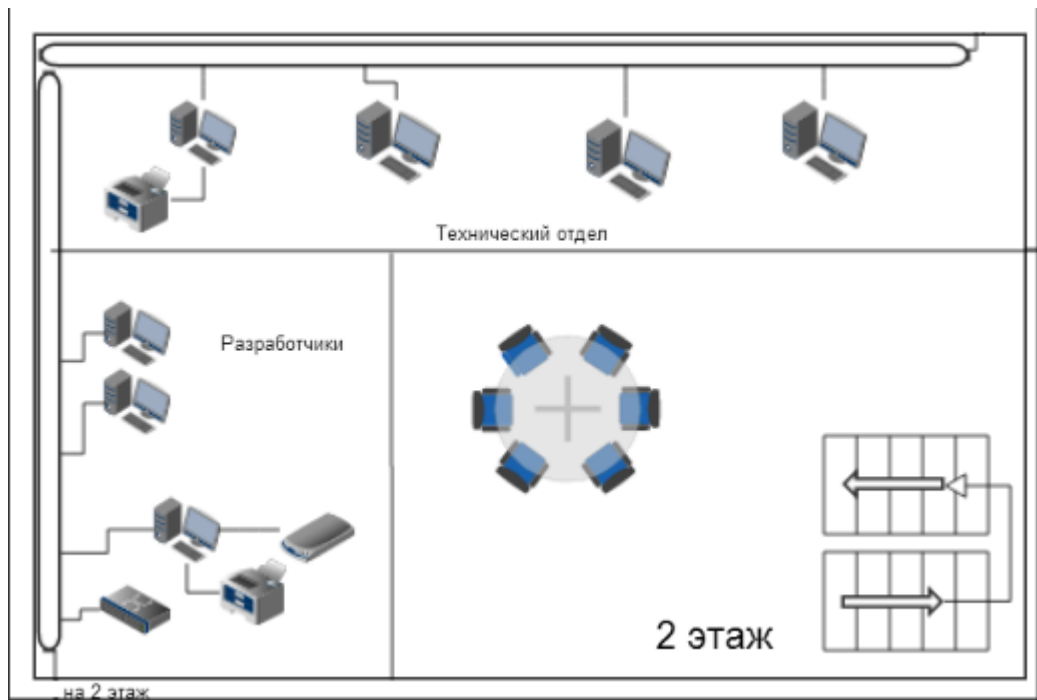


Рисунок 2.5 – Планирование сети на 2 этаже

2.2.1 Выбор топологии сети и методов доступа

Мною выбрана топология сети – звезда, технология – NGN.

Звезда - базовая топология сети, в которой все сетевые компьютеры подключены к центральному узлу (обычно переключатель) формирования физического сегмента сети. Такой сегмент сети может работать как по отдельности, так и в условиях сложной топологии сети (как правило, "дерево"). Вся информация обменивается исключительно через центральный компьютер, который, таким образом, лежит очень большая нагрузка, так что ничего, кроме сети, он не может справиться. Как правило, центральный компьютер является самым мощным, и оно несет в себе функции валютного контроля. в сети с звездообразной топологии Никаких конфликтов не возможна, в принципе, потому что управление полностью централизованы.

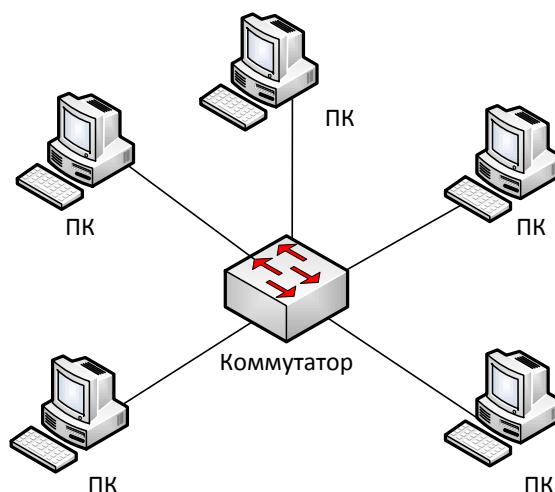


Рисунок 2.6 – Топология сети – Звезда

2.2.2 Планирование IP адресации

Таблица 2.2 – Планирование IP – адресации на предприятии

Отдел	IP – адрес/Маска	Шлюз
Reception	192.168.2.2 – 4/24	192.168.2.1
Юридический отдел	192.168.2.5 – 11/24	192.168.2.1
Отдел кадров	192.168.2.12 – 16/24	192.168.2.1
Бухгалтерия	192.168.2.17 – 21/24	192.168.2.1
Разработчики	192.168.2.22 – 41/24	192.168.2.1
Технический отдел	192.168.2.42 – 81/24	192.168.2.1
Инженерный отдел	192.168.2.82 – 111/24	192.168.2.1

2.2.3 Выбор сетевой операционной системы. Выбор программного обеспечения для защиты информации

Связывая программные компоненты включают в себя операционные системы и сетевые приложения или сетевые службы. Сетевая операционная система - это основа любой компьютерной сети.

Сетевая операционная система необходима для управления потоком сообщений между рабочими станциями и серверами. Это может позволить любой рабочей станции работать с совместно используемой сетевой диск или принтер, который физически не подключен к станции.

Потребуется сетевая операционная система, обеспечивающая разделение ресурсов в сети. Сетевая ОС определяет "язык", на котором общаются между собой сетевые устройства. Сетевые средства могут быть встроены в операционную систему (например, Apple или UNIX) или добавляться к ней как LANtastic или WindowsforWorkgroups.

Выбранная сетевая операционная система - **Windows Server 2008**.

Семейство Windows Server 2008 является следующим поколением

программного обеспечения Windows, серверных операционных систем. Windows Server 2008 основана на ОС Windows 2003Server. Это высокопроизводительная платформа для поддержки подключенных приложений, сетей и веб-служб XML для рабочих групп, отделов и предприятий любого размера.

В WindowsServer 2008, администраторы могут установить минимальную необходимую среду для определенных ролей. Это также повышает безопасность сервера (уменьшение поверхности атаки), снизить затраты на управление, а также потребности в ресурсах. Для установки в режиме ServerCoreInstallation на жестком диске достаточно свободного места на 2 Гб. Я уверен, в ближайшее время, многие компании будут двухпроцессорных серверов (4 или 8-ядерный), виртуальному с программным обеспечением, которое будет вращаться два или четыре режима ServerCoreInstallation WindowsServer 2008, каждый со своей ролью.

В режиме ServerCoreInstallation можно инсталлировать роли:

- Active Directory Domain Services.
- Active Directory Lightweight Directory Services (AD LDS).
- DHCP Server.
- DNS Server.
- File Services.
- Print Server.

Для администратии и фильтрации Интернета используем программу UserGate.

Данный набор программ позволяет наладить эффективную работу на автоматизированных рабочих местах, а также обеспечить их безопасность.

2.3 Описание UNetLab

Что такое UNetLab (Единая лаборатории УНЛ) является мультивендорной, и мульти-платформа для создания и моделирования различных лабораторий, и дизайн, который позволяет смоделировать виртуальную сеть из маршрутизаторов, коммутаторов, устройств безопасности и др. На момент разработки законопроекта-Интернет-завершается, разрабатывается только UNetLab и не замена оборудования для подготовки специальной инженерной сети, в том числе устранение неполадок. Это продолжение того же девелопера, который сделал Интернет-интерфейс для расписка. Это, по сути, убийца ГНС расписку и VIRT даже. Например, Cisco VIRT личная версия ограничена до 15 узлов, и набор устройств достаточно умеренная. Вы можете запустить столько экземпляров оборудования (маршрутизаторы, коммутаторы, устройства безопасности и т. UNetLab – совершенно безвозмездно) сколько хочешь и что хочешь. Например, полный как не похоже, и маршрутизатор с последовательным интерфейсом. Аппаратная поддержка в UNetLab чрезвычайно широк. Вы

сможете работать с Cisco ИОЛ изображений, изображений VIRL (vios-i vios L2-L3), ASA брандмауэр изображений (в качестве портативного 8.4(2), 9.1(5), официальные и Асав), изображения Cisco для предотвращения вторжений (IPS) на серии снимков серии xrv и CSR1000v, образы виртуальных машин с ГНС, образы Циско vWLC и vWSA, а также образы других производителей, таких как можжевельник, л. с., КПП и т. д. Когда пользователи запускают общий стенд независимо друг от друга. На той же ВМ, каждый авторизованный пользователь может сделать свои стенды независимо друг от друга, и работать вместе с общим щитом, который является общим для пары юзеров сразу. Кроме того, начиная с версии 0.9.54 UNetLab у любой многопользовательской функциональности. В настоящее время поддерживает следующий список оборудования:

- Aruba Clear Pass.
- Alcatel 7750 SR.
- Arista vEOS.
- Brocade Virtual ADX.
- Citrix Netscaler VPX virtual.
- Checkpoint Firewall.
- Cisco ASA (porting).
- Cisco ASA v.
- Cisco CSR 1000V.
- Cisco IPS (porting).
- Cisco IOS 1710/3725/7206 (dynamips, ethernet only).
- Cisco IOL (for Cisco internal use only).
- Cisco NX-OSv –titanium (for VIRL customers only).
- Cisco vIOS (for VIRK customers only).
- Cisco vIOS L2 (for VIRL customers only).
- Cisco XRv.
- Cisco WSA virtual appliance.
- Cisco Wireless controller – vwlc.
- Extreme Networks virtual.
- F5 BIG-IP LTM VE.
- Fortinet FortiGate (new).
- HP VSR1000.
- Juniper Olive (porting).
- Juniper Networks vMX router.
- Juniper vSRX.
- Palo Alto VM-100 Firewall.
- VyOS.
- MS Windows hosts.

Эта Платформа подходит для начинающих, чтобы подготовить для ссна/сспр и экспертов для подготовки CCIE маршрутизации и коммутации,

безопасности ССІЕ, услуги ССІЕ предусматривает, центров обработки данных, ССІЕ, и др. и для других различных инженерных задач. В отличие от предыдущего проекта, долговая расписка-Интернет, UNetLAB полностью реализованы топологии, графический интерфейс, что-то подобное сделать в СЦ. Теперь не нужно писать netmap файл для каждой топологии. Недостатком является полное отсутствие совместимости с предыдущим проектом. Файлы, собранные в топологии вексель-веб, необходимо переписать для УСЯ. Но в последней версии разработчики предоставляют скрипт, который поможет автоматизировать процесс. УНЛ также включены так называемые пользовательские топологии, т.е. кликабельные картинки красивые диаграммы, которые можно нарисовать в MS Visio и импортировать его в вашу лабораторию, как это было в долговая расписка-веб.

2.3.1 Построение сети на эмуляторе UNetLab

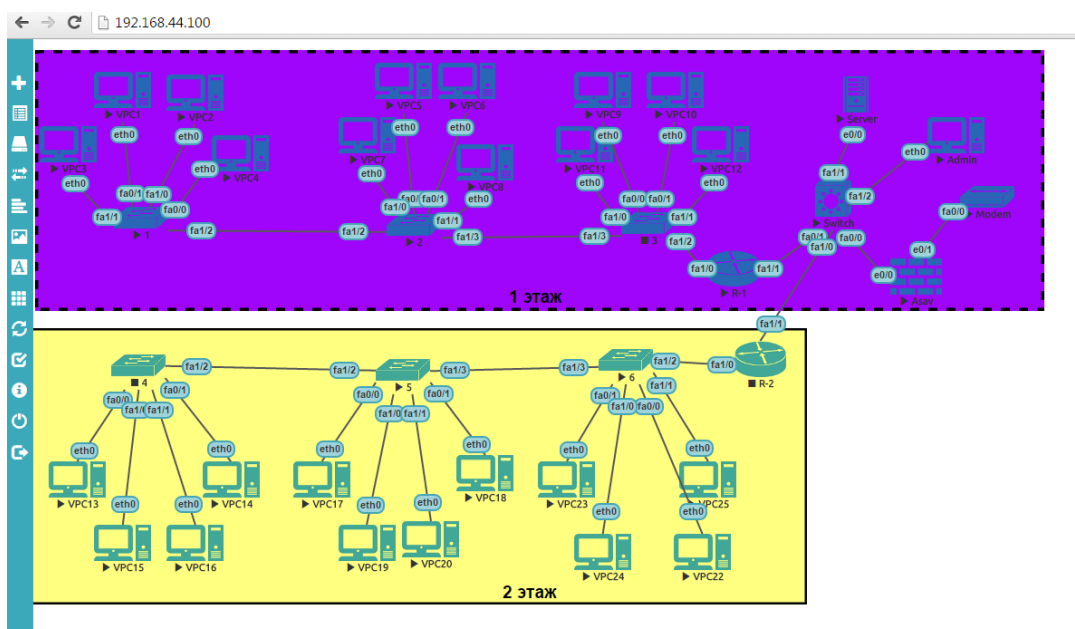


Рисунок 2.7 – Сеть на эмуляторе UNetLab

На данном рисунке 2.7 представлена построение сети на инновационном эмуляторе UNL.

2.4 Обеспечение информационной безопасности

Информационная безопасность - это процесс продвижения управления рисками, а не после него, то есть, предупреждая модель работает, прежде чем что-то случится.

В ответной модели общие затраты на безопасность неизвестны.

Общие затраты на безопасности равны стоимости ущерба от аварии, плюс стоимость контрмер. Правильное планирование и управление рисками позволит значительно сократить, если не исключить, количество ущерба, причиненного в результате инцидента. При принятии правильных мер противодействия для предотвращения подобных инцидентов в будущем стоимость будет составлять:

Общие затраты на безопасность = Стоимость контрмер.

Правильный подход к информационной безопасности - это предупреждение принять необходимые меры.

Информационная безопасность – это непрерывный процесс, который включает в себя пять основных шагов:

- 1) Оценку.
- 2) Политику.
- 3) Реализацию.
- 4) Квалифицированную подготовку.
- 5) Аудит.



Рисунок 2.10 – Обеспечение информационно безопасности

Индивидуально, каждый из этих этапов повышает уровень безопасности организации. И только вместе они составляют основу, которая позволит эффективно управлять рисками.

2.4.1 Оценка стоимости

Процесс оценки недвижимости начинается с обеспечения информационной безопасности, выявление информационных активов, угроз информации и уязвимости, значение общего риска для организации.

В зависимости от свойства и будет подготовлена программа защиты этих активов. После того, как риск определен и будет состоять из его количественная оценка, можно выбрать экономически эффективные контрмеры для снижения данного риска.

Цели оценки информационной безопасности:

- определить ценность информационных активов;
- определить угрозы для конфиденциальности, целостности, доступности и/или идентифицируемости этих активов;
- определить существующие уязвимые места в практической деятельности организации;
- установить риски организации в отношении информационных активов;
- предложить изменения в существующей практике работы, которые позволят сократить величину рисков до допустимого уровня;
- обеспечить базу для создания соответствующего проекта обеспечения безопасности.

Пять основных видов оценки:

1) Оценки уязвимости на уровне системы. Компьютерная система обследованы на наличие известных уязвимостей и элементарного соблюдения политики с техническими требованиями.

2) Оценка на уровне сети. Оценку существующей компьютерной сети и информационной инфраструктуры и определены зоны риска.

3) Общая оценка рисков внутри организации. Анализ всей организации для выявления угроз для информационных активов организации. Установлен уязвимостей в областях обработки информации по всей организации. Исследованная информация, представленная в электронном виде или на физическом носителе [3].

4) Аудит. Исследована существующая политика и соответствие организации этой политике.

5) Тест на проникновение. Способность организации реагировать на моделируемой проникновения.

При проведении оценки необходимо изучить следующие моменты:

- сетевое окружение;
- физические меры безопасности;
- существующие политики и процедуры;
- меры предосторожности, принятые на местах;
- осведомленность работников в вопросах безопасности;
- персонал;

- загруженность персонала;
- взаимоотношения работников;
- строгое соблюдение работниками установленной политики и мероприятий;
- специфику деятельности.

2.4.2 Сетевое окружение

Исследования сети начинают с построения сетевого графика и рассмотреть все точки возможного подключения, потому что в сети можно найти точки открытого доступа к информации и систем.

На сетевом графике должно быть полностью представлено местоположение серверов, рабочих станций, доступ в Интернет, подключений удаленного доступа, связь с удаленными офисами и партнерами. Исходя из данной схемы будем:

- тип и количество систем в сети;
- операционные системы и их версии;
- топология сети (коммутаторы, маршрутизаторы, мосты и т. д.)
- точки доступа к интернету;
- использование интернета;
- типы, количество и версии всех межсетевых экранов;
- точки входа соединений наборного доступа;
- беспроводные точки доступа;
- тип удаленного доступа;
- топология глобальной сети;
- точки доступа в удаленных офисах;
- точки доступа других организаций;
- расположение веб-серверов, FTP-серверов и почтовых шлюзов;
- используемые протоколы;
- лица, осуществляющие управление сетью.

Определение архитектуры сети, раскрываем внутренние механизмы защиты сети:

- списки управления доступом маршрутизаторов, правила межсетевых экранов на всех точках доступа в интернет;
- механизмы идентификации, используемые для удаленного доступа;
- защитные механизмы во всех точках доступа других организаций;
- механизмы шифрования, используемые для передачи и хранения информации;
- механизмы шифрования, используемые для защиты переносных компьютеров;
- антивирусные системы, установленные на серверах, рабочих станциях и службах электронной почты;

- настройки безопасности сервера.

Параметры безопасности сервера должны включать требования для паролей, параметры аудита для каждой системы, а также используемые обновления и системных программ. Далее, вам нужно собрать информацию о типах предупреждений и людей, которые следят за системой и сбор данных, которые могут быть полезны для выявления нарушителей в случае системных администраторов обнаружения вторжений. И, наконец, необходимо сканировать все системы с целью обнаружения уязвимостей. Это может быть сделано с помощью компьютера, расположенного внутри системы (внутреннее сканирование) или размещенный в сети Интернет, за пределами организации межсетевое экрана.

Физическая безопасность.

Физическая охрана помещений - самый важный компонент систем информационной безопасности. Определение физических мер безопасности включают в себя контроль физического доступа к управлений и департаментов и в тайных комнатах.

Поэтому, при определении мер физической безопасности необходимо выявить следующее:

- тип физической защиты здания, офисных помещений, документов на бумажных носителях и центра обработки данных;
- наличие ключей у персонала;
- засекреченные помещения здания или отдела (исключая центр обработки данных).

Необходимо определить расположение линий связи внутри помещений и в местах, где линии связи входят в здание, так как эти места идеально подходят для размещения подслушивающих устройств. Таким образом, эти точки должны быть включены в перечень критических областей, а также в помещениях, где это возможно отключение электричества.

Объекты физической безопасности также являются источниками энергии, система государственных систем управления и пожарной безопасности окружающей среды, используемых в центре обработки данных.

Соберите следующую информацию об этих системах:

- какую мощность потребляет подразделение;
- какую мощность потребляет центр обработки данных;
- какие типы источников бесперебойного питания установлены;
- как долго имеющиеся источники бесперебойного питания смогут поддерживать работоспособность системы;
- какие системы соединены с источниками бесперебойного питания;
- кто будет извещен в случае отключения электроэнергии;
- какая система контроля состояния окружающей среды подключена к источнику бесперебойного питания;

- какая система контроля состояния окружающей среды связана с центром обработки данных;
- кто будет извещен в случае выхода из строя системы контроля состояния окружающей среды;
- какой вид системы противопожарной безопасности установлен в центре обработки данных;
- может ли система противопожарной безопасности центра обработки данных среагировать на пожар, не угрожающий центру.

Политики и процедуры.

При проведении оценки должны быть исследованы следующие документы:

- политика безопасности;
- информационная политика;
- план восстановления в случае чрезвычайных происшествий;
- процедуры контрмер на чрезвычайное происшествие;
- политика и процедуры резервного копирования;
- справочное руководство работника или инструкции;
- процедуры найма-увольнения работников;
- принципы конфигурирования систем;
- правила межсетевых экранов;
- фильтры маршрутизатора;
- политика сексуальных домогательств на рабочем месте;
- политика физической безопасности;
- методология разработки программного обеспечения;
- методология смены программного обеспечения;
- телекоммуникационные политики;
- диаграммы сети;
- организационная диаграмма.

После получения вышеуказанных политик и процедур, каждая из которых исследовали на актуальность, законность, полноту и актуальность, поскольку политика и процедуры должны соответствовать цели, поставленной в документе. В изучении действия документа должны быть проверены на предмет соответствия каждому требованию установить цели или процедур в отношении политики.

Политика и процедуры могут стать устаревшими в течение долгого времени, в причине небрежности. Таким образом, вся политика и процедуры должны быть своевременно и разумно обновление.

При оценке необходимости изучения программы в области осведомленности о вопросах безопасности и материалов, используемых в соответствующей подготовки.

И, наконец, процедура оценки должна включать изучение информации о недавних инцидентов и инспекций.

Меры предосторожности.

Основными компонентами являются мерами предосторожности резервного копирования и план восстановления в случае чрезвычайных ситуаций и восстановления здорового состояния.

Осведомленность.

Осознание постоянных сотрудников по вопросам политики компании и процедур, а также практики надлежащих положений, касающихся безопасности, может значительно повысить безопасность организации.

Администратор должен знать политику компании в части конфигурации системы должны быть осведомлены об угрозах и уязвимостях, о признаках вторжения в систему. И самое главное, они должны знать, какие действия необходимо предпринять при обнаружении атаки.

Человеческий фактор.

Отсутствие навыков или, наоборот, их избыток сотрудников, может стать причиной отказа от хорошо продуманной программы безопасности. Персонал, отвечающий за вопросы безопасности, должен понимать свою работу в плане общей политики, а также для понимания последних событий в своей сфере. Администраторы должны иметь соответствующие навыки до высокого уровня для управления системой и сетевую среду в организации. Пользователи должны обладать базовыми навыками в области компьютерных технологий. И от аудиторов потребуются организация экспертизы систем и сетей в рамках своего рабочего задания.

Загруженность персонала.

Даже высококвалифицированные и опытные работники не смогут поддерживать безопасность, если они перегружены работой. С увеличением объема работы, первым делом следует забывать, вопросы безопасности.

Отношение.

Отношение административного персонала к безопасности определяется назначением лиц, ответственных за безопасность в рамках организации. Управление в полной мере осознает важность процессов безопасности, но если они не передают это своим сотрудникам, последний не поймут.

Следование правилам.

При составлении плана безопасной среде информации необходимо определить реальную обстановку в плане безопасности. Кино- установлен политику, правила и существующие механизмы. Фактическая среда определяется фактическое согласие участвовать в процессе руководителей служб безопасности и персонала.

Специфика деятельности.

И, наконец, изучить специфику организации и определить поток информации в нем, между отделами и рабочими местами внутри отдела и в других организациях. Узнайте, как это звенья в цепи информации находится под угрозой, как взаимосвязанных частей организации. В рамках процесса оценки заключается в выявлении систем и сетей, которые имеют решающее значение для выполнения основных функций организации.

Результаты оценки.

После сбора и анализа всей информации, группа оценки будет исследовать все уязвимости безопасности в контексте организации. Не все уязвимости превращаются в риски. Некоторые уязвимости защищены каким-либо образом, что бы предотвратить их использование.

После завершения анализа, группа по оценке требуется представить полный набор рисков и рекомендаций по организации. Риск в порядке - от самого большого до самого маленького. Для каждой группы риска показывает возможные затраты на любых условиях (деньги, время, ресурсы, потеря репутации, а также о прекращении сделки). Каждый риск должен сопровождаться рекомендацией по управлению рисками.

И последняя оценка шаг - это разработать план обеспечения безопасности действий. Организация должна определить, является ли оценки фактического состояния безопасности дисплея, и принимать их во внимание при распределении ресурсов и планы.

2.4.3 Разработка политики

После оценки необходимости рассматривать вопрос о разработке политики и процедур, которые определяют ожидаемый статус безопасности и перечень необходимых работ. Нет политики - нет никакого плана, на основании которого организация будет разрабатывать и осуществлять эффективную программу информационной безопасности [6].

Необходимо разработать следующие политики и процедуры.

- Информационная политика. Выявляет секретную информацию и способы ее обработки, хранения, передачи и уничтожения.

- Политика безопасности. Определяет технические средства управления для различных компьютерных систем.

- Политика использования. Обеспечивает политику компании по использованию компьютерных систем.

- Политика резервного копирования. Определяет требования к резервным копиям компьютерных систем.

- Процедуры управления учетными записями. Определяют действия, выполняемые при добавлении или удалении пользователей.

- Процедура управления инцидентом. Определяет цели и действия при обработке происшествия, связанного с информационной безопасностью.

- План на случай чрезвычайных обстоятельств. Обеспечивает действия по восстановлению оборудования компании после стихийных бедствий или инцидентов, произошедших по вине человека.

Порядок разработки политик.

В зависимости от рисков, выявленных в процессе оценки, то получается, что политика должна быть разработана в первую очередь.

Время, затраченное - еще один фактор в порядке выбора разработки политики.

Информационная политика – единственная политика, которая должна быть разработана на начальной стадии процесса

Информационная политика формирует основу для понимания того, почему внутренняя информация важна и как она должна быть защищена. Этот документ будет служить основой для программы подготовки специалистов безопасности, наряду с использованием политики и политики паролей.

Возможности и разработка ряда стратегий в качестве заинтересованных сторон будут объединены общими интересами.

2.4.4 Реализация политики безопасности

Она заключается в применении технических средств и непосредственного контроля, и отбора персонала безопасности. Может потребоваться изменения в конфигурации системы, которые находятся вне компетенции отдела безопасности, поэтому проводить программу по безопасности должны включать в себя системных и сетевых администраторов.

Необходимо исследовать каждый этап для определения взаимодействий с другими системами управления.

Системы отчетности по безопасности.

Это механизм, с помощью которого служба безопасности следит за соблюдением политики и процедур, общее состояние уязвимости в рамках организации. Для этой цели, как ручные и автоматизированные системы.

Мониторинг использования.

Механизмы мониторинга будут обеспечивать, чтобы сотрудники следовать политике с помощью компьютера. Они включают в себя программное обеспечение, которое отслеживает использование Интернета. Цель состоит в том, чтобы выявить работников, постоянно нарушая политику компании. Некоторые механизмы способны блокировать такой доступ, и пытается сохранить журнал.

Сканирование уязвимых мест систем.

Установка операционной системы с настройками по умолчанию, как правило, сопровождается запуском ненужных процессов и появление уязвимостей. Для обнаружения этих уязвимостей легко, но гораздо труднее исправить, так что информация о вновь установленных систем должны быть привлечены к системному администратору немедленно.

Аутентификация систем.

Этот механизм предназначен для определения подлинности пользователей, желающих получить доступ к системе или сети. Она также позволяет идентифицировать людей, которые пытаются взять на себя организацию оборудования. Проверка подлинности Механизмы - это пароли, смарт-карты и биометрические.

Безопасность в интернете.

Межсетевые экраны и виртуальные частные сети (VPN) осуществление сетевой безопасности и привести к изменениям в сетевой архитектуре.

Наиболее важным аспектом внедрения является установка контроля доступа устройства (например, брандмауэр) между Интернетом и внутренней сетью организации. Без такой защиты все внутренние системы открыты для бесконтрольного нарушения безопасности.

Размещение брандмауэра или другого устройства контроля доступа приводит к изменению архитектуры. Эта операция не должна выполняться до тех пор, пока будет определяться базовую архитектуру сети: необходимо установить межсетевой экран соответствующую мощность и установить его в соответствии с правилами, используемыми политикой организации.

Системы обнаружения вторжений (IDS).

Эта сеть охранной сигнализации. Охранная сигнализация предназначена для обнаружения попыток вторжения в защищенной зоне, и IDS - провести различие между уполномоченным въездом и вторжением нарушителя в защищенной сети.

Имеется несколько типов систем обнаружения вторжения.

Самым распространенным механизмом обнаружения вторжений является антивирусное программное обеспечение. Это программное обеспечение должно работать на каждой рабочей станции, и конечно же на сервере. Антивирусное программное обеспечение - наименее ресурсоемкий способ обнаружения вторжений.

Перечислим другие способы обнаружения вторжений:

- ручная проверка журнала;
- автоматическая проверка журнала;
- клиентское программное обеспечение для обнаружения вторжения;
- сетевое программное обеспечение для обнаружения вторжения.

Лучший способ проверить это, чтобы войти создание программ или сценариев, сканирование компьютера журналы в поисках возможных отклонений.

Шифрование.

Шифрование обычно используется для защиты чувствительных или частных интересов и используется для защиты, передаваемой или хранимой информации. давайте рассмотрим, прежде чем использовать шифрование, какие алгоритмы и управления ключами для защиты.

Когда выбор алгоритма шифрования управляется конечной цели. Шифрование секретного ключа быстрее, чем на открытом воздухе. Тем не менее, этот метод не позволяет использовать цифровую подпись или подписи информации. Важно выбрать хорошо известные и хорошо изученные алгоритмы. Эти алгоритмы, более вероятно, чтобы устранить лазейки, через которые вы можете получить доступ к защищенной информации.

Развертывание механизмов шифрования должна включать в себя управление ключа безопасности. При использовании блочного шифра (шифрования устройства для трафика, передаваемого от узла к узлу), система должна позволять периодическое изменение ключа. Система управления ключами безопасности должна быть соразмерна всей системы.

Персонал.

При применении каких-либо новых систем безопасности, вы должны иметь соответствующий персонал. Вам потребуется обученный штат сотрудников в проведении образовательных программ по повышению осведомленности.

Проведение профессиональной переподготовки.

Организация не может обеспечить защиту конфиденциальной информации, не привлекая своих сотрудников. Грамотная профессиональная переподготовка - механизм для обеспечения сотрудников с необходимой информацией.

Сотрудники.

Сотрудники должны знать, почему безопасность настолько важна, должны быть подготовлены в целях выявления и защиты конфиденциальной информации. Грамотная профессиональная переподготовка безопасности предоставляет им необходимую информацию в области политики, выбора пароля и предотвращения поломки техники[5].

Администраторы.

Они должны знать о прошлом в настоящий момент технические приемы хакеров, угроз безопасности и обновлений продукта. Это обучение должно происходить часто (возможно, один раз в месяц) и осуществляется отделом безопасности.

Разработчики.

Образование для развития должна быть расширенной версией учебных занятий для сотрудников. Дополнительный материал включает в себя конкретные методы технического программирования для устранения уязвимостей и адекватного понимания роли отдела безопасности в процессе развития.

Руководители.

Презентация для руководителей организации - это своего рода и обучение, и маркетинг. Без поддержки программы по безопасности управления просто не может существовать. Поэтому управление должно быть проинформировано о ситуации в области безопасности и о дальнейшем развитии программы.

Персонал отдела безопасности.

Сотрудники службы безопасности должны быть осведомлены о текущем состоянии дел с тем, чтобы должным образом выполнять свою работу.

2.4.5 Проведение аудита

Аудит - это последний шаг в реализации информационной безопасности. Он определяет состояние информационной безопасности в рамках организации, создание соответствующей политики и процедур, приведения в действие технических средств контроля и обучения. В свою

очередь, это позволит убедиться, что все элементы управления настроены правильно.

Обсуждая место аудита в процессе безопасности, выделим три функции:

- аудит соблюдения политики;
- периодическая оценка существующих проектов и оценка новых проектов;
- проверка возможности нарушения защиты.

Аудит соблюдения политики.

Аудит определяет реальное состояние дел. Любые отклонения отмечаются как нарушения. Он должен проявлять интерес к тому, как выполняются другие формы управления информацией. Соблюдается ли информационная политика? Как хранятся и передаются секретные документы?

Периодическая оценка проектов и оценка новых проектов.

Компьютеры и сетевое окружение внутри организации находятся в постоянном состоянии изменения, что приводит к быстрому старению результатов оценки за счет снижения некоторых рисков и внедрения новых. По этой причине, оценка должна проводиться периодически.

Небольшие оценки должны проводиться в случае разработки новых проектов или изменений в организационной среде. Проверки должны проводиться на стадии проектирования, чтобы определить, является ли какой-либо из рисков проекта, и есть ли результат развития проекта появление или уменьшить риски в рамках организации.

Проверка возможности нарушения защиты.

Они имеют ограниченную ценность в программе безопасности в связи с тем, что в тестах пытаются использовать установленные уязвимости для получения доступа к информационным системам, а также в рамках организации. Если этот тест, то единственный вывод из всего этого - обнаружено, по крайней мере, одну уязвимость. Если тест не нарушение безопасности, вывод - проверяет, не смогли обнаружить и использовать эту уязвимость. Но это вовсе не означает, что уязвимость не существует.

Проверка защиты подходит для следующих случаев.

- способность системы обнаружения вторжений выявить попытку нарушения защиты;
- уместность процедуры реагирования на инцидент, связанный с безопасностью;
- информация о сети, которую можно узнать через средства управления сетевым доступом;
- уместность физической безопасности помещения;
- адекватность информации, предоставляемой сотрудникам программой повышения осведомленности в плане безопасности.

3 Безопасность жизнедеятельности

3.1 Анализ условий труда технического персонала

В дипломной работе мы проводим анализ трафика сети NGN. В начале тезиса раскрывают NGN архитектуру сети, а затем рассмотреть мультимедиа и голосового трафика. В научно-исследовательской работе, мы анализируем голосового трафика в сети NGN. В начале это определение трафика и его основных вариантов СПП. Одним из основных отличий от концепции NGN реализуется в этой сетевой инфраструктуре является переход к принципиально иной функциональной модели. Это очень распространенная сеть, поэтому, для большей ясности, блок-схемы и состав оборудования. Анализ трафика, чтобы определить его самой простой. NGN сетевых приложений входящий поток существенно отличается от Пуассона (самый простой). Для этого параметра потока была рассчитана с использованием Pascal программы, где мы показали, что поток не является простым. Далее мы анализируем характеристики сети NGN со значительным увеличением объема трафика и определяет, к какой группе абонентов отправляется самый большой трафик.

Для анализа статистики трафика, обязательны для заполнения оператор, взятый с персонального компьютера. Для нормальной работы компьютера необходим постоянный ток, а вход блока питания (БП) подается переменное напряжение 220 В. Блок питания переменного тока преобразуется в постоянный ток. Средняя мощность современных ВР составляет от 300 до 500 Вт.

БП вырабатывает следующие напряжения:

- основное стабилизированное напряжение +5 В (сила тока 10–50А);
- (+12) В (сила тока 3,5–15А) – для питания двигателей устройств и интерфейсных цепей;
- (–12) В (сила тока 0,3–1А) – для питания интерфейсных цепей;
- (–5) В (сила тока 0,3–0,5А) – обычно не используется, оставлено для совместимости со стандартом ISA Bus);
- (+3,3) В – для питания ОЗУ.

В большинстве случаев, полумостовой импульсный источник питания. Импульсный источник питания - регулятор напряжения, в котором блок управления работает в режиме переключения, то есть большую часть времени он либо в режиме отсечки, когда сопротивление является максимальным, или режим насыщения - с минимальным сопротивлением, и, таким образом, может рассматриваться в качестве ключа. Плавное изменение напряжения происходит из-за наличия интегрирующего элемента: напряжение возрастает по мере накопления энергии и уменьшается, когда он возвращается к

нагрузке. Этот режим работы позволяет существенно снизить потери энергии и повысить вес и габаритные размеры.

Помещение, для которого будут производиться расчеты, представляет собой операторскую комнату. Работают 6 человек: 3 сменных оператора. В дневную смену работают 3 человека : старший инженер и 2 инженера. Операторская находится на первом этаже, которая имеет размеры: длина $L=8$ (м), ширина $B=5$ м, высота $H=4$ м. Здание расположено в г. Алматы, который имеет 44 географическую широту. На южной стороне операторской расположены 2 окна шириной 2.2 м и высотой 2.5 м каждое.

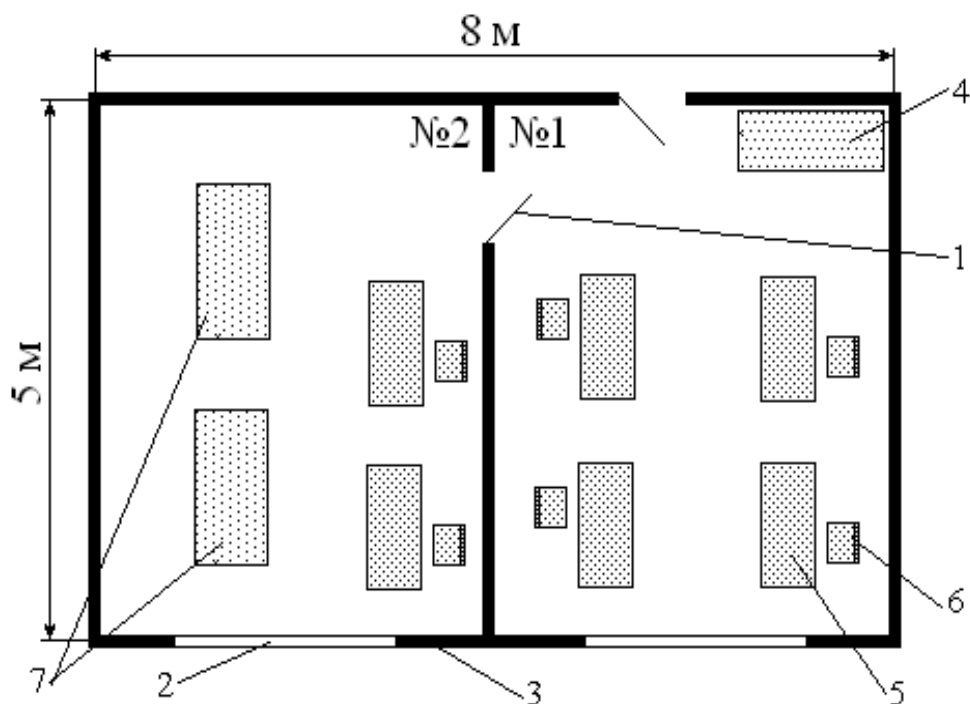


Рисунок 3.1 – План помещения

1- дверь; 2 – окно; 3 – стена; 4 – шкаф; 6 – стол; 6 – стул; 7 – стойки.

Компания установила восьмичасовой рабочий день. В соответствии со статьей 1 Закона РК «О труде в РК» рабочее время - время, в течение которого работник в соответствии с актами работодателя и условиями индивидуального трудового договора выполняет трудовые обязанности. Акты работодателя или коллективным договором могут быть установлены 5-ти дневной или 6 дневная рабочая неделя. По продолжительности рабочей недели шесть дней ежедневной работы не может превышать 7 часов, пятидневная рабочая неделя - 8 часов. Рабочий день нормальной длины предназначен для рабочих и служащих, работающих в условиях, которые не требуют высокой физической и нервно-интеллектуального напряжения. Зрительные персональные компьютеры имеют разряд IV (б).

Для искусственного освещения используется люминесцентная газоразрядных ламп LD мощность 40 Вт и номинальным световым потоком

3120 лм / л. По мере того как лампы будут использовать приборы, такие как низко-2h40-1001.Dlya поддерживать необходимый микроклимат. Оператор 6 рабочих столов, которые расположены на персональных компьютерах, необходимых для работы операторов. Рисунок 3.1 представляет собой план этажа.

При непрерывной работе с компьютером работник часто начинает испытывать некоторый дискомфорт: у него возникают головные боли и боли в глазах появляются усталым и раздражительным. У некоторых людей, нарушение сна, ухудшение зрения, начинают болеть руки, шеи, нижней части спины, и тому подобное. Для того чтобы минимизировать этот дискомфорт, необходимо организовать рабочее место право. Особенно важно, чтобы обеспечить необходимое освещение, как природные, так и искусственные.

В операторской работы проводятся по 1,а категории работ. Микроклиматические условия согласно ГОСТ 12.0.003-74. ССБТ можно охарактеризовать как оптимальные (таблица 5.1), [20]:

Таблица 3.1 – Оптимальные нормы параметров микроклимата

Период работы	Категория работы	T, °C	Скорость движения воздуха, м/с, не более
Холодный	I б	31-23	0,1
Теплый	I б	22-24	0,2

Он должен быть размещен таким образом, чтобы рабочие столы мониторы были ориентированы на сторону окон в крыше, чтобы позволить естественный свет падает в основном на левой стороне. Искусственное освещение особенно необходимо в вечернее время.

Кроме того, долгосрочные операции зависит от состояния окружающего воздуха в рабочем помещении. Организм человека постоянно находится в эксплуатации теплообмен с окружающей средой. На тепловое состояние организма зависит от климатических параметров, а также физические упражнения - масштабы и интенсивность мышечной работы, связанные с трудовой деятельностью. Тяжесть физического труда определяется общее потребление мощности. В настоящее время широко реализованного оператора энергии на единицу профессий время истекло 80...200 Вт.

3.2 Выбор системы освещения рабочих мест. Расчет производственного освещения

3.2.1 Расчет естественного освещения

Помещения с постоянным пребыванием людей должны иметь естественное освещение.

При проектировании новых помещений, реконструкция старых, с конструкцией естественного освещения судна и других объектов, необходимых для определения площади световых проемов, обеспечивая нормированное значение КЕО в соответствии с требованиями СНиП РК 2.04 - 05-2002 "Естественное и искусственное освещение. Нормы проектирования» [10].

Помещения с постоянным пребыванием людей должны иметь естественное освещение. Длина комнаты $L = 4$ м, ширина комнаты $B = 5$ м, комната высота $H = 4$ м. Высота рабочей поверхности над полом $H_p = 0,75$ м. Источники света газоразрядные лампы. Номинальная мощность - 40 Вт, световой поток - 3120 лм.

В номере есть два окна шириной 2,2 м и 2,5 м в высоту каждая. Нижний край окна начинается на уровне 1,5 м над уровнем пола. Окна расположены на одной стороне комнаты, глубина $L = B-1 = 3$. Ранг зрительной работы IV, б. Рядом находится жилой 1-этажный жилой дом, расположенный на расстоянии $P = 60$ м. План производственных мощностей показан на рисунке 3.1. Так как оба помещения одного и того же размера, и того же размера, что и окна.

Нормированные значения КЕО приводятся для III пояса светового климата формуле:

$$e_{н}^{IV} = e_{н}^{III} * m \quad (3.1)$$

где $e_{н}^{III}$ - значение КЕО III пояса;

$$e_{н}^{III} = 1,2;$$

m – коэффициент светового климата, для IV пояса $m = 0,9$.

Значение КЕО с учетом коэффициентов m равно:

$$e_{н}^{IV} = 1,2 \cdot 0,9 = 1,08 [\%].$$

Коэффициент естественного освещения зала рассчитаем по формуле:

$$e_{н} = \frac{100 \cdot S_0 \cdot \tau_0 \cdot r_1}{S_{п} \cdot \eta_0 \cdot K_{з} \cdot K_3}, \quad (3.2)$$

где S_0 – суммарная площадь боковых световых проёмов, $S_0 = 3,79$ м²;

$S_{п}$ - площадь пола помещения (м²), $e_{н}$ - нормированное значение КЕО; K_3 - коэффициент запаса, $K_3 = 1,2$ при естественном боковом освещении;

$\tau_0 = \tau_1 * \tau_2 * \tau_3 * \tau_4$ - общий коэффициент светопропускания;

η_0 - световая характеристика окон;

r_1 - коэффициент, учитывающий повышение КЕО при боковом освещении благодаря свету, отраженному от поверхностей помещения и подстилающего слоя, прилегающего к зданию;

$k_{зд}$ - коэффициент, учитывающий затенение окон противостоящими зданиями.

Площадь пола помещения:

$$S_{\cdot} = L \times B = 4 \times 5 = 20 \text{ (м}^2 \text{)}.$$

В качестве прозрачного материала используется деревянная рама Двустворчатые стеклопакеты, как несущих конструкций из железобетона используются фермы и арки. В этом случае коэффициент τ_0 равен:

$$\tau_0 = 0,8 * 0,6 * 0,8 = 0,384 .$$

Для определения соотношения η_0 необходимо знать соотношение длины к глубине (точка самый дальний от окна). Поскольку окна расположены только с одной стороны, это отношение:

$$\frac{L}{l} = \frac{4}{3} = 1,33 .$$

Также необходимо знать отношение l/h_1 , где h_1 - высота от уровня условной рабочей поверхности до верха окна.

$$h_1 = h_{ок} + h_{н.ок} - h_{пов},$$

$$h_1 = 2,5 + 1 - 0,75 = 2,75 \text{ (м)}.$$

Таким образом, отношение B/h_1 равно:

$$\frac{B}{h_1} = \frac{4}{2,75} = 1,45 .$$

Для найденных отношений определяем, что коэффициент η_0 равен $\eta_0 = 10,5$.

Для определения коэффициента r_1 необходимо также знать соотношение l/B , где l - расстояние расчетной точки от наружной стены при боковом одностороннем освещении. Для данного случая для самой удаленной от окна точки можно принять $l=3$, в этом случае данное отношение равно 1.

Приняв коэффициент $\rho_{-p} = 0,5$, найдем коэффициент r_1 , который равен: $r_1=2,1$.

Для определения коэффициента $K_{зд}$ определим высоту близлежащего дома. Для этого условно примем с учетом межэтажных перекрытий приходится 3,5 м, а на чердак приходится 2 м. Таким образом высота здания равна $H = 3,5 + 2 = 5,5$ м.

Определим высоту расположения карниза противостоящего здания над подоконником рассматриваемого окна, если рабочее помещение находится на первом этаже. Тогда:

$$H_{к\ddot{у}б} = 5,5 - 1 = 4,5 \text{ (м)}.$$

Коэффициент $k_{зд}$ определяется по соотношению $P/H_{зд}$, которое в данном случае равно:

$$P/H_{к\ddot{у}б} = \frac{60}{4,5} = 3,125.$$

Из данного соотношения определяем, что $k_{зд}=1$.

И так, подставляя числовые значения в формулу (4.2) получаем:

$$e_n = \frac{100 \cdot 3,79 \cdot 0,384 \cdot 2,1}{20 \cdot 10,5 \cdot 1 \cdot 1,2} = 1,2128.$$

Сравниваем $e_n > e_n^{IV}$. Следовательно площадь окон обеспечивает нормированное освещение. Так как режим работы является круглосуточной работой необходимо будет рассчитать искусственное освещение.

3.2.2 Расчет искусственного освещения

Для помещений, в которых предусматриваются общее равномерное освещение горизонтальных поверхностей, освещение рассчитывают методом коэффициента использования светового потока. Длина комнаты $A=4$ м, ширина комнаты $B=5$ м, высота $H=4$ м. Высота рабочей поверхности над уровнем пола $h_p=0,8 - 1$ м. Расстояние от светильника до перекрытия $h_c=0 - 1,5$ м. План производственных помещений приведен на рисунке 3.1.

Данный метод заключается в определении значения коэффициента η , равного отношению светового потока падающего на расчетную поверхность, к полному потоку осветительного прибора.

Значение коэффициента η находится из таблиц, связывающих геометрические параметры помещений (индекс помещений i) с их оптическими характеристиками (коэффициентами отражения потолка $\rho_{пот}$, стен $\rho_{ст}$ и пола $\rho_{п}$

Индекс помещения i определяется по формуле (3.4):

$$i = \frac{A * B}{h * (A + B)}, \quad (3.4)$$

где A - длина помещения;

B - ширина помещения, $h = H - h_c - h_p$ - расчетная высота.

Определим значение h :

$$h = 4 - 0 - 0,8 = 3,2 \text{ (м)}.$$

При найденном значении расчетной высоты определяем индекс помещения:

$$i = \frac{4 * 5}{3,2 * (4 + 5)} = 0,69.$$

Значения коэффициентов отражения примем следующими:

$$\rho_{\text{пот}} = 70 \text{ (\%)}, \rho_{\text{ст}} = 50 \text{ (\%)}, \rho_{\text{п}} = 30 \text{ (\%)}.$$

Для найденного индекса помещения и выбранных значений коэффициентов отражения по таблице “Значения коэффициента использования светового потока определяем коэффициент η , который равен: $\eta = 28 \text{ (\%)}$.

Для освещения помещений будем использовать люминесцентные газоразрядные лампы ЛД мощностью 40 Вт и номинальным световым потоком 3120 лм.. В качестве светильников будем использовать светильники типа ЛОУ-2x40-1001. В каждый светильник устанавливается по две лампы. С учетом вышесказанного можно определить количество светильников по формуле (3.5).

$$N = \frac{E * k_3 * S * z}{n * \Phi_{\text{л}} * \eta}, \quad (3.1)$$

где E – освещенность, для IV (б) разряда работ нормируемая освещенность по таблице 3.12 [9] – 200 лк;

k_3 - коэффициент запаса;

S - площадь помещения;

$z=1,1 \div 1,2$ - коэффициент неравномерности освещения;

n - число ламп в светильнике;

$\Phi_{\text{л}}$ - световой поток одной лампы;

η - коэффициент использования.

Для помещений общественных зданий (рабочих помещений) при искусственном освещении газоразрядными лампами, исходя их СНиП РК 2.04-05-2002, коэффициент запаса $K_3 = 1,2$.

Площадь рассматриваемого помещения равна: $S=A*B=4*5=20$ [м²].

Число светильников равно:

$$N = \frac{200 * 1,2 * 20 * 1,1}{2 * 3120 * 0,28} = 3 \text{ (шт.)}$$

Рассчитаем расстояние между светильниками по формуле:

$$L_{A,B} = \lambda \cdot h_p$$

Примем $\lambda = 1,2$, тогда:

$$L_a = 1,2 \cdot 3,2 = 3,84 \text{ м.}$$

Далее найдем расстояние до стены по следующей формуле:

$$l_{a,b} = (0,3 \div 0,5) \cdot L_{A,B} \tag{3.6}$$

$$l_a = 0,5 \cdot 3,84 = 1,92 \text{ м}$$

Расстояние L_A в нашем случае отсутствует, так как имеется всего 3 светильника. Расстояние l_b примем равным 1,4 м, так как длина светильника составляет 1,2 м, ширина помещения равна 5 м. Схема размещения светильников приведена на рисунке 4.2.

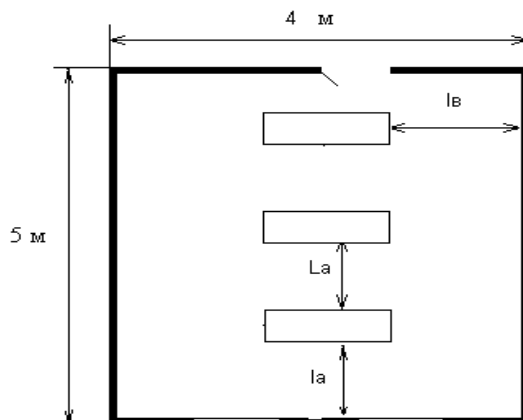


Рисунок 3.2 – Схема размещения светильников

3.3 Расчет системы кондиционирования

В операторском помещении находится 6 рабочих места (мужчин - 3, женщин - 3). Для поддержания необходимого состояния воздушной среды используется система кондиционирования воздуха. Для правильного выбора кондиционера необходимо:

- рассчитать тепловые нагрузки в помещении внутренние и наружные;
- рассчитать количество воздуха, необходимого для подачи в помещение;
- по найденному значению количества воздуха подобрать соответствующую модель кондиционера.

Определим внутренние тепловые нагрузки в помещении. В первую очередь определяем теплопоступления от оборудования. В операторской имеется 6 персональных компьютера (ПК) мощностью 0,5 кВт/ч. Теплопоступления определим по формуле:

$$Q_{об} = P_{об} \cdot \eta, \quad (3.7)$$

где $P_{об}$ – мощность, потребляемая оборудованием кВт/ч;

η - коэффициент перехода в помещение тепла, для ПК $\eta = 0.86$.

Общая мощность равна:

$$P_{об} = 6 \cdot 0.5 = 3, \text{ кВт}.$$

Теплопоступления от оборудования:

$$Q_{об} = 3 \cdot 0.86 = 2.58, \text{ кВт}.$$

Теплопоступления от ламп определяются по формуле:

$$Q_{осв} = \alpha \cdot N_{осв} \cdot \beta \cdot \cos \varphi, \quad (3.8)$$

где α - коэффициент перехода электрической энергии в тепловую, для люминисцентных ламп $\alpha = 0,7$;

$\cos \varphi = 0,7$;

$N_{осв}$ - мощность лампы, хорошего освещения помещений

$$N_{осв} = 40 \text{ Вт/м}^2;$$

$$Q_{осв} = 40 \cdot 3 \cdot 2 \cdot 0.7 \cdot 0.7 \cdot 1 = 117.6 \text{ Вт}.$$

Теплопоступления от людей определим следующим образом:

$$Q_{л} = n \cdot q_{явн}, \quad (3.9)$$

где $q_{\text{явн}}$ - явное тепло от человека, принято считать, что женщины выделяют 85 % тепла от нормы тепло выделений взрослого мужчины (положение сидя) для теплого периода – 61 Вт, для холодного периода – 82 Вт;

n – количество людей (мужчин – 3; женщин – 3).

На летний период теплоступления от людей будут равны:

$$Q_{\text{л}} = (3 \cdot 61 + 3 \cdot 61 \cdot 0,85) = 0,334 \text{ кВт.}$$

Также по формуле (3.3) рассчитаем теплоступления от людей в зимний период:

$$Q_{\text{л}} = (3 \cdot 82 + 3 \cdot 82 \cdot 0,85) = 0,455 \text{ кВт.}$$

Учитывая параметры и расчеты, приведенные в пункте 3.2.1, определим теплоступления от солнечного излучения через остекление по формуле:

$$Q_p = m \cdot F(q^I + q^{II})\beta \cdot K_1 \cdot K_2 \quad (3.10)$$

где m - количество окон в помещении, 2;

F - площадь окон, $F = 5,5 \text{ м}^2$;

β - коэффициент теплопропускания для штор и жалюзей - 0,15 (таблица 4 в [10]);

q^I, q^{II} - тепловые потоки от прямой и рассеянной радиации Вт/м^2 , принимаются для расчетного часа суток в зависимости от географической широты, равны соответственно для Ю – 288 и 85 (таблица 5 в [1]);

K_1 – коэффициент затемнения остекления деревянными переплетами - 0,65 (таблица 6 в [1]);

K_2 – коэффициент для умеренного загрязнения остекления, 0,9 (таблица 7 в [1]).

$$Q_p^{Ю} = 2 \cdot 5,5 \cdot 0,15 \cdot 0,65 \cdot 0,9 \cdot (288 + 85) = 0,360, \text{ кВт};$$

Теплоступления и теплопотери в результате разности температур:

$$Q_{\text{отд}} = V_{\text{ном}} \cdot X_0 \cdot (t_{\text{в}} - t_{\text{н}}) \quad (3.11)$$

где $t_{\text{в}}$ - температура внутреннего помещения, $20 \text{ }^{\circ}\text{C}$;

$t_{\text{н}}$ - наружная температура воздуха, $(-26) \text{ }^{\circ}\text{C}$;

$V_{\text{ном}}$ - объем помещения, м^3 (длина – 4, ширина – 5 м, высота – 4 м);

X_0 – удельная тепловая характеристика, $0,42 \text{ Вт/м}^3 \text{ }^{\circ}\text{C}$.

$Q_{отд} = 0$ – для теплого периода времени.

$$Q_{отд} = 4 \cdot 5 \cdot 4 \cdot 0,42 \cdot (20 - (-26)) = 1,545, \text{ кВт}.$$

Определим тепловой баланс в помещении:

$$Q_{изб} = Q_{об} + Q_{осв} + Q_{л} + Q_{р} - Q_{отд} \quad (3.12)$$

Для летнего периода тепловой баланс равен:

$$Q_{изб.летн} = 2,58 + 0,117 + 0,334 + 0,360 - 0 = 3,391, \text{ кВт}$$

Для зимнего периода:

$$Q_{изб.зимн} = 2,58 + 0,117 + 0,455 + 0,360 - 1,545 = 1,967, \text{ кВт}$$

Теплонапряженность воздуха:

$$Q_n = \frac{Q_{изб} \cdot 860}{V_n}, \quad (3.13)$$

$$Q_n \leq 20 \text{ ккал/м}^3 \Rightarrow \Delta t = 6 \text{ } ^\circ\text{C};$$

$$Q_n > 20 \text{ ккал/м}^3 \Rightarrow \Delta t = 8 \text{ } ^\circ\text{C}.$$

Учитывая, что $Q_{изб.лет} > Q_{изб.зим}$, то для расчета будем использовать $Q_{изб}$ для летнего периода:

$$Q_n = \frac{3,391 \cdot 860}{80} = 36,45 \text{ ккал/м}^3.$$

Так как $Q_n = 36,45 > 20 \text{ ккал/м}^3 \rightarrow \Delta t = 8 \text{ } ^\circ\text{C}$.

Количество тепла, необходимого для поступления (удаления) воздуха в помещение.

$$L = \frac{(Q_{изб} \cdot 860)}{c \cdot \Delta t \cdot \gamma}, \text{ м}^3/\text{ч} \quad (3.14)$$

где c – теплоемкость воздуха, $0,24 \text{ ккал/кг}^\circ\text{C}$;

Δt - выбираем в зависимости от теплонапряженности воздуха Q_n ;

γ - удельная масса приточного воздуха, $1,206 \text{ кг/м}^3$.

$$L = \frac{(3,391 \cdot 860)}{0,24 \cdot 8 \cdot 1,206} = 1259, \text{ м}^3/\text{ч}.$$

Определяем кратность воздухообмена по следующей формуле:

$$n = \frac{L}{V_n}, \quad (3.15)$$

$$n = \frac{1259}{80} = 15/ч.$$

В соответствии с вычисленным значением настенный кондиционер потока воздуха выбрать одну компанию серии DELONGHI CP40 стены. Управление работа кондиционера производится с пульта дистанционного управления, который позволяет установить режим работы: нагрев, охлаждение, сушка, вентиляция, ночной режим; установить желаемую температуру, которая должна поддерживать в автоматическом режиме; выбрать режим работы: Установите таймер, включения или выключения кондиционера в заданное время; автоматически регулировать положение жалюзи и изменить, таким образом, чтобы направление потока воздуха.

Приведем его параметры:

- электрическое питание: 230/1/50;
- расход воздуха внутреннего блока: макс. – 640;
- производительность по холоду: 5073 Вт;
- потребляемая электрическая мощность: 1603 Вт;
- удаление влаги(max): 2,2 л/4;
- производительность по теплу: 5542 Вт;
- размеры: высота – 967 мм, ширина – 300, глубина – 195.

Расположение кондиционера приводится на рисунке 4.1.

Согласно расчетам, для создания удовлетворительных условий и обеспечения благоприятных условий в воздушной среде оператора, подходящих сплит-систем кондиционирования воздуха. Преимущество этих подразделений является относительная простота конструкции, что позволяет нам получить достаточно низкую стоимость для быстрой и легкой установки кондиционера. Недостатком является невозможность подачи свежего воздуха в помещение.

4 Бизнес план сети NGN

4.1 Резюме

В условиях рыночных отношений любой интеллектуальной работы должны быть оценены, чтобы вся работа экспериментального характера, необходимо оценить, что для расчета стоимости и цены и т.д.

Анализ выполнения услуги и повышение ее качества.

Оператор работает на рынке телекоммуникационных услуг, должны внедрить в практику постоянную проверку процессов обслуживания с целью повышения его качества. Для решения этой важной задачи необходимо создать и поддерживать информационную систему, предназначенную для обеспечения сбора и обработки данных по качеству услуг. Она должна быть определена ответственность за улучшение качества услуг и функционирования информационной системы. Предоставление услуг проверяется путем систематических испытаний и измерений заранее разработанной методике. Во время измерения необработанных данных подлежат соответствующей обработке, чтобы получить конечные данные:

- оценки качества услуги пользователем;
- оценки качества оператором;
- оценки качества экспертами.

Процедуры измерения и сбора данных для анализа с целью выявления ошибок. Причины ошибок в процессе измерения характеристик услуг могут быть как субъективные (низкоквалифицированных работников, недостаточная следить за контроль процедуры измерения), а также цели.

4.2 Стратегия маркетинга

Маркетинговые услуги. Основная функция маркетинга - определение спроса на услугу и продвижения своих потребностей. В процессе изучения потребностей службы должны быть проведены опросы и зарядки количество обзоров мастерства. Маркетинг должен включать в себя следующие виды деятельности:

- установление спроса на услугу и уровня ее качества;
- установление спроса на дополнительные услуги;
- анализ требований пользователя;

– консультации со всеми заинтересованными службами и подразделениями оператора для определения состава характеристик (атрибутов) и уровня качества, которые они способны контролировать и обеспечить;

– анализ деятельности конкурентов,

– анализ отечественного законодательства, международных и национальных стандартов, имеющих отношение к безопасности и защите прав пользователей;

– оценку эффекта применения системы управления качеством;

– систематическое изучение изменяющихся потребностей рынка.

Оператор заинтересован в том, что его обязательства по отношению к пользователю было документально. Таким образом, до публикации этих обязательств, оператор должен согласовать их с возможностями реализации и законодательных требований.

Официальные регистрационные обязательства по отношению к пользователю будет способствовать оператору эффективно взаимодействовать с ним.

4.3 Компания и отрасль

В Казахстане, как и во многих других странах СНГ, отношения стали одним из наиболее быстро растущих отраслей промышленности. Более широкий объем работ по внедрению и развитию новых технологий. Учитывая, что страна не имеет больших производственных мощностей по производству поставщиков телекоммуникационного оборудования отбираются на основе открытого конкурса. Таким образом, были подписаны рамочные соглашения на поставку оборудования от ведущих мировых производителей-Cisco Systems, Lucent Technologies, Nortel Networks, Siemens, Nokia.

Предоставление услуг IP-телефония - это относительно новая услуга. Эта услуга ориентирована на передачу голосовых данных. Так можно сказать, что услуги IP-телефонии имеют следующие характеристики:

– это отрасль нематериального производства;

– продукция имеет невещественный характер;

– при передаче сообщений участвует несколько предприятий;

– процессы производства и потребления продукции отрасли неразрывны;

– поступление нагрузки неравномерно по часам суток, дням недели, месяцам года.

Без телекоммуникаций, современные системы управления и не может быть нормальное функционирование материального производства, которая является основой общества. В этих условиях, управление производством и использованием телекоммуникационных сетей становится существенным

элементом всей системы общественных отношений. Таким образом, внимание к отрасли не случайно.

Цель развития отрасли - наиболее полное удовлетворение населения и национальной экономики в передаче различных типов информации на высоком уровне качества.

4.4 Основные продукции (услуги)

Основная цель сети IP на основе является быстрое, эффективное и экономичное предоставление информационных услуг и услуг связи для пользователя.

Пользователь получает его желаемую услугу, где это необходимо, в то время, когда она нуждалась в нем. Таким образом, скорость и эффективность предоставления услуг обеспечивает ее эффективность, и, следовательно, принципиальное различие между IP - сеть от традиционных сетей.

В настоящее время существует необходимость в насытить рынок высококачественных условий связи, продолжая при этом получать традиционные и новые услуги. Таким образом, существующая сеть была наложена IP - сети для удовлетворения растущих потребностей. Кроме того, в настоящее время она растет и растет потребность в других областях телекоммуникаций. Неимоверно увеличил поток информации в виде телефонных звонков, факсимильной связи, электронной почты и наборов данных указывает на более активное использование телекоммуникационных объектов, меняющихся бизнес, образ жизни и общества в целом. Улучшение телекоммуникационных услуг в интересах потребителей требует хорошей финансовой базы.

4.5 Анализ рынка сбыта. Изучение рынка услуг

В связи с напряжённой экономической ситуацией в Республике Казахстан, для традиционных операторов от всего спектра услуг, оплаченных по привлекательности наиболее спорным является услуга IP-телефонии. В конце концов, традиционные услуги междугородной и международной связи - основные источники доходов, а также снижение цен на междугородние звонки с использованием технологии передачи голоса по IP может привести к их снижения.

Но это только одна сторона медали. С другой стороны, некоторое снижение цен оператор может привлечь дополнительный трафик. Тем не менее, не все пользователи готовы принять возможное ухудшение качества речи даже при более низкой цене, так что, скорее всего, чтобы воспользоваться этой услугой, только те клиенты, которые до появления ее почти никогда не используется междугородной связи, с тем чтобы сохранить.

4.6 Финансовый план

Определяем затраты на проведение научно – исследовательского или экспериментального расчета.

Таблица 4.1 – План проведения научно исследовательских работ

Наименование этапов и содержание работ	Исполнитель	Трудоемкость, нормы – час	Количество исполнителей	Длительность цикла, дни
Контроль качества обслуживания на сети	Ведущий инженер	7	1	365
	Инженер-программист	7	1	365

4.6.1 Трудоемкость

Самая сложная и ответственная часть в планировании исследований для расчета объема работы, как затраты на рабочую силу часто составляют основную часть стоимости НИР, а также прямое влияние на время разработки. При расчете сложности научно - исследовательской работы лишь частично можно использовать нормативно-правовую базу. Основные методы определения затрат на рабочую силу для осуществления научно-исследовательских тем является метод прямого счета сложность работы руководителя.

Длительность цикла в днях по каждому виду работы укрупненно можно определить по формуле (4.1):

$$tn = \frac{T}{qn \cdot 7k} \quad (4.1)$$

где T – трудоемкость этапа, норма – час;

qn – количество исполнителей по этапу;

7 – продолжительность рабочего дня, час;

K – коэффициент выполнения норм времени (K=1,1).

$$tn = \frac{T}{qn \cdot 7k} = \frac{7}{2 \cdot 7 \cdot 1,1} = 0,45 = 1 \text{ день.}$$

4.7 Расчет потребностей инвестиций

Рассчитаем сумму капитальных вложений, необходимые для сборки организации. В то же время мы принимаем во внимание не только покупку стоимости оборудования, но и дополнительные средства, необходимые для завершения работы сайта. Стоимость оборудования указана в таблице 4.1.

Наиболее капиталоемкой частью сетевого оборудования коммутационного оборудования маршрутизаторов Cisco, которая выполняет все функции для обеспечения качества обслуживания и предоставляют главным образом новые в режиме реального времени услуг связи.

Стоимость дополнительных средств будет состоять из нескольких компонентов (мебели, инструментов, расходных материалов, а также единовременных расходов). На мебель запланировано 150 000 тенге; на все прочие материалы – 100 000 тенге.

Таблица 4.2 – Стоимость основных средств

Наименование	Кол-во, шт.	Сумма в тенге
Коммутатор 5300	1	620 000
Коммутатор 7505	1	638 000
Коммуникационный шкаф	1	21 900
ИБП	2	24 300
Компьютер	2	16 060
Коммутатор Cisco Catalyst	1	81 500
Коммутатор 3600	1	217 000
Итого:		1 618 760

Капитальные затраты определяются по формуле

$$K_3 = C_0 + K_{тр} + K_{мон} + K_{зч} + П_о + K_м + П_р, \quad (4.2)$$

где C_0 – оптовая цена оборудования;

$K_{тр}$ – стоимость перевозки к месту эксплуатации;

$K_{мон}$ – стоимость монтажа оборудования на месте эксплуатации;

$K_{зч}$ – стоимость запчастей.

$П_о$ – стоимость программного обеспечения.

$K_м$ – стоимость мебели.

$П_р$ – прочие материалы.

Стоимость оборудования $C_0 = 1\,618\,760$ тенге.

Стоимость монтажа 20 процентов от стоимости оборудования,
 $K_{мон} = 1\,618\,760 * 0,2 = 323\,752$ тенге.

Стоимость перевозки оборудования к месту эксплуатации 3 процента от стоимости оборудования, $K_{тр} = 1\,618\,760 * 0,03 = 48\,560$ тенге.

Стоимость запчастей 5 процентов от стоимости оборудования, $K_{зч} = 1\,618\,760 * 0,05 = 80\,940$ тенге.

Стоимость программного обеспечения составляет $P_0 = 1\,122\,000$ тенге.

Стоимость дополнительных средств будет складываться из нескольких составляющих (мебель, инструмент, расходные материалы, а также единовременные расходы). На мебель запланировано $K_m = 150\,000$ тенге.

На все прочие материалы – $P_p = 100\,000$ тенге.

Таким образом капитальные затраты на оборудование составят:

$K_з = 1\,618\,760 + 48\,560 + 323\,752 + 80\,940 + 1\,122\,000 + 150\,000 + 100\,000 = 3\,444\,012$ тенге.

4.8 Эксплуатационные расходы

В состав эксплуатационных расходов входят следующие статьи затрат:

– заработная плата работников. В себестоимость включаются расходы на заработную плату инженерно–технических, руководящих работников, служащих и обслуживающего персонала;

– социальный налог;

– электроэнергия для производственных нужд;

– амортизационные отчисления, т.е. расходы на возмещение износа основных фондов предприятия в денежной форме;

– кредиты (банковские расходы);

– накладные расходы. К ним относятся расходы на рекламу, аренда помещения и прочие.

$$\Sigma \mathcal{E} = \text{ФОТ} + O_c + \mathcal{E} + A_o + H, \quad (4.3)$$

где ФОТ – фонд оплаты труда всех работников предприятия;

O_c – отчисления на социальное страхование;

\mathcal{E} – затраты на электроэнергию;

A_o – амортизационные отчисления;

H – накладные расходы.

Расчёт заработной платы работников, т.е. ФОТ. В ФОТ необходимо включить надбавки за вредность в размере 10% от оклада всем ИТР. Для АУП надбавки не предусматриваются. В сумме все вышеперечисленные расходы дают фонд ЗП работников узла.

Таблица 4.3 – Должностные оклады руководящих работников и ИТР в тенге

Должность	Должностной оклад, тенге	Надбавка 10%, тенге	Оклад и надбавка, тенге	Кол–во шт. единиц	Годовая ЗП, тенге
Директор	400000	–	400000	1	4 800 000

Бухгалтер	280000	–	280000	1	3 360 000
Инженер	200000	20000	220000	1	2 640 000
Оператор–технолог	100000	10000	110000	3	3 960 000
Уборщица	50000	5000	55000	1	660 000
Итого ФОТ:					15 420 000

Итог ФОТ в год равен 15 420 000 тенге.

Премиальный фонд:

$$\text{ПрФ} = \text{ФОТ}_{\text{осн}} * 0,1, \quad (4.4)$$

$\text{ПрФ} = 15\,420\,000 * 0,1 = 1\,542\,000$ тенге.

Итого:

$$\text{ФОТ} = \text{ФОТ}_{\text{осн}} + \text{ПрФ}, \quad (4.5)$$

$\text{ФОТ} = 15\,420\,000 + 1\,542\,000 = 16\,962\,000$ тенге.

В соответствии со статьей 385 Налогового кодекса РК социальный налог составляет 11% от начисленных доходов и рассчитывается по формуле:

$$O_c = 0,11 * (\text{ФОТ} - \text{ПО}) \quad (4.6)$$

где ПО - отчисления в пенсионный фонд;

ФОТ - фонд оплаты труда;

0,11 - ставка на социальные нужды.

Отчисления в пенсионный фонд составляют 10% от ФОТ, социальным налогом не облагаются и рассчитываются по формуле:

$$\text{ПО} = 0,1 * \text{ФОТ} \quad (4.7)$$

Исходя из формулы 5.10, пенсионные отчисления будут равны:

$\text{ПО} = 0,1 * 16\,962\,000 = 1\,696\,200$ тенге.

Тогда исходя из формулы 5.9, социальный налог будет равен:

$O_c = 0,11 * (16\,962\,000 - 1\,696\,200) = 1\,679\,238$ тенге.

4.8.1 Затраты на электроэнергию

Ввиду необходимости круглосуточной работы оборудования суммарная мощность будет вычисляться по следующей формуле:

$$P = P_{\text{оборуд}} * 365 * 24, \quad (4.8)$$

где P – суммарная мощность, потребляемая основным оборудованием в год, кВт;

$P_{\text{оборуд}}$ – суммарная мощность, потребляемая основным оборудованием в час, кВт.

$$P = 5,7 * 365 * 24 = 49\,932 \text{ кВт.}$$

Мощность, потребляемая на прочие нужды, берется в размере 5 процентов от мощности, потребляемой основным оборудованием.

Таблица 4.4 – Затраты на электроэнергию

Суммарная мощность, потребляемая основным оборудованием узла в год, кВт	Суммарная мощность в год на проч. нужды, кВт	Полная мощность, потребл. за год, кВт	Тариф за 1 кВт/час потребляемой электроэнергии, тенге	Затраты на электроэнергию для произв. нужд, тенге
49 932	2 496,6	52 428,6	27,05	1 418 193

4.8.2 Амортизационные отчисления

Сумма амортизационных отчислений начисляется по единым нормам, которые устанавливаются в процентах от стоимости основных фондов рассчитываем по формуле (5.13):

$$A_0 = \Phi * N_A / 100\%, \quad (4.9)$$

где Φ – балансовая стоимость основных фондов, 1 618 760 тенге
 N_A – норма амортизационных отчислений, где $N_A = 25\%$ – для ПЭВМ.

$$A_0 = (\Phi * 0,25) = 1\,618\,760 * 0,25 = 404\,690 \text{ тенге}$$

4.8.3 Расчет накладных расходов

Накладные расходы составляют 30% от ФОТ и рассчитывается по формуле:

$$H = 0,3 * \text{ФОТ} \quad (4.10)$$

Тогда, исходя из формулы (4.10), накладные расходы составят:

$$H = 0,3 * 16\,962\,000 = 5\,088\,600 \text{ тенге.}$$

Таким образом, эксплуатационные расходы составят из формулы (4.11):

$$\text{Э} = 16\,962\,000 + 1\,679\,238 + 1\,418\,193 + 404\,690 + 5\,008\,000 = 25\,480\,000 \text{ тенге.}$$

Расчет эффективности затрат. Расчет эффективности затрат. Сырая - (абсолютная) экономическая эффективность капитальных вложений - в строительстве нового объекта, компания.

$$E_a = (\text{ЧД} + A_o) / K = \text{ОЧДП} / K, \quad (4.12)$$

где ЧД - чистый доход (20 % - корпоративный налог);

A_o - амортизационные отчисления;

K - капитальные вложения.

Чистый доход:

$$\text{ЧД} = \text{Д} - \text{Э} = 26\,535\,600 - 25\,480\,000 = 1\,055\,000 \text{ тг.}$$

где Д - годовой доход, тг;

Э – эксплуатационные расходы, тг.

Отсюда ожидаемый чистый денежный поток за первый год эксплуатации ОЧДП:

$$\text{ОЧДП} = 1\,055\,000 + A_o = 1\,055\,000 + 404\,690 = 1\,459\,690 \text{ тг.}$$

Рассчитаем срок окупаемости:

$$T = K / \text{ОЧДП}, T = 3\,444\,012 / 1\,459\,690 = 2.3 = 2 \text{ года и 4 месяца.}$$

Таким образом, средства, выложенные в проектирование защищенной корпоративной сети на базе протокола NGN на канальном уровне, компания вернет вложенные деньги за 2 года и 4 месяца

Заключение

В дипломном проекте я рассматривал построение сети NGN предприятия. Мной были проанализированы подходы к построению данной, а также был произведен выбор технологии, используемой при построении сети.

Была определена функциональная архитектура предприятия, выявлены преимущества и недостатки NGN. Также проанализирована архитектура построения современных сетей.

В процессе проектирования выяснилось, что сеть нового поколения должна с одной стороны, сочетать в себе гибкость и возможности быстрого внедрения новых услуг, которые потребуются рынку завтра, а с другой стороны, открывать пути перехода к тем видам обслуживания, которые способны обеспечить высокие прибыли уже сегодня.

В разделе безопасность жизнедеятельности проведен анализ условий труда операторов, сделан расчет освещения.

Список литературы

- 1 Росляков А.В. Учебное пособие NGN Зарубежные и отечественные платформы сетей. – М.: Эко-Трендз, 2014 - 400 с.
- 2 Бакланов И.Г. NGN. Принципы построения и организации – М.: Эко-Трендз, 2013 – 943 с.
- 3 Олифер В., Олифер О., Компьютерные сети, 4 издание. – М.: Питер – 214 с.
- 4 Фриманн Р. Волоконно-оптические системы связи. - М.: Техносфера, 2003 - 543 с.
- 5 Фокин В.Г. Оптические сети и принципы передачи - М.: ТИД «ДС», 2002 - 358 с.
- 6 Гольдштейн Б.С. Протоколы сети доступа. - М.: Радио и связь, 1999. - 292с.
- 7 Соколов Н.А. Сети абонентского доступа. Принципы построения. - Пермь: ЗАО "ИГ "Энтер-профи", 1999. - 99с.
- 8 Соколов Н.А. Выбор технологии коммутации для сетей следующего поколения - <http://www.nicksokolov.ru>
- 9 СНиП РК 2.02-05-2002 «Пожарная безопасность зданий и сооружений».
- 10 СНИП РК 4.04-23-2004 «Электрооборудование жилых и общественных зданий».