ОТЧЕТ
о прохождении практики

обучающимся группы _____
(код и номер учебной группы)

_____
(фамилия, имя, отчество обучающегося)

Место прохождения практики:
Образовательная автономная некоммерческая организация
высшего образования «Московский технологический институт»
(полное наименование организации)

Руководитель учебной практики от Института:

_____
(фамилия, имя, отчество)

Заведующий кафедрой _____
(ученая степень, ученое звание, должность)

1. Индивидуальный план-дневник учебной практики

Индивидуальный план-дневник учебной практики составляется обучающимся на основании полученного задания на учебную практику в течение организационного этапа практики (до фактического начала выполнения работ) с указанием запланированных сроков выполнения этапов работ.

Отметка о выполнении (слово «Выполнено») удостоверяет выполнение каждого этапа учебной практики в указанное время. В случае обоснованного переноса выполнения этапа на другую дату, делается соответствующая запись («Выполнение данного этапа перенесено на… в связи с…»).

Таблица индивидуального плана-дневника заполняется шрифтом Times New Roman, размер 12, оформление – обычное, межстрочный интервал – одинарный, отступ первой строки абзаца – нет.

№ п/п	Содержание этапов работ, в соответствии с индивидуальным заданием на практику	Дата выполнения этапов работ	Отметка о выполнении
1	Изучить деятельности выбранного предприятия/подразделения, которое будет являться объектом информатизации. Описать организационную структуру предприятия или подразделения с помощью диаграмм, схем, таблиц. Изучить действующие в организации стандарты, положения и инструкции, используемую техническую документацию;		
2	Ознакомиться с кругом решаемых задач на рабочем месте сотрудника предприятия/подразделения, чья деятельность подлежит информатизации, обосновать необходимость информатизации. Описать функции, выполняемые сотрудником на рабочем месте. Создать схемы информационных потоков		

	с помощью современных программных средств		
3	Ознакомиться с основными требованиями к информатизации Изучить особенности ИКТ-продуктов и технологий, применимых для информатизации, найти наиболее удачные, по вашему мнению, готовые решения.		
4	Описать требования потребителя к разрабатываемому информационному продукту (сайт / база данных / модуль информационной системы). Оформить техническое задание на создание или доработку готового решения.		
5	Описать средства реализации программного продукта, выбранные средства должны соответствовать современному состоянию технологий разработки. Описать процесс инсталляции необходимых программных средств для внедрения планируемого программного продукта на предприятии/подразделении.		
6	Привести план затрат на создание проекта, реализацию и внедрение программного продукта, включая оклад и премиальную часть заработной платы специалистов, привлекаемых к созданию проекта информатизации.		
7	Изучить алгоритм работы выбранного программного продукта. Привести блок-схему алгоритма работы изучаемого программного продукта.		
8	Изучить основные технологии создания и внедрения информационных систем, стандарты управления жизненным циклом информационной системы. Описать процесс составления плановой и отчетной документации по управлению проектами создания программного продукта на стадиях жизненного цикла.		
9	Описать документацию для отчета и презентации заказчику, формы документов, формат презентации, необходимые пользовательские инструкции.		
10	Оформление отчета (текст, рисунки, чертежи)		
11	Сдача отчета		

« » _____ 202__ г.

Обучающийся _____ _____

(подпись) И.О. Фамилия

2.Технический отчет

(характеристика проделанной обучающимся работы, выводы по результатам практики)

В рамках практики была выполнена разработка эффективного и безопасного решения задачи организации связи между удаленными филиалами и офисами предприятия на основе технологии VPN.

Локальная вычислительная сеть (ЛВС) — это совокупность аппаратного и программного обеспечения, объединяющая компьютеры в единую распределённую систему обработки и хранения информации. К аппаратному обеспечению относятся компьютеры, с установленными сетевыми адаптерами, повторители, концентраторы, коммутаторы, мосты, маршрутизаторы и др., соединённые между собой сетевыми кабелями.

Основные возможности локальных (компьютерных) сетей:

обмен данными (файлами);

совместное использование сетевых ресурсов (файлов данных и программ, принтеров и другого оборудования);

обмен сообщениями, общение (электронная почта, телефония, видеоконференции);

координация совместной работы;

упорядочивание делопроизводства, контроль доступа к информации, защита информации.

Эти возможности позволяют реализовать в вычислительной сети эффективную обработка информации и делают актуальной данную работу целью которой является разработать проект развертывания сети передачи для компании, которая имеет территориально-распределенную инфраструктуру.

Компания с полным наименованием ООО ПК «ВЕНТКОМПЛЕКС» зарегистрирована 30.10.2018.

Род деятельности – Торговля товарами народного потребления.

Компания образована в 2018 году, численность 500 чел.

Офисные помещения головного офиса расположены на 1 этаже 11 секции дома.

В здании расположены 7 помещений (офисов).

Структура головного офиса компании:

- Правление
- Бухгалтерия
- Отдел ИТ и безопасности
- Отдел маркетинга
- Отдел логистики и поставок
- Отдел по работе с клиентами
- Юридический отдел

Правление. Выполняет административные функции организации. Осуществляет руководство организацией, отбор кадров, управление финансовой, правовой и другими видами деятельности.

Бухгалтерия. Занимается всеми направления бухгалтерской деятельности на организации.

Отдел ИТ и безопасности. Выполняет функции инфокоммуникационного обеспечения деятельности предприятия, а также за решение вопросов информационной безопасности и обеспечения охраны собственности.

Отдел маркетинга. Отвечает за продвижение услуг компании на рынке. Выработку маркетинговых программ. Изготовление рекламной продукции. Осуществляет деятельность по предоставлению рекламных услуг.

Отдел логистики и поставок. Основной (прибылеобразующий отдел). Непосредственно занимается вопросами закупки, доставки, распределения товаров по торговым точкам.

Отдел по работе с клиентами. Организовывает и обеспечивает взаимодействие между компанией и клиентами (консультации, ответы на вопросы, решение проблем и т.д.) Кроме того, отвечает за работу дежурных служб.

Юридический отдел. Занимается вопросами юридического обеспечения деятельности компании.

Компания имеет территориально-распределенную архитектуру. Имеет в своем составе 7 филиалов (склады, магазины, транспортный сектор, головной офис)

Число филиалов: 7

Число рабочих мест в филиалах: 60/60/20/10/90/90/4

Для расчета точного трафика, вызываемого одним пользователем, необходимо очень дорогостоящее оборудование или программа, которые бы отслеживали потоки приходящих и уходящих пакетов таких как SolarWinds Real-Time NetFlow Traffic Analyzer, Colasoft Capsa Free, Angry IP Scanner. Поэтому при расчете будет оцениваться трафик исходя из предполагаемых к использованию приложений.

Самый большой трафик создают следующие приложения:

- 1С Бухгалтерия (включающая в себя разнообразные бухгалтерские формы и отчеты);
- ГИС Торговля (содержит правовые базы и юридические консультации).
- КИС SAP

Рассчитаем трафик для бухгалтерского приложения 1С.

Будем исходить из того, что электронная таблица, которыми в основном и пользуются бухгалтера, имеет размер 2 Мб. В среднем одному пользователю в бухгалтерии необходимо загрузить с сервера 10-15 электронных таблиц. Следовательно, необходимый объем для загрузки равен 30 Мб. Теперь рассчитаем время реакции системы и пропускную способность для Fast Ethernet и Gigabit Ethernet, при условии, что для обоих технологий будет использоваться один и тот же объем в 30 Мб. Для технологии Fast Ethernet максимальное и минимальное значение интенсивности передачи кадров составляют:

$$V_{мин} = 8130 \text{ к/с}$$

$$V_{макс} = 148810 \text{ к/с}$$

Минимальный размер кадра составляет 64 байта, а максимальный 1518 байт.

Для того что бы рассчитать время реакции системы переведем полученный объем 30 Мб в пакеты.

$$30 \text{ Мб} = 30*1024*1024 = 31457280 \text{ байт}$$

31457280*8 = 251658240 бит

Чтобы получить пакет

251658240 / 1518 (максимальный размер кадра) = 165782 пакетов

Время реакции t

t = 165782 / 8130 = 20,3 с

Пропускная способность рассчитывается: передаваемый объем делится на время передачи, таким образом получаем минимальное значение пропускной способности (Fast Ethernet скорость передачи 100 Мбит/с)

251658240 бит / 20,3 с = 100 Мбит/с

Таким образом, получаем, что в наихудшем случае для передачи 30 Мб через 100 Мбитный канал потребуется 20,3 секунды.

Теперь определим те же параметры для технологии Gigabit Ethernet.

V мин = 81270 к/с

V макс =1 488 090 к/с

Время реакции t

t = 165782 / 81270 (для кадра максимальной длинны) = 2 с

Пропускная способность для 30 Мб равна:

251658240 бит / 2 с = 120 Мбит/ с

Трафик остальных приложений примерно равен трафику 1С.

Большие объемы можно передавать через 100 и через 1000 Мбит/с, а на меньших скоростях не будет ощущаться эффективной отдачи от локальной сети, велика вероятность перегрузки канала. Заметим еще, что даже простой документооборот на сегодняшний день может составлять десятки мегабайт. По этой причине выбор делается в пользу 100/1000 Мбитного канала.

Для достижения поставленной цели необходимо решить следующие задачи:

выбрать сетевую топологию;

разработать функциональную схему сети;

выбрать требуемую физическую среду: кабель или обосновать использование технологии WiFi;

рассчитать и выбрать коммутационное оборудование для канального уровня;

провести IP-планирование подсетей: выбрать единое адресное пространство, рассчитать требуемое количество подсетей и элементов в каждой сети, рассчитать адресное пространство, диапазон адресов, маску подсети и шлюз по умолчанию для каждого сегмента;

сформировать таблицы маршрутизации для каждого маршрутизатора;

составить спецификацию оборудования, включая кабель требуемой категории;

рассчитать ориентировочную стоимость монтажных работ;

рассчитать общую стоимость развертывания сети для заказчика;

сформировать календарный план работ по развертыванию сети.

Сеть должна выполнять следующие функции:

объединять всех новых пользователей в едином информационном пространстве;

предоставлять пользователям информацию, созданную в разное время и в разном программном обеспечении для ее обработки;

обеспечивать устойчивые к сбоям каналы связи для обмена данными со всеми структурными подразделениями учреждения;

повысить достоверность и надежность хранения информации за счет создания устойчивой информационно вычислительной системы, а также архивов данных которые можно использовать в дальнейшем;

обеспечить эффективную систему накопления, хранения и поиска финансово–экономической и другой информации по текущей и проделанной за некоторый период времени работе (архивная информация);

обеспечивать прозрачный доступ к информации авторизованному пользователю в соответствии с его правами и привилегиями;

обеспечивать оперативное получение коммерческих, финансовых и научных новостей из глобальной сети INTERNET;

обеспечивать взаимодействие с другими сегментами корпоративной сети

предприятия.

Для создания корпоративной сети, удовлетворяющей описанным требованиям, необходимо произвести анализ возможностей существующих средств построения сетей и обеспечения их бесперебойной и надежной работы, а также оценить обстановку с целью принятия оптимального решения.

Исходя из всего вышеперечисленного, можно сделать вывод: поставленная задача является сложной по степени реализации и имеет много способов решения. Для реализации поставленной задачи потребуется не так много времени и затрат, но общий эффект должен повысить экономическую эффективность работы компании, снизить затраты и увеличить общий доход. Ожидается снижение времени работы персонала, что позволит увеличить поток клиентов, нежели это было до создания локальной сети.

Архитектура корпоративной сети - это совокупность компонентов, протоколов и технологий, которые определяют ее структуру и функциональные возможности.

Основные компоненты корпоративной сети:

- Клиентские устройства: компьютеры, ноутбуки, смартфоны, планшеты и другие устройства, которые используются для доступа к ресурсам сети.

- Сетевое оборудование: маршрутизаторы, коммутаторы, брандмауэры, прокси-серверы и другие устройства, которые обеспечивают передачу данных между устройствами сети.
- Серверы: файловые серверы, серверы электронной почты, серверы баз данных и другие устройства, которые предоставляют доступ к приложениям и данным сети.
- Средства защиты: антивирусные программы, системы обнаружения вторжений, протоколы аутентификации и другие технологии, которые обеспечивают безопасность корпоративной сети.

Архитектура корпоративной сети может быть построена в виде различных типов топологий сетей, таких как звезда, шина, кольцо или комбинированная

топология. В зависимости от конкретных требований и задач корпоративной сети, архитектура может включать в себя различные слои, такие как слой доступа, слой распределения и слой ядра.

Типичная архитектура корпоративной сети включает следующие слои:

Слой доступа: включает в себя коммутаторы и устройства, которые обеспечивают доступ к сети для клиентских устройств.

- Слой распределения: включает в себя маршрутизаторы и другие устройства, которые обеспечивают передачу данных между устройствами в различных сегментах сети.
- Слой ядра: включает в себя устройства, которые обеспечивают высокоскоростную передачу данных между сегментами сети.

Кроме того, архитектура корпоративной сети может включать в себя следующие компоненты:

- Систему управления сетью (NMS): программа или сервис, который позволяет администраторам управлять и контролировать работу сети, анализировать данные и решать проблемы в работе сети.
- Системы обеспечения безопасности: устройства и программы, которые обеспечивают защиту корпоративной сети от угроз, таких как вирусы, хакеры и другие типы атак.

- Системы резервирования: устройства и программы, которые обеспечивают бесперебойную работу сети в случае отказа основных компонентов.
- Системы мониторинга и анализа: устройства и программы, которые позволяют администраторам мониторить работу сети, анализировать данные и определять проблемы в работе сети.

В целом, архитектура корпоративной сети должна быть гибкой, масштабируемой и легко управляемой. Кроме того, она должна быть построена таким образом, чтобы обеспечить высокую производительность и надежность работы сети, а также обеспечить безопасность передачи данных внутри сети.

Настройка оборудования для работы с технологией VPN включает в себя

несколько шагов:

Установка и настройка VPN-шлюза: VPN-шлюз является основным компонентом системы VPN, и его необходимо установить и настроить для работы. Настройка включает в себя создание пользовательских учетных записей, определение сетей, которые будут доступны через VPN-туннель, а также настройку параметров безопасности.

Настройка удаленных узлов: для работы сети VPN необходимо настроить все удаленные узлы, которые будут подключаться к VPN-шлюзу. Это может быть выполнено путем установки VPN-клиентов на каждом узле или настройки VPN-соединения встроенными средствами операционной системы.

Настройка маршрутизаторов и коммутаторов: для обеспечения правильного маршрутизации трафика через VPN-туннель необходимо настроить маршрутизаторы и коммутаторы. В зависимости от сетевой инфраструктуры, маршрутизация может выполняться на уровне маршрутизатора или на уровне коммутатора.

Настройка брандмауэров: для обеспечения безопасности сети необходимо настроить брандмауэры для обеспечения защиты от внешних угроз и атак.

Тестирование сети: после настройки сети VPN необходимо провести тестирование для проверки правильности работы всех компонентов. Тестирование может включать в себя проверку маршрутизации трафика, проверку соединения между удаленными узлами, проверку скорости передачи данных и другие тесты.

При настройке сети VPN рекомендуется использовать специализированные программные решения, такие как Cisco AnyConnect, OpenVPN или другие подобные программы. Эти программы обеспечивают удобный интерфейс для настройки и управления сетью VPN, а также имеют встроенные средства защиты данных и безопасности.

Под топологией корпоративной сети понимается физическое размещение компьютеров сети друг относительно друга и способ соединения их между собой. Топология определяет тип используемого кабеля, требования к

оборудованию, надежность работы, методы управления обменом, возможности расширения сети.

Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне. Формат кадров и протоколы управления доступом к среде — на канальном уровне модели OSI. Ethernet в основном описывается стандартами IEEE группы 802.3. Ethernet стал самой распространённой технологией ЛВС в середине1990-х годов, вытеснив такие устаревшие технологии, как Arcnet и Tokenring.

Название «Ethernet» (буквально «эфирная сеть») отражает первоначальный принцип работы этой технологии: всё, передаваемое одним узлом, одно-временно принимается всеми остальными (то есть имеется некое сходство с радио вещанием). В настоящее время практически всегда подключение происходит через коммутаторы (switch), так что кадры, отправляемые одним узлом, доходят лишь до адресата (исключение составляют передачи на широковещательный адрес) — это повышает скорость работы и безопасность сети.

FastEthernet, 100 Мбит/с

Технология Ethernet 100 Мбит/с, она же «быстрый Ethernet (FastEthernet). Имеет много разновидностей, при этом обозначение 100BASE-T чаще всего используется как собирательное название. Как и в технологии 10BASE-T, в работе только зеленая и оранжевая пары (прием контакты 3, 6, передача контакты 1, 2), хотя поводились эксперименты по использованию всех 4 пар, которые затем привели к созданию гигабитного Ethernet (см. 1000BASE-T). Для реализации приложений 100-мегабитного Ethernet используется витая пара категории 5 (без буквы «е») или выше. Существует возможность использования для этих приложений и оптической среды передачи, однако в настоящее время волоконная оптика используется для более высоких скоростей, от 1 гигабита и выше.

Гигабитный Ethernet,1 Гбит/с

- 1000BASE-T, IEEE 802.3ab — стандарт, использующий витую пару

категорий 5e. В передаче данных участвуют 4 пары. Скорость передачи данных — 250 Мбит/с по одной паре. Используется метод кодирования PAM5, частота основ-ной гармоники 62,5 МГц. Расстояние до 100 метров

• 1000BASE-TX был создан Ассоциацией Телекоммуникационной Промыш-ленности (англ. Telecommunications IndustryAssociation, TIA) и опубликован в марте 2001 года как «Спецификация физического уровня дуплексного Ethernet 1000 Мб/с (1000BASE-TX) симметричных кабельных систем категории 6.

Operating Over Category 6 Balanced Twisted-Pair Cabling (ANSI/TIA/EIA-854-2001)»). Стандарт, использует раздельную приём и передачу (по одной паре в каждом направлении), что существенно упрощает конструкцию.

В проекте оптимальным будет использование топологии «иерархическая звезда» из-за особенности расположения рабочих мест предприятия и его филиалов, функциональных задач.

Данная топология обладает следующими преимуществами:

выход из строя или отключение одной рабочей станции не отражается на работе всей сети в целом;

хорошая масштабируемость сети;

лёгкий поиск неисправностей и обрывов в сети;

высокая производительность сети (при условии правильного проектирования);

гибкие возможности администрирования.

Для реализации данной сети возможно использование следующих технологий:

1. «Иерархическая звезда» с использованием технологии FastEthernet по кабелю «витая пара» UTP-5E;

2. «Иерархическая звезда» с использованием технологии GigabitEthernet по кабелю «витая пара» UTP-5E или UTP-6E

3. «Иерархическая звезда» с использованием технологии

GigabiteEthernet по волоконнооптическому кабелю.

4. Беспроводным технологиям по протоколу IEEE-802.11n, ac.

Построение сети в филиалах решено выполнять по топологии «иерархическая звезда», с использованием технологии GigabitEthernet по кабелю «витая пара» UTP-5E или UTP-6E. Выбор в пользу данного решения продиктован соображениями:

- более высокого уровня безопасности по отношению с беспроводными технологиями;

- более высокой пропускной способностью линий по сравнению с технологием FastEthernet;

- более низкой стоимостью работ и оборудования по сравнению с волоконнооптическим кабелем.

Таблица 1 – Сравнительные характеристики технологии Gigabit Ethernet

Стандарт	Тип	Скорость передачи (Mbps)	Максимальная длина сегмента в метрах	Тип среды передачи сигналов
IEEE 802.3z	1000Base-CX	1000	25 м	UTP/STP cat 5,5e,6
	1000Base-LX	1000	Одномод — 5 км Многомод — 550 м	оптоволоконный
	1000Base-SX	1000	550 м	
IEEE 802.3ab	1000Base-T	1000	100 м	UTP/STP cat 5,5e,6,7
TIA 854	1000BASE-TX	1000	100 м	UTP/STP cat 6,7
IEEE 802.3ah	1000BASE-LX10	1000	10 км	оптоволоконный
IEEE 802.3ah	1000BASE-BX10	1000	10 км	
non-standard	1000BASE-EX	1000	40 км	оптоволоконный
non-standard	1000BASE-ZX	1000	70 км	

Построение соединительных линий между филиалами решено выполнять

по топологии «иерархическая звезда», с использованием технологии VPN-MPLS за счет предоставления данной услуги провайдером Интернет. Подключение филиалов к сети провайдера осуществлять по технологии 10 GigabiteEthernet по волоконнооптическому кабелю.

VPN (Virtual Private Network) - это технология, которая позволяет устанавливать безопасное соединение между удаленными компьютерами или сетями через неприватный сетевой канал, такой как Интернет. Она обеспечивает защиту передаваемых данных путем шифрования трафика и создания "виртуального" частного канала связи между удаленными устройствами.

Основные принципы работы VPN:

Шифрование: все данные, передаваемые по VPN-каналу, шифруются, что обеспечивает безопасность передачи конфиденциальной информации.

Туннелирование: VPN-канал создает "туннель" через неприватный сетевой канал, такой как Интернет, и защищает передачу данных внутри этого туннеля.

Аутентификация: VPN-канал обеспечивает аутентификацию пользователей, что позволяет предотвратить несанкционированный доступ к защищенным данным.

Сокрытие IP-адреса: VPN-канал скрывает реальный IP-адрес отправителя и получателя, что делает невозможным отслеживание передачи данных.

Удаленный доступ: VPN-канал позволяет удаленным пользователям подключаться к защищенной сети организации из любого места в мире, используя доступ к Интернету.

Поддержка различных протоколов: VPN-технология поддерживает различные протоколы, такие как PPTP, L2TP, IPSec, SSL/TLS, которые обеспечивают различные уровни безопасности и функциональности.

Масштабируемость: VPN-технология легко масштабируется и может поддерживать большое количество пользователей и сетевых устройств.

Использование технологии VPN для подключения удаленных филиалов к корпоративной сети обеспечивает безопасный доступ к ресурсам организации и позволяет снизить затраты на коммуникации, так как не требуется использование

выделенных линий связи.

Типы VPN

Существует несколько типов VPN-протоколов, каждый из которых имеет свои особенности и применяется в различных ситуациях:

PPTP (Point-to-Point Tunneling Protocol) – один из самых распространенных протоколов, который обеспечивает быстрое соединение и хорошую производительность. Однако, он имеет некоторые уязвимости в безопасности, поэтому не рекомендуется использовать его для передачи конфиденциальной информации.

L2TP (Layer 2 Tunneling Protocol) – комбинация PPTP и L2F (Layer 2 Forwarding Protocol). Обеспечивает более высокий уровень безопасности, чем PPTP, так как использует шифрование данных. Но, L2TP имеет некоторые ограничения при прохождении через NAT (Network Address Translation).

IPSec (Internet Protocol Security) – протокол, который обеспечивает высокий уровень безопасности. Он может быть использован как в туннельном режиме (шифрует весь IP-пакет) или в режиме транспортного уровня (шифрует только данные). IPSec поддерживает различные алгоритмы шифрования и аутентификации, что делает его очень гибким протоколом.

SSL/TLS (Secure Sockets Layer/Transport Layer Security) – протокол, который обеспечивает безопасный канал связи на основе шифрования SSL или TLS протоколов. Он часто используется для защиты передачи данных через веб-браузеры или для доступа к веб-приложениям.

OpenVPN – открытый протокол, который обеспечивает высокий уровень безопасности и гибкость. Он может использоваться для создания как туннельных, так и точка-точка соединений, а также поддерживает различные алгоритмы шифрования и аутентификации.

Каждый из этих протоколов имеет свои преимущества и недостатки, поэтому выбор протокола зависит от конкретных требований и задач. Важно выбрать подходящий протокол, который обеспечит необходимый уровень безопасности и производительности при использовании VPN-технологии.

Подключение удаленных филиалов через VPN-соединение имеет свои особенности:

Надежность и безопасность - VPN обеспечивает защиту данных от несанкционированного доступа, обеспечивая надежное и безопасное подключение к корпоративной сети. При подключении удаленных филиалов через VPN-соединение все данные передаются по зашифрованному туннелю, что позволяет обеспечить надежную защиту информации.

Гибкость и масштабируемость - VPN-соединение позволяет гибко масштабировать сеть и подключать удаленные филиалы в зависимости от потребностей компании. При необходимости можно добавлять или удалять удаленные филиалы, а также настраивать параметры VPN-соединения в соответствии с требованиями бизнеса.

Удобство использования - VPN-соединение позволяет удаленным сотрудникам работать на удаленном филиале так, как будто они находятся в офисе. При этом они могут использовать все ресурсы корпоративной сети, включая файлы, приложения, базы данных и другие ресурсы.

Ограниченная пропускная способность - при использовании VPN-соединения может возникнуть ограничение по пропускной способности, особенно при передаче больших объемов данных. В таких случаях можно использовать специальные технологии, такие как мультиплексирование или комбинирование различных типов соединений.

Затраты на оборудование - для организации VPN-соединения может потребоваться дополнительное оборудование, такое как VPN-концентраторы или маршрутизаторы с поддержкой VPN. Важно учитывать затраты на оборудование при планировании внедрения VPN-технологии.

В целом, использование VPN-технологии позволяет эффективно организовать удаленный доступ к корпоративной сети и обеспечить безопасность и надежность передачи данных. Однако, при выборе решения необходимо учитывать конкретные требования бизнеса и особенности сетевой инфраструктуры.

Основные преимущества VPN:

1. Безопасность: VPN защищает передаваемую информацию от несанкционированного доступа, зашифровывая данные и создавая защищенное соединение.

2. Гибкость: VPN позволяет удаленным сотрудникам подключаться к корпоративной сети из любого места в мире с доступом в Интернет, что повышает гибкость работы и повышает производительность.

3. Низкая стоимость: VPN не требует дополнительных инвестиций в оборудование и позволяет снизить расходы на связь между удаленными филиалами.

4. Упрощение настройки и управления: VPN позволяет создавать защищенные соединения между удаленными устройствами без необходимости настройки сложной инфраструктуры.

5. Улучшение производительности: VPN может повысить производительность сети, уменьшив задержки и увеличивая пропускную способность.

Основные недостатки VPN:

1. Значительное снижение скорости: VPN может снизить скорость передачи данных из-за дополнительной обработки, связанной с шифрованием и дешифрованием информации.

2. Необходимость надежной сети: VPN работает через Интернет, поэтому требуется надежное и быстрое соединение для обеспечения стабильной работы.

3. Сложность настройки: Настройка VPN может быть сложной и требовать высокой квалификации специалистов для обеспечения безопасной работы.

4. Ограничения по безопасности: При использовании общей сети, такой как Интернет, возможны риски нарушения безопасности.

5. Необходимость лицензирования: Для использования некоторых видов VPN может потребоваться лицензирование, что может увеличить затраты на внедрение.

При выборе оборудования для построения корпоративной сети с использованием VPN, можно рассмотреть следующие типы оборудования:

VPN-шлюзы: это специализированные устройства, которые обеспечивают шифрование и передачу данных между удаленными узлами сети.

Маршрутизаторы: это устройства, которые обеспечивают маршрутизацию и пересылку данных в сети.

Коммутаторы: это устройства, которые обеспечивают коммутацию данных между узлами сети.

Брандмауэры: это устройства, которые обеспечивают защиту сети от внешних угроз и атак.

Серверы: это устройства, которые предоставляют различные службы, такие как хранение данных, веб-сервисы, электронная почта и т.д.

Персональные компьютеры: это устройства, которые используются для работы сетевых пользователей.

Выбор конкретного оборудования зависит от потребностей организации, объема данных, количества пользователей и других факторов.

Для построения корпоративных сетей в настоящее время лидирующие позиции занимают радиочастотный эфир и проводная среда распространения электрических сигналов. Свою область применения имеют волоконнооптические линии связи, коаксиальные линии, оптические каналы и т.д.

Витая пара (англ. twisted pair) – разновидность кабеля связи, который представляет собой сочетание нескольких пар изолированных электрических проводников, определенным образом свитыми между собой и покрытых пластиковой оболочкой.

Витки проводников выполняются с рассчитанным шагом и с целью повышения помехозащищенности проводников одной пары при этом помеха

одинаково влияет на оба провода в паре, но с различной фазой что и приводит к последующему уменьшению внешних электромагнитных помех, а также взаимных наводок при передаче различных сигналов. Для уменьшения взаимовлияния отдельных пар кабеля в кабелях UTP, проводники в различных парах свиваются с отличным друг от друга шагом. Данный тип кабеля самый распространенный в настоящее компонент современных структурированных кабельных систем. Он находит применения в телекоммуникационных системах и в компьютерных сетях различного уровня и типов в качестве физической среды распространения сигнала. Благодаря дешевизне и лёгкости монтажа, стал самым распространённым решением для построения кабельных (проводных) ЛВС.

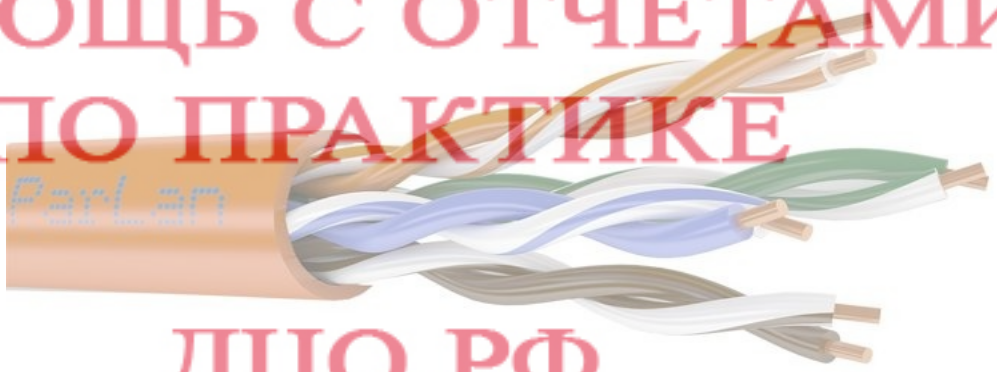

Рисунок 1 - Витая пара

Кабель к сетевым устройствам подключается при помощи разъёма типа 8P8C, который также получил название RJ45.

Рисунок 2 – Разъем RJ 45

Существует и используются следующие виды кабеля, которые относятся к кабелям «витая пара»

Защита кабеля может строится за счет электрически заземленной медной оплетки, а также алюминиевой фольги, намотанной вокруг пар, тип защиты определяет следующие разновидности исполнения кабеля:

Unshielded twisted pair (UTP – с англ., незащищенная витая пара). Кроме пластиковой защиты собственно проводников никаких дополнительных элементов защиты (экранирования, заземления) не используется.

Рисунок 3 – Незащищенная витая пара

Foiled twisted pair (F/UTP – с англ., фольгированная витая пара). Все пары проводников этого кабеля покрыты общим экраном из алюминевой фольги:

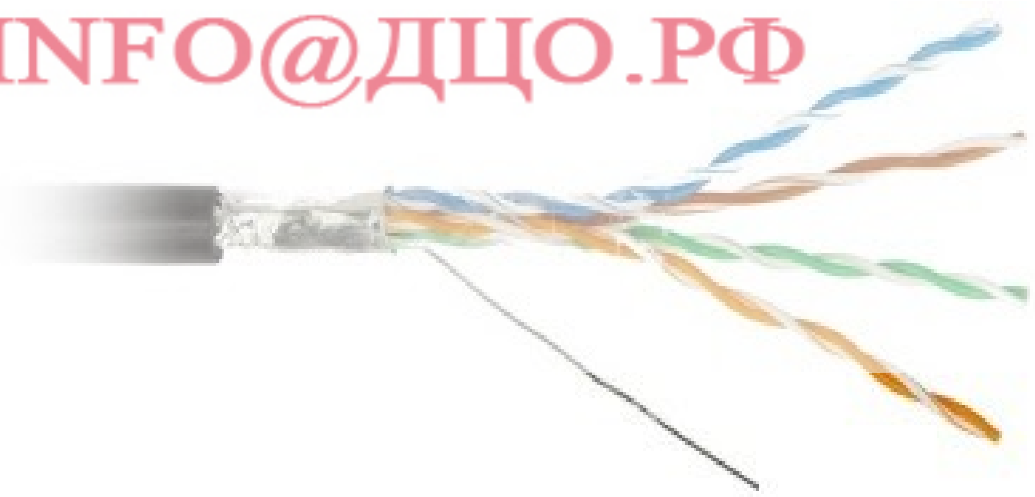

Рисунок 4 - Фольгированная витая пара

Shielded twisted pair (STP, – с англ., защищенная витая пара). В данном кабеле каждая пара экранирована собственной экранирующей оплеткой, а также

все пары закрыты общим сеточным экраном.

Рисунок 5 – Защищенная витая пара

Screened Foiled twisted pair (S/FTP, – с англ., фольгированная экранированная витая пара). В этом типе кабеля каждая пара находится в собственной оплетке из фольги, а все пары помещены в медный экран.

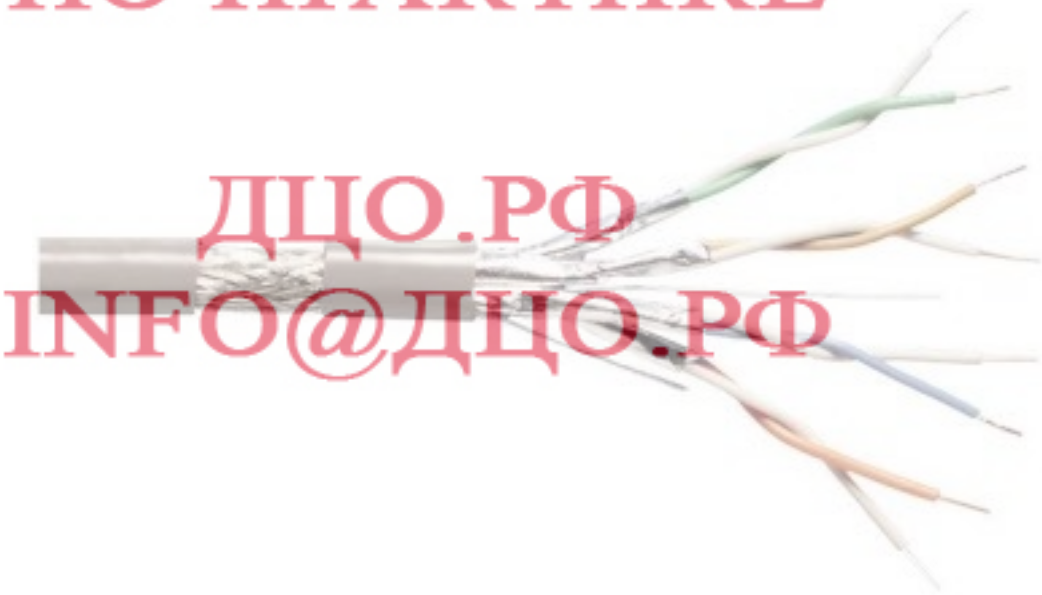

Рисунок 6 – Фольгированная экранированная витая пара

Screened Foiled Unshielded twisted pair (SF/UTP, – с англ., незащищенная экранированная витая пара). Характеризуется двойным общим экраном из медной оплетки и из фольги.

Рисунок 7 – Незащищенная экранированная витая пара

В зависимости от структуры проводников – кабель применяется одно- и многожильный. Для первого случая каждый провод изготавливается из одной медной жилы (жила-монолит), а для второго – каждый провод состоит из нескольких медных жил (жила-пучок).

Многожильный кабель плохо монтируется («врезается») в разъёмы патч-панелей (тонкие жилы разрезаются), но отлично переносит изгибы и скручивание, однако обладает большей величиной затухания сигнала. Эти свойства многожильного кабеля обусловили его применение для изготовления патч-кордов (англ. patchcord), соединяющих оборудование с розетками и соединения между розетками.

Существует несколько категорий кабеля «витая пара». Они пронумерованы от CAT1 до CAT7 и определяются эффективной пропускаемой полосой частот (ЭППЧ). Кабели более высоких категорий содержат большее число пар проводников, а каждая пара имеет большее число витков на единицу длины. Данные категории для неэкранированной витой пары описываются в стандарте EIA/TIA 568 (Американский стандарт проводки в коммерческих зданиях). Так согласно этого стандарта:

CAT5 (ЭППЧ – 100 МГц) — 4-парный кабель, нашел широкое применение при построении локальных сетей 100BASE-TX и для прокладки телефонных линий связи, поддерживает скорость передачи данных до 100 Мбит/с по 2 парам проводов. При прокладке новых сетей применяется усовершенствованный

кабель CAT5e, который обычно и называют кабелем «витая пара», является самой распространённой сетевым средой распространения, использующимся в компьютерных сетях, благодаря высокой скорости передачи (до 100 Мбит/с по 2 парам, до 1000 Мбит/с по 4 парам). Максимальная длина кабеля между устройствами (компьютер-свитч, свитч-компьютер, свитч-свитч) может достигать 100 м.

CAT6 (ЭППЧ – 250 МГц) – применяется в сетях FastEthernet и GigabitEthernet, в его устройство входит 4 пары проводников, максимальная скорость передачи данных до 1000 Мбит/с. Включена в стандарт в июне 2002 года. Описана в стандарте категория CAT6a, в которой увеличена ЭППЧ до 500 МГц. Согласно данных IEEE, 77 % установленных сетей в 2016 году, использовали кабель категории CAT6.

CAT7 скорость передачи данных до 100 Гбит/с, ЭППЧ пропускаемого сигнала до 600 – 700 МГц. Кабель данной категории экранирован. Седьмая категория, это кабель не UTP, а S/FTP (Screened Fully shielded Twisted Pair).

Каждая отдельно взятая витая пара, входящая в состав кабеля, предназначенного для передачи данных, должна иметь волновое сопротивление равное 120 Ом, при невыполнении этого условия форма электрического сигнала будет необратимо искажаться, и передача данных станет невозможной. К этому может привести не только некачественный кабель, но также наличие "скруток" в кабеле и использование розеток более низкой категории, чем кабель.

Для построения спроектированной сети потребуется клиентское оборудование, сетевое и серверное оборудование.

Для проектируемой сети можно сформулировать следующие требования:

- скорость подключения филиалов к Интернет – 10 Гбит/с;
- скорость подключений в сетях филиалов – 1 Гбит/с;
- требования к клиентским ПЭВМ – максимальная производительность для работы графических и видеоредакторов под управлением ОС Windows 10; низкая стоимость; большая диагональ мониторов;
- требования к серверам - оптимальная для работы типовых серверных

приложений производительность; низкая стоимость;

- требования к активному сетевому оборудованию: использовать оборудование от одного вендора; высокая надежность; высокая производительность; техническая поддержка; обучение персонала.

Исходя из требований, предлагается оборудование компании Cisco, как полностью удовлетворяющее требованиям заказчика и обладающее широкими возможностями для дальнейшего развития и совершенствования сети, в т.ч. и в вопросах обеспечения информационной безопасности.

Сетевое оборудование

Коммутатор Симанитрон SWME-48GT-4XG

Сетевой коммутатор Симанитрон SWME-48GT-4XG - устройство промышленного исполнения RACKMOUNT, обеспечивающее широкополосное подключение оконечных устройств на скорости 10/100/1000 Мбит/с, подключение к верхней ступени сети агрегации или ядру на скорости Gigabit Ethernet или 10 Gigabit Ethernet (10 GbE).

Ключевые особенности:

Высокоскоростная маршрутизация трафика

Обеспечивает высокопроизводительную маршрутизацию трафика IP. Программное обеспечение SMI поддерживает статическую, RIPv1 и RIPv2 маршрутизацию, а EMI – еще и OSPF, IGRP, EIGRP, а также маршрутизацию multicast трафика (PIM, DVMRP, IGMP snooping)

Высокая безопасность

Поддержка протокола 802.1x, функциональность Identity-Based Networking Services (IBNS), списки доступа для трафика, коммутируемого на втором уровне (VLAN ACL), на третьем и четвертом уровнях (Router ACL), а также Port-based ACLs (PACL) и Time-based ACL. Для обеспечения безопасности при администрировании поддерживаются протоколы SSH и SNMPv3, а также централизованная аутентификация на TACACS+ и RADIUS серверах.

Высокая доступность

Для защиты от сбоев внутренних блоков питания

коммутаторы Симанитрон SWME-48GT-4XG поддерживают резервную систему питания, протоколы 802.1D, 802.1s, 802.1w, функциональность UplinkFast, HSRP, UDLD, Aggressive UDLD, Switch port Auto-recovery.

Поддержка качества обслуживания (QoS)

Классификация трафика по полям DSCP или 802.1p (CoS), стандартные и расширенные списки доступа для выделения заданного типа трафика, WRED, очередность Strict Priority, Shaped Round Robin. Существует возможность определения максимальной полосы для определенного вида трафика, а также выделения гарантированной полосы CIR.

Отличная управляемость

Внедренное в коммутатор ПО CMS, поддержка управления с помощью SNMP-платформ, поддержка SNMP версий 1, 2, 3, Telnet, RMON, SPAN, RSPAN, NTP, TFTP.

Технические характеристики

Параметр	Описание
Производитель	Симанитрон-Электрикс
Количество портов	48 x X2
Интерфейсы	1 x RJ-45 сетевого управления, 48 x X2 10 Gigabit Ethernet
Управление	Интерфейс командной строки (CLI), DHCP, VLAN, QoS, SNMP v1, 2, 3, RMON
Поддерживаемые стандарты	EEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s
Внутренняя пропускная способность	128 Гбит/сек
Объем оперативной памяти	128 Мб
Объем флеш-памяти	64 Мб
Блок питания	2
Размеры	445 x 44 x 460 мм
Вес	10,7 кг

Варианты программного обеспечения

- Standard Multilayer Software Image (SMI). Включает расширенную поддержку QoS, списки доступа, возможность статической маршрутизации и маршрутизации с помощью протокола RIP.
- Enhanced Multilayer Software Image (EMI). Помимо функциональности SMI также обеспечивает расширенную функциональность корпоративного класса, включая аппаратную маршрутизацию одноадресного (unicast) и многоадресного (multicast) IP трафика, PBR, протокол WCCP.

Межсетевое оборудование

Маршрутизаторы Eltex ESR-3100 — это устройства, представляющие собой универсальную аппаратную платформу и способные выполнять широкий круг задач, связанных с сетевой защитой, шифрованием передаваемых данных, терминированием пользователей и т.д.

В линейке представлены модели, ориентированные на применение в сетях различных масштабов — от сетей предприятий различного масштаба до сетей операторов связи и дата-центров.

Ключевыми элементами серии являются средства для программной и аппаратной обработки данных. За счет оптимального распределения функций обработки данных между частями устройства достигается максимальная производительность.

Интерфейсы

- 8xEthernet 10/100/1000BASE-T (LAN/WAN)
- 8x10GBASE-R SFP+/1000BASE-X SFP (LAN/WAN)
- 1xConsole (RJ-45)
- 2xUSB 3.0
- 1 слот для SD-карт

Подключаемые интерфейсы

- USB 3G/4G/LTE модем
- E1 TopGate SFP

Системные характеристики

- Количество VPN-туннелей - 500

- Статические маршруты - 11000
- Количество конкурентных сессий - 512000
- Поддержка VLAN - до 4k активных VLAN в соответствии с 802.1Q
- Количество маршрутов BGP - 5000000
- Количество BGP-соседей - 1000
- Количество маршрутов OSPF - 500000
- Количество маршрутов RIP - 10000
- Количество маршрутов ISIS - 500000
- Таблица MAC-адресов - 2000 записей на бридж
- Размер базы FIB - 1700000
- VRF - 32

Клиенты Remote Access VPN

- PPTP/PPPoE/L2TP/OpenVPN/IPsec XAUTH

Сервер Remote Access VPN

- L2TP/PPTP/OpenVPN/IPsec XAUTH

Site-to-site VPN

- IPSec: режимы "policy-based" и "route-based"
- DMVPN
- Алгоритмы шифрования DES, 3DES, AES, Blowfish, Camelia
- Аутентификация сообщений IKE MD5, SHA-1, SHA-2

Туннелирование

- IPoGRE, EoGRE
- IPIP
- L2TPv3
- LT (inter VRF routing)

Функции L2

- Коммутация пакетов (bridging)
- Агрегация интерфейсов LAG/LACP (802.3ad)
- Поддержка VLAN (802.1Q)
- Логические интерфейсы

- LLDP, LLDP MED
- VLAN на основе MAC

Функции L3 (IPv4/IPv6)

- Трансляция адресов NAT, Static NAT, ALG
- Статические маршруты
- Динамические протоколы маршрутизации RIPv2, OSPFv2/v3, IS-IS, BGP
- Фильтрация маршрутов (prefix list)
- VRF
- Policy Based Routing (PBR)
- BFD для BGP, OSPF, статических маршрутов

BRAS (IPoE)1

- Терминация пользователей
- Белые/черные списки URL
- Квотирование по объёму трафика, по времени сессии, по сетевым приложениям
- HTTP/HTTPS Proxy
- HTTP/HTTPS Redirect
- Аккаунтинг сессий по протоколу Netflow
- Взаимодействие с серверами AAA, PCRF
- Управление полосой пропускания по офисам и SSID, сессиям пользователей
- Аутентификация пользователей по MAC- или IP-адресам

Функции сетевой защиты

- Система обнаружения и предотвращения вторжений (IPS/IDS)[1]
- Взаимодействие с Eltex Distribution Manager для получения лицензируемого контента - наборы правил, предоставляемые Kaspersky SafeStream II
- Web-фильтрация по URL, по содержимому (cookies, ActiveX, JavaScript)

- Zone-based Firewall
- Фильтрация на базе L2/L3/L4-полей и по приложениям
- Поддержка списков контроля доступа (ACL) на базе L2/L3/L4-полей
- Защита от DoS/DDoS атак и оповещение об атаках
- Логирование событий атак, событий срабатывания правил

Качество обслуживания (QoS)

- До 8-ми приоритетных или взвешанных очередей на порт
- L2- и L3-приоритизация трафика (802.1p (cos), DSCP, IP Precedence (tos))
- Предотвращение перегрузки очередей RED, GRED
- Назначение приоритетов по портам, по VLAN
- Средства перемаркирования приоритетов
- Применение политик (policy-map)
- Управление полосой пропускания (shaping)
- Иерархический QoS
- Маркировка сессий

Управление IP-адресацией (IPv4/IPv6)

- Статические IP-адреса
- DHCP-клиент
- DHCP Relay Option 82
- Встроенный сервер DHCP, поддержка опций 43, 60, 61, 150
- DNS resolver
- IP unnumbered

Средства обеспечения надежности сети

- VRRP v2,v3
- Tracking на основании VRRP или SLA теста
  - Управление параметрами VRRP
  - Управление параметрами PBR
  - Управление административным статусом интерфейса
  - Активация и деактивация статического маршрута

- Управление атрибутом AS-PATH и preference в route-map

- Балансировка нагрузки на WAN-интерфейсах, перенаправление потоков данных, переключение при оценке качества канала
- Резервирование сессий firewall

Мониторинг и управление

- Поддержка стандартных и расширенных SNMP MIB, RMONv1
- Встроенный Zabbix agent
- Аутентификация по локальной базе пользователей, RADIUS, TACACS+, LDAP
- Защита от ошибок конфигурирования, автоматическое восстановление конфигурации. Возможность сброса конфигурации к заводским настройкам
- Интерфейсы управления CLI
- Поддержка Syslog
- Монитор использования системных ресурсов
- Ping, traceroute (IPv4/IPv6), вывод информации о пакетах в консоли
- Обновление ПО, загрузка и выгрузка конфигурации по TFTP, SCP, FTP, SFTP, HTTP(S)
- Поддержка NTP
- Netflow v5/v9/v10 (экспорт статистики URL для HTTP, host для HTTPS)
- Локальное управление через консольный порт RS-232 (RJ-45)
- Удаленное управление, протоколы Telnet, SSH (IPv4/IPv6)
- Вывод информации по сервисам/процессам
- Локальное/удаленное сохранение конфигураций маршрутизатора

MPLS

- Поддержка протокола LDP
- Поддержка L2VPN VPWS
- Поддержка L2VPN VPLS Martini Mode

- Поддержка L2VPN VPLS Kompella Mode
- Поддержка L3VPN MP-BGP

В состав операционной системы входят сервисные программы – утилиты, позволяют обслуживать диски (проверять, сжимать, дефрагментировать и так далее), выполнять операции с файлами (архивировать и т.д.), работать в компьютерных сетях и так далее.

Сейчас практически все ОС поддерживают работу с сетью и обеспечивают выход как в локальную сеть, к общим ресурсам рабочей группы, так и во всемирную глобальную сеть Интернет. Каждая из ОС требует для своей работы определенных ресурсов, таких как объем оперативной памяти, объем винчестера, тип процессора и его производительность.

Для того что бы определиться в качестве выбранных сетевых серверных решений необходимо сравнить представленные аналоги бесплатных Linux систем, платных систем семейства Windows Server и Unix подобных платных систем Solaris. Сравнение представлено в таблице 2

С точки зрения производительности, безопасности и ориентированности на пользователя операционная система Windows Server 2016 является оптимальной. Затраты на операционную систему составляют 48961р. Клиентское программное обеспечение включает в себя программы, которые позволяют вычислительной системе работать в составе локальной вычислительной сети и выполнять вычисления и позволять пользователю работать с прикладными программами, которые ему необходимы для работы.

Таблица 2 – Сравнение сетевых серверных операционных систем

Характе-ристики	**Windows Server 2016**	**Debian**	**FreeBSD 8.2**	**Solaris**
Безопасность	Высокая	Высокая	Высокая	Высокая
Исходный код	Закрытый	Открытый	Открытый	Закрытый
Интерфейс	Грфический	Консоль/ Графический	Консоль/ Графический	Консоль/ Графический
Ядро	Многоядерная	Многоядерная	Многоядерная	Многоядерная
Многопроцесорность	+	+	+	=

Совместное использование	Многопользовательская	Многопользовательская	Многопользовательская	Многопользовательская
Резервирование	Отдельная служба	Отдельная служба	Отдельная служба	Отдельная служба
Отказоустойчивость	Высокая	Высокая	Высокая	Высокая
Пользователи	Разделение доступа	Разделение доступа	Разделение доступа	Разделение доступа
Серверные роли	В виде отдельных служб	Отдельные службы и оснастки	Отдельные службы и оснастки	Отдельные службы и оснастки
Аппаратная платформа	Многоплатформенная	Многоплатформенная	Многоплатформенная	Многоплатформенная
Цена, рублей	48961	Свободная	Свободная	54889

Сравнение операционных систем представлено в таблице 3.

Исходя из выбора пользовательского ПО наиболее оптимальным и распространенным программным обеспечением операционной системы является Windows 10.

Пользовательское программное обеспечение для выполнения повседневной работы и автоматизации управленческих задач состоит из служебного ПО и пользовательского.

Таблица 3 – Сравнение клиентских операционных систем

Критерий	Операционная система	
	Windows 10	Linux
Безопасность	•Улучшает безопасность с помощью дополнительных программ, но остается главной целью для вредоносных программ. •Встроенный firewall и антивирус	•Linux более безопасная система, чем Windows. Например, Ubuntu, по - умолчанию, даже не создает администраторский аккаунт, который является непременной целью для вредоносных программ. •В сердце Unix — более строгая система, что ведет к меньшему количеству дыр в безопасности по сравнению с архитектурой Windows.
Интерфейс	•Перегруженный интерфейс. Измененные положения не	•Интерфейсы Gnome и KDE похожи на интерфейсы Mac

	которых элементов в Панели управления. •Эффекты полупрозрачности, анимации	OS и Windows соответственно. •Встроенная возможность использования нескольких виртуальных рабочих столов. •Возможность включения графического ускорения присутствует
Нагрузка на систему	•Требует больше оперативной памяти и места на диске, но работает не медленнее Windows 7 на одинаковом компьютере. •Высокие системные требования.	•Отлично работает даже на очень старых компьютерах из-за незначительных системных требований. •Поддержка нового оборудования зачастую отстает, потому что производители аппаратных средств в первую очередь ориентируются на Windows и Mac OS.
Цена	11349	Бесплатно Red Hat - 3585

К служебному программному обеспечению относятся:

Squid – прокси-сервер;

Dovecot – агент доставки почты (MDA);

Postfix – агент передачи почты (MTA);

OpenVPN - Свободная реализация технологии виртуальной частной сети (VPN);

Active Directory;

DNS-сервер — приложение, предназначенное для ответов на DNS-запросы по обращению к хостам;

DHCP-сервер;

SMB-сервер.

К специальному программному обеспечению относят автоматизированные средства:

операционная система рабочих станций MS Windows 10.

пакет офисных программ Microsoft Office 2016;

антивирусное программное обеспечение Kaspersky Endpoint Security;

интернет-браузер Mozilla Firefox.

Adobe Reader;

Microsoft SQL Server Experess.

Для обеспечения безопасности необходимо использовать отдельные аппаратные средства защиты, или специальное программное обеспечение.

Существуют специализированные программные средства, которым помогают предотвратить проникновения, утечки, изменения и взлом.

Firewalls - брандмауэры (дословно firewall — огненная стена). Между локальной и глобальной сетями создаются специальные промежуточные сервера, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней.

NAT («преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Также имеет названия IP Masquerading, Network Masquerading и Native Address Translation. Когда весь исходящий из локальной сети трафик посылается от имени сервера, скрывая тем самым внутреннюю структуру локальной сети [7].

Антивирусное ПО — программа для обнаружения вредоносных компьютерных программ, удаления их и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом [4].

В программную архитектуру локальной вычислительной сети входят операционные системы и всё программное обеспечение, которое установлено на компьютерах, входящих в техническую архитектуру. Сервера работают под управлением Windows Server 2016, а рабочие станции под управлением Windows 10.

Таким образом, цель и задачи практики достигнуты. В рамках следующей практики будет расписана практическая работа.

В результате выполнения работы были выработаны решения по

проектированию корпоративной сети с подключением удаленных филиалов по технологии VPN для ООО ПК “Венткомплекс”.

Программная подсистема представляет собой прикладное и платформенное программное обеспечение, а также операционные системы рабочих станций и серверов компании. Аппаратная подсистема включает в себя аппаратные средства корпоративной сети. Необходимо отметить, что корпоративная сеть компании базируется на многоуровневой архитектуре, используя принципы иерархичности и модульности.

Приведённые решения, технологии построения локальной вычислительной сети, а также выбранные аппаратные средства реализации сети позволили спроектировать инфокоммуникационную сеть, которая будет отвечать всем поставленным требованиям по надёжности, по защищённости, по масштабируемости и по комплексности. Основными плюсами среди полученных результатов являются возможность для дальнейшего расширения сети и полученная высокая производительность, что очень важно при быстрорастущих требованиях у пользователей и увеличивающихся объёмах передаваемой информации.

В данной работе был проведён анализ оборудования, из которого были выбраны конкретные модели с наиболее оптимальными параметрами для ООО ПК “Венткомплекс” «подходящими для настоящей разработки.

Внедрение локальной сети в учреждении ООО ПК “Венткомплекс” позволит:

- уменьшить сроки доставки для информации, в том числе распоряжений, приказов, поручений и т.д.;

- сократить время на поиски документов и их прохождения по структурным подразделениям;

- исключить потерю важных документов и уменьшение количества ошибок при работе с потоком документов большого объема;

- сократить время на исполнение главных функций;

- повысить надежность выбора решений за счет полноты предоставленной

информации;

- улучшить локальную систему администрирования, контроля и управляемость на предприятии;

- разделить доступ к документам, опираясь на основу организационной структуры учреждения;

- предоставить единый поиск по хранилищу документов.

«___»_____ 202__г. _____ _____

подпись ФИО обучающегося

3. Основные результаты выполнения задания на учебную практику

В этом разделе обучающийся описывает результаты анализа (аналитической части работ) и результаты решения задач по каждому из пунктов задания на учебную практику.

Текст в таблице набирается шрифтом Times New Roman, размер 12, оформление – обычное, межстрочный интервал – одинарный, отступ первой строки абзаца – нет.

№ п/п	Результаты выполнения задания по практике
1	Изучены основные требования к информатизации Изучены особенности ИКТ-продуктов и технологий, применимых для информатизации, найти наиболее удачные, по вашему мнению, готовые решения.
2	Описаны требования потребителя к разрабатываемому информационному продукту (сайт / база данных / модуль информационной системы) Оформлено техническое задание на создание или доработку готового решения.
3	Описаны средства реализации программного продукта, выбранные средства должны соответствовать современному состоянию технологий разработки. Описаны процесс инсталляции необходимых программных средств для внедрения планируемого программного продукта на предприятии/подразделении.
4	Приведен план затрат на создание проекта, реализацию и внедрение программного продукта, включая оклад и премиальную часть заработной платы специалистов, привлекаемых к созданию проекта информатизации
5	Изучен алгоритм работы выбранного программного продукта Приведена блок-схема алгоритма работы изучаемого программного продукта
6	Изучены основные технологии создания и внедрения информационных систем, стандарты управления жизненным циклом информационной системы. Описан процесс составления плановой и отчетной документации по управлению проектами создания программного продукта на стадиях жизненного цикла.
7	Подготовлен отчет по практике

4.. Заключение руководителя от Института

Руководитель от Института дает оценку работе обучающегося исходя из анализа отчета о прохождении учебной практики, выставляя балл от 0 до 20 (где 10 указывает на полное соответствие критерию, 0 – полное несоответствие) по каждому критерию. В случае выставления балла ниже пяти, руководителю рекомендуется сделать комментарий.

Итоговый балл представляет собой сумму баллов, выставленных руководителем от Института.

№ п/п	Критерии	Балл (0…20)	Комментарии (при необходимости)
1	Понимание цели и задач задания на учебную практику.		
2	Полнота и качество индивидуального плана и отчетных материалов.		
3	Владение профессиональной терминологией при составлении отчета.		
4	Соответствие требованиям оформления отчетных документов.		
5	Использование источников информации, документов, библиотечного фонда.		
	Итоговый балл:		

Особое мнение руководителя от Института (при необходимости):

_____
_____
_____
_____
_____
_____
_____

Обучающийся по итогам прохождения учебной практики (практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) заслуживает оценку «_____».

« » _____ 202__ г.

Руководитель от Института

_____ _____

(подпись) И.О. Фамилия