**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН**

**Некоммерческое акционерное общество**
**«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»**
**Кафедра** Телекоммуникационных сетей и систем

«Допущен к защите»
**Зав.кафедрой** Темырканова Э.К., доктор PhD, доц.
(Ф.И.О., ученая степень, звание)
_____«____» _____2020 г.
(подпись)

# ДИПЛОМНЫЙ ПРОЕКТ

**На тему:** Организация корпоративной сети посредством VPN по протоколу L2TP (IP sec)
**Специальность** 5В071900 – Радиотехника, электроника и телекоммуникации
**Выполнила** Юсибов Ш.Р. **Группа** РЭТ-16-3
**Научный руководитель** Жунусов К.Х. к.ф.м.н., доцент АУЭС
(Ф.И.О., ученая степень, звание)

**Консультанты**
**по технической части:**
Панченко С.В. доцент
(Ф.И.О., ученая степень, звание)
_____«____» _____2020 г.
(подпись)

**по экономической части:**
Ибришев Н.Н., д.э.н., профессор
(Ф.И.О., ученая степень, звание)
_____«____» _____2020 г.
(подпись)

**по безопасности жизнедеятельности:**
Бекбасаров Ш.Ш., д.т.н
(Ф.И.О., ученая степень, звание)
_____«____» _____2020 г.
(подпись)

**по применению вычислительной техники:**
Панченко С.В. доцент
(Ф.И.О., ученая степень, звание)
_____«____» _____2020 г.
(подпись)

**Нормоконтролер:** Гармашова Ю.М., доц.
(Ф.И.О., ученая степень, звание)
_____«____» _____2020 г.
(подпись)

**Рецензент:** _____
(Ф.И.О., ученая степень, звание)
_____«____» _____2020 г.
(подпись)

**Алматы 2020 г.**

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН**

**Некоммерческое акционерное общество**
**«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»**
**Институт** Космической инженерии и телекоммуникаций (ИКИТК)
**Кафедра** Телекоммуникационных сетей и систем
**Специальность** 5В071900 – Радиотехника, электроника и телекоммуникаций

**ЗАДАНИЕ**
на выполнение дипломного проекта

Студенту Юсибову Шухрату Руслан угли
Тема проекта Организация корпоративной сети посредством VPN по протоколу L2TP (IP sec)

Утверждена приказом ректора № 147 от «11» ноября . 2019 г.

Срок сдачи законченного проекта «25» мая . 2020 г.

Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта: Данные к проекту и требуемые параметры для организации прокетирование исходные данные обьектов. Расчет полосы пропускания методом СМО системой массового обслуживания по проекту был расчет на ширину канала 50-80 мбит/. Моделирование корпоративной сети в Аспан телеком на виртуальной программе NetCracer 4. Программное обеспечение «Router Cisco». Технические расчеты обеспечения для обеспечения освещения и комфортного микроклимата в помещении. Расчеты экономического бизнес плана Аспан телеком.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: Организация корпоративной сети VPN в офисном помещении для персонала компании проект по обеспечению удаленного доступа к рабочему месту. Расчет полосы пропускания и параметров качества обслуживания. Безопасность жизнедеятельности. Бизнес план.

Перечень графического материала (с точным указанием обязательных чертежей): Цель дипломного проекта; Задачи дипломного; Схема сети Аспан телеком, Схема организации сети VPN, Расчеты объема и полосы пропускания, Смоделированная сеть в NetCracker. Безопасность жизнедеятельности. Технико-экономические показатели.

Основная рекомендуемая литература:

1 В. Олифер, Н. Олифер «Компьютерные сети. Принципы, технологии, протоколы. Учебники», 2016.

2 А. Сергеев «Основы локальных компьютерных сетей», 2016.

3 А. Робачевский «Интернет изнутри. Экосистема глобальной сети», 2017.

4 М. В. Кульгин «Технологии корпоративных сетей» , 1999.

5 А.П Пятибратов, Л. П. Гудыно, А. А. Кириченко «Вычислительные системы, сети и телекоммуникации» 2014.

Консультанты по проекту с указанием относящихся к ним разделов проекта

| Раздел | Консультант | Сроки | Подпись |
|---|---|---|---|
| Техническая часть | Панченко С.В. | 09.10.2019 г. | |
| Экономическая часть | Ибришев Н.Н | 27.05.2020 г. | |
| Безопасность жизнедеятельности | Бекбасаров Ш. Ш | 1.06.2020 г. | |
| Применение вычислительной техники | Панченко С.В. | 18.05.2020 г. | |
| Нормоконтроль | Гармашова Ю.М. | 15.06.2020 г. | |

График
подготовки дипломного проекта

| № п/п | Наименование разделов, перечень разрабатываемых вопросов | Сроки представления научному руководителю | Примечание |
|---|---|---|---|
| 1 | Обзор компании «Аспан телеком» | 13.01.-15.02. 2020 г. | |
| 2 | Предложения по модернизации сети | 25-30.01. 2020 г. | |
| 3 | Проект модернизированной сети передачи данных | 02-20.02. 2020 г. | |
| 4 | Топология сети Аспан телеком | 22.02-01.03. 2020 г. | |
| 5 | Настройка оборудования | 02.03-01.04. 2020 г. | |
| 6 | Тестирование канала | 02-20.04. 2020 г. | |
| 7 | Расчет полосы пропускания | 21-30.04. 2020 г. | |
| 8 | Расчет параметров качества обслуживания | 16.04.-10.05. 2020 г. | |
| 9 | Бизнес план | 13.04.-25.05. 2020 г. | |
| 10 | Безопасность жизнедеятельности | 12.04.-25.05. 2020 г. | |

Дата выдачи задания «9» октября 2019 г.

Заведующий кафедрой _____ (Темырканова Э.К.)
(подпись) (Ф.И.О.)

Научный руководитель проекта _____ (Жунусов К.Х.)
(подпись) (Ф.И.О.)

Задание принял к исполнению студент _____ (Юсибов Ш.Р.)
(подпись) (Ф.И.О.)

**Аннотация**

Дипломдық жоба vpn L2TP(IPsec) технологиясын пайдалана отырып, Aspan Telecom компаниясында Корпоративтік желі құруға бағытталған.жергілікті желі де орнатылды.

Осы бөлімдерге бөлінген бес тараудан, онда келтірілген есептеулер өткізу қабілетін пайдалана отырып, қосу, сондай-ақ есеп айырысу сапасының параметрлерін желісі жобаланды пайдалана отырып, бағдарламаның NetCracer 4.1. сонымен қатар, әртүрлі қатынау нүктелеріне қосылған және бір ортақ корпоративтік желіге біріктірілген екі түйін арасында VPN-туннель құрылды.

Өміртіршілік қауіпсіздігі бөлімінде жарықтандыру, сондай-ақ үй-жайлардың қолайлы микроклиматы және еңбек жағдайлары бойынша есептеулер жүргізілді. Экономикалық бөлімге арналған тарауда кәсіпорынның пайдасы барлық шығындар мен жылдық өтелімділік есебімен есептелді

**Аннотация**

Дипломный проект направлен для создания корпоративной сети в компании Аспан Телеком с помощью технологии VPN L2TP(IP-sec) так же было настроена локальная сеть.

В данной работе разделы разделены на пять глав где имеются расчеты пропускной способности с помощью суммирования а так же расчеты параметров качества, сеть была спроектирована на программе NetCracer 4.1 так же было выбрано оборудование с помощью которого был создан VPN туннель между двумя узлами которые подключены к разными точкам доступа, и объединены в одну общую корпоративную сеть .

В главе по безопасности жизнедеятельности были произведены расчеты освещения а так же благоприятного микроклимата помещений и условий труда. В главе по экономической части было рассчитано прибыль компании с учетом всех затрат и год окупаемости.

**Annotation**

The diploma project is aimed at creating a corporate network in Aspan Telecom using VPN L2TP(IP-sec) technology.the local network was also configured. In this work, the sections are divided into five chapters where there are calculations of throughput using summation as well as calculations of quality parameters, the network was designed using the NetCracer 4.1 program. also, the equipment was selected with which a VPN tunnel was created between two nodes that are connected to different access points, and combined into one common corporate network . In the Chapter on life safety, calculations were made for lighting, as well as for the favorable microclimate of premises and working conditions. In the Chapter on the economic part, the company's profit was calculated taking into account all costs and the payback year

## Содержание

## Введение

В современном мире все предприятия нуждаются в точки доступа в интернет тем самым они осуществляют передачу документов, различные аудио форматы, и так же видео, с помощью точки доступа в интернет они управляю своим предприятием

И за прогресса IP сетей (в основном это Интернет) была открыта новая тенденция использования для создания общей корпоративной сети в первую очередь не дорого и общедоступного транспорта IP сети для использования во (внешние сети).

Однако решение отправки данных через сеть Интернет является опасной имеется веду кража информации тем более если это корпоративная сеть, могут быть перехвачены важные документы банковские счета сотрудников.

Для решения этой проблемы можно будет использовать технологии виртуальных частных сетей это VPN. По технологии VPN строится защищенный туннель с уже известной скоростью по которому передается информация, это технология очень востребована и используется почти везде.

## 1 Что такое VPN и для чего он нужен

Это виртуальная частная обеспечивает без всяких сложностей подключится к серверу компании с любой точки земли где есть доступ к интернету не важно какое это устройство будь то ноутбук либо смартфон используя VPN можно работать с любой точки земли где конечно же есть интернет. Огромные компании которые имеют несколько филиалов либо большое число сотрудников они все используют технологию VPN так ка за технологию не нужно платить она бесплатная.

VPN используются для расширения интернета:

– в основном крупных частных сетях;

– по всему миру они обеспечивают удаленный доступ к более широкой базе пользователей. VPN (виртуальная частная сеть);

– это технологии, которая обеспечивает одно или несколько сетевых защищенных подключений поверх другой сети (к примеру Интернет).

Ваши данные автоматически шифруются, когда вы используете Интернет через службу VPN. Процесс подключения к VPN известен как тунель. Когда это происходит, VPN начинает работать на вашем IP-адресе и заменяет его на тот, который используется в VPN. Это означает, что происхождение ваших действий будет происходить от сервера VPN, а не от вас. Следовательно, никто не может знать, чем вы занимаетесь через Интернет, пока вы используете VPN.

Так как туннель который строится в VPN и все проходящая информация шифруется и идет дальше по зашифрованному туннелю и никто не знает об его существовании кроме пользователя самой сети VPN. Если выходить в интернет без VPN это может поставить вашу конфиденциальность и безопасность под угрозу, так как на просторах интернета все ресурсы, сайты, видео хостинги, соц-сети они все распознают ваш IP – адрес сети, и могут отслеживать ваши геоданные, тем самым эти источники анализируют информацию, потом предлагают по мере анализа вам рекламу, то что вы именно искали, либо когда то вводили в поиске в интернете. Есть хакеры которые могут взломать обычного пользователя, но если использовать VPN то взлома можно избежать, так весь канал шифруется, и ваше место положение не возможно определить, он будет знать тип подключения но не сможет обнаружить вас и тупо не будет  вся информация проходит через так называемый «туннель», никто не имеет доступа к этой информации. Из многих причин использования VPN одной из важнейших является поддержание конфиденциальности и безопасности информации. Вы можете подумать, что ваши данные и работа в Интернете всегда безопасны, но использование Интернета без VPN может подвергнуть вас многочисленным угрозам от хакеров. Потребность в VPN возникла у компаний, требующих от всех своих сотрудников доступа к системе при соблюдении тех же характеристик, что и у других. В том числе те, которые работают удаленно. Таким образом, VPN также можно рассматривать как способ объединить всех

и поддерживать их на виртуальной платформе, даже в случае если они физически разделены.

Другая основная причина, по которой люди используют VPN, заключается в том, что им необходим доступ к контенту, который недоступен в определенном регионе или заблокирован по любой иной причине. Цензура со стороны правительств может быть побеждена с помощью VPN. Кроме того, файлы и документы, которыми вы обмениваетесь с другими людьми в Интернете, и общедоступные соединения Wi-Fi, к которым вы подключаетесь, также защищены, когда вы выходите в Интернет и выполняете действия по VPN.

Хотя есть много причин, по которым вам следует использовать VPN, анонимность не является одной из них. VPN не обещает анонимности, так как некоторые местоположения требуют, чтобы поставщики услуг VPN хранили данные в законных целях. Это сделано для того, чтобы никто из пользователей, представляющих угрозу для сообщества, не мог использовать такой сервис. Даже в этом случае VPN имеет возможность оградить вас от многих распространенных опасностей при просмотре онлайн через незащищенную сеть.

Зашифрованные данные, передаваемую по общественной сети, нельзя считать либо распознать, ведь все данные будут зашифрованы. Шифрование происходит от отправителя, а расшифровка информации от получателя по заголовку сообщения. Далее расшифровки сообщения между ними происходит установка VPN соединений, позволяющих работать в общественной сети.

VPN сеть в основе применяют с такими протоколами как OpenVPN, L2TP /IPSec, PPTP, PPPoE – они являются защищенными и безопасными для передачи данных.

VPN-соединение обеспечивает:

– безопасную работу в корпоративной сети;

– простота и очень удобна в настройки подключения;

– высокую скорость соединения без каких либо обрывов;

– защищённый канал без хакерских атак.

Также VPN можно использовать на телефонах либо на планшетах суть в том что можно зайти в сеть подключивших к VPN это сеть может быть не доступна с вашего провайдера но через сменив сеть с помощью VPN можно обойти ограничения тем самым большинство пользователей используют VPN для обхода ограничений который выставил вышестоящий провайдер, и за этого провайдерам приходится блокировать весь ресурс что бы он не работал вообще, в разных случаях провайдеры договариваются между собой, и выставляют для обхода ограничений который выставил вышестоящий провайдер, и за этого провайдерам приходится блокировать весь ресурс что бы он не работал вообще, в разных случаях провайдеры договариваются между собой, и выставляют ограничения на сеть, тем самым даже с помощью VPN вы не сможете зайти на ресурс который был заблокирован но есть один

минус это очень не легкая задача, сети интернета очень тяжело контролировать.

Основной функцией применения VPN : отслеживание корпоративной почты, видеоконференция с сотрудниками, проведение совещаний.

### 1.1 Типы VPN и чем они отличаются

1.1.1 Востребованные протоколы VPN. Протоколы в Виртуальных приватных сетях. Протокол PPTP. Операционная система с Windows NT/2000 с них поддерживает эти протокола. С развитием операционных систем она поддерживается во всех брандмауэрах так же VPN. Протокол PPTP начинает работать по протоколам IP, IPX. На рисунке ниже показана структура протокола PPTP (см. рисунок 1.1).

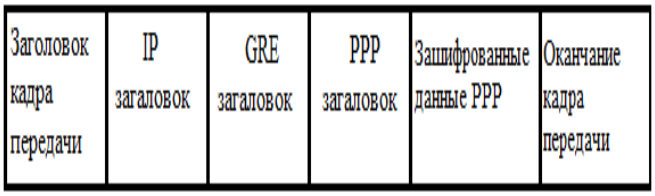



Рисунок 1.1 - Структура пакета для передачи по туннелю PPTP

Ниже изображена структура типа протокола PPTP, показано как проходит режим туннелирования с помощью удаленного пользователя который подключен через сеть интернет изображено на рисунке 1.3.

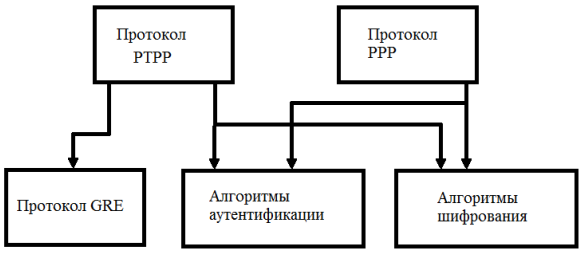



Рисунок 1.2. - Архитектура протокола PPTP


Рисунок 1.3 – На данной схема показано что подключение идет на прямую и с помощью

Протокол L2TP и L2f.

L2TP был разработан на основе ядра L2F, который был создан в Cisci Systems в качестве PPTP. Модель и структура протокола на рисунке 1.4.

L2TP берет начало от расширенного протокола PPP с возможным видом авторизации удаленных пользователей, туда так же входит удаленное соединение которым можно будет управлять. Протокол L2TP использует UDP для передачи данных. На рисунке 1.5 показана структура пакета для передачи по туннелю L2TP.


Рисунок 1.4 - Архитектура протокола L2TP

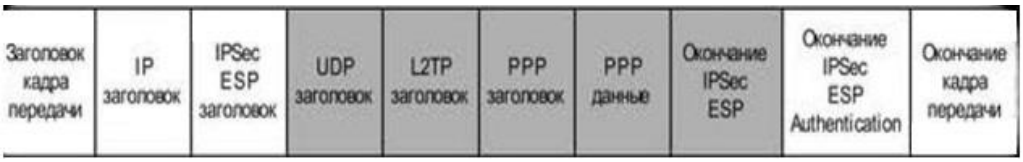



Рисунок 1.5 - Структура пакета для передачи по туннелю L2TL

В этом моменте создается виртуальный туннель по которому идет соединение между локальной сетью сервера и маршрутизатором провайдера который предоставляет интернет трафик. Так же можно обеспечить множество туннелей по которому будет передаваться трафик. Роль сервера удаленного доступа провайдера ложится на концентратор доступа LAC,

который создает клиентскую часть протокола L2TL и реализует доступ пользователя к локальной сети через Интернет. Схема показана на рисунке 1.6.

Удаленный доступ к сети осуществляется с помощью подключения к серверу. С стороны провайдера ISP устанавливает соединение с PPP пользователем. Концентратор-(HUB) создает соединение с PPP и LAC принимает аутентификацию. Так же идет авторизация у провайдера и конечный узел провайдера находится в HUB. И уже отталкиваясь от этого выше стоящий провайдер понимает что пользователю нужен туннель на базе L2TP. При необходимости создается туннель и:

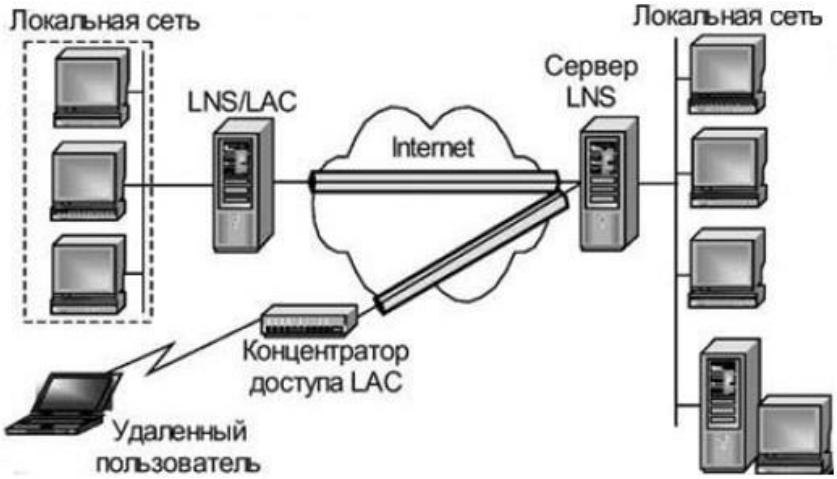



Рисунок 1.6 - Схема туннелирования по протоколу L2TL

– тогда аутентификация пользователя выполняется на сервере LSN этой сети;

– после успешной аутентификации создается зашифрованный туннель между концентратором доступа LAC и сетевым сервером LNS.

L2TP не имеет специальных криптографических методов.

Протокол безопасности на сетевом уровне служит - IPSec.

IPsec обеспечивает:

– целостность - передаваемые данные не будут искажаться, дублироваться и теряться;

– конфиденциальность - предотвращает от несанкционированного просмотра;

– аутентичность отправителя.

Протокол работает на основе криптографических технологий:

– с обменом ключей Д. Хеллмана;

– криптография с открытым ключом;

– облачное шифрование;

– аутентификация на основе Хеша.

Следующие компоненты включены в IPSec:

– ESP и AH, работающие с заголовками и работающие с базами данных SAD и SPD для определения политик безопасности для пакетов;

– обмен ключевыми данными IKE.

SPD - База данных политики безопасности.

SAD - сохраняет список безопасных ассоциаций SA для отправленной и полученной информации.

Ядро IPSec содержит три протокола:

– AH (заголовок протокола аутентификации);

– ESP (инкапсулирующий протокол безопасности);

– IKE (протокол для согласования управления ключами и параметрами виртуального канала).

Архитектура протокола в IPSec показана на рисунке 1.7.


Рисунок 1.7 - Архитектура протоколов в IPSec

Протокол AH обеспечивает аутентификацию и целостность данных, а ESP реализует функции AH и алгоритмы шифрования.

Протоколы IKE, AH и ESP работают следующим образом:

– IKE создает безопасную ассоциацию SA между двумя точками. Когда IKE аутентифицирует конечные точки линии, выбираются определенные функции конфиденциальности. В установленной безопасной ассоциации SA, AH или ESP функционируют защита и передача данных;

– Нижний уровень архитектуры основан на доменной интерпретации DOI. AH и ESP основаны на модульной конструкции, которая позволяет

пользователю выбирать между используемыми алгоритмами шифрования и аутентификации. Именно DOI координирует все факторы и адаптирует IPSec по выбору пользователя.

Формат заголовка пакета AH и ESP, изображены, на рисунке 1.8.

AH защищает весь IP-пакет, кроме полей в Ip-заголовке и поля TTL и вида службы, которые могут быть модифицированы при передаче в сети.


Рисунок 1.8 - Формат заголовков AH и ESP

Протокол AH работает в двух режимах: туннельный и транспортный. Расположение заголовка AH зависит от того, в каком режиме он находится. В транспортном режиме заголовок исходного IP-пакета становится внешним заголовком, а затем заголовком AH. В этом режиме IP-адрес адресата / адресата читается третьими лицами. [14].

В туннельном режиме новый заголовок создается как заголовок внешнего IP-пакета. Это показано на рисунке 1.9. и на рисунке 1.10 показаны два режима работы протокола ESP.


Рисунок 1. 9 - Режимы применения заголовка AH

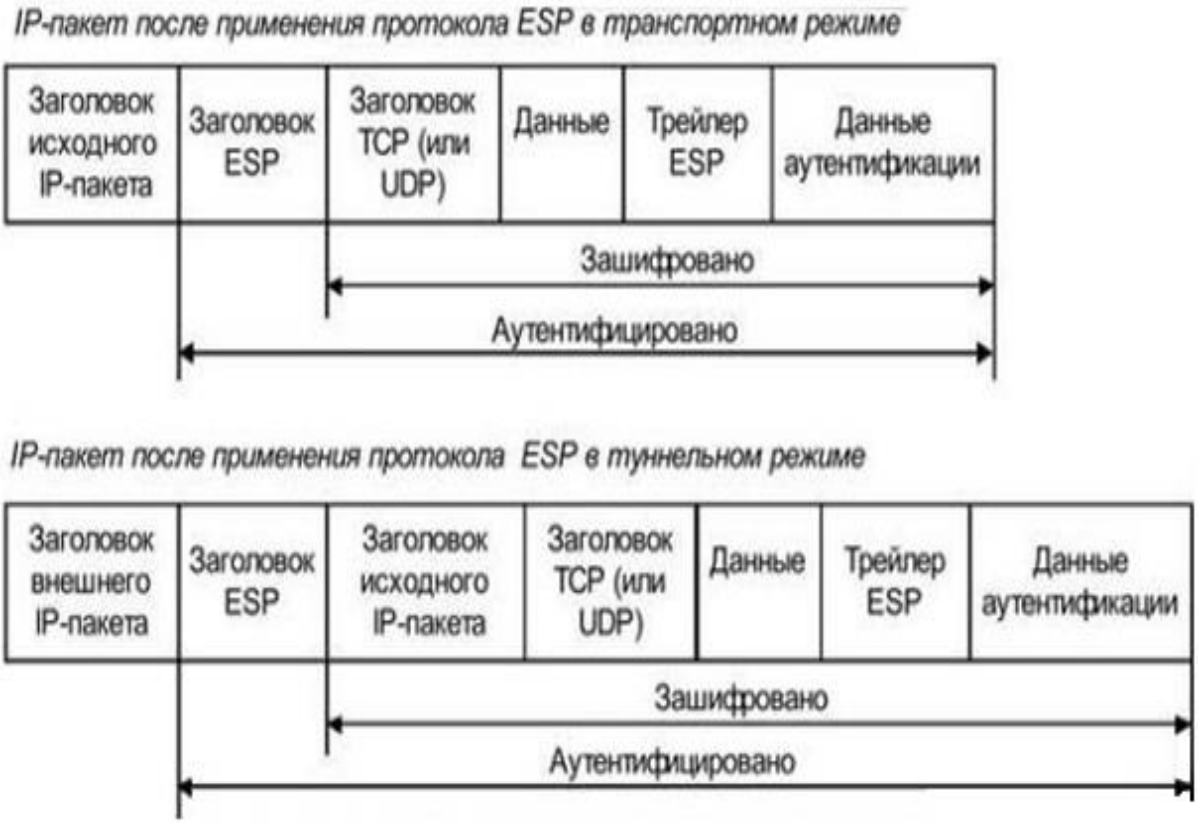



Рисунок 1.10- Режимы применения ESP

IPSec защищает сеть от многих сетевых атак, откидывая посторонние пакеты вплоть до того, как все они дойдут к уровню IP на узле. На узел смогут войти исключительно те пакеты, которые поступают от аутентифицированных пользователей.

Протоколы защиты на сеансовом уровне

Уровень сеанса - это самый высокий уровень, на котором создается защита виртуального канала.

Протоколы SSL и TLS. [9].

Следует отметить, что SSL и TLS - это один и тот же протокол. Сначала был SSL, но он был взломан и решили изменить и выпустить TLS. Конфиденциальность реализуется путем шифрования информации с использованием симметричного сеансового ключа. Ключи сеанса также шифруются, основываясь только на открытых ключах, извлеченных из сертификатов абонентов. Установка SSL-соединения включает в себя следующие операции:

– аутентификация сторон;

– согласование криптоалгоритмов для реализации;

– создание общего секретного мастер-ключа;

– генерация сеансовых ключей на основе мастер-ключа.

На рисунке 1.11 показано, как аутентифицировать клиента с помощью SSL непосредственно на сервере.

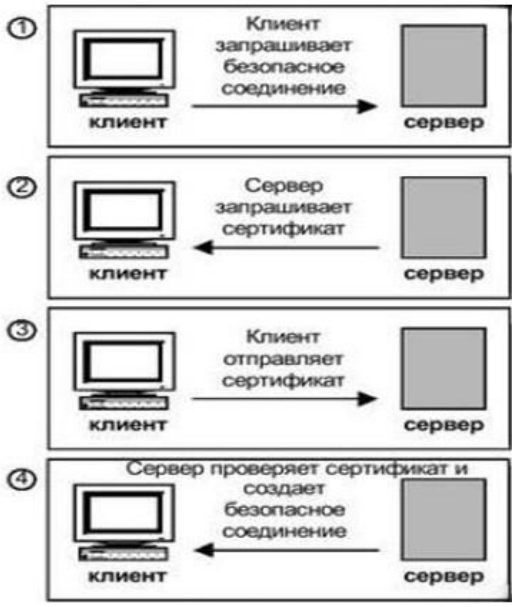



Рисунок 1.11- Процесс аутентификации клиента сервером с помощью протокола SSL

Недостатком TLS и SSL является то, что они могут работать только с одним и тем же протоколом сетевого уровня (IP). [16].

IPSec – очень гибкая технология она довольна сложна в самой конструкции и так же гибка настраивается. Если рассматривать структуру IPSec то она состоит из множества протоколов которые работают с ним для безопасности переданной информации.

Внутренних протоколов, которые можно подключать и отключать для контроля степени защиты отправляемых данных. Он может использовать множество сторонних алгоритмов шифрования, таких как MD5, SHA-1, DES и 3DES. При правильно настроенном IPSec вы можете быть уверены, что ваш VPN защищен от несанкционированного доступа.

Функции IPSec: как в туннеле, так и в транспортном режиме. В транспортном режиме шифруются только данные пакета. В туннельном режиме весь пакет повторно собирается и шифруется, а заголовки также перезаписываются. Транспортный режим лучше использовать, если для организации туннеля используется другой протокол, например: Например, L2TP, и когда организация решения VPN полностью основана на IPSec. В транспортном режиме с IPSec зашифрованные пакеты весят немного меньше. Однако в транспортном режиме отображаются фактические адреса получателя /отправителя, что недопустимо при использовании VPN по причинам анонимности. Даже при наличии большого количества различных данных для проверки целостности и аутентификации многие из них можно отключить, и выбор алгоритмов шифрования и длины ключей довольно велик.

Процессы функции IPSec можно разделить на две части: [14].

– согласование параметров соединения, т.е. поддержка создания (в терминологии IPSec эта часть называется IKE - Internet Key Exchange);

– обработка IP-пакетов и защита данных в них.

Для успешного подключения IPSec необходимо подключиться с использованием протокола Security Association (SA). SA-соединение - однонаправленное (определяется как отправителем, так и получателем). Такие соединения необходимы для согласования параметров передачи:

– используемые типы шифрования;

– выполнение проверки целостности данных на хеш-суммы.

Какой режим IPSec использовать (транспортный или сетевой), выполнять ли аутентификацию и т.д. Данные SA хранятся в базе данных SAD (Security Association Database), а три основных параметра используются для быстрого обнаружения и создания соединений:

– SPI (индекс параметров безопасности);

– IP-адрес отправителя и получателя;

– используемый протокол безопасности (AH, ESP или оба) очень безопасен;

– прост в настройке.

### 1.2 Реализация VPN

VPN Сети в основном применяется в частных компаниях, интернет провайдерами, страховые компании, и различные частные предприятия, технология очень востребована во всем мире, и в реализации она очень проста не нужно покупать кучу доп-оборудований для соединения с VPN, достаточно иметь ноутбук либо персональный компьютер выходом в интернет с любой точки земли. С VPN можно уменьшить количество затраты компании, тем самым не нужно покупать отдельный канал у провайдера, и протягивать от него ПД-канал (Канал Передачи Данных), в зависимости от планов предприятия можно как угодно настроить сеть VPN под каждого пользователя. преимущественно используют большие организаций, банковские учреждения, а также учреждения государственного назначения. Факторы такой заинтересованности исходят из того, что виртуальные приватные сети и вправду делают возможным не только значительно уменьшить затраты на создание новых каналов передачи информации с отдаленными филиалами, но и вдобавок улучшить защищенность при передаче и принятии данных. Реализация данного рода сетей воплощаются определенным количеством способов, в зависимости от планов и условий виртуальной приватной сети.

По методу технического построения виртуальные приватные сети строятся на базе: [11].

– роутеров;

– брандмауэров;

– программных решений;

– специальных оборудований с внедренными процессорами для шифровании.

GRE туннели - протокол туннелирования сетевых пакетов.

OpenVPN.

PPTP - Поддержка встроена в Windows.

L2TP - Поддержка встроена в Windows. Для создания защищённой VPN его используют совместно с IPSec. Приемник PPTP.

MPD 5 настройка - сервер, клиент VPN PPTP, L2TP FreeBSD. MPD реализован исключительно для FreeBSD.

PPTP-linux - клиент VPN PPTP, L2TP Linux.

Настройка pptpd Debian - сервер для Linux. Point to Point Tunneling Server.

SymVPN - клиент VPN PPTP Symbian OS - платный.

1.2.1 VPN на базе сетевой ОС. PPTP на базе ОС Windows Server. При соединении PPTP-серверу пользователь проходит аутентификацию по протоколам PAP, CHAP или MS-CHAP. С переданными пакетами происходит инкапсуляция в пакеты GRE/PPTP. Преимущество интеграции с Windows и низкая себестоимость. [18].

1.2.2 VPN на базе программного обеспечения. AltaVista Tunnel 97 компании Digital.

1.2.3 VPN на базе управляемых маршрутизаторов. При использовании роутеров для реализации сетей VPN с целью проектирования виртуальных каналов, нужно учитывать что все сети, проходят через маршрутизатор, с точки зрения безопасности это совершенно правильно дать полное шифрование ему. На оборудования «Cisco Systems» для виртуальных сетей есть иллюстрированная моделей виртуальных сетей.

Роутеры, разработанные компанией «CiscoSystems», оснащены поддержкой стандартов L2TP и IPSec. Не включая простейшего шифрования проходящих сообщений Cisco имеют поддержку и других опций виртуальных приватных сетей, таких как аутентификация при созданий туннелированного канала и обмен паролей. [14].

На рисунке 1.12 изображен метод построение частных виртуальных сетей с применением роутеров


Рисунок 1.12 — VPN на базе роутеров

Для реализации виртуальной частного сети Cisco Systems использует безопасный логический канал с шифрованием каждого IP-пакета. Однако можно установить туннельный канал на основе идентификационных номеров отправителя и получателя, номера порта TCP или UDP и указанного QoS. Чтоб повысить функциональность маршрутизатора можно применять дополнительные модули шифрования ESA (EncryptionServiceAdapter).

1.2.4 VPN на базе брандмауэров. Идея: весь IP-трафик пропускается через брандмауэр, то лучше его шифровать.

Брандмауэр во всех операционных системах настраивается без настроек все настройки в не по умолчанию но это все гибко настраивается и почти без всяких сложностей можно настроить туннель и всех персональных компьютерах.

В итоге есть пример сетевого экрана BarracudaWebApplicationFirewall на применяется сетевой экран. В качестве примера построения на основе межсетевых экранов можно привести BarracudaWebApplicationFirewall компаний «Barracuda». BarracudaWebApplicationFirewall применяет для проектирования виртуальных приватных сетей простой метод на основе протокола IPSec. Поток пакетов, проходящий через межсетевой экран, декодируется, затем к нему реализуются обычные нормы контроля доступом. BarracudaWebApplicationFirewall работает под контролем операционных систем Windows.

Изображение на рисунке 1.13 иллюстрирует случай построения VPN канала при помощи брандмауэра.

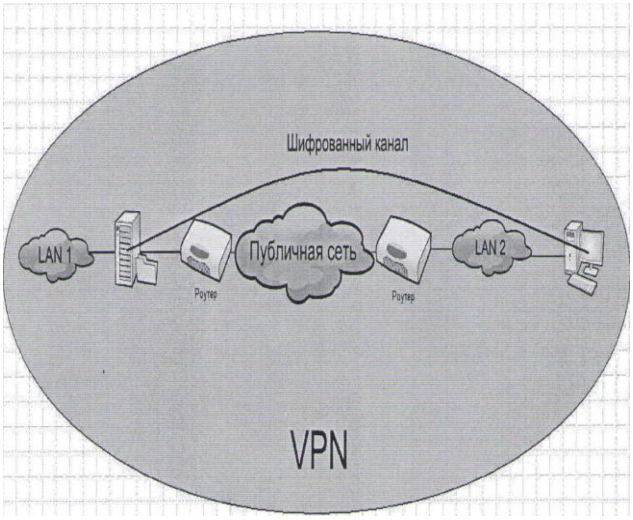



Рисунок 1.13— Виртуальная приватная сеть на базе брандмауэра

VPN на базе программного обеспечения (ПО). [29].

Все виртуальные сети строятся на программном обеспечении тем самым все пишется в программе и очень гибко настраивается под каждое устройство но, тем не менее, имеют большую мощность для построения

виртуальных приватных сетей. Следовательно, исключительно программные средства с легкостью дают производительность, которая хватает для удаленной работы. Огромным преимуществом программных средств служит простота в использовании и вдобавок сравнительно маленькая стоимость.

1.2.5 VPN на базе аппаратных средств. Виртуальные частные сети на базе специализированного оборудования. Большим достоинством данных виртуальных приватных сетей является достаточно большая эффективность, так как быстрая работоспособность выражена тем, что кодировка в них про изводится специально предназначенными микросхемами. Такие аппаратные продукты гарантируют высокую защищенность, но минус в них это их дороговизна. Способ реализаций виртуальных приватных сетей на специализированных аппаратных средствах можно применять в сетях, которые требуют большую производительность.

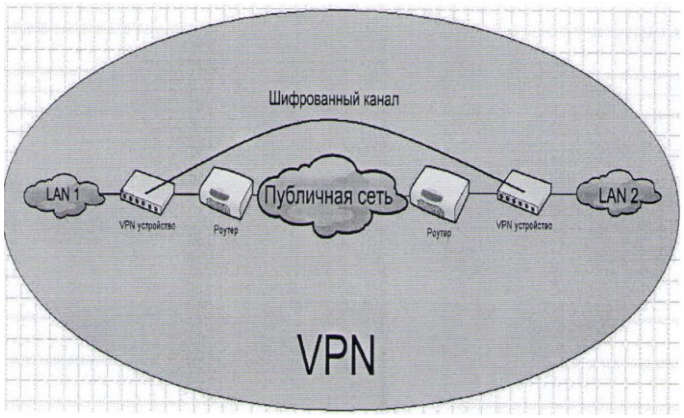



Рисунок 1.14-VPN на основе аппаратных продуктов

В IPSec содержится защищенный канал в котором содержится скомпилированный код в нем содержится зашифрованная информация по которому и будет подниматься туннель VPN, это алгоритм по которому будет подниматься зашифрованный туннель и в следствии чего информаци будет очень сложно прочитать и украсть. Кроме того, представленное аппаратное средство имеет функцию трансляции сетевых адресов (NAT) и может дополняться специализированной микроплатой, который дополняет функции межсетевого экрана.

Из соображений соотношения цены и качества, так как имеется потребность в достаточной скорости, эффективности, и по стоимости выгодно использовать роутеры, чем узкоспециализированные аппаратные средства кодирования данных.

Кроме того есть много протоколов для логических соединений регионально разделенных сетей:

– Generic Routing Encapsulation;

– IPSecurity (притуннельномрежиме);

– Generic Routing Encapsulation IP Security;

– Dynamic Multipoint VPN4.

Первый протокол имеет недостатки:

При использовании третьего способа пакету назначается идентификация с помощью GRE, а вся информация кроме заголовка кодируется IPSecurity. Вместе с тем возможен случай использования динамической маршрутизации, остается проблема масштабирования, которую может решить Dynamic.

В данной корпаративной сети был выбран VPN L2TP (IP sec).

### 1.3 Преимущества и недостатки VPN

Преимущества VPN.

Использование Интернета как канала связи широко распространено, что снижает стоимость. VPN - идеальный выбор для предприятия, нуждающихся в гибкости.

Недостатки VPN.

Сложно настраиваемая сеть, нужно обладать навыками настройки сети как локальной так и внешней, сложно настраиваемый файервол который обеспечит безопасность данной сети из внешнего мира, то есть из глобальной сети интернета, в основном взломы происходят и за халатности самих пользователей которые принимают участие в ней.

С помощью VPN-сервисов можно получить доступ к контенту, заблокированному по географическому признаку — например, к Netflix или BBC. Это самый лучший способ посмотреть передачи из американского каталога Netflix, находясь за пределами США, или посмотреть BBC там, где доступ к этому каналу ограничен.

Некоторые сайты меняют контент частично или полностью в зависимости от того, из какой страны мира зашел посетитель. С помощью VPN-сервиса вы сможете обойти эту практику.

Собственно говоря, VPN-сервисы — это просто отличные инструменты для тех, кто хочет получить доступ к заблокированному контенту (например, к сайтам, где можно смотреть потоковое видео).

Тем не менее, эта же самая технология пригодится и тем, кто хочет заняться чем-то незаконным — например, загрузкой торрентов.

Суть же в том, что вся ответственность за работу с VPN-сервисов лежит на пользователе и только на нем.

Безусловно, большинство общих моментов одинаковы и тут, и там (речь про скорость, пропускную способность канала, число поддерживаемых одновременно подключений и т.д.). Тем не менее, VPN-сервисы для бизнеса по-другому улучшают свои функции, нежели VPN-сервисы для обычных пользователей

Мало кто из нас в первую очередь думает про дизайн и все такое, выбирая VPN-сервис. Тем не менее, порой удобство работы с сервисом оказывается определяющим фактором (позволяющим, к примеру, избежать лишней головной боли).

Если не учесть правильную настройку VPN то ваш сервис VPN будет использовать в качестве преступных и других корыстный целей, и так же ваши личный данные будут украдены и вы ничего с этим не сможете поделать. Так что нужно грамотно и правильно настроить IP- адреса и фаервол чтобы он блокировал пул адресов которые не должны иметь доступ к нашей сети.

Преимущества IPsec VPN:

– масштабируемость. VPN очень легко масштабируется и для этого не нужно сложных настроек сети, создается акаунт пользователя в котором прописан его логин и пароль и так же IP – адрес и так для каждого пользователя не зависит с какой точки земли он будет подключатся, все данные и тип подключения зашифрованы, имеется веду что если у компании которая предоставляет VPN доступ мощное железо то можно иметь очень большое количество VPN доступов;

– с приходом VPN отпала нужда покупать выделенный канал и создавать мосты между компанией это все не нужно, это все прошлый век где у всех был свой канал, даже при том что был выделенный канал информацию все равно воровали и это не было безопасно, это не решение проблемы и плюс это стоит очень дорого не эффективно;

– защита IP-адресов. Самое классное в VPN это анонимность ведь когда вы подключены к сети через VPN ваш IP – адрес автоматически заменяется на адрес VPN сети и ваше место положение в сети тоже меняется, ведь вы буквальном смысле можете быть в Америке и подключится к Казахстану и интернет ресурсы и будут думать что вы из Казахстана но точка доступа у вас в другой стране. В этом то огромный плюс сети VPN анонимность.;

– обмен файлами. Обмен файлами в по сети VPN более безопасней чем просто передать информацию через открытую сеть, это всемирная паутина интернета она все почти кишит теми кто хочет украсть вашу информацию, когда украдут вашу информацию то будет уже доступ где вы проживается какого вы года и где работаете, тем самым далее хакеру будет нужно только подключится к вашей точки доступа WIFI- и все он может украсть все что ему нужно и как за хочет использовать ваши данные в сети, вы даже об этом не будите догадываться;

– удаленный доступ. VPN основная функция это удаленное соединение это может быть через персональный компьютер и ноутбук, планшет и телефон. С помощью удаленного доступа мы может управлять серверным оборудованием которое до пустим находится в другом городе либо за городом, можно управлять камерами и различными датчиками и тд;

– обход веб-фильтра, это по сути основная задача VPN обходить различные интернет ресурсы которые заблокировал провайдер либо стороны провайдеров не договорились в одной стране этот ресурс работает а другой нет эти проблемы очень часто возникают в итоге не возможно работать либо закончить начатое дело так как заблокирован ресурс.

При правильном выборе VPN получаем:

– безопасный канал связи, который во много раз дешевле выделенных линий;

– не требует изменения топологии сети, обучение пользователей, экономию;

– масштабирование;

– применение любых модулей криптографии в соответствии с национальными стандартами той или иной страны;

– интегрирование сети с другими программными продуктами и бизнес-приложениями.

## 2 VPN определение

Необходимо определить параметры сети, что необходимо для определения состояния сети, параметров и возможностей организации канала передачи данных на модернизированном оборудовании.

### 2.1 Топология сети Аспан телеком

На рисунке 2.1 показана схема подключения работников Аспан телком каждый отдел и находится в разных подсетях, на каждого из отделов выделен канал по которому предается аудио, видео, почта и документы.

Схема помещения Аспан телеком представлена на рисунке 2.2.

### 2.2 Технические характеристики организации сети

Чтобы эффективно организовать VPN сеть нужно рассчитать параметры сети. Самыми главными задачами нужно рассчитать нагрузку на сеть, а так же по смотреть топологию сети и от нее уже строить сеть.

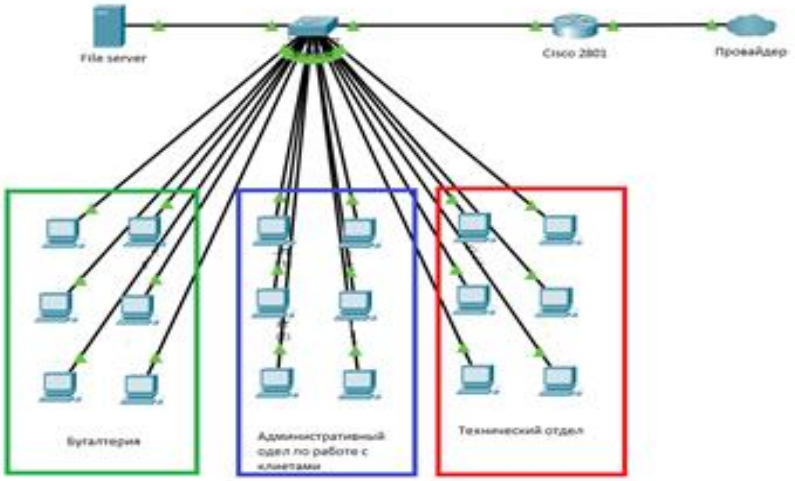



Рисунок 2.1 – Схема сети Аспан телеком [2.1]

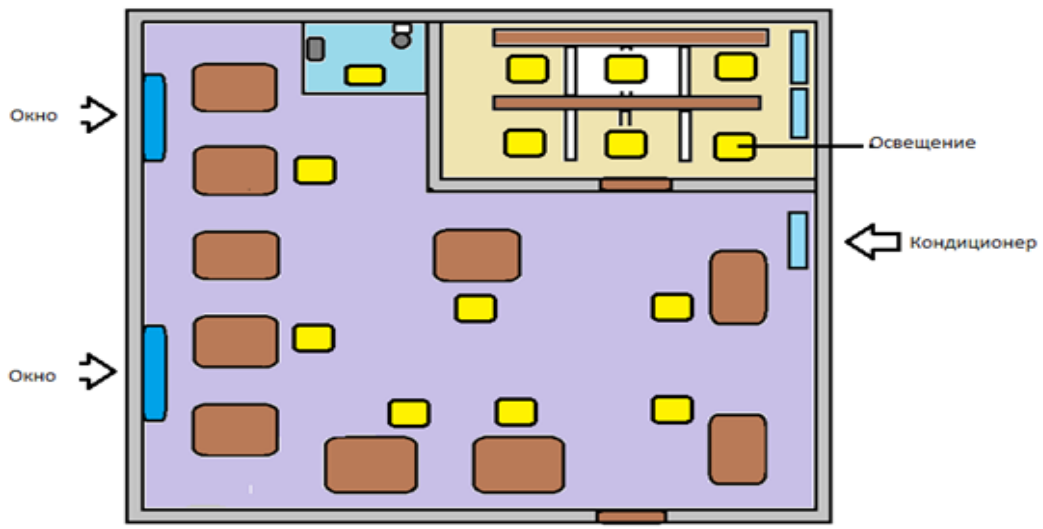



Рисунок 2.2 – Схема помещения Аспан телеком [2.1]

2.2.1 Протоколы сети. Сетевые протоколы – для передачи любой информации через инетнет либо через локальную сеть они все работают по протоколам передача информации не произойдет если не будет указан протокол либо просто не будет ничего работать, протоколы которые используется в VPN: FTP, WAIS, WAP, SMTP, TCP/IP, HTTP, POP3, Gorpher. Самый основной протокол на сегодня является TCP/IP. [10].

TCP/IP этот протокол используется в сетях передачи данных в локальной сети если включена (NAT) технология тем самым он пересылает пакеты по кускам и делит их передает по сети в конце после того как пакет проходит до конечного устройства он собирается опять заново тем самым этот протокол передачи данных наиболее распространен

2.2.2 Адреса сети подключения. Адресация сети нужна для всех участников сети, при построение сети учитывается сколько участников сети войдет в общую сеть у каждого устройства должен быть свой адрес по которому он будет обращаться к маршрутизатору для выхода в интернет либо в локальную сеть, адреса делятся на статические и динамические, в локальной сети задается статика что бы отслеживать работу каждого персонального компьютера удаленно.

Главная особенность что им не угрожает взлом так как до них стоит маршрутизатор а нем стоит фаервол который не даст доступ к серым адреса из в не то есть из интернета.

2.2.3 Пользователи сети. Компания Аспан телеком является интернет провайдером она предоставляет интернет, телефонию, и канал передачи данных оборудование в компании имеется 20 компьютеров, и сервер пример приведен в таблице 2.1.

Таблица 2.1 – Список используемых компьютеров

| Пользователи | Кол-во компьютеров |
|---|---|
| Сотрудники Аспан телеком | 20 |
| Тех.Директор | 1 |
| IT инженер | 1 |
| Радио инженер | 1 |
| VoIP инженер | 1 |
| Начальник линейного отдела | 1 |
| Бухгалтер | 3 |
| Менеджера | 12 |

Параметры используемых компьютеров приведены на таблице 2.2.

Таблица 2.2 – Параметры компьютеров

| Параметры ПК | Компьютеры сотрудников ПК |
|---|---|
| Материнская плата | Asus |
| Видеокарта | Nvidia Geforce 510G |
| Система охлаждения | Cooler  CPU Thermaltake Contac 9 |
| Операционная система | Windows 7 Max |
| Монитор (Гц) | 60 |
| Процессор | Intel Core i5-5300H |
| Блок питания | System Power 9 CM 500W |

Персональные компьютеры используются для работы если это технический отдел, производится настройка оборудование для сервера и в основном все настройки делаются через командную строку и тут не особо важна мощность персонального компьютера, другое дело в административном отделе там идет работа уже с поиском клиентов, переговоры по видео skype, whatsapp, и другие различные видео стриминговые сервисы тем самым в административный отдел нужна более мощные персональные компьютеры так как требуется много функциональность

### 2.3 Описание LanBilling для работы в Аспан телеком

Система биллинга в компании девствует как регистрация абонентов для авторизации и контроля баланса клиента и так же она может блокировать тех кто не оплатил счет, система биллинг служит для блокировок абонентов у которых идет подозрительный трафик либо ошибочные авторизации это сигнализирует о том что клиента либо взломали, проще говоря в системе биллнга отображается статут клиента и его баланс заблокирован он или нет см. рисунки 2.3, 2.4, 2.5). [2.2.3]


Рисунок 2.3 – Окон входа в систему LanBilling

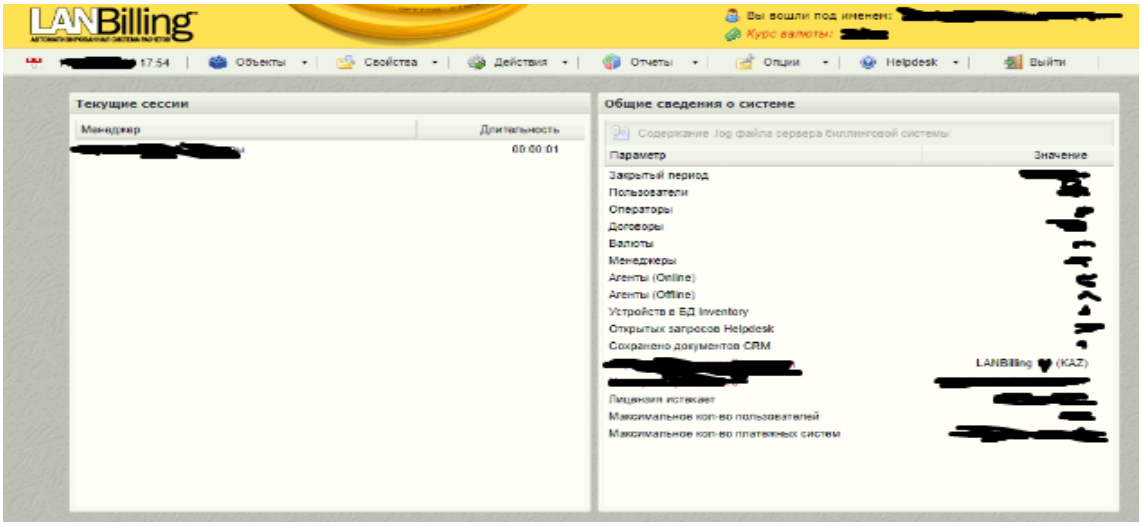



Рисунок 2.4 - Главное окно биллинга

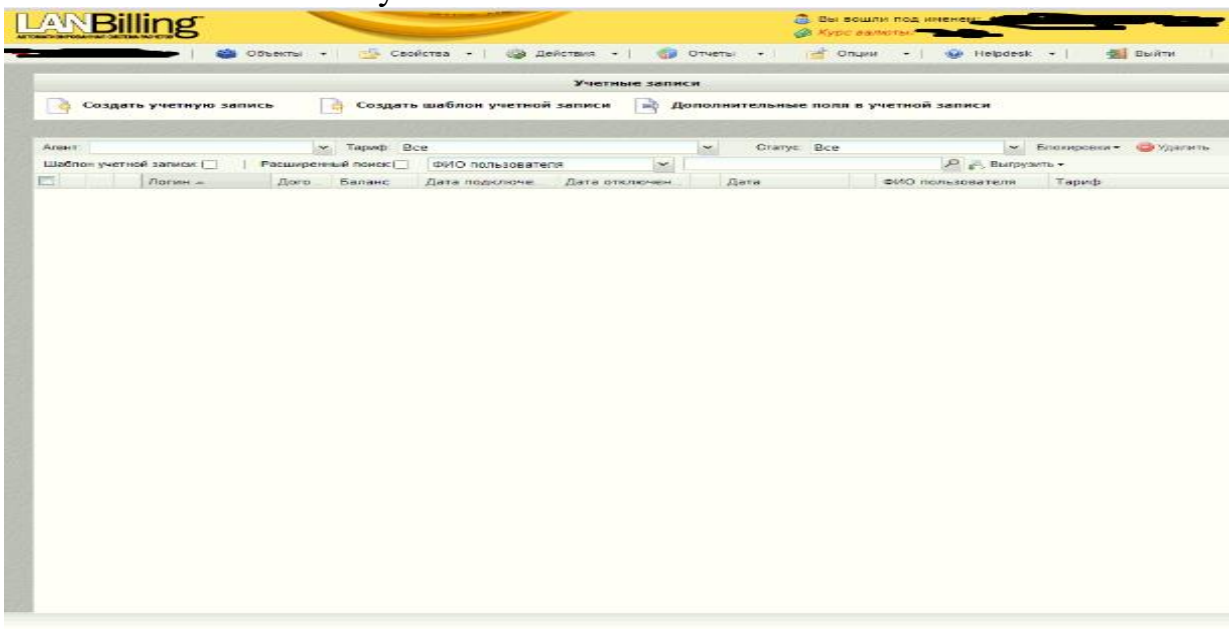



Рисунок 2.5 - Окно управление системой и проверка клиента

## 2.4 Настройка оборудования

Самая важная часть построения любой сети передачи данных является настройка оборудования. Каждая настройка производится поэтапно, сперва тщательно продумывается, затем проектируется и наконец-то реализуется.

Для начала, чтобы иметь представление задач, необходимо построить схему организуемой сети передачи данных.

Схема организации сети передачи данных представлена на рисунке 2.6.

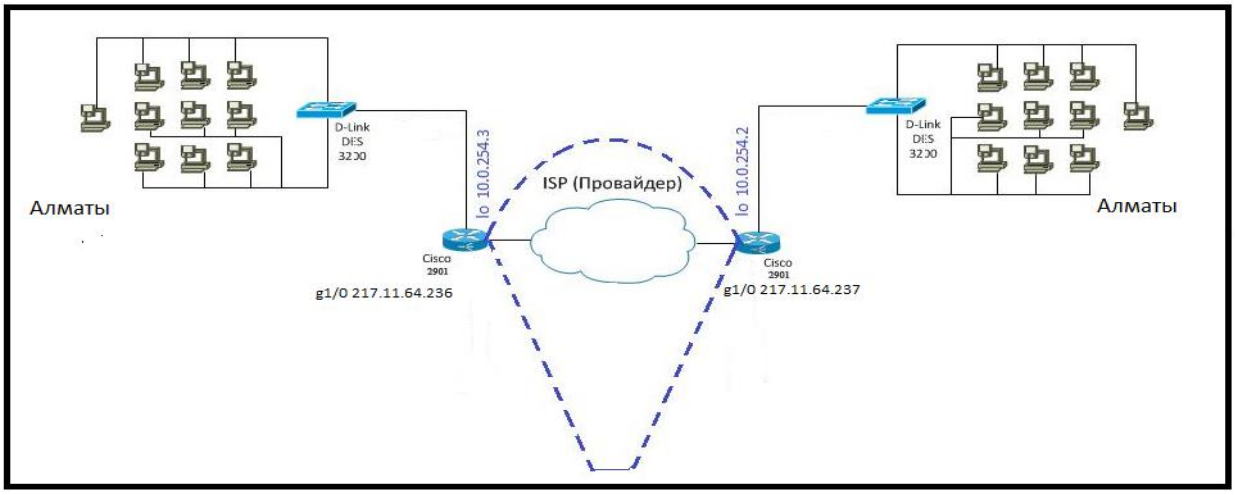



Рисунок 2.6 – Схема организации сети VPN

Если посмотреть на рисунок 2.6, видно что два пограничных маршрутизатора подключены между собой через сеть провайдера тем самым можем наблюдать последовательность подключений все по цепочке так же указаны IP-адреса по которым поднимается VPN туннель, далее указаны серые IP адреса по которым дальше строится сеть.

После этого требуется составление IP адресации, который предоставлен ниже в таблицах 2.3.

Таблица 2.3 – IP адресации внешних и внутренних сетей

| IP – адрес | Примечания |
|---|---|
| 217.11.64.236/24 | Адрес выделенный провайдером |
| 217.11.64.235 | Роутер провайдера |
| 10.0.1.0/24 | IP – адрес локальной сети |
| 10.0.2.0-10.0.254.254 | Резерв |

Следующим этапом идет сама настройка.

Используется оборудование cisco, поэтому в настройке используется встроенная операционная система IOS.

Идея DMVPN заключается в том, что вручную настраивается всего один виртуальный туннель на одном узле, который будет считаться hub-ом, а остальные узлы, клиенты, подключаются и строят между собой туннели динамически, обращаясь к hub-маршрутизатору за информацией. Делается это посредством протокола NHRP, Он позволяет маршрутизатору динамически запомнить ip адреса удаленных точек, подключающихся к нему, а при запросах рассылает эту информацию клиентам. [5]

На всех маршрутизаторах запускается протокол NHRP. Hub, который будет считаться маршрутизатором в г. Алматы, выступает как NHS – Next-Hop Server, а удаленные узлы, маршрутизаторы в городах Астана и Караганда, как NHC – Next-Hop Client.

Так как на этом узле будет держаться вся внутренняя сеть офиса, совершенно не целесообразно экономить на этой точке. Поэтому было принято решение приобрести надежный качественный продукт от компании cisco.

Просмотрев технические характеристики, а также цены на оборудование, был сделан выбор. [27]

Маршрутизаторы от компании Cisco поддерживающие протоколы туннелирования и безопасности начинаются от 1900 серии. Однако пропускная способность таких маршрутизаторов свыше 26 Мбит/с начинается лишь с 2901 серии. Поэтому маршрутизатором подходящий под мои требования является из линейки 2901 серии – «Cisco 2901».

На рисунке 2.7 изображен сам маршрутизатор Cisco 2901.


Рисунок 2.7 – Маршрутизатор «cisco 2901»

Cisco 2901 – это лучшее соотношение цены-качества в моем случае. В этом маршрутизаторе собраны все наборы технологии VPN.

И так на hub-маршрутизаторе необходима следующая настройка: - *interface Tunnel0* – поднимается туннельный интерфейс;

– *ip address 10.0.254.1 255.255.255.0* – присваивается адрес интерфейсу;

– *ip nhrp map multicast dynamic* – запускается протокол NHRP, и включается динамическое запоминание ip адресов;

и включается динамическое запоминание ip адресов;

– *ip nhrp network-id 1* – определяется идентификатор network ID;

– *tunnel source ge1/0* – туннельный интерфейс привязывается к физическому порту;

– *tunnel mode gre multipoint* – включается режим туннелирования mGRE.

На рисунке 2.8 показана настройка NHRP в городе Алматы через терминал putty. [28]

```
R4
alm-R1(config)#username admin pri
alm-R1(config)#username admin privilege 15 se
alm-R1(config)#username admin privilege 15 secret dnjhjq31337dpkjv2
alm-R1(config)#int tun
alm-R1(config)#int tunnel 0
alm-R1(config-if)#
*Mar  1 00:07:19.571: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
alm-R1(config-if)#ipad
alm-R1(config-if)#ipadd
alm-R1(config-if)#ip ad
alm-R1(config-if)#ip add
alm-R1(config-if)#ip address 10.0.254.1 255.255.255.0
alm-R1(config-if)#ip bh
alm-R1(config-if)#ip nh
alm-R1(config-if)#ip nhrp ma
alm-R1(config-if)#ip nhrp map
alm-R1(config-if)#ip nhrp map mul
alm-R1(config-if)#ip nhrp map multicast d
alm-R1(config-if)#ip nhrp map multicast dynamic
alm-R1(config-if)#ip nh
alm-R1(config-if)#ip nhrp net
alm-R1(config-if)#ip nhrp network-id 1
alm-R1(config-if)#tun
alm-R1(config-if)#tunnel so
alm-R1(config-if)#tunnel source fa1/0
```

Рисунок 2.8 – Настройка туннеля на маршрутизаторе

## 2.5 Выбор коммутатора

На втором уровне доступа работает коммутатор, нам необходим управляемый коммутатор для настройки портов для локальной сети что бы разделить все сети. Коммутатор второго уровня поддерживает настройку VLAN (VirTUAL Local Aria Network) это туннель который разделяет все VLAN тем самым мы можем построить большую сетку из множества локальных адресов, и они не будут перехватывать данные друг у друга, и обеспечим безопасность в локальной сети. D-Link DES 3200\10, которые будут осуществлять доступ от оконечного оборудования к пограничному маршрутизатору.

Коммутатор DES-3200 является моделью управляемого коммутатора и относится ко 2 уровню моделю OSI. Metro Ethernet (ETTX и FTTX) и корпоративных сетей. Коммутаторы этой серии оснащены 8/16/24/48 портами 10/100 Мбит/с Fast Ethernet, а также 1/2/4 комбо-портами Gigabit Ethernet/SFP.

Коммутаторы DES-3200-10/18 выполнены в корпусе шириной 9/11 дюймов обладает системой охлаждения с двух сторон, и требуется комнатная температура в среднем от 20 до 26 градусов, можно разместить на рабочем столе и в серверной на стенде. D-link «DES-3200-10 показан коммутатор На

рисунке 2.4».

Рисунок 2.9 D-link «DES-3200-10»

Таблица 2.4 – Характеристики коммутатора D-Link DES 3200/10

| Наименования | Характеристики |
|---|---|
| Тип коммутатора | Управляемый (Layer 2) |
| Технология доступа | Ethernet |
| Количество LAN портов | 8 шт |
| Тип LAN портов | 10/100base-TX (100 мбит/с) |
| Количество uplink-портов | 1 шт |
| Тип uplink-портов | 10/100/1000 Base-TX (1000 мбит/с) Combo SFP |
| Наличие SFP (mini GBIC) | Есть |

### 2.6 Выбор кабеля

В качестве соединительных линий локальной сети в компьютерном клубе будет использоваться кабель – витая пара. Этот кабель состоит из нескольких или одной пары проводников, которые свиты между собой. Это скручивание делается с целью уменьшения внешнего электромагнитного влияния.

Данный вид кабеля имеет несколько видов и для выбора надо учитывать характеристики передачи данных.

Разделение определяется разными показателями:

а) CAT1 – имеет одну пару, его чаще используют при включении телефонной связи. Частотная полоса 0,1МГц;

б) CAT2 – кабель с низкой скоростью передачи данных. Частотная полоса 1 МГц;

в) CAT3 – имеет две пары, скорость до 10 Мбит/с, раньше применялся для построения сетей 10BASE-T. Частотная полоса 16 МГц;

г) CAT4 – имеет четыре пары, скорость передачи данных – 16 Мбит/с. Частотная полоса 20 МГц;

д) CAT5 – имеет четыре пары, во время использования двух пар скорость передачи данных – 100 Мбит/с. Частотная полоса 100 МГц;

е) CAT5e – наиболее популярный вид кабеля, так же имеет четыре пары. Используют при конструировании сетей, во время использования двух пар

скорость передачи – 100 Мбит, если использовать четыре пары то 1000 Мбит/с. Частотная полоса 100 МГц;

ж) CAT6 – применяется в сетях Fast Ethernet, Gigabit Ethernet. Скорость передачи данных до 10 Гбит/с. Частотная полоса 250 МГц;

з) CAT7 – имеется двойной экранизированный кабель, что обеспечивается максимальная длина передачи данных. Частотная полоса 600 МГц.

Виды витой пары различаются по разновидностям защитных характеристик кабеля от наводок и по наличию:

а) UTP – это неэкранированная витая пара. Данный кабель без защитного экрана. Этот кабель используется в тех местах где нет материалов, что создало бы помеху кабелю. Его применяют на не больших расстояниях;

б) FTP – кабель с одним экраном сделанных из фольги. Кабель защищен от внешних, внутренних и электромагнитных наводок;

в) STP – кабель с одним общим экраном в виде сетки и с защитой каждой пары;

г) Для этих трех основных видов витой пары существуют улучшенные версии кабелей этих видов;

д) S/FTP – каждая пара находится в экране из фольги и общая оплетка из меди;

е) U/STP – кабель без внешней защиты, но каждая пара находится в экране из фольги;

ж) SF/UTP – Кабель содержит 10 пар витых медных проводников, выполнен в неэкранированном исполнении, соответствует категории 5 и предназначен для внешней прокладки. Поставляется на фанерных барабанах в картонных коробках.

Выбор кабеля был сделан исходя из области применения и себестоимости. Необходим кабель, с целью применения внутри здания, но для того чтобы использованные материалы, пребывающие возле кабеля никак не воздействовали на качество передачи данных. Принимая во внимание эти факторы, наиболее подходящим видом является витая пара типа FTP, с общей защитной фольгированной оплеткой. [30.

Кабель FTP представляет собой такой же UTP кабель, у которого расположен слой фольги под защитной оболочкой. UTP кабель не требует проводника. Следовательно, кабель FTP может быть менее гибким и более объемным, все зависит от толщины экрана. Различие этих двух кабелей показаны на рисунках 2.9– 2.10. [31].

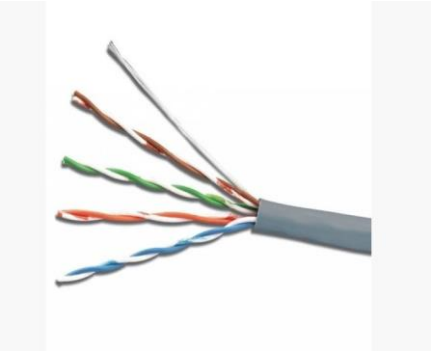


Рисунок 2.10 – UTP кабель

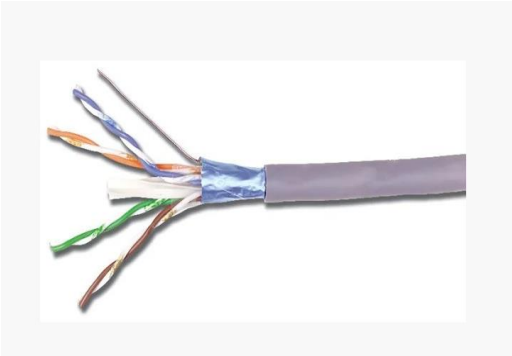


Рисунок 2.11 – FTP кабель

Электрические характеристики кабеля FTP CAT5 приведены на таблице 2.5.

Таблица 2.5 – Электрические характеристики кабеля FTP

| Наименование | Характеристики |
|---|---|
| Искажение, не более 100 МГц | 45 нс/км |
| Волновое сопротивление | 100±15 Ом |
| Электрическое сопротивлении жил не более | 9,5 Ом/100м |
| Сопротивление изоляции жил не менее | 5000 мОм*км |
| Электрическая емкость цепи не более | 5,2 нФ/100м |
| Асимметрии жил рабочей пары не более | 3% |
| Пробивное напряжение между проводниками | |
| При постоянном токе | 750 В |
| При переменном токе частотой 50 Гц | 500 В |

Каждая пара данного кабеля, предназначенная для передачи данных, обязана иметь сопротивление 100±15 Ом, либо сигнал будет искажен. Исходя, из таблицы 2.5 кабель соответствует требованиям.

### 2.7 Настройка сети VPN

Для настройки подключения, нужно убедится что на рабочем компьютере есть интернет, далее пройти в пуск  панель управления:

– нажать параметры управления в главном окне «Пуск»;

– нажать значок «Сеть и Интернет» в открытом окне нужно войти в настройки параметров адаптера «Панель управления»;

– в открытом окне «Сеть и Интернет» щелкаем на значок «Центр управления сетями и общим доступом»;

– зайдя в «Центр управления сетями и общим доступом» нажимаем «Изменить настройки адаптера»;

– в открытом окне «Сетевые подключения» нажимаем правой кнопкой мыши «Подключение по локальной сети» и выбираем «Свойства»;

– выбираем вкладку «Протокол Интернета версии 4 (TCP / IPv4)» на вкладке «Сеть» и щелкаем правой кнопкой мышью «Свойства»;

– нужно убедится что компьютер получил IP – адреса автоматически и нажимаем правой мышью «ОК».

Для защиты канала связи, нужно выбрать указать либо выбрать нужные алгоритм шифрования и так же назначить WINS для DNS-сервер. А если в сетях множество маршрутизаторов нужно их вносить в таблицу маршрута VPN которые находятся в VPN-туннеле.

Настройка VPN подключения (Windows 7):

– в меню Пуска щелкаем на Панель управления;

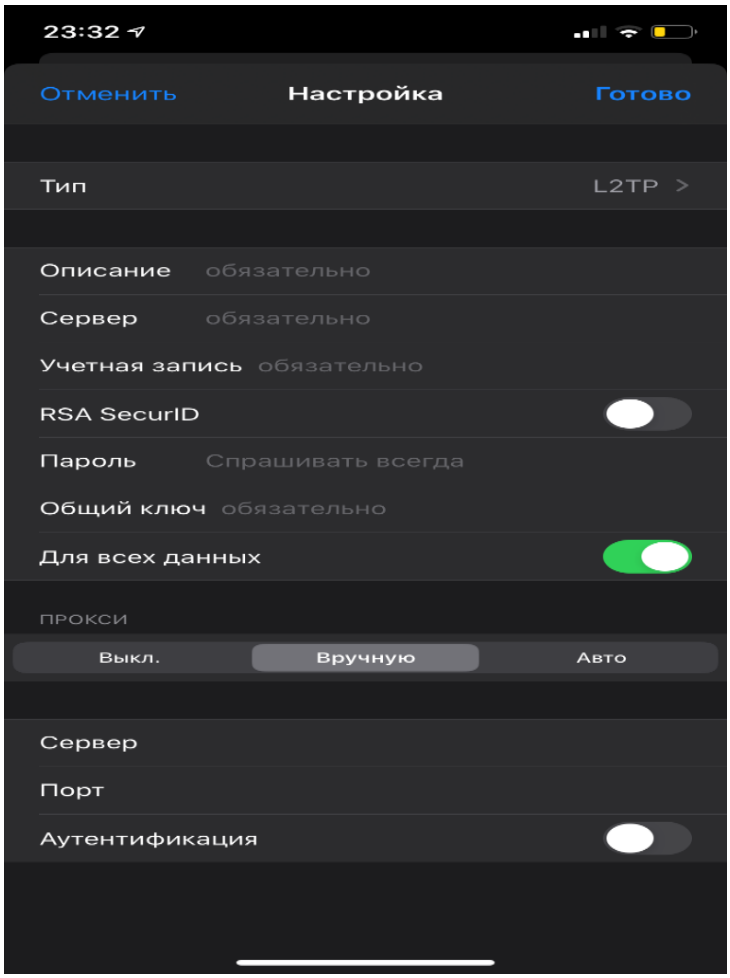



Рисунок 2.12 - Один из видов настроек VPN в операционной системе IOS


Рисунок 2.13 – Открытом меню пуск заходим в настройки

– в панель управления щелкаем на  Сеть и Интернет (см. рисунок 2.14);

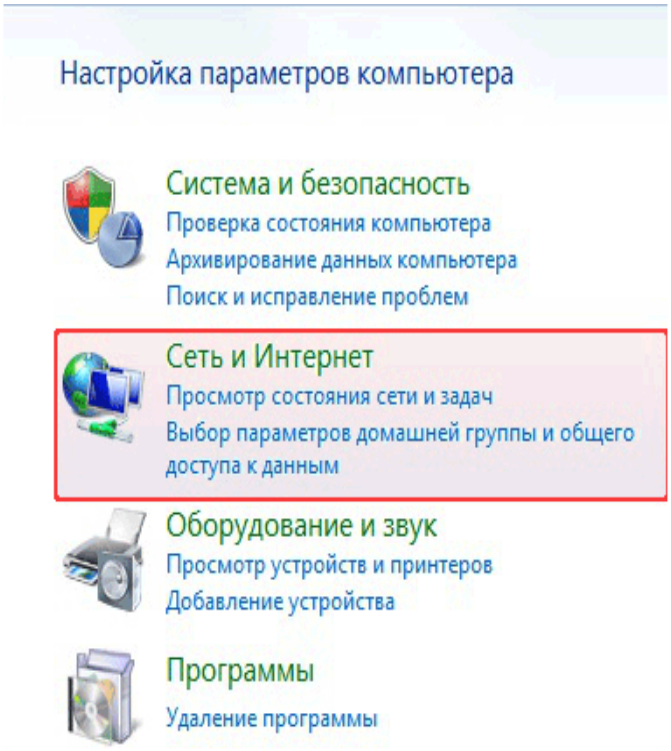



Рисунок 2.14 - В отрытом окне нажимаем сеть и интернет

– в данном окне Сеть и Интернет щелкаем  на значок Центр управления сетями и общим доступом (см. рисунок 2.15);

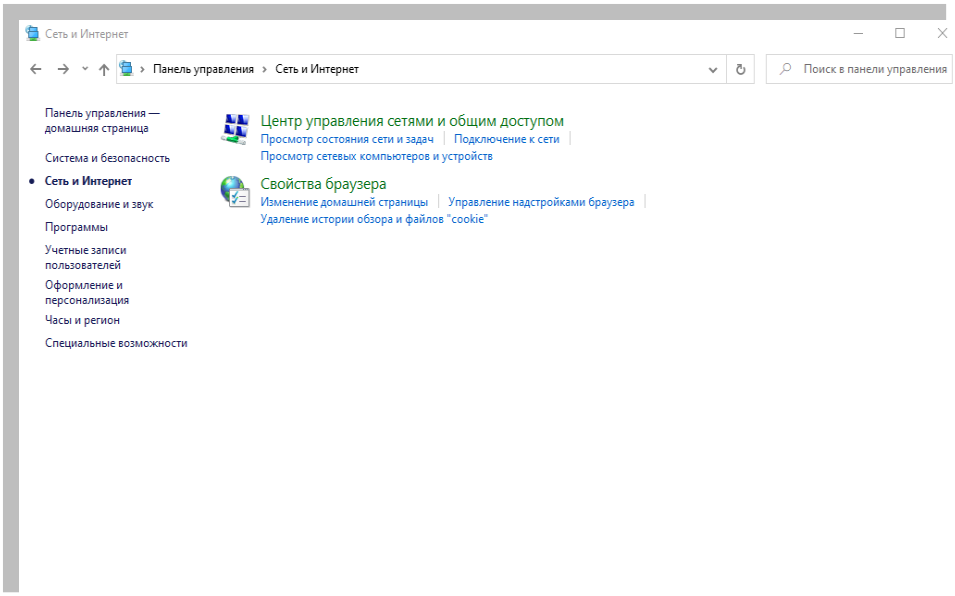



Рисунок 2.15 - Окно сеть и интернет

– в окне центр управления сетями и общим доступом щелкаем настройка нового подключения (см. рисунок 2.16);

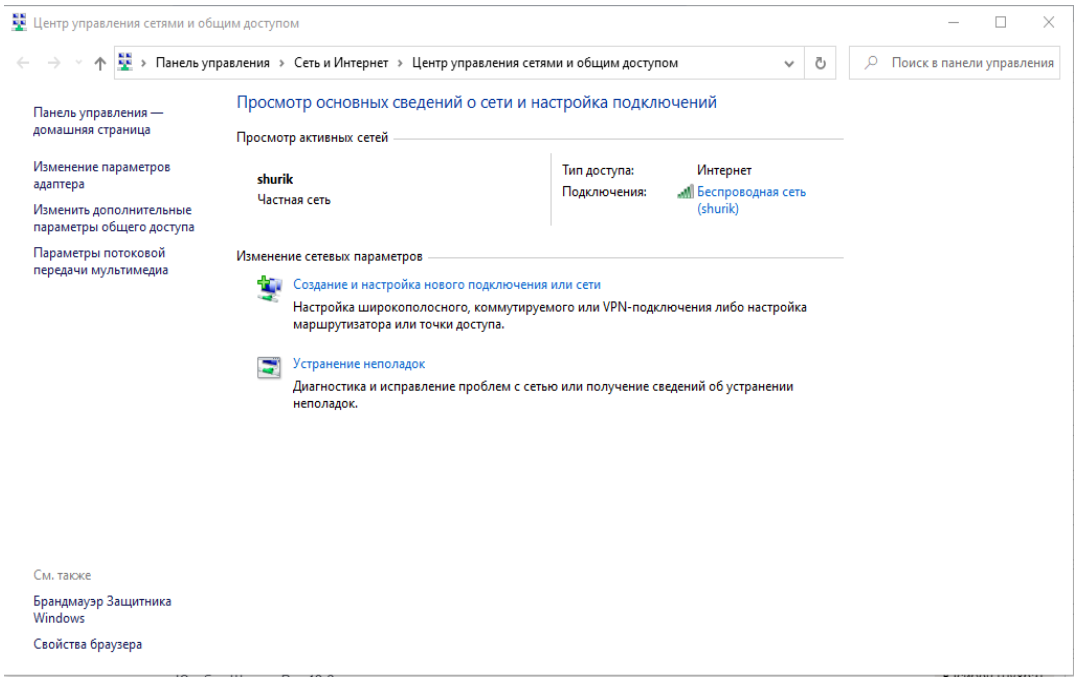



Рисунок 2.16 - Центр управления сетями и общим доступом

– в окне Настройка нового подключения или сети, щелкаем на пункт Подключение к рабочему месту и щелкаем кнопку Далее (см. рисунок 2.17);

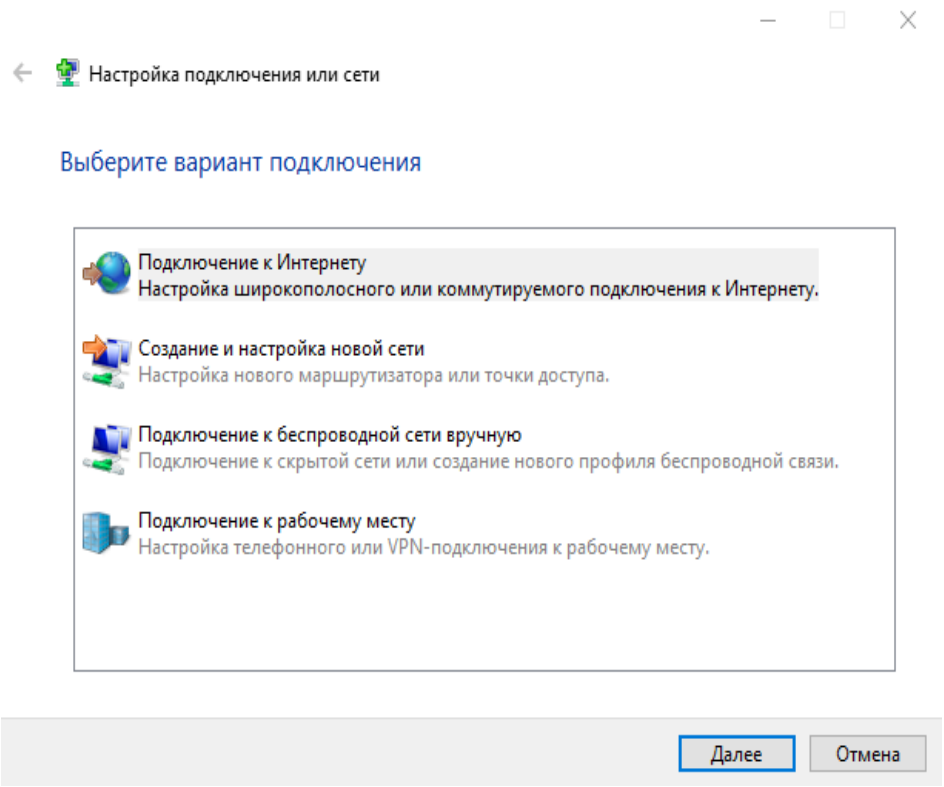



Рисунок 2.17 - Окно Настройка нового подключения или сети

– в окне Подключение к рабочему месту щелкаем вариант Использовать мое подключение к Интернету (VPN) (см. рисунок 2.18);

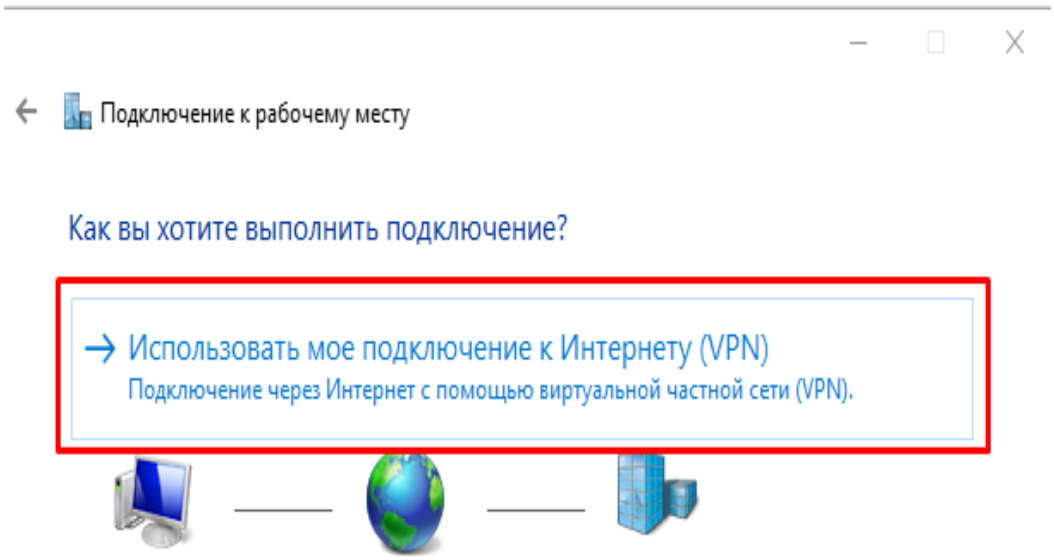



Рисунок 2.18 - Окно подключение к рабочему месту

– на следующем окне следует указать адрес VPN-сервера и имя подключения и щелкните на кнопку Далее (см. рисунок 2.19);

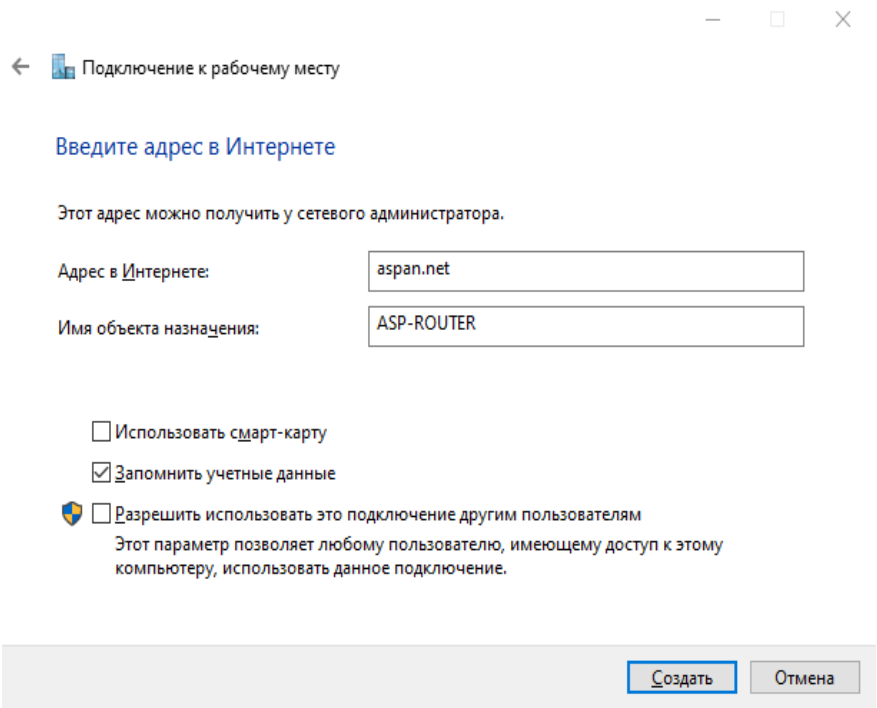



Рисунок 2.19 - Окно подключение к рабочему месту

– на следующей странице введите Имя пользователя и Пароль выданный Вам при заключении договора, установите флажок Запомнить этот пароль и щелкните на кнопку Создать (см. рисунок 2.20);

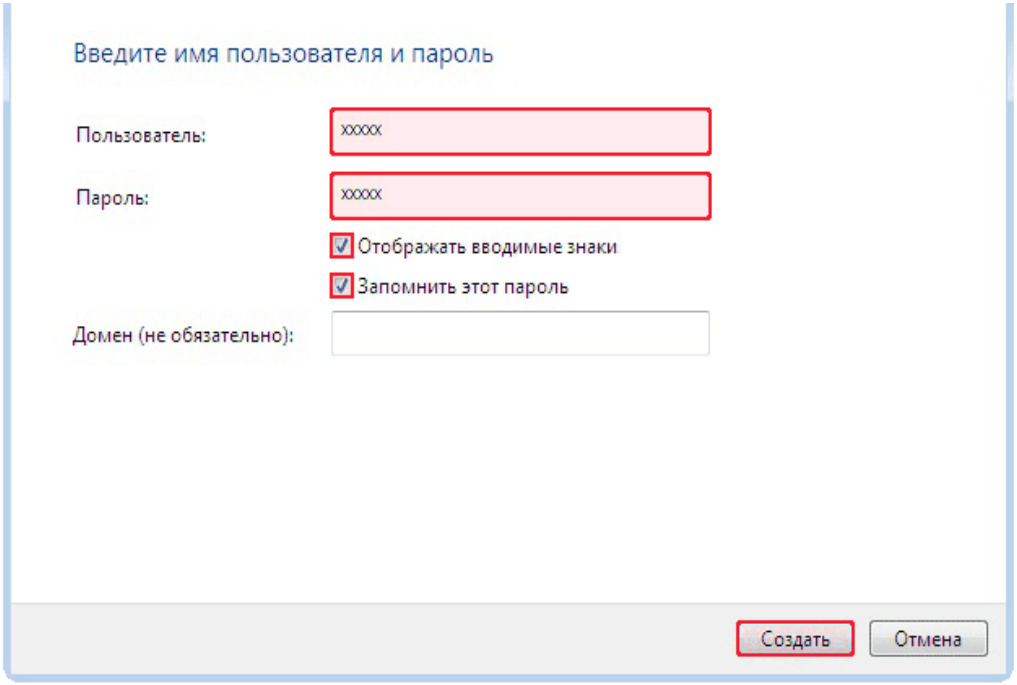



Рисунок 2.20 - Окно подключение к рабочему месту

– на следующей окне щелкните на кнопку Закрыть (см. рисунок 2.21);

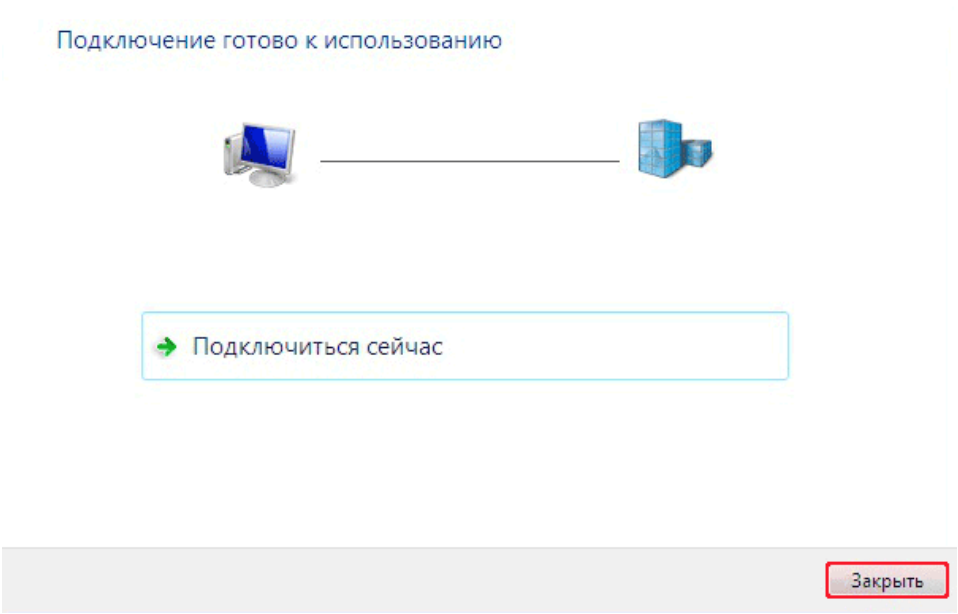



Рисунок 2.21 - Окно подключение к рабочему месту

– в левой панели окна Центр управления сетями и общим доступом щелкните на ссылку Изменение параметров адаптера (см. рисунок 2.22);

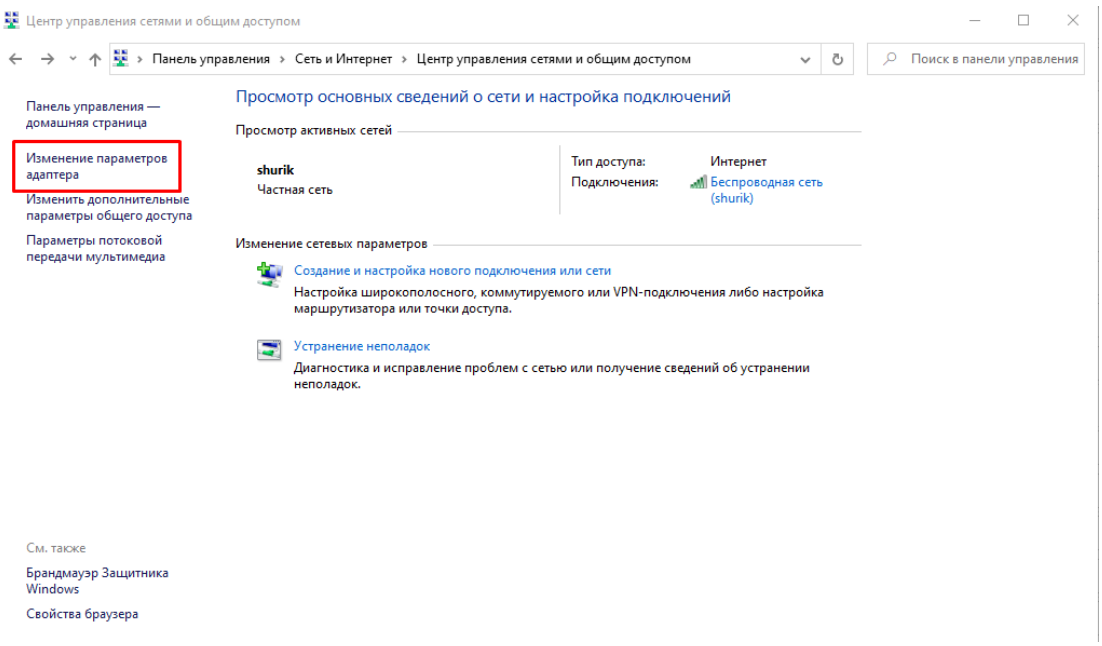



Рисунок 2.22 - Окно Центр управления сетями и общим доступом

– в открывшемся окне Сетевые подключения щелкните правой кнопкой мыши на созданном VPN-подключении ASP-ROUTER и выберите в контекстном меню пункт Свойства (см. рисунок 2.23);

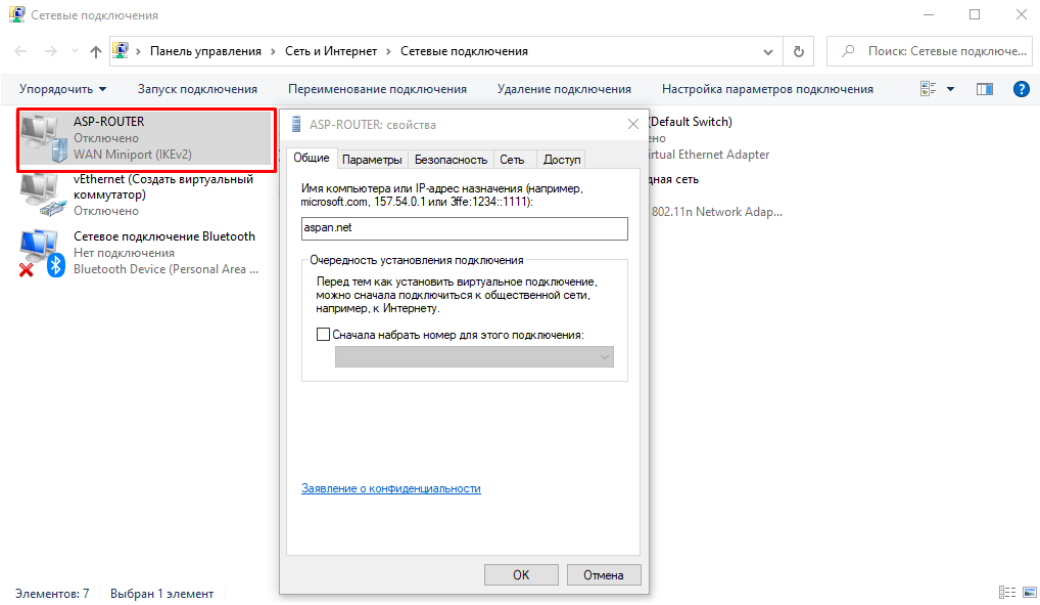



Рисунок 2.23 - Окно Свойство в сети VPN

– в открытом окне адрес VPN-сервера aspan.net (см. рисунок 2.24);

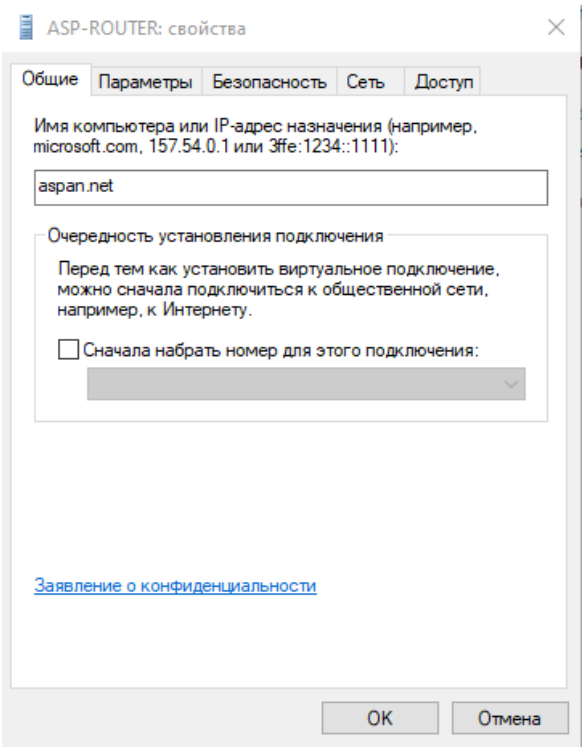



Рисунок 2.24 - Окно VPN- подключение Свойство

– перейдите на вкладку Параметры и снимите флажок Включать домен входа в Windows (см. рисунок 2.25);

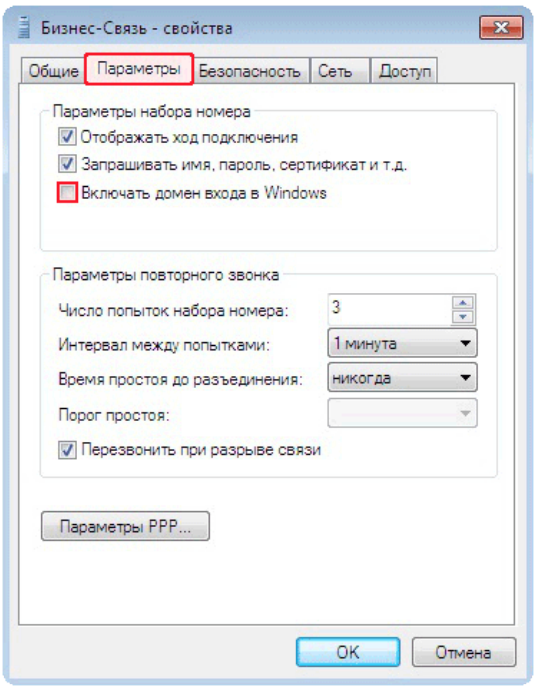



Рисунок 2.25 - Окно Свойство "параметры" VPN - сетей

– переходим по меню Безопасности и в выпавшем списке Типы VPN выбираем Протокол L2TP с IPsec (L2TP/IPsec), далее в выпавшем списке Шифрование данных выбераем (подключится не шифруя данные) и щелкаем на Ок (см. рисунок 2.26);

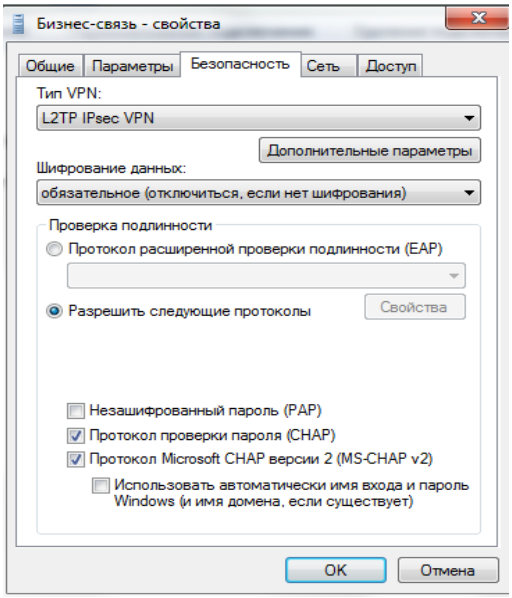



Рисунок 2.26 - Меню Свойства "безопасность" VPN – сети

– в отрытом окне нужно выбрать Сетевые подключения тем самым щелкая правой кнопкой мыши на подключения ASP-ROUTER и выбераемв меню пункт Создать ярлык;

– в открытом меню щелкаем на кнопку Подключения (см. рисунок 2.27);.

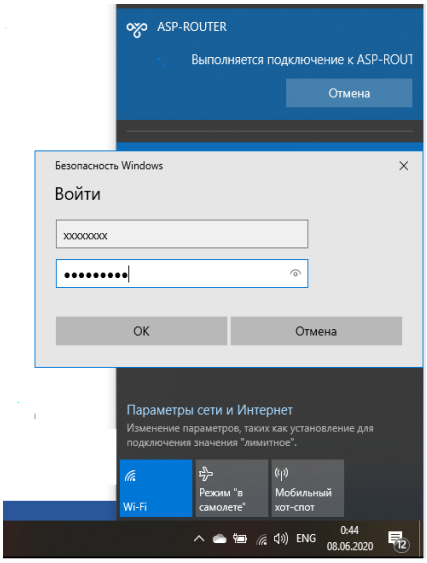



Рисунок 2.27 – Окно с Подключение VPN –сети

Вывод: В ходе проделанных действий ознакомились с главным типом VPN с его преимуществом и недостатком каждого а так же типа подключения. Была рассмотрена структура протокола, реализация VPN, а так же настройка.

С прогрессом технологий развития программ и алгаритмов повзолляет использовать технологию VPN как организациям так же и частным лицам которые выходя в интернет для удаленного доступа либо обходя блокировки различных провайдеров, главный плюс VPN надежность и скорость работы а так же обмен информацией в сети, и все это можно за шифровать и не беспокоится о сохранности данных. VPN – помогает расширить границы и возможности удаленного доступа, для работы и обхода различных блокировок.

## 3 Нужные технические расчеты для поднятие сети

### 3.1 Расчеты для корпоративной сети

Что бы эффективно проектировать в любых сетях, с начало нужно по считать и знать точные параметры сети. Нужно учесть что, первой задачей является расчет интенсивностей нагрузок на сеть и вычислить необходимые полосы пропускания канала с провайдеров до пограничных маршрутизаторов. В основом эти расчеты нужно для покупки отдельного канала связи, и полос пропускания а так же выбор оборудования на полученных расчетах.

### 3.2 Состав людей, которые используют сеть

В корпоративная сеть VPN, связана между собой двумя офисами, общее число сотрудников 29, Внизу таблица 3.1 в котором указан список сотрудников офисов.

Таблица 3.1 – Список сотрудников офиса

| Должности сотрудников в компании | Кол-во сотрудников |
|---|---|
| Маркетинговый отдел работа с клиентом | 7 |
| Инженер IT и ПД | 2 |
| V-oIP-Инженер | 1 |
| Радиоинженер | 1 |
| Начальник линейного отдела | 1 |
| Заведующий склада /монтажник | 1 |
| Технический Директор | 1 |
| Монтажники | 15 |
| Бухгалтерия | 4 |

Что бы лучше и точно рассчитать на нагрузку на транспортную сеть (накал сети интернет который дает провайдер), Для более точно расчета нужно учесть всю нагрузку на сеть и какой из пользователей сети сколько потребляет интернет трафика, далее по расчетам нагрузки можно рассчитать сколько канала интернет трафика покупать. Ниже указана таблица 3.2 в которой есть список сотрудников которые используют разные приложения и службы для работы.

Таблица 3.2 – Используемые пользователями службы

| Должности в компании | Службы которые сотрудники используют каждый день |
|---|---|
| Менеджер по работе с клиентами | почта, skype, обращение к базе данных |
| Инженер IT | Удален. Доступ к серверу, skype, почта |
| Бухгалтер | базы 1С, почта, skype |
| Радиоинженер | Почта, skype, база данных |
| V-oIP-Инженер | удал. доступ к оборудованию, почта, skype |

### 3.3 Проверка и тест каналов связи

Смотря на таблицу 3.1, на канале была замерена скорость загрузки канала и мы может отталкиватся от них так же мы можем расчитать сколько будет расходоватся трафик на каждого персонала в компании тем самым будем контролиовать нагрузку, и в случаи привышения загрузки наканала выставить ограничения на нем.

Из ходя из статистики видно, нагрузку на канал при видео конференции, так же видно скорость за средний переиод $a_{sk}$ = 632 кбит/с (см. рисунок 3.1).

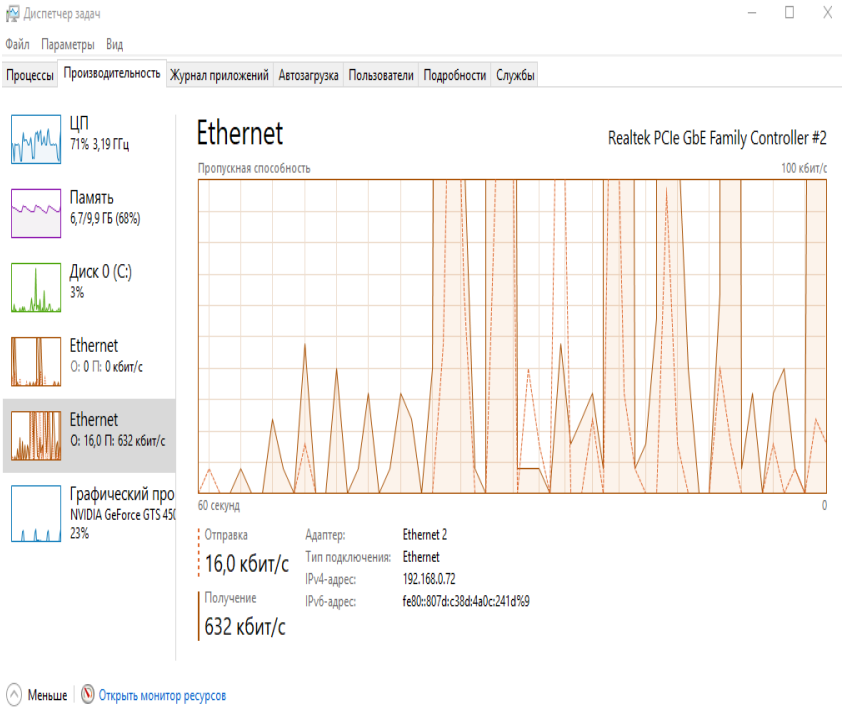



Рисунок 3.1 – Загруженность канала связи при видео конференции

Нагруженность в результате работы с почтовым сервером в среднем выходит 128 кбит/с (см. рисунок 3.2).

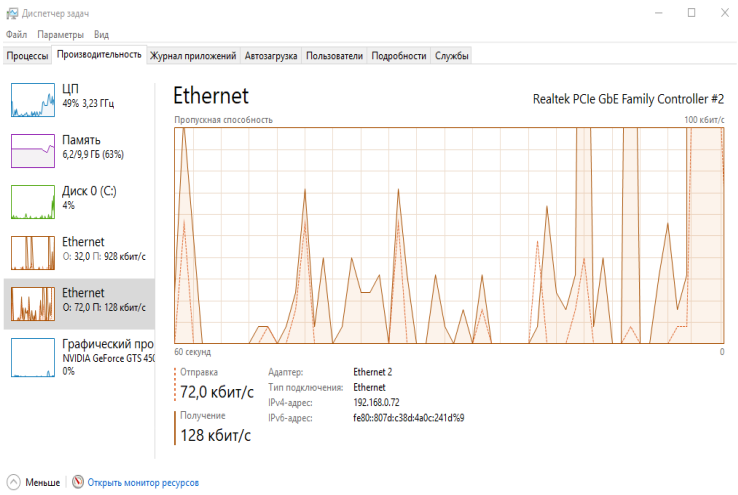



Рисунок 3.2 – Загруженность канала при работе с почтовым сервером

В результате работы удаленно IT-инженером была нагруженность канала составляет $a_{ssh}$ = 72 кбит/с (см. рисунок 3.3).

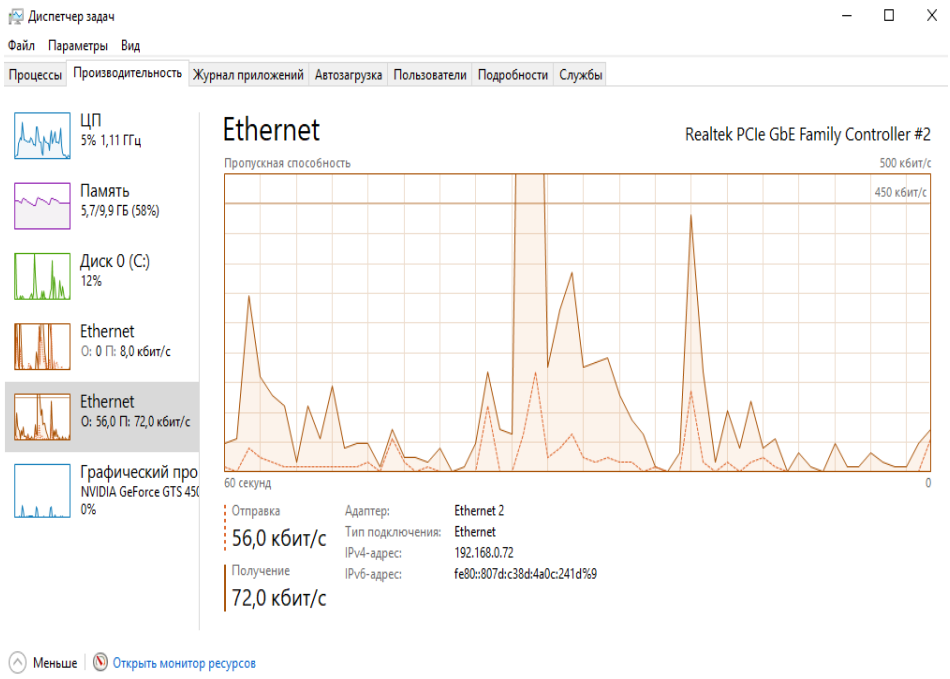



Рисунок 3.3 – Нагруженность, когда подключение идет через клиент ssh

При подключении удаленно можно видеть, что нагрузка на диспетчере задач 260 кбайт/с, что в среднем канал загружен не значительно, так же можно увидеть другие параметры пользователя как загрузку ЦП и ОЗУ, что загрузить сайт либо другой web ресурс требуется от 252 до 512 Кбайт/с.

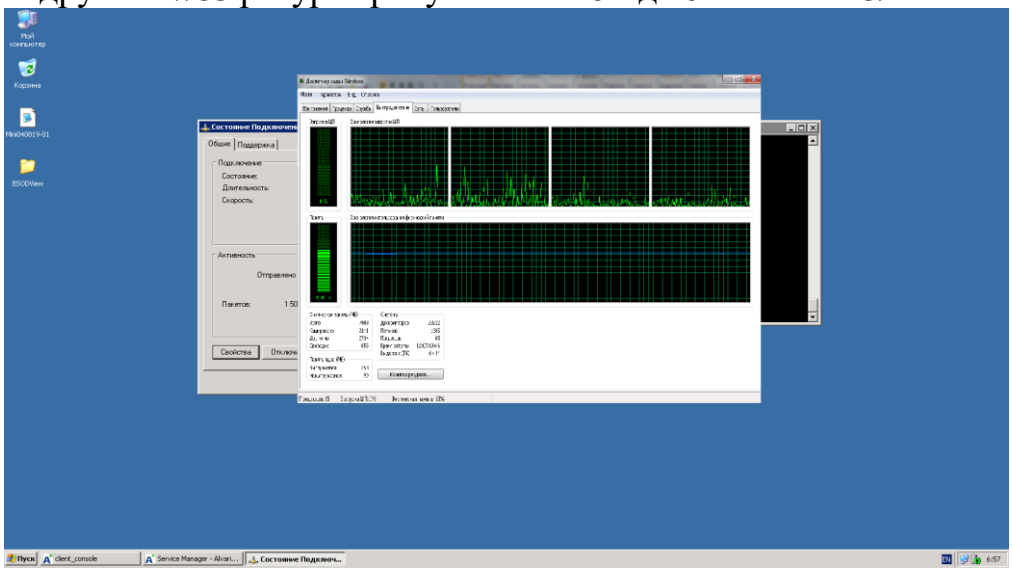


Рисунок 3.4 – Нагруженность на канале когда подключение идет через удаленный рабочий стол

Смотря на это можно рассчитать что для запуска сайта 252 Кбайт/с будет достаточно можно рассчитать сколько будет загружен канал

$$a_{сайт} = 252 * 6 = 1{,}5 \text{ (Мбит/с)}.$$

В работе с клиентом Shh нагрузка будет 128 до 252 кбит/с и может доходить до 1 Мбит/с в зависимости, загрузки файлов на сервер, так как обновление ПО (Программного обеспечения) может достигать не малых размеров.

Расчеты объема и полосы производиться, с замера полосы пропускания и суммируя трафик всех пользователей сети.

Нагрузки, которые создают пользователи сети во время рабочего процесса.

$$M_{менед} = a_{почт} + a_{video} + a_{бд} + a_{сайт} = 460 + 252 + 128 + 2048 = 3 \text{ (Мбит/с)}.$$

Сеть нагружаемая техническим отделом составляет: 40.

$$T_{тех} = a_{ssh} + a_{дост} + a_{почт} + a_{video} + a_{сайт} = 60 + 230 + 460 + 256 + 2048 = \\ = 5 \text{ (Мбит/с)}.$$

Нагрузка сети с Бухгалтерий составляет:

$$B_{бух} = a_{бд} + a_{почт} + a_{video} + a_{сайт} = 128 + 460 + 256 + 2048 = 2{,}9 \text{ (Мбит/с)}.$$

Не трудно предполагать, что в Административном отделе сеть интернета используют не слишком интенсивном, в том плане чтобы забить весь канал им понадобится всем одновременно обращаться ко всем сервисам что происходит очень редко, разумней будет выделить канал по шире Тех-офису для регулярных бэкапов (резеврное копирование данных), и обновление ПО.

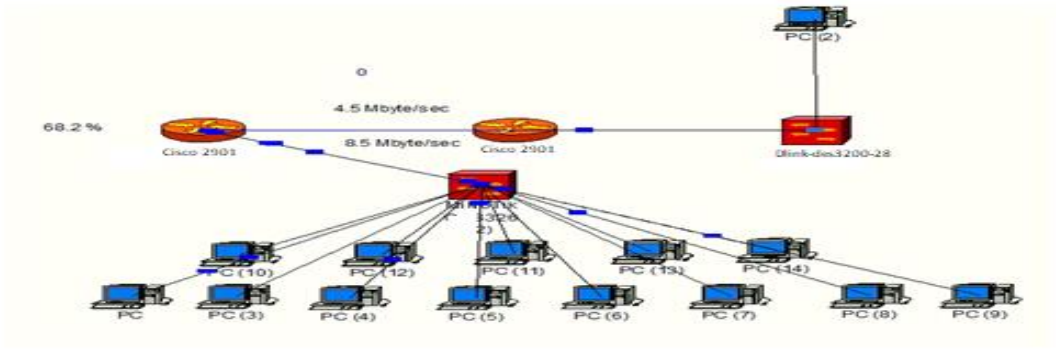



Рисунок 3.5 – Смоделированная сеть в NetCracker [6]

### 3.4 Анализ и расчет трафика для организации сети

В методиках расчета есть свои погрешности, но плане качественного облуживание и быстро действия сети нужно рассчитать, сколько объема

трафика будет нужно для организации сети. Есть стандартная схема под название (ТМО) Теория массового обслуживания она заключается в том, что помогает рассчитать нужный объем трафика, для передачи данных без потерь и задержек. Так как в сеть входит пограничный маршрутизатор который может без малейших задержек передать информацию, если привести пример для расчетов возьмем пользователей сети, если предположить что в середине рабочего дня работники компании передают более 2500000 пакетов данных. В день передается N=5000000 пакетов. Средняя длина пакета, согласно MTU, $L_{ср}$ = 1500 байт. Если рабочий день составляет более 8 часов то, более 5000000 пакетов в день передается по сети.

$$\lambda = \frac{N}{3600 \cdot 8} = \frac{52000000}{3600 \cdot 8} = 1805{,}5 \left(\frac{\text{пакетов}}{\text{с}}\right). \quad (3.1)$$

Пропускная способность системы равна A = 56700160 бит/с.

Время обслуживания одного пакета длинной 1500 байт, в таком случае равно:

$$T_{ob} = \frac{L_{ср}}{A} = \frac{15000 \cdot 8}{56700160} = 2.116 \cdot 10^{-4} \left(\frac{a}{c}\right). \quad (3.2)$$

Средняя скорость обслуживания (величина обратная к ожидаемому времени обслуживания) равна:

$$V_{ср} = \frac{1}{T_{ob}} = 4259, \left(\frac{\text{пакетов}}{\text{с}}\right). \quad (3.3)$$

Степень использования технических возможностей обслуживающего устройства (в нашем случае степень использования маршрутизатора – P) в одноканальной однофазной системе можно определить, поделив среднюю скорость поступления заказов на среднюю скорость обслуживания.

$$P = \frac{\lambda}{V_{ср}} = \frac{1111}{4259} = 26(\%). \quad (3.4)$$

Вероятность отсутствия очереди кадров в маршрутизаторе составляет:

$$P0 = 1 - P = 70(\%). \quad (3.5)$$

Значение L дает ожидаемое число пакетов, находящихся в маршрутизаторе или передаваемых по глобальной сети. Поделим скорость поступления заказов на разность между скоростью поступления заказов и скоростью обслуживания. В этом случае значение L равно:

Таким образом, в буфере маршрутизатора и линии связи в любой момент находится 57% пакета. Чтобы определить среднее число объектов в очереди Lq, перемножим степень использования обслуживающего

устройства на число объектов в системе. Наша система обрабатывает кадры данных, поэтому длина очереди равна

$$\lambda = \frac{\lambda}{(V_{CP}-\lambda)} = \frac{1111}{(4259-1111)} = 0{,}35\ \left(\frac{\text{пакетов}}{\text{с}}\right). \quad (3.6)$$

$$Lq = P \cdot L = 0,.26 \cdot 0{,}35 = 0{,}091, \left(\frac{\text{пакетов}}{\text{с}}\right). \quad (3.7)$$

Итак, в любой момент времени в очереди маршрутизатора нашей сети (пропускная способность 56700160 бит/с, интенсивность трафика 52000000 пакетов в день) находится 20% пакета. Чуть выше мы выяснили, что общее число пакетов в системе составляет 36%, поэтому разность этих величин (0,57 и 0,207), равная 0,36, дает нам число кадров, передаваемых в данный момент времени по каналу глобальной сети.

Теория массового обслуживания позволяет рассчитать среднее время нахождения объекта в системе (W) и среднее время ожидания в очереди (Wq).

Среднее время нахождения в системе представляет собой величину, обратную разнице между скоростью обслуживания и скоростью поступления заказов. Подставив числа, найдем, что в данном случае каждый пакет проводит в системе в среднем

$$\mathrm{W} = \frac{1}{\mathrm{Vcp}-\lambda} = \frac{1}{4259-1111} = 3{,}179 \cdot 10^{-4}(\text{с}). \quad (3.8)$$

Таким образом, можно ожидать, что вызванная наличием очередей задержка пакетов при передаче по линии пропускной способностью 35 Мбит/с составит в среднем 0,513 мс.

Очереди в системе можно охарактеризовать еще одним параметром, а именно временем ожидания. В нашем случае значение Wq равно произведению времени ожидания в системе на степень использования обслуживающего устройства. Таким образом, для нашей сети Wq равно:

$$Wq = W \cdot P = 3{,}176 \cdot 10^{-4} \cdot 0{,}26 = 8{,}259 \cdot 10^{-4}(\text{с}). \quad (3.9)$$

Все рассчитанные параметры качества обслуживания приведены в таблице 3.3.

Проведя анализ из расчетов и применив теорию массового обслуживания, приходим к тому что, время между ожиданием пакетов которые отравились и те которые стоят в очереди на отправку время между обслуживанием минимально. Тем самым говоря нам, что когда будет идти нагрузка, маршрутизатор справится с максимальной загрузкой без проблем, тем самым пакет меньше будет задерживатся в очереди.

На основе данных можем сделать оптимизацию пропускных

способностей канал проще говоря можем на много уменьшить нагрузку Wq не привысит $T_{ob}$

Таблица 3.3 - Параметры качества обслуживания

| Параметры | Значения | Единицы измерения |
|---|---|---|
| В день передается | 52000000 | пакеты |
| Средняя длина пакета | 1500 | байты |
| Интенсивность пакетов $\lambda$ | 1111,111111 | Пакетов/с |
| Пропускная способность - А | 26500260 | бит/с |
| Время обслуживания пакета - | 0,000326974 | с |
| Средняя скорость $Vcp$ | 4239,346667 | Пакетов/с |
| Степень использования маршрутизатора Р | 0,260204501 | Р |
| Вероятность отсутствия очереди - Р0 | 0,702525099 | Р |
| Ожидаемое число кадров, в | 0,350200502 | пакетов |
| маршрутизаторе или в глобальной сети -L | 0,091955001 | пакетов |
| Среднее число в очереди - Lq | 0,000317649 | пакетов |
| Среднее время нахождения в системе - W | | С |
| Среднее время ожидания в очереди - Wq | 0,000852085 | С |

Чтобы автоматически рассчитать все приведенные данные, они были занесены в таблицу и тем самым упрощая работу.

Результаты исследований приведены в таблице 3.4.

Таблице 3.4 – Исследования оптимальной полосы пропускания

| Параметры расчета | Полоса пропускания | | |
|---|---|---|---|
| | 52 Мбит/с | 30 Мбитс | 26 Мбит/с |
| 1 | 2 | 3 | 4 |
| В день передается, пакетов | 32000000 | 30000000 | 32000000 |
| Средняя длина пакета, байт | 1500 | 1500 | 1500 |
| Интенсивность поступления пакетов, пакетов/с | 1111,1111111 | 1111,1111111 | 1111,1111111 |
| Пропускная способность, бит/с | 52700160 | 31563295 | 275852976 |
| Время обслуживания пакета, с | 0,000528994 | 0,00032857 | 0,000460457 |
| Средняя скорость обслуживания, пакетов/с | 5085,355867 | 2621,44 | 2271,914667 |
| Степень использования маршрутизатора - Р | 0,48418801 | 0,38835852 | 0,456068852 |
| Вероятность отсутствия очереди - Р0 | 0,636695499 | 0,588214146 | 0,510936248 |
| Ожидаемое число кадров, в маршрутизаторе или в глобальной сети -L, пакетов | 0,598528962 | 0,723585998 | 0,948559988 |

*Продолжение таблицы 3.4*

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Среднее число в очереди - Lq, пакетов | 0,252899558 | 0,35898558 | 0,426584588 |
| Среднее время нахождения в системе - W, с | 0,000455845 | 0,000662107 | 0,0095885 |
| Среднее время ожидания в очереди - Wq, с | 0,000018528 | 0,000385877 | 0,000524784 |

Для наглядности сравнения характеристик качества обслуживания так же были построены графики зависимостей разных параметров.

Для сравнения проведен расчет характеристик качества обслуживания при изменении полосы пропускания от 52 Мбит/с до 26 Мбит/с.

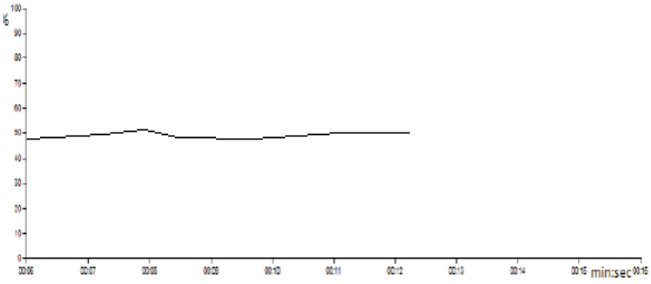



Рисунок 3.6 - График нагрузки на Netcracer [45]

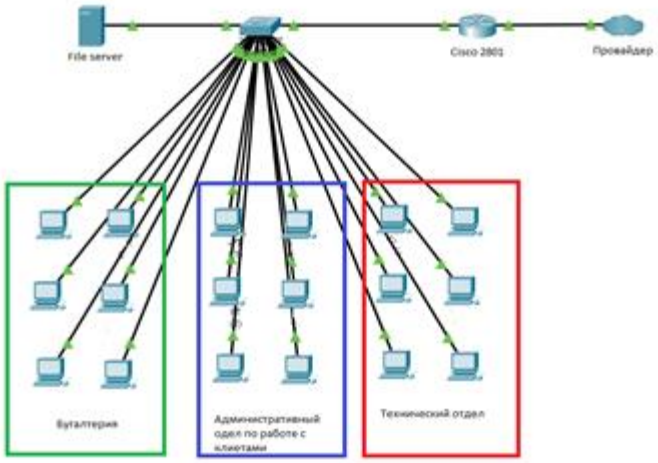



Рисунок 3.7 – Локальное подключение сети Аспан телеком

Сеть в компании делится на три категории: это бухгалтеры, административный отдел туда же входят менеджеры по продажам и совет председателей компании, далее технический отдел. Нужно учитывать что это лишь модель сети, над сетью может производится модернизация и она расширяется. Для корректной работы производится расчет трафика и подсчет нагрузок на сеть, а так же ставится доп-оборудование (маршрутизатор и свитч

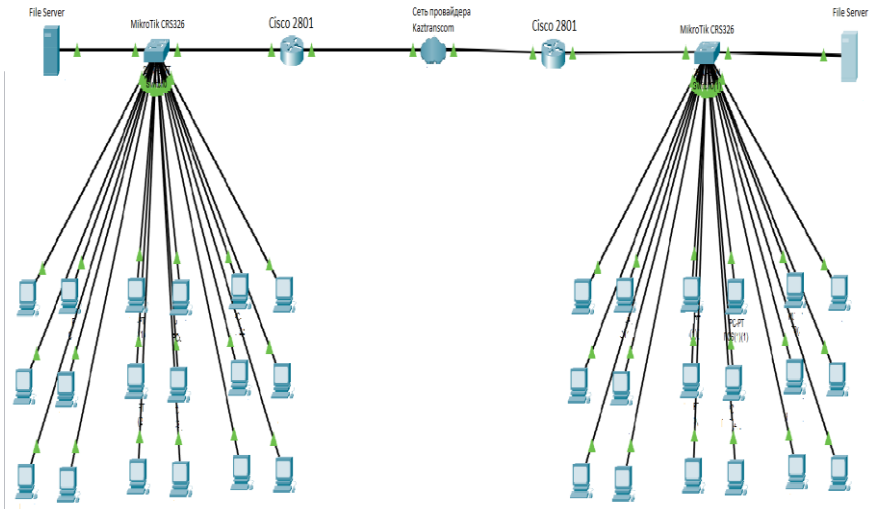



Рисунок 3.8 - Сеть подключения к пограничному маршрутизатору

По расчетам ясно, что для оптимальной работы пропускной способности канала сети, в которой не произойдет очередь пакета это 30 бит/с. В такой полосе пропускания если брать среднее время ожидания обслуживания одного пакета составит 0,440 мс, и среднее время ожидания 0,421 мс. Опираясь на расчеты нужно купить у выше стоящего провайдера канал с размером 52 мбит/с для оптимальной работы.

## 4 Мероприятия по обеспечению безопасности жизнедеятельности

### 4.1 Анализ условий труда

В данном разделе мы рассмотрим условия труда в Аспан телеком, в котором расположено семь компьютера и работают непосредственно десять человек.

Помещение где находится серверный отдел в отдельном помещении содержится оборудование, оно требует стабильное охлаждения для нормальной работы. Так же нужно обеспечить стабильное освещение для комфортной работы сотрудников компании, из естественного освещения только два окна в комнате.

В административном отделе поменяли систему охлаждения вентиляции на сплит-системы кондиционирования что повысит охлождения помещения и комфорт. В этой работе будут произведены замены и реконструкция естественного освещения и так же будет расчет искусственного освещения. В нашем помещении не достаточно хорошее освещение и за расположения офиса не с солнечной стороны даже в дневное время суток и это затрудняет работу. И за этой проблемы требуется заменить текущее освещение и произвести реконструкцию всего освещения офиса заменить старые лампы на новые и так же нужно правильно расположить их.

Для анализа достаточно будет произвести для начало естесвенное освещение и так же произведем анализ труда в помещении. В помещении расположены два окна не с солнечной стороны свет там минимальный и в течении дня темно. Высота рабочей поверхности над уровнем пола - 0,8 м, окна с размерами длина – 1,4 м, ширина – 1,4 м.

Помещение с размещенным оборудованием имеет размеры: длина L=15 м, ширина B=10 м, высота H=3 м рисунок 4.1.

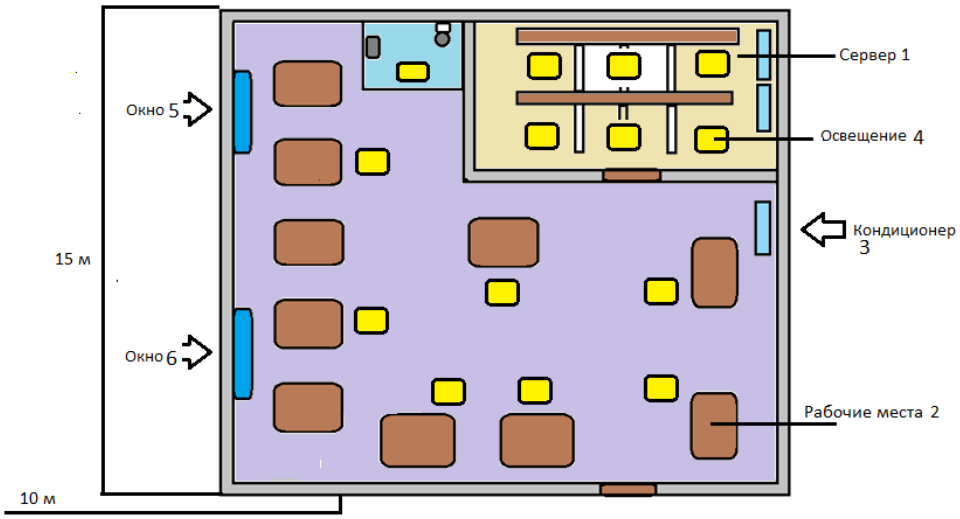



Рисунок 4.1 - План помещения

Оптические усилители которые находятся в серверной они являются основной из узлов базовой станции. На текущее время эти усилители применятся и находятся в широком применении. Современное состояние технологического развития позволяет вводить различные примеси в оптические волокна кварцевых волокон. В частности, редкоземельные элементы со спектром люминесценции в окнах прозрачности волокна (I = 1,54 мкм, I = 1,32 мкм и др.) и пики поглощения в области производства полупроводниковых лазеров (I = 808 нм, I = 980 нм, I = 1480 нм), через которые оптическое волокно, активированное таким образом, может накачиваться излучением этих лазеров.

### 4.2 Расчет естественного освещения

Произведем общий расчет освещения для рабочего помещения длинной A = 15 м, шириной B = 10 м, высотой H = 3 м, двумя окнами с раскрытыми жалюзи. Площадь каждого окна составляет 1,96 м$^2$ , размеры окон составляют 1,4 метра по длине и 1,4 метр по высоте.

Рассчитаем значение требуемой поверхности светового потока, которое обеспечивает нормированные значения естественного коэффициент света, это значение можно рассчитать по формуле в процентах от занимаемой площади

$$100 \cdot \frac{S_0}{S_n} = \frac{e_{H*}\eta_0 * К_з * К_{зд}}{\tau_0 * r_1}, \quad (4.1)$$

где $S_0$- площадь света, м$^2$;

$S_n$- диапазон зоны пола, м$^2$;

Площадь пола определяется по данной формуле. [50].

$$S_n = L \cdot B, \quad (4.2)$$

$$S_n = 15 \cdot 10 = 150 \ (м^2).$$

$e_N$ - нормируемое значение КЕО;

Нормированные значения КЕО для зданий располагаемых в различных районах следует определить по формуле:

$$e_N = e_H * m_N. \quad (4.3)$$

$$e_N = 1.5 \cdot 0.65 = 0.975 \ (e_N).$$

где N –номер группы обеспеченности естественным светом;

$e_н$ = 1,5 значения КЕО при боковом естественном освещении (для работ средней точности IV разряда) по таблице 3.12;

$m_N$ = 0,65 – коэффициент светового климата Алматы при ориентации окон на запад по таблице 3.1.

$К_з$ =1,2 – коэффициент запаса при вертикальном расположении светопропускаемого материала, берем данное значение из таблицы 3.11;

$К_{зд}$ =1,2 – коэффициент, учитывающий затемнение окон противостоящими зданиями по таблице 3.8;

$\tau_0 = 0{,}4$ – общий коэффициент светопроницаемости оконного проема.

Далее определяем $\eta_0$. Отношение длины к глубине (т.е. более удаленной точки окна).

$$l = B - 1м = 10 - 1 = 9 \ (м) \quad (4.4)$$

$$\frac{L}{l} = \frac{15}{9} = 1.666 \quad (4.5)$$

Отношение глубины помещения к высоте от уровня условной рабочей поверхности до верха окна

$$\frac{1}{h_1} = \frac{9}{2.2} = 4.09\ (h1) \qquad (4.6)$$

$$h_1 = h_{ок} + h_{н\ ок} - h_{р.п} \qquad (4.7)$$

где $h_1$ – высота уровня рабочего слоя до верха окна;

$h_{р.п}$ –высота рабочей поверхности над полом (0,8÷1,4) м;

$\eta_0$= 10,5 - световая характеристика окон, принимают по таблице 3.2.

Для улутшения труда офиса следует в помещение где находится серверный отдел в отдельном помещении содержится оборудование, оно требует стабильное охлаждения для нормальной работы. Так же нужно обеспечить стабильное освещение для комфортной работы сотрудников компании, из естественного освещения только два окна в комнате. В качестве легкого раздаточного материала мы используем двухслойные, двухслойные окна, двойные кожевенные деревянные держатели, виды покрытия подшипников – стальную ферму. Мы используем регулируемые шторы, получаемые в качестве устройства защиты от солнечных лучей.

Определим общий коэффициент светопропускания

$$\tau_0=\tau_1 \cdot \tau_2 \cdot \tau_3 \cdot \tau_4, \qquad (4.8)$$

где $\tau_1$ – коэффициент светопропускания материала по таблице 3.3;

$\tau_2$ – коэффициент, учитывающий потери света в переплетах светопроема;

$\tau_3$ – коэффициент, учитывающий потери света в несущих конструкциях;

$\tau_4$ – коэффициент, учитывающий потери света в солнцезащитных устройствах.

$$\tau_1 = 0{,}8;\ \ \tau_2 = 0{,}7;\ \tau_3 = 0{,}9;\ \ \tau_4 = 1.$$

$$\tau_0=0{,}8 \cdot 0{,}7 \cdot 0{,}9 \cdot 1{,}4=0{,}705.$$

Определяем коэффициент r1 – для бокового освещения. Для этого находим: отношение глубины к высоте от уровня условной рабочей поверхности до верха окна

$$\frac{l}{h_1} = \frac{3}{2{,}2} = 1{,}36,$$

отношение глубины помещения к ширине помещения

$$\frac{l}{B} = \frac{3}{10} = 0{,}3,$$

отношение длины помещения к его глубине

$$\frac{L}{l} = \frac{15}{3} = 1{,}833.$$

Коэффициент r1=1.9 .

Величину средневзвешенного коэффициента отражения $\rho_{ср}$ потолка, стен и пола определяется по формуле

$$\rho_{ср} = \frac{(\rho_1 \cdot S_1 + \rho_2 \cdot S_2 + \rho_3 \cdot S_3)}{S_1 + S_2 + S_3} \cdot 100(\%). \quad (4.9)$$

Площадь потолка $S_1$=15·10=150 (м$^2$); площади стен $S_2$=2·(15+10) · 3=150 (м$^2$); площадь пола $S_1$=15· 10=150 (м$^2$).

$$\rho_{ср} = \frac{(70 \cdot 150 + 50 \cdot 150 + 30 \cdot 150)}{150 + 150 + 150} = 50\% = 0{,}5.$$

Подставляя все значения в формулу (5.1) получим значение КЕО

$$S_0 = \frac{150 \cdot 0{,}705 \cdot 10{,}5 \cdot 1{,}2 \cdot 1{,}2}{100 \cdot 0{,}504 \cdot 1{,}9} = 8{,}6 \text{ (м}^2\text{)}.$$

Вывод: Мы рассчитали площадь боковых световых проемов, которая необходима для создания нормируемой освещенности на рабочих местах для разряда зрительной работы IV, б. Так как в помещении имеются окна площадью $S_{ок}$=1,4 м$^2$ , а рассчитанное значение площади боковых проемов получилось равным 8,6 м$^2$, то требуются дополнительные источники света, т.е. необходимо провести расчет искусственного освещения.

### 4.3 Расчёт искусственного освещения точечным методом

Рассчитаем искусственное освещение для операторской комнаты.

Исходные данные:

– ширина комнаты равна значению B = 10м;

– длина комнаты помещения составляет L = 15м;

– высота комнаты равна значению H = 3 м.

В помещении смонтированы два светильника Philips мощностью 40 Вт, со световым потоком 2248 лм, диметром 54мм и длиной 1,5 м.

Общая схема помещения представлена на рисунке 4.2.

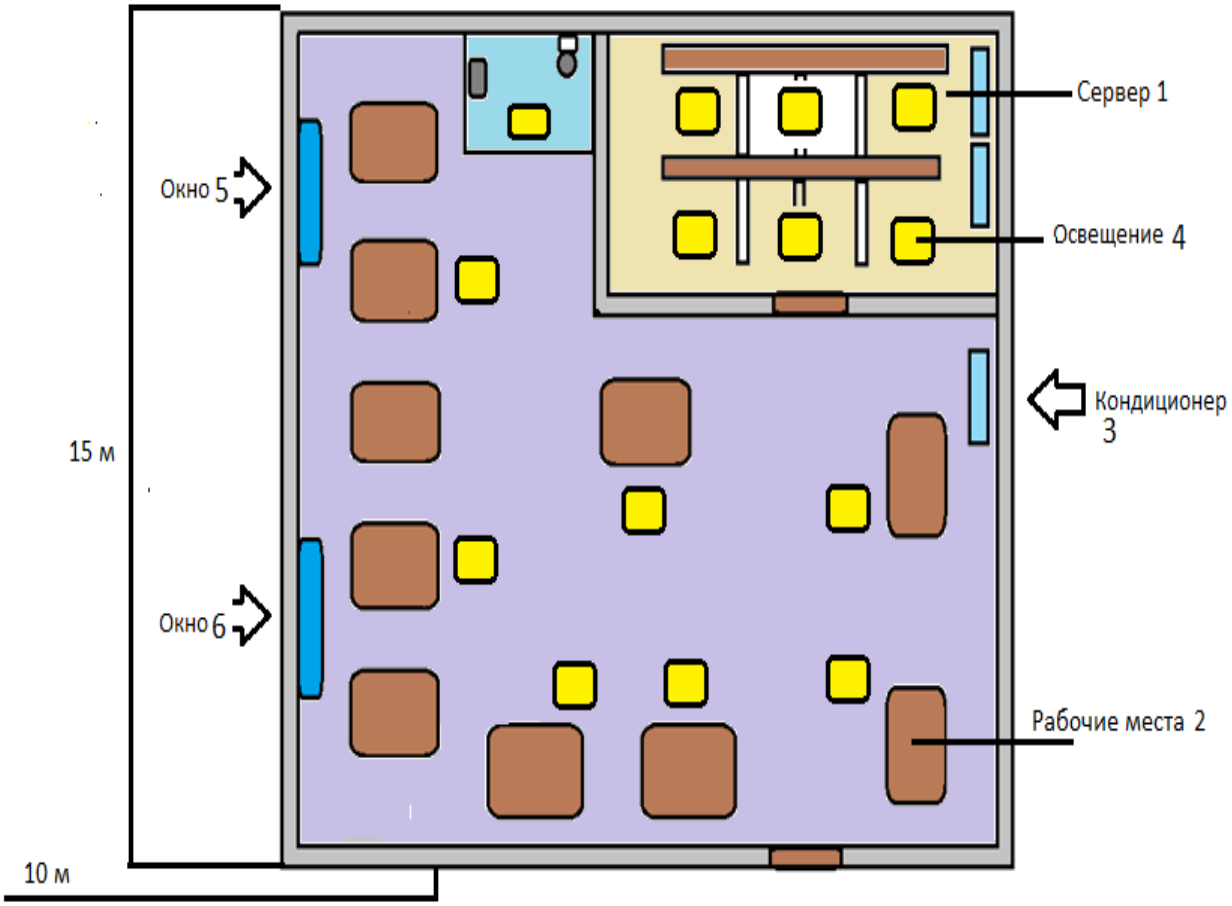



Рисунок 4.2–Схема размещения светильников до изменения

Размещение светельников в помещении определяется следующими параметрами:

- H – высота помещения;
- $h_c$ – расстояние свеса ламп (0,5 м);
- $h_{рп}$ – высота рабочей поверхности над полом (0,8м);
- hp=Hп−hсвеса−hр.пов. – расчетная высота, высота светельника над рабочей поверхностью.

$$h_р=H_п-h_{свеса}-h_{р.пов}\,, \qquad (4.10)$$

$$h_р=3-0{,}5-0{,}8=1{,}7\ (м).$$

Расстояние от светильника до исследуемых точек $d_1$, $d_2$. [54].

$$C=\frac{l_1}{2}=\frac{3}{2}=1{,}5\ (м), \qquad (4.11)$$

$$b_1=1{,}5\ м;\ b_2=2\ (м),$$

$$d1=\sqrt{1,5^2+1,5^2} = 2,12,$$

$$d2=\sqrt{2^2+1,5^2} = 2,5.$$

Угол α и $I_a$ определим силу света для каждого светильника по формуле.

$$\text{tg}\ \alpha=\frac{d}{h}, \qquad (4.12)$$

отсюда для d1

$$\text{tg}\ \alpha_1=\frac{2,12}{1,3}=1,63,$$

$$\alpha_1= \text{arctg}(1,63) = 58,47°,$$

$$\cos^3 \alpha_1 = 0,141,$$

отсюда для d2:

$$\text{tg}\ \alpha_2=\frac{2,5}{1,3}=3,25,$$

$$\alpha_2= \text{arctg}(3,25) = 72,9°,$$

$$\cos^3 \alpha_2 = 0,02.$$

Находим силу света от каждого источника по рисунку 4.3.

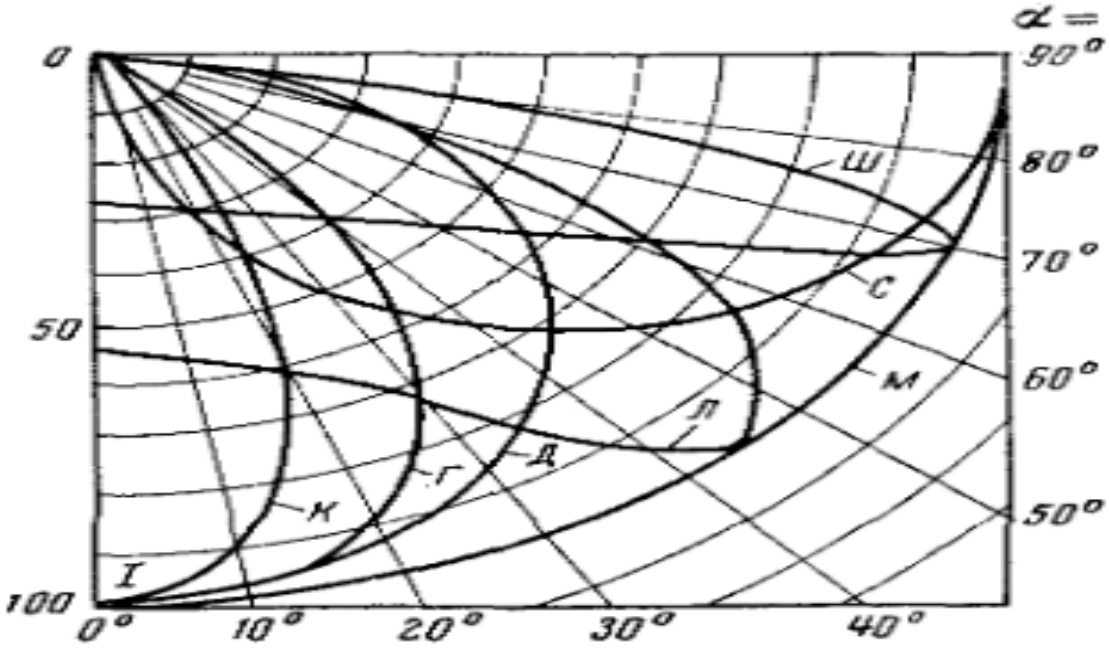


Рисунок 4.3 - Типовые кривые силы света светильников

$I_{\alpha 1}$=74 (кд),

$I_{\alpha 2}$=36 (кд).

Горизонтальная освещенность в точке А от одного светильника определяется по формуле

$$e_г = \frac{I_\alpha \cdot \cos^3\alpha}{h^2}. \quad (4.13)$$

Подставим полученные значения в формулу 5.11

$$e_{г1} = \frac{74 \cdot 0{,}141}{1{,}7^2} = 3{,}61 \text{ (лк)},$$

$$e_{г2} = \frac{36 \cdot 0{,}02}{1{,}7^2} = 0{,}25 \text{ (лк.)},$$

$$\Sigma e_г = 3.61 + 0{,}25 = 3.86 \text{ (лк)}.$$

Освещенность в точке определяется по формуле

$$E_Г = \frac{n \cdot Ф \cdot \mu}{1000 \cdot К_з} \cdot \sum e_г \text{, лк.} \quad (4.14)$$

Подставим значения в формулу

$$E_Г = \frac{1{,}1 \cdot 2248 \cdot 2}{1{,}2 \cdot 1000} \cdot 3{,}86 = 15{,}9 \text{ (лк)}.$$

Вывод: Данного освещения недостаточно для комфортной работы, исходя из расчетов видно, что данное условие не выполняется, т.е . Er = 15,8 лк<200 лк, следовательно нужно провести реконстукцию Требуется увеличить мощность лампочек, либо количество светильников.

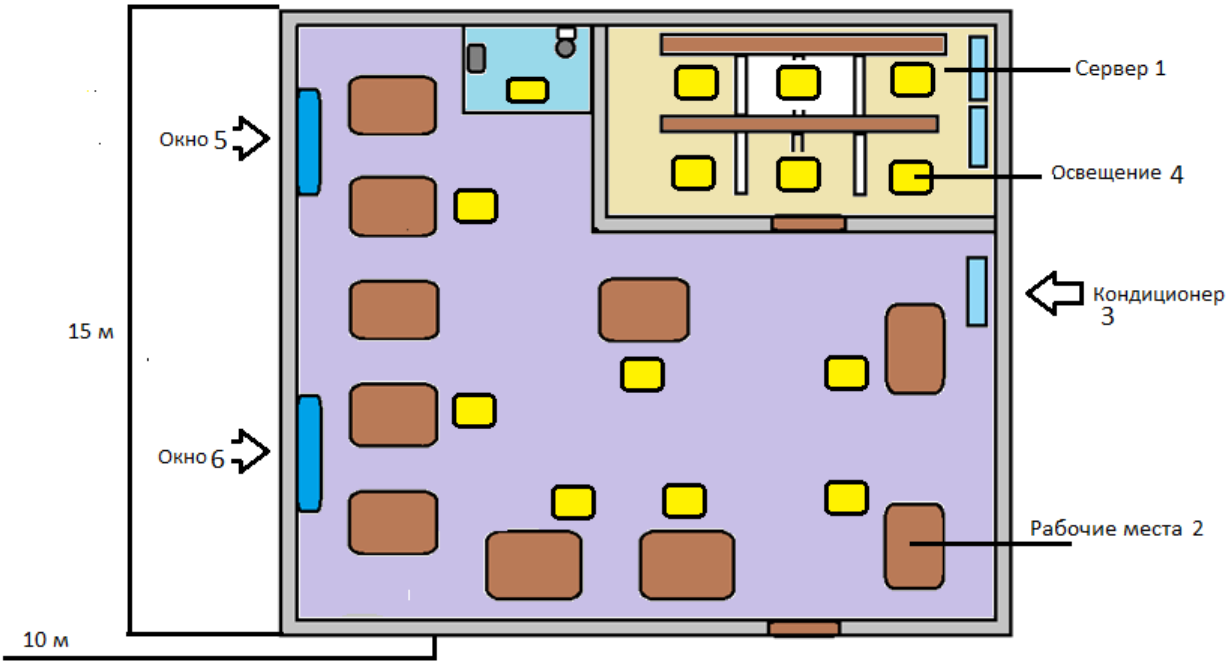
### 4.4 Расчет искусственного освещения методом коэффициента использования светового потока

Трудовое место для выполнения работы, в положении сидя, отвечает требованиям ГОСТа (ГОСТ 12.2.032-78. «ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования»). В устройстве его элементов учтем характер работы, психологические особенности человека и его антропометрические данные.

Техническое помещение обладает следующими размерами: длина А=15 м, ширина В=10 м, высота Н=3 м. Высота трудовой поверхности над уровнем

пола составляет 0,8 м, окна устанавливаются с высоты 0,8 м от уровня пола, высота окон составляет 1,4 м.

План размещения оборудования представлен на рисунке 4.4.




2 -окна, 10 - рабочих мест, 3 шт - систем кондиционирования.

Рисунок 4.4 – Внутреннее расположение объектов в офисе.

Анализируемое в дипломном проекте офисное помещение прямоугольной формы, размерами: длина – 15 метров, ширина – 10 метров, высота – 3 метра. Данное помещение рассчитано на 10 рабочих мест т.к. на 1 человека полагается 6,2 м$^2$ трудового пространства.

Организация необходимого освещения. Одним из важнейших условий жизни для человека является свет. Он воздействует на само состояние организма, верно сформированное освещение стимулирует протекание процессов высшей нервной деятельности и поднимает работоспособность. При недостаточном освещении человек стремительно устает, возрастает возможность ошибочных действий, что повергает к ухудшению здоровья.

Освещение рабочего помещения удовлетворяет следующим условиям:

– освещенность рабочих поверхностей соответствует гигиеническим нормам для данного вида работы;

– имеется 2 окна размером 2х1,4 метра. Величина коэффициента естественной освещенности (к. е. о.) при выполнении работ средней зрительной точности не ниже 1,2%. Искусственное освещение осуществляется в виде общей системы освещения с использованием люминесцентных источников света;

– пульсация освещенности используемых люминесцентных ламп не превышает 10%. В качестве средств затемнения используются регулируемые. Окна размещены с одной стороны рабочего помещения.

Выбор параметров освещения рабочего места зависит от характера производимой работы. Объект различения определяется наименьшим размером предмета (детали) или его части. В зависимости от размеров объекта различения и расстояния предмета от глаз, работающего, все работы делятся на восемь разрядов точности. Если расстояние от глаз до предмета меньше 0,5 м, разряд работы определяется размером объекта различения.

Нормирование параметров микроклимата. Для поддержания необходимых микроклиматических условий в соответствии с требованиями «Санитарных норм, микроклимата производственных помещений» и нормального функционирования оборудования в операторной установлен кондиционер. Нормативные показатели микроклимата приведены в таблице 4.1.

Организация кондиционирования воздуха. В офисном помещении размером 15х10х3 метра объемом 450 $м^3$ работает 10 человек. В помещение подается следующий объем наружного воздуха: при кубатуре помещения до 30 $м^3$ на одного работающего – не менее 20 $м^3$/ч на человека. Воздух, поступающий в офисное помещение, очищен от загрязнений, в том числе от пыли и микроорганизмов.

Контроль состояния микроклимата в производственных помещениях позволяет поддерживать условия труда, близкие к нормам, что увеличивает комфортность труда и производительность. Поскольку в офисе для сотрудников основной является работа за компьютером, то тяжесть работ, производимых в помещении можно отнести к средней.

Таблица 4.1 – Нормы микроклимата производственных помещений при выполнении работ средней тяжести

| Период года | Температура, С | | Оптимальная влажность, % | | Скорость движения воздуха, м/с | |
|---|---|---|---|---|---|---|
| | Оптим. | Допуст. | Оптим. | Допуст. | Оптим. | Допуст. |
| Холодный период года | 18-20 | 17-23 | 40-60 | 75 | 0,2 | Не более 0,1 |
| Теплый период года | 21-23 | 18-27 | 40-60 | 65 при 26 С | 0,3 | 0,2-0,4 |

Так как температура и оптимальная влажность в операторской не соответствует требованиями «Санитарных норм, микроклимата производственных помещений» (таблица 5.6), необходим расчет кондиционирования. Ниже приведён подробный расчёт системы обеспечения

оптимального микроклимата с выбором конкретного оборудования.

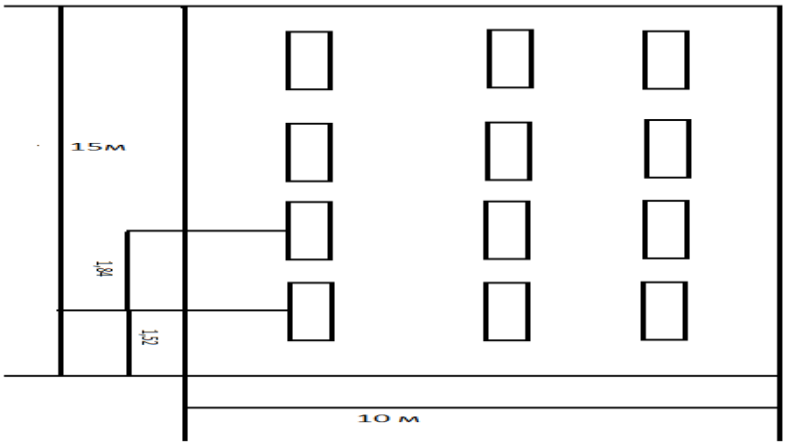



Рисунок 4.5 – Расположение светильников

Вывод: Мы произвели расчет искусственного освещения точечным методом. Исходя из расчетов, можно увидеть, что текущее искусственное освещение в комнате не удовлетворяло соответствующим нормам. Поэтому была произведена реконструкция операторской комнаты, заменены старые светильники на новые, а также добавлен еще один дополнительный светильник.

# 5 Бизнес план

## 5.1 Цели и задачи

Главной цель этого проекта является объединение компании для предоставления услуги интернета и доступа к серверам через сети VPN что является для организации экономией так как не нужно дополнительно строить сеть где сети Аспан телеком не пересекаются, следовательно снижаются затраты на строительстве и тем самым мы экономим ресурсы компании что является основной целью.

## 5.2 Компания и отрасль

Компания занимается услугами предоставления интернета и телефонии. Эти услуги пользуются огромным спросом так как подключение идет юридических лиц, то есть идет подключение сетей общепита, бизнес центров, магазины и сети занимающиеся предоставлением разных услуг, подключение идет по средством радио, оптика, VPN, и канал ПД.

## 5.3 Описание услуги

Предоставление услуг идет по техногиям которые используется в компании то есть это оптика, радио, vpn и канал ПД. Компания развивается в основном в технологии радио тем самым предоставляя доступ интернета в трудно доступные участки где не возможно подключится иным способом к

сети интернет у компании много выделенных радио частот на оборудование wi-max и wifi они являются основным козырем компании, потому как на этих частотах работает только оборудование компании Аспан телеком оно обеспечивает стабильную скорость даже в плохих погодных условиях, с экономической точки зрения идет экономия на расходных материалах, нужно всего две антенны радио доступа и все.

### 5.4 Оперативный план

Для выполнения плана стоят конкретные задачи в порядке действий для каждого города:

- аренда помещения под офис;
- купить подходящее оборудования для настройки сети;
- транспортировка и установка оборудования;
- закуп инвентаря и оборудования для организации рабочих мест;
- транспортировка инвентаря и организация рабочих мест;
- поиск и найем сотрудников;
- начало деятельности.

В работе предоставления услуги интернета нужно иметь базу с клиентами тем самым база будет хранится на сервере либо в нашем случае в техническом офисе, база представляет собой биллинговую систему где хранятся все данные о клиенте для создания системы биллинга нужен сервер с большим файловым пространством и более мощным железом.

С целью экономии больших средств на сервере, можно использовать уже существующий сервер для обьдинение и создание общей базы в городе Алматы для этого используется технология Виртуальная Локальная Сеть (VPN) она объеденяет в одну локальную сеть офисы компаний в разных местах расположения. Это решение позволяет не прокладывать провода и радио доступ, соединить в сеть офисы компании что экономит большие денежные средства компании.

Нужное оборудование для создания VPN сети указано и приведено ниже таблице 5.1.

Таблица 5.1 – Оборудование для организации локальной сети офиса

| Наименование | Ед.измерения | Цена, тенге | Сумма, тенге |
|---|---|---|---|
| Cisco 2901 | 2 шт. | 720000 | 1 440 000 |
| D-Link DES-3200-28/C1A 24 | 2 шт. | 114770 | 229 540 |
| Модуль SFP TX | 2 шт. | 77000 | 154 000 |
| Модуль SFP TRJ45 | 2 шт. | 78000 | 156 000 |
| FTP кабель | 1000 м. | 100 | 100 000 |
| Итого | | | 2 069540 |
| Доп. Расходы неучтенные расходы (10%) | | | 2079540 |
| Всего | | | 2 287494 |

Необходимое оборудование и инвентарь для организации рабочих мест приведены в таблице 5.2.

Таблица 5.2 – Оборудование для организации рабочих мест

| Наименование | Кол-во, шт. | Цена, тенге | Сумма, тенге |
|---|---|---|---|
| Персональный компьютер | 20 | 80 000 | 1 600000 |
| Ноутбук | 4 | 110000 | 440 000 |
| Стол офисный | 20 | 25000 | 500 000 |
| Стул офисный | 2 | 10585 | 211700 |
| Принтер Work Ce-B215 | 2 | 108500 | 217000 |
| Итого | | | 2 968700 |
| Доп. расходы | (10%) | | 2968700 |
| Всего | | | 3265570 |

Что было удобно работать в коллективе было решено создать иерархию должностей для того что бы работник был постоянно в сети не зависимо где н находится в какой точки мира, что бы получал письмо на корпоративную почту и мог спокойно работать в удаленно и ведь так работа сотрудника будет более продуктивна.

Таблица 5.3– Основной персонал в городе Алматы

| Должность | Кол-во сотрудников | Ежемесячная зар. плата одного сотрудника, тенге | Ежемесячная зар. плата всех сотрудников, тенге |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| Тех.Директор | 1 | 300000 | 300000 |

*Продолжение таблицы 5.3*

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| IT инженер | 1 | 200000 | 200000 |
| Радио инженер | 1 | 200000 | 200000 |
| VoIP инженер | 1 | 200000 | 200000 |
| Начальник линейного отдела | 1 | 150000 | 150000 |
| Монтажники | 6 | 110000 | 660000 |
| Итог | 11 | | 1710000 |

Таблица 5.4 - Основной персонал в городе Алматы на Шевченко 165

| Должность | Кол-во сотрудников | Ежемесячная зар. плата одного сотрудника, тенге | Ежемесячная зар. плата всех сотрудников, тенге |
|---|---|---|---|
| Коммерческий директор | 1 | 300000 | 300000 |
| Менеджера | 7 | 80000 | 560000 |
| Бухгалтер | 1 | 120000 | 120000 |
| Итог | 9 | | 980000 |

## 5.5 Финансовый план

В этой части проведены расчеты общих затрат, дохода, прибыли, экономической эффективности и срока окупаемости.

Капитальные затраты определяются по формуле

$$K = Ц + K_{П} + K_{У} + K_{Пом} + K_{оргрм}, \quad (5.1)$$

где Ц – цена оборудования сети;

$К_П$ – стоимость перевозки оборудования;

$К_У$ – стоимость монтажа и установки оборудования;

$К_{Пом}$ – стоимость аренды помещения;

$К_{оргрм}$ – стоимость организации рабочих мест.

В таблице 5.5 приведены капитальные затраты на оборудование.

Таблица 5.5 – Капитальные затраты на оборудование

| Наименование | Стоимость, тенге |
|---|---|
| Стоимость оборудования, (Ц) | 2 287494 |
| Перевозка оборудования, (Кп, составляет 5% от стоимости оборудования) | 114374,7 |
| Установка и монтаж оборудования, (Ку, составляет 8% от стоимости оборудования ) | 182999,52 |
| Итого | 2584868,22 |
| Доп. неучтенные расходы (10%) | 258486,2 |
| Всего | 2 843354,42 |

Таблица 5.6 – Общие капитальные затраты

| Наименование вложений | Стоимость, тенге |
|---|---|
| Капитальные затраты на оборудование, транспортировку и установку | 2 843354,42 |
| Капитальные затраты на организацию рабочих мест | 3419200.1 |
| Капитальные затраты на аренду помещения в г. Алматы | 250000 |
| Капитальные затраты на аренду помещения в г. Алматы на Шевчнко 165 | 300000 |
| Итого (К=) | 6599340,1 |

Эксплуатационные расходы определяются по формуле

$$Э = ФОТ + О_с + А + М + С_{ЭЛ} + С_{АДМ}, \quad (5.2).$$

где ФОТ – Фонд оплаты (основная и дополнительные заработные платы)

$О_с$ – социальный налог

А – амортизационные отчисления;

М – затраты на материалы и запасные части;

$С_{ЭЛ}$ – электроэнергия со стороны производственных нужд;

$С_{АДМ}$ – прочие административные управленческие и эксплуатационные расходы;

Основная заработная плата за год составит

$$ЗП_{ОСН} = 32\ 280000 \text{ (тенге).}$$

Дополнительная заработная плата – это 30% от основной

$$ЗП_{ДОП} = ЗП_{ОСН} \cdot 0.3 = 9684000 \text{ (тенге).} \quad (5.3)$$

Фонд оплаты труда есть сумма основной и дополнительной заработной платы

$$ФОТ = ЗП_{ОСН} + ЗП_{ДОП} = 32280000 + 9684000 = 41964000 \text{ (тенге).} \quad (5.4)$$

Социальный налог составляет 11% от фонда оплаты труда

$$О_с = ФОТ \cdot 0,13 = 41964000 \cdot 0,13 = 5455320 \text{ (тенге).} \quad (5.5)$$

Амортизационные отчисления для оборудования в отрасли связи может быть до 25% в год от стоимости оборудования. Возьмём примерное значение 12%:

$$А_1 = 2287494 \cdot 0,12 = 274499,28 \text{ (тенге).}$$

Амортизационные отчисления для компьютерной техники составляет до 40% в год, возьмем 20%. [62].

$$А_2 = (1600000 + 440000 + 211700) \cdot 0,2 = 450340 \text{ (тенге).}$$

Амортизация офисной мебели составляет 15% от цены:

$$А_3 = (500000 + 211700) \cdot 0,15 = 106755 \text{ (тенге).}$$

$$А = А_1 + А_2 + А_3 = 294016,8 + 450340 + 106755 = 851111,8 \text{ (тенге).} \quad (5.6)$$

Затраты на электроэнергию рассчитываются следующей формулой

$$С_{ЭЛ} = W \cdot T \cdot S, \quad (5.7)$$

Для города Алматы.

где W = 25,40 кВт - потребляемая мощность;
T = 2160 ч/год – Количество часов работы;
S = 14,76 тг/кВт×час – Стоимость киловатт-часа электроэнергии.

$C_{ЭЛ1}$ = 25,40· 2160 ·14,76 = 809792,64 (тенге).

Для города Алматы: Шевченко 165.

Где W = 6,45 кВт - потребляемая мощность;
T = 2160 ч/год – Количество часов работы;
S = 14,76 тг/кВт*час – Стоимость киловатт-часа электроэнергии.

$$C_{ЭЛ2} = 6,45 \cdot 2160 \cdot 14,76 = 205636,32 \text{ (тенге).}$$

$$C_{ЭЛ} = 809792,64 + 205636,32 = 1015428,96 \text{ (тенге).}$$

Затраты на материалы и запасные части для оборудования ценятся в размере 5% от стоимости оборудования

$$M = 2287494 \cdot 0,05 = 114374,7 \text{ (тенге).}$$

Прочие расходы составляют 40% от фонда оплаты труда

$$C_{АДМ} = ФОТ \cdot 40\% = 41964000 \cdot 0,4 = 16785600 \text{ (тенге).} \quad (5.8)$$

Теперь посчитаем эксплуатационные расходы

$$Э = ФОТ + O_c + A + M + C_{ЭЛ} + C_{АДМ} = 66185835,46 \text{ (тенге).} \quad (5.9)$$

На рисунке 5.1 приведены доли эксплуатационных расходов.

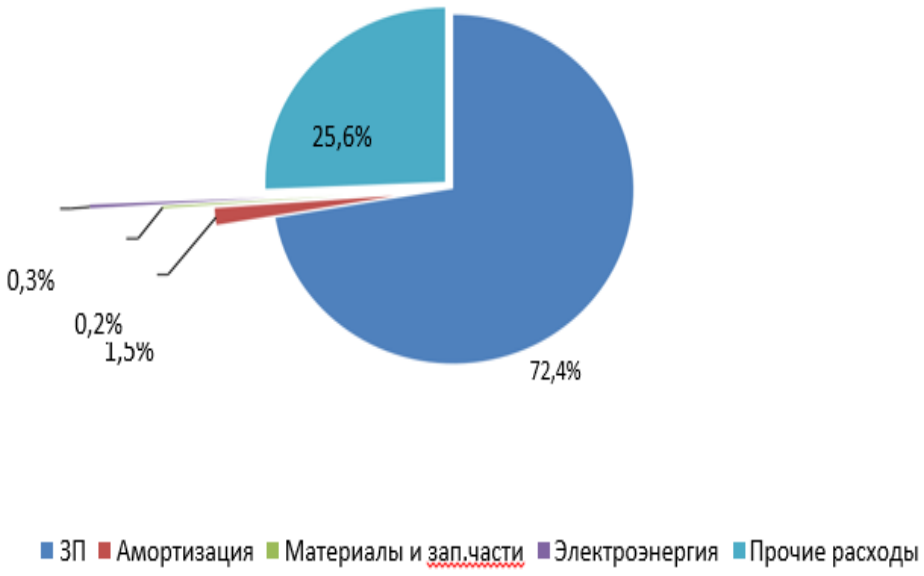



Рисунок 5.1 – эксплуатационные расходы по частям в процентах

В городе Алматы очень развиты отрасли производства и бизнеса им постоянно не обходим доступ в интернет так как работа связана на прямую через онлайн обслуживание так же нету необходимости ездить и тратить время все компании занимаются обслуживанием онлайн, основными клиентами компании являются бизнес центры, рестораны и кафе, заводы, торговые центры и заправочные станции. Всем им нужно выходить в сеть интернет для оплаты счетов, проверки почты, для облсуживание клиентов и взаимодействия с ними. республике

В городе Алматы насчитывается население в 1916822 человек. Примерно 35% на долю населения насчитывается владельцы частных предприятий бизнеса. Это означает, что 670887,7 владеют бизнесом и предприятию нужен доступ в интернет для работы в сфере услуг.

Мною были насчитаны около 8 конкурентоспособных известных интернет компаний действующих на территории Алматы.

Цена за подключение составляет 20 000 тг.

Таким образом, годовой доход от подключенных клиентов в городе Алматы примерно составляет 91 345 531 тг. с вычетом 45% убыток с оборудований.

Аналогичным образом проведен расчет годового дохода в городе Алматы и показан в таблице 5.7.

Таблица 5.7 – В г. Алматы

| Параметры | Расчет |
|---|---|
| Население в Алматы | 1916822чел. |
| Колличество конкурентоспособных компаний | 10 компаний |
| Доля население владеющие бинеснесом | 75% |
| Убыток компании в сфере услуг интернета | 45% |
| Цена за подключение интернета | 20000 тг. |
| Доход от подключенных клиентов | 61647846,4тг. |

Таблица 5.8 –В г. Алматы Шевченко 165 б

| Параметры | Расчет |
|---|---|
| Население в Алматы | 1916822 чел. |
| Колличество конкурентоспособных компаний | 10 компаний |
| Доля население владеющие бинеснесом | 75% |
| Убыток компании в сфере услуг интернета | 45% |
| Цена за подключение интернета | 16000 тг. |
| Доход от подключенных клиентов | 50288472 тг. |

Общий годовой доход ожидаемый от данного проекта составляет 111936318 тг.

Доход от основной деятельности

$$Д_{осн} = Д_{реал}(год) – Эр, \quad (5.10)$$

$$Д_{осн} = 111936318 – 66185835,46 = 45750483 \text{ (тенге)}.$$

С учетом налогообложений чистый доход будет равен

$$Д_{чист} = Д_{осн} – 0.2 \cdot Д_{осн} = 45750483 – 0.2 \times 4112812.292 = 44927920,5416 \text{ (тенге)}.$$

Таким образом Абсолютная экономическая эффективность будет равна

$$E = 41637670,708 / 6599340,1 = 6,8 \text{ (Е)}.$$

Расчетный срок окупаемости определяется как величина, обратная абсолютной экономической эффективности

$$T = 1/E = 1/6.8 = 2 \text{ (месяца)}. \quad (5.12)$$

Проект планируется окупить в 9 месяцев.

Далее определим величину дисконтированных доходов по формуле

$$PV = \sum_{t=1}^{t=n} \frac{Pt}{(1+r)_t}, \qquad (5.13)$$

где r – ставка дисконты (20%)

t – год:

| | |
|---|---|
| 1 год | 13709374.30 тенге |
| 2 год | 11424478.58 тенге |
| 3 год | 9520398.82 тенге |
| 4 год | 7933665.68 тенге |
| 5 год | 6611388.07 тенге |

Чистый приведенный эффект (NVP) определяется по формуле:

NPV=PV-И [64].

(5.14)

Далее осуществляется выбор проекта, исходя из следующих случаев:

NPV>0, проект прибыльный и его следует принять;

NPV<0, проект убыточный и его следует отвергнуть;

NPV=0, проект не прибыльный и не убыточный. Такой проект может быть реализован из других соображений (например, престижа).

Для определения экономической эффективности проекта рассчитываем чистую текущую стоимость проекта.

Чистая текущая стоимость проекта определяется по формуле

$$NPV = \sum_{t=1}^{n} \frac{Pt}{(1+r)^t} - И, \qquad (5.15)$$

где И – сумма первоначальных инвестиций; [65].

r – норма дисконта;

n – срок проекта, лет;

Pt – денежный поток в году t:

NPV = (13709374,30 + 11424478,58 + 9520398.82 + 7933665,68 + 6611388,07) – -12957401=36241904,478 (тенге).

$$NPV = \frac{(12918974{,}31 + 10765811{,}92 + 9520398.82 + 7476258{,}279 + +6230215{,}233)}{12957401} = 3{,}797(P).$$

PI = (12918974,31 + 10765811,92 + 9520398,82 + 7476258,279 + +6230215,233)/ 12957401 = 3,797 (Pi).

Из этого становится ясно, что проект очень эффективный и выгодный, так как индекс рентабельности очевидно больше единицы.

В таблице 5.9 приведены итоговые показатели расчета.

Таблица 5.9 – Итоговая таблица

| Наименование | Значение |
|---|---|
| Капитальные затраты, тг. | 6599340.1 |
| Эксплуатационные расходы, тг. | 65346555.46 |
| Годовой доход основной деятельности, тг. | 20 564 061 |
| Чистый годовой доход, тг. | 16 451 249 |
| Экономическая эффективность | 1.27 |
| Срок окупаемости, месяцев | 8 |
| NPV, тг. | 36 241 904 |
| Индекс рентабельности (PI) | 3.797 |

Подведу итоги данного бизнес плана. Была смоделирована корпоративная сеть Аспан телеком на условии работы компании был произведен расчет рынка и услуги компании тем самым мы примерно по считали затраты на оборудование которое будет стоят так же затраты на содержание рабочего состава, в общем был проведен полный анализ и подведены итоги, тем что корпоративная сеть Аспан телеком окупится от 2 до 11 месяцев.

## Заключение

Данный дипломный проект является актуальным для корпоративной сети, была рассмотрена технология VPN и которая объединяет корпоративную сеть в одну общую, тем самым облегчая удаленную работу сотрудникам компании это увеличивает продуктивность работников, и даже когда они находятся в дали от работы они могут проверять корпоративную почту и отправлять документы. Самым главным плюсом сети VPN является безопасное удаленное соединение которое шифрует передаваемые данные в режиме реального времени. Так же подобрано оборудование которое обеспечит стабильную работу сети . На выбранном оборудовании произвелась настройка VPN 3 уровня на базе протокола шифрования IPsec. Экономический расчет показал, что проект весьма выгоден, при этом срок окупаемости затрат составляет 8 месяцев, что является отличным показателем. Технология VPN была раскрыта а так же ее достоинства

## Список сокращений

VPN – Virtual Private Network

DMVPN – Dynamic Multipoint Virtual Private Network Ipsec – IP security

LCP – Link Control Protocol

MPLS – Multiprotocol Label Switching

ISP – Internet Service Provider

DHCP – Dynamic Host Configuration Protocol NAT – Network Address Translation

Vlan – Virtual Local Area Network

GRE – Generic Routing Encapsulation

OSPF – Open Shortest Path First

EIGRP – Enhanced Interior Gateway Routing Protocol BGP – Border Gateway Protocol NHRP – Next Hop Resolution Protocol

## Список литературы


1 Журнал «Теле-Спутник» - выпуск 156, стр 45, Октябрь 2008 г. «Сети Ethernet. часть. Metro Ethernet».

2 Аллен Д.,1-Глава,3 стр, Следующая волна VPN на базе IP.

3 Алгоритмы шифрования на Delphi.URL https://delphisources.ru/pages/faq/base/base64.html, (дата обращения: 1.04.2020г.).

4 NetCrackerProfessional 4.1.URL:http://soft-landia.ru/netcracker.html(датаобращения: 11.04.2020).

5 Назаров А.Н. Модели и методы расчета структурно-сетевых параметров сетей АТМ. – М.: Изд-во «Горячая линия-Телеком», 2002. -256 с.

6 Вишневский В.М. Теоретические основы проектирования компьютерных сетей- Москва.: 2003. – 506с.

7 Битнер В.И, Михайлова Ц.Ц –Сети нового поколения NGN – Москва.: Изд-во «Горячая линия-Телеком», 2011. - 226с.

8 Ложковский А.Г., Голубенко В.В. – Теория телетрафика – Одесса.: 2013г.

9 Росляков, А. В. Виртуальные частные сети. Теория и практика применения / А. В. Росляков. - М.: Эко-Трендз, 2007. - 304 с.

10 Корпоративные территориальные сети связи. Выпуск 3. Под ред. М.Б. Купермана. - М.: Информсвязь, 1997.

11 Рыжиков Ю. И. Теория очередей и управление запасами. - СПб: 2001.

12 Тихоненко О.М. Модели массового обслуживания в информационных системах: Учебное пособие для студ. вузов. - Минск: Технопринт, 2003. - с.

13 Ивченко Г.И., Каштанов В.А., Коваленко И.Н. Теория массового обслуживания / Рецензенты: кафедра математической статистики, теории надёжности и массового обслуживания факультета прикладной математики — процессов управления ЛГУ им. А.А. Жданова и д.т. н., профессор Р.Я. Судаков. — Учебное пособие для вузов. — М.: Высшая школа, 1982. — 256 с.

14 Вентцель Е. С., Овчаров Л. А. Теория вероятностей. Глава 10. Теория массового обслуживания. М., 1969, 368 стр.

15 Матвеев В. Ф., Ушаков В. Г. Системы массового обслуживания, 1984г.

16 Матвеев В. Ф., Ушаков В. Г. Системы массового обслуживания, 1979г.

17 Лифшиц А.Л., Мальц Э.А. Статистическое моделирование систем массового обслуживания, М.: Советское радио, 1978. - 249 с.

18 Проскурин В. Г., Крутое С. В., Мацкевич И. В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: учеб. пособие для вузов. М.: Радио и связь, 2000.

19 Шаньгин В.Ф. Информационная безопасность компьютерных

систем и сетей. // М.: Форум, 2008, 416 с.

20 Мельников В. П. и др. Информационная безопасность. // М.: Академия, 2005. 333 с.

21 Зима В. М., Молдовян А. А., Молдовян Н. А. Компьютерные сети и защита передаваемой информации. СПб.: Изд. СПбГУ, 1998.

22 Романец Ю. В., Тимофеев П. А., В. Ф. Шаньгин. Защита информации в компьютерных системах и сетях. 2-е изд. М.: Радио и связь, 2001.

23 Н. Девянин, О. О. Михальский, Д. И. Правиков Теоретические основы компьютерной безопасности: учеб. пособие для вузов / П. и др. М.: Радио и связь, 2000.

24 Человеческий фактор в обеспечении безопасности и охраны труда: Учебное пособие / П.П. Кукин, Н.Л. Пономарев, В.М. Попов, Н.И. Сердюк.— М.: Высшая школа, 2008.— 317 с.

25 Безопасность жизнедеятельности. Безопасность технологических процессов и производств. Охрана труда: Учебное пособие для вузов / П.П.Кукин, В.Л.Лапин, Н.Л. Пономарев. - Изд. 4-е, перераб. – М.: Высшая школа, 2007. – 335 с.

26 В.Н. Башкин Экологические риски: расчет, управление, страхование: Учебное посо-бие / В.Н. Башкин. — М.: Высшая школа, 2007. — 360 с

27 Кнорринг Г. М Справочная книга для проектирования электрического освещения / Г. М. Кнорринг, И. М. Фадин, В. Н. Сидоров — 2-е изд., перераб. и доп. — СПб.: Энергоатомиздат. Санкт-Петербургское отд-ние, 1992. —448 с

## Приложение А

## Полная конфигурация alm-R1

```
Connected to Dynamips VM "R4" (ID 5, type c3725) - Console
port Press ENTER to get the prompt.
##################################################################
### #################### [OK]

Smart Init is disabled. IOMEM set to: 5

Cisco IOS Software, 3700 Software (C3725-ADVENTERPRISEK9-M),
Version 12.4(25b), RELEASE SOFTWARE (fc1)
Technical Support:
http://www.cisco.com/techsupport Copyright (c)
1986-2009 by Cisco Systems, Inc. Compiled Wed
12-Aug-09 14:10 by prod_rel_team

R4#
R4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#hostname alm-R1
alm-R1(config)#username admin privilege 15 secret dnjhjq31337dpkjv2
alm-R1(config)#int tunnel 0
alm-R1(config-if)#
*Mar 1 00:07:19.571: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel0, changed state to down
alm-R1(config-if)#ip address 10.0.254.1 255.255.255.0
alm-R1(config-if)#ip nhrp map multicast dynamic
alm-R1(config-if)#ip nhrp network-id 1
alm-R1(config-if)#tunnel source fa0/1
alm-R1(config-if)#tunnel mode gre multipoint
alm-R1(config-if)#ip ospf network broadcast
alm-R1(config)#router ospf 1
alm-R1(config-router)#network 10.0.0.0 0.0.255.255 area 0
alm-R1(config-router)#ex alm-
R1(config)#crypto isakmp policy 1 alm-
R1(config-isakmp)#authentication pre-share
alm-R1(config-isakmp)#ex
alm-R1(config)#crypto isakmp key dnjhjq31337dpkjv2 address 0.0.0.0 0.0.0.0
alm-R1(config)#crypto ipsec transform-set DAN2711-NET esp-aes esp-sha-
hmac alm-R1(cfg-crypto-trans)#mode transport
alm-R1(cfg-crypto-trans)#ex alm-R1(config)#crypto
ipsec profile DAN-VPN alm-R1(ipsec-profile)#set
transform-set DAN2711-NET
```

```
alm-R1(ipsec-profile)#ex
alm-R1(config)#int tunnel 0
alm-R1(config-if)#tunnel protection ipsec profile DAN-VPN
alm-R1(config-if)#ex
alm-R1(config)#int fa0/1
alm-R1(config-if)#ip address 217.11.64.235
255.255.255.0 alm-R1(config-if)#no shutdown alm-
R1(config-if)#

*Mar 1 04:43:22.490: %LINK-3-UPDOWN: Interface FastEthernet0/1,
changed state to up
*Mar 1 04:43:23.490: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/1, changed state to up
*Mar 1 04:43:29.590: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel0, changed state to up
alm-R1(config-if)#
*Mar 1 04:43:29.634: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
*Mar 1 04:54:46.410: %SYS-5-CONFIG_I: Configured from console by
console alm-R1#
```

**Полная конфигурация ast-R2:**

```
Connected to Dynamips VM "R5" (ID 6, type c3725) - Console
port Press ENTER to get the prompt.
#################################################################
### #################### [OK]

Smart Init is disabled. IOMEM set to: 5

Cisco IOS Software, 3700 Software (C3725-ADVENTERPRISEK9-M),
Version 12.4(25b), RELEASE SOFTWARE (fc1)
Technical Support:
http://www.cisco.com/techsupport Copyright (c)
1986-2009 by Cisco Systems, Inc. Compiled Wed
12-Aug-09 14:10 by prod_rel_team

R5#
R5#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R5(config)#hostname ast-R2
```

```
ast-R2(config)#
ast-R2(config)#int tunnel 0
ast-R2(config-if)#
*Mar 1 00:01:08.063: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel0, changed state to down
ast-R2(config-if)#ip address 10.0.254.2 255.255.255.0
ast-R2(config-if)#ip nhrp map 10.0.254.1 217.11.64.236
ast-R2(config-if)#ip nhrp map multicast 217.11.64.235
ast-R2(config-if)#ip nhrp network-id 1
ast-R2(config-if)#ip nhrp nhs 10.0.254.1
ast-R2(config-if)#ip nhrp registration no-unique
ast-R2(config-if)#tunnel source fa0/1
ast-R2(config-if)#tunnel mode gre multipoint
ast-R2(config-if)#ip ospf network broadcast
ast-R2(config-if)#ip ospf priority 0
ast-R2(config-if)#ex
ast-R2(config)#router ospf 1
ast-R2(config-router)#network 10.0.0.0 0.0.255.255 area 0
ast-R2(config-router)#ex ast-R2(config)#crypto
isakmp policy 1 ast-R2(config-
isakmp)#authentication pre-share ast-R2(config-
isakmp)#ex
ast-R2(config)#crypto isakmp key dnjhjq1337dpkjv2 address 0.0.0.0 0.0.0.0 ast-
R2(config)#crypto ipsec transform-set DAN2711-NET esp-aes esp-sha-hmac ast-
R2(cfg-crypto-trans)#mode transport
ast-R2(cfg-crypto-trans)#ex ast-
R2(config)#crypto ipsec profile DAN-VPN
ast-R2(ipsec-profile)#set transform-set DAN2711-NET
ast-R2(ipsec-profile)#ex
ast-R2(config)#int tunnel 0
ast-R2(config-if)#tunnel protection ipsec profile DAN-VPN
ast-R2(config-if)#ex
ast-R2(config)#int fa0/1
ast-R2(config-if)#ip address 217.11.64.235 255.255.255.0
ast-R2(config-if)#no sh
ast-R2(config-if)#
*Mar 1 01:42:45.039: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed
state to up
*Mar 1 01:42:46.039: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
ast-R2(config-if)#
```