введение

Компьютерные сети давно стали неотъемлемой частью нашей жизни. Сети предоставляют пользователям широкий спектр возможностей для доступа к различной информации и коммуникации, а локальные сети позволяют совместно пользоваться общими устройствами и ресурсами.

Основными преимуществами локальных сетей являются возможность доступа к общим устройствам, например, к принтерам и сканерам, общим ресурсам, например, базы данных, вычислительные мощности, возможность корпоративной работы и обмена данными.

Локальные компьютерные сети были разработаны в 1960-х годах для использования в колледжах, университетах и исследовательских центрах, в первую очередь для соединения нескольких вычислительных машин. Широко применяться локальные сети стали после того, как была разработана и стандартизирована технология Ethernet. Возможность беспроводного соединения значительно расширила количество разных типов устройств, которые могут соединяться с локальной сетью. Типичные примеры мест, где используются такие сети: школы, заводы, предприятия, научные лаборатории.

Помимо многих преимуществ, локальные компьютерные сети имеют и проблемы, такие как проектирование и необходимость обслуживания. Непредвиденные ситуации могут вывести из строя оборудование, что приведёт к остановке работы организации и огромным убыткам. Также опасность представляет возможность хищения данных посредством компьютерной сети. Несмотря на это, локальные компьютерные сети получают всё большее распространение и всё глубже проникают во многие сферы деятельности человека.

В современном мире, использование компьютерных сетей является необходимостью в любой сфере деятельности для того, чтобы успешно конкурировать с другими организациями, действующими в этой области.

Целью данной курсовой работы является проектирование локальной компьютерной сети для организации, занимающейся торговлей овощами и фруктами.

Задачами курсовой работы являются:

- разработка логической топологии сети;

- выбор и настройка сетевого оборудования;

- проектирование физической топологии сети.

1. Обзор литературы

Согласно заданию, в здании организации необходимо организовать систему видеонаблюдения. Перед началом проектирования данной системы следует ознакомиться с основными выполняемыми задачами, правилами построения и видами систем.

К основным задачам систем видеонаблюдения относятся мониторинг, обнаружение и идентификация. Видеокамеры в режиме реального времени передают оператору изображение. Данные должны определенное время храниться на запоминающих устройствах. Для грамотного подбора системы наблюдения необходимо иметь план территории/помещения, габаритные размеры, архитектурные нюансы (наличие колонн, выступов, ниш в комнате). Затем определяются места размещения камер, их количество, технические свойства.

На сегодняшний день выделяют два типа видеонаблюдения: аналоговое и цифровое.

Принцип аналогового видеонаблюдения заключается в следующем: аналоговая видеокамера воспринимает входной видеосигнал, производит его обработку и отправляет в аналоговом виде на видеорегистратор. Аналоговое видеонаблюдение обладает разрешением не более двух мегапикселей, что является существенным недостатком. Также к недостаткам следует отнести требование прямого соединения камеры с видеорегистратором, что может увеличить длину кабельных линий, и слабую помехозащищенность сигнала. Главные преимущества – низкая цена, простота установки, универсальность оборудования.

Цифровое видеонаблюдение для передачи сигнала от видеокамеры к видеорегистратору использует протокол TCP/IP по сети Ethernet. Оцифровка сигнала осуществляется на самой видеокамере, которая преобразует сигнал для передачи по сети Ethernet. Сетевые видеорегистраторы (Network Video Recorder – NVR) предназначены для работы в IP-системах видеонаблюдения. В отличие от обычных DVR (Digital Video Recorder, цифровой видеорегистратор), NVR получают видеоданные уже в сжатом виде. Особенностью NVR является то, что они могут полноценно работать лишь с ограниченным списком моделей IP-видеокамер, которые были интегрированы в программное обеспечение видеорегистратора Некоторые из устройств могут работать автономно, без дополнительного оборудования, а для других необходим видеорегистратор.

К преимуществам систем IP-видеонаблюдения можно отнести следующие:

* неограниченное максимальное разрешение видеокамер;
* гибкость построения архитектуры и масштабируемости;
* возможность подключения удаленных видеокамер через Internet;
* реализация функций видеоаналитики на видеокамерах.

К недостаткам систем IP-видеонаблюдения следует отнести следующие факторы:

* высокая нагрузка на локальную сеть, что может потребовать создания отдельной сети видеонаблюдения;
* высокий объем архива системы видеонаблюдения;
* проприетарность форматов протоколов передачи данных от видеокамер;
* дороговизна оборудования.

К системам IP-видеонаблюдения применяется ряд требований ТНПА, согласно которым накладываются определенные условия при проектировании и установке систем видеонаблюдения на объектах общественной безопасности и местах массового скопления людей.

Интеграция IP камер системы видеонаблюдения в ЛКС предприятия может осуществляться по нескольким вариантам. Например, камеры могут быть подключены к ЛКС как независимые абоненты сети. Такое подключение самое простое, но в тоже время и самое плохое, так как. сложно осуществлять администрирование и контроль доступа к видеопотоку. Кроме того, требуется решать вопрос с питанием камер и организацией файлового хранилища для сохраненных видеоданных. Второй вариант интеграции предусматривает, что в локальной сети размещается специальный коммутатор для подключения камер, а также организуется доступ к существующему или специально организованному файловому серверу. Хорошее решение для системы видеонаблюдения в системах с большим количеством камер и повышенными требованиями к объему файлового хранилища. Третий вариант – это размещение в ЛКС видеорегистратора. Это устройство совмещает в себе функции коммутатора и специализированного файлового сервера для просмотра, регистрации и хранения видеопотоков от IP камер.

2. структурное проектирование

В данном разделе будет рассмотрена структура локальной сети.

Чертёж структурной схемы СКС представлен в приложении А.

Для того, чтобы спроектировать структуру сети, нужно рассмотреть планировку здания, в котором располагается организация.

По заданию организация размещается в здании квадратной формы на трёх этажах: нулевой, первый и второй. Общая площадь помещений, занимаемых организацией, составляет 430 метров квадратных.

На нулевом этаже находится складское помещение и кабинет заведующего складом. В кабинете находятся две пользовательские станции и принтер. В складском помещении установлены две камеры видеонаблюдения, в коридоре – одна камера.

На первом этаже располагаются торговый зал, пост охраны и комната с сетевым оборудованием. Единственная пользовательская станция, находящаяся на этом этаже, располагается в комнате охранника. В комнате с сетевым оборудованием находится модем, маршрутизатор, коммутатор, web-сервер, сетевой видеорегистратор. В торговом зале находятся три камеры видеонаблюдения.

На втором этаже находится кабинет отдела кадров, комната администратора сети, кабинет начальника организации и его приёмная, бухгалтерия, кабинет маркетолога. В кабинетах начальника организации, администратора сети, маркетолога, отделе кадров и приёмной находится по одной пользовательской станции. В бухгалтерии находятся 2 пользовательские станции. В коридоре этажа установлены две камеры видеонаблюдения.

На нулевом и втором этажах находится по одному коммутатору, к которым подключается оконечное оборудование этих этажей.

На первом этаже находится корневой коммутатор, к которому подключены коммутаторы нулевого и второго этажей, а также оконечное оборудование первого этажа.

3. функциональное проектирование

## **3.1 Обоснование выбора типа подключения к Internet**

## Прежде чем приступить к выбору технологии подключения к интернету, необходимо определить требования, удовлетворяющие нуждам организации. В первую очередь стоит учесть, что у организации есть web-сервер, доступный из внешней сети.

## Обычно, собственный web-сервер используется для размещения сайта организации. При анализе статистики посещений сайтов организаций, работающих в такой же сфере, стало понятно, что в среднем сайт будет посещать 10000 пользователей в месяц. Распределение количество посещений между днями месяца можно считать равномерным, поэтому среднее количество посещений в день равно 333. Теперь нужно определить пиковое количество одновременных посещений сайта. Количество посещений зависит от времени суток, количество посещений подобных сайтов в промежуток времени с 20.00 до 8.00 составляет менее одного процента от общего дневного количества, поэтому ими можно пренебречь. Распределение посещений в период активности пользователей примем равномерным. Тогда среднее количество одновременных посещений составит 28. За максимальное количество посещений примем среднее количество, увеличенное на 20%. Максимальное количество посещений составит 34. В таком случае можно допустить, что соединение с интернетом должно обеспечить комфортную работу для 34 одновременных пользователей.

## Нагрузку рассчитаем для случая, когда всем пользователям необходимо загрузить страницу сайта. Средний размер одной страницы сайта составляет 2 Мбайт. Оптимальное время загрузки одной страницы – 3 секунды. Таким образом, если 34 пользователям понадобится одновременно загрузить страницу сайта, и мы хотим обеспечить им оптимальное время загрузки, соединение с интернетом должно обеспечить скорость загрузки до 181 Мбит/с. Из этого следует, что соединение посредством ADSL2+, VDSL2, 3G и 4G не подходят. Также следует сразу отказаться от соединения посредством витой пары, так как она имеет большое количество ограничений на использование. Среди оставшихся способов подключения можно выделить DOCSIS, Gigabit Ethernet с использованием оптоволокна и GPON как наиболее предпочтительные. Сеть организации является бюджетной, а подключение посредством оптоволоконных кабелей значительно дороже, чем подключение по коаксиальному кабелю. Кроме того, Gigabit Ethernet и GPON обеспечивают избыточную для нужд организации пропускную способность.

## Максимальная скорость восходящего потока DOCSIS 3.0 составляет 200 Мбит/с. Этого удовлетворяет описанным выше требованиям, поэтому подключение посредством DOCSIS является наилучшим вариантов в данном случае.

## **3.2 Обоснование выбора оборудования для защиты от сильных перепадов напряжения**

Защитить оборудование от сильных перепадов напряжения можно с помощью реле контроля напряжения, стабилизаторов напряжения или источников бесперебойного питания. В среднем, реле дешевле, чем стабилизатор напряжения и ИБП, однако оно отключает приборы от сети при перепаде напряжения большем, чем значение, на которое оно было настроено. Такое решение не подходит для нашей организации, так как при частых отключениях рабочих станций и сетевого оборудования от сети, сотрудники организации не смогут эффективно работать. Более хорошим вариантом является стабилизатор напряжения, так как он стабилизирует напряжение в сети, и приборы не отключаются при перепадах напряжения. ИБП также стабилизируют напряжение, не отключая приборы от сети и позволяет им проработать некоторое время в случае отключения электричества. Это может быть полезно, так как при отключении электричества у сотрудников будет время, чтобы сохранить данные, потеря которых может привести к убыткам организации. Пользовательские станции, в совокупности с мониторами, потребляют не более 400 Вт. Исходя из этого, минимальная допустимая мощность для источника бесперебойного питания должна составлять не менее 600 Вт. В таблице 3.1 приведены характеристики источников бесперебойного питания, подходящих под описанные выше требования.

Таблица 3.1 – Сравнение источников бесперебойного питания

|  |  |  |  |
| --- | --- | --- | --- |
| Характеристики | Powerman Smart Sine 1000 | Powercom Raptor RPT-1000AP 1000VA | APC Easy UPS BV 1000 BA BV1000I |
| Мощность, Вт | 700 | 600 | 600 |
| Полная мощность, ВА | 1000 | 1000 | 1000 |
| Максимальное время переключения, мс | 6 | 4 | 10 |
| Запас энергии, Вт\*ч | 168 | 108 | 84 |
| Цена | 185$ | 84$ | 159$ |

Из таблицы 3.1 видно, что источник питания Powerman Smart Sine 1000 имеет большую ёмкость батареи и мощность, поэтому может обеспечить большее время работы оборудования при отключении электричества, однако он значительно дороже, чем модель Powercom Raptor RPT-1000AP 1000VA, которая также удовлетворяет описанным ранее требованиям. С учётом того, что источником бесперебойного питания нужно обеспечить каждую рабочую станцию в организации, а также сетевое оборудование, значительно выгоднее будет использовать модель Powercom Raptor RPT-1000AP 1000VA.

## **3.3 Обоснование выбора пользовательской операционной системы.**

Наиболее распространёнными операционными системами на сегодняшний день являются Windows, MacOS и Linux.

MacOS устанавливается только на устройства компании Apple. Продукция этой компании выделяется высокой стоимостью. С учётом того, что разрабатываемая сеть является бюджетной, а производительность современных устройств Apple избыточна для офисных работников, их покупка является нецелесообразной, поэтому от использования MacOS следует отказаться.

Большинство дистрибутивов операционной системы Linux распространяется бесплатно, и совместимы с большинством процессоров Intel, выпущенными за последние 30 лет. Так как персональные компьютеры будут использоваться для работы с офисным программным обеспечением, следует рассматривать только операционные системы, имеющие графический интерфейс. Наиболее популярными среди пользователей дистрибутивами Linux с графическим интерфейсом являются Ubuntu, Fedora, Mint. Эти операционные системы могут быть использованы офисными работниками, однако следует учитывать, что наиболее распространённой операционной системой, которую обычные пользователи используют дома и в офисах, является Windows. Сотрудники могут испытать трудности при работе с незнакомой операционной системой, что скажется на эффективности их работы. По этой причине было принято решение использовать операционную систему Windows 10. Таким образом, сотрудники организации смогут пользоваться программным обеспечением Microsoft Office, которое предоставит большую часть необходимого для их работы функционала.

## **3.4 Обоснование выбора операционной системы web-сервера.**

Чаще всего, для серверов используется операционная система Linux. Она потребляет меньшее количество аппаратных ресурсов, чем современные Windows, и даёт много возможностей опытному пользователю.

Было решено использовать дистрибутив Debian. Этот дистрибутив отличается стабильной работой, регулярно получает обновления и имеет большое сообщество пользователей.

В качестве web-сервера был выбран сервер Apache. Apache является популярным и проверенным web-сервером, а также обладает хорошей документацией.

## **3.5 Обоснование выбора пользовательских станций.**

Так как организация, для которой разрабатывается сеть, занимается торговлей овощами и фруктами, и её сотрудники использую офисное программное обеспечение, которое не требует большого количества оперативной памяти, высокопроизводительных процессора и видеокарты, можно выделить следующие требования для пользовательских станций:

1. Шестиядерный процессор intel core i5 8400 является оптимальным выбором для офисного компьютера в бюджетном ценовом сегменте. Характеристик процессора хватает для производительной работы сотрудников организации;

2. 8 ГБ DDR4 оперативной памяти и накопителя HDD 1000 ГБ достаточно для комфортной работы сотрудников;

При изучении готовых сборок, представленных на рынке, были выбраны для сравнения модели, представленные в таблице 3.2.

Таблица 3.2 – Сравнение пользовательских станций

|  |  |  |
| --- | --- | --- |
| Характеристики | Jet Office 5i8400D8HD1VGALW50 | Jet Office 5i12400D8HD1VGALW50 |
| Процессор | Intel Core i5 8400 | Intel Core i5 12400 |
| Оперативная память | DDR4 8 Гб | DDR4 8 Гб |
| Конфигурация накопителя | HDD 1000 Гб | HDD 1000 Гб |
| Видеокарта | Intel UHD Graphics 630 | Intel UHD Graphics 630 |
| Цена | ≈400$ | ≈500$ |

Как видно из таблицы 3.2, станции различаются только моделью процессора. Процессор Intel Core i5 12400 имеет большую тактовую частоту и большее количество кэш-памяти, поэтому обеспечивает большую производительность, однако для работы сотрудников организации хватит производительности более дешёвой станции Jet Office 5i8400D8HD1VGALW50, поэтому была выбрана эта модель.

## **3.6 Обоснование выбора web-сервера**

Для сервера важно иметь ECC RAM, поэтому в первую очередь нужно выбрать процессор, поддерживающий работу с таким типом памяти.

8 ГБ DDR4 оперативной памяти хватит для стабильной работы сервера при ожидаемых нагрузках. HDD накопителя на 1000 ГБ достаточно для хранения необходимых данных.

В таблице 3.3 представлены характеристики трёх серверов, подходящих под описанные выше требования.

Таблица 3.3 – Сравнение серверов

|  |  |  |  |
| --- | --- | --- | --- |
| Характеристики | Dell EMC PowerEdge T150 M83C9 | HPE ProLiant MicroServer Gen10 P16005-421 | Dell EMC PowerEdge T40 550HK |
| Установленная память | DIMM 8GB DDR4 PC4-3200 ECC, SingleRank x8 | DIMM 8GB DDR4 PC4-2666 ECC, SingleRank x8 | DIMM 8GB DDR4 PC4-2666 ECC, SingleRank x8 |
| Установленные HDD | HDD 1000GB SATA 7200rpm | HDD 1000GB SATA 7200rpm | HDD 1000GB SATA 7200rpm |
| Процессор | Intel Xeon E-2314 | Intel Pentium Gold G5420 | Intel Xeon 2224G |
| Видеоадаптер | Matrox® G200eW 16MB Integrated Graphics Controller | Matrox® G200eW 16MB Integrated Graphics Controller | Matrox® G200eW 16MB Integrated Graphics Controller |
| Порты LAN | 2 x GbE | 2 x GbE | 2 x GbE |
| Цена | 834,54 $ | 671,63 $ | 572,81 $ |

Для сравнения были выбраны серверы из одной ценовой категории, имеющие схожие характеристики. Как видно из таблицы 3.3, основным отличием трёх моделей является процессор.

Процессоры Intel Xeon E-2314 и Intel Xeon 2224G близки по своим характеристикам. Intel Pentium Gold G5420 имеет меньшее количество ядер и меньшую тактовую частоту. С учётом характеристик и цен, был выбран сервер Dell EMC PowerEdge T40, так как сеть организации является бюджетной, а данная модель значительно дешевле и имеет характеристики не хуже, чем две другие.

## **3.7 Обоснование выбора чёрно-белого принтера А4**

Сотрудникам организации часто нужно распечатывать рабочие документы, поэтому важно обеспечить хорошее качество и оптимальную скорость печати. Из этого следует, что следует выбирать из лазерных принтеров, так как они имеют более высокую скорость печати, чем струйные, и обеспечивает более хорошее качество печати текстовых документов. Для сравнения были выбраны принтеры, представленные в таблице 3.4.

Таблица 3.4 – Сравнение принтеров

|  |  |  |  |
| --- | --- | --- | --- |
| Характеристики | Pantum P2207 | Pantum 3010D | Pantum P2507 |
| Скорость печати | 20 стр/мин | 30 стр/мин | 22 стр/мин |
| Разрешение | 1200 dpi | 1200 dpi | 1200 dpi |
| Цена | 113.74$ | 197,75$ | 126,4$ |

Из таблицы 3.4 видно, что принтеры имеют схожие характеристики, и основным отличием является скорость печати. Так как сотрудникам организации может понадобиться печатать многостраничные документы, следует принять во внимание, что принтер Pantum 3010D обеспечивает скорость печати, в 1,5 раза превышающую скорость двух других моделей, что позволит сэкономить время сотрудников. Разница в цене не велика, поэтому был выбран Pantum 3010D.

## **3.8 Обоснование выбора компонентов системы видеонаблюдения**

Для того, чтобы охватить все важные места в здании, система видеонаблюдения должна включать в себя 7-9 камер.

При изучении видеорегистраторов, представленных на рынке, стало понятно, что для бюджетной сети подойдёт модель HIKVISION Standart DS-7608NI-K2, позволяющая подключить 8 камер посредством витой пары. Приводить сравнение с другими видеорегистраторами, поддерживающими подключение 8 камер не имеет смысла, так как другие модели находятся в другом ценовом сегменте, то есть значительно дороже выбранного видеорегистратора, и не имеют видимых преимуществ.

Среди камер для сравнения были выбраны модели, представленные в таблице 3.5.

Таблица 3.5 – Сравнение камер

|  |  |  |
| --- | --- | --- |
| Характеристики | Dahua DH-IPC-HDW2831TMP-AS-0360B-S2 | Dahua DH-IPC-HFW2831SP-S-0360B-S2 |
| Разрешение | 8 МП | 8МП |
| Корпус | купольная | уличная |
| Подсветка | ИК | ИК |
| Цена | ≈180$ | ≈190$ |

Основные характеристики камер схожи, обе модели имеют разъём для подключения к видеорегистратору посредством витой пары. Камеру с корпусом купольного типа имеет преимущество над камерой с уличным корпусом, поскольку направление объектива камеры неочевидно для злоумышленника. Также модель Dahua DH-IPC-HDW2831TMP-AS-0360B-S2, поэтому была выбрана она.

## **3.9 Обоснование выбора активного сетевого оборудования**

Полный перечень оборудования представлен в приложении «В».

**3.9.1 Обоснование выбора кабельного модема**

Найти доступный для покупки в Беларуси кабельный модем от компании Allied Telesis не удалось, поэтому было решено рассмотреть модемы от других производителей. При изучении рынка было найдено два подходящих модема, характеристики которых представлены в таблице 3.6.

Таблица 3.6 – Сравнение кабельных модемов

|  |  |  |
| --- | --- | --- |
| Характеристики | D-Link DCM-301 | Cisco DPC3008 |
| Стандарт DOCSIS | 3.0 | 3.0 |
| Максимальная скорость восходящего потока | 160 Мбит/с | 120 Мбит/с |
| Максимальная скорость нисходящего потока | 343 Мбит/с | 340 Мбит/с |
| Цена | 35$ | 32.49$ |

Как видно из таблицы 3.6, наиболее удачным выбором будет D-Link DCM-301, так как он обеспечивает большую скорость восходящего потока, что очень важно для web-сервера. В пункте 3.1 было сказано, что необходимая для обеспечения комфортного просмотра сайта организации при максимальной нагрузке скорость восходящего потока составляет 181 Мбит/с. Выбранный модем не может обеспечить такой скорости, и при максимальной нагрузке страницы сайта для пользователей будут загружаться около 3,5 секунд, что на 0,5 секунды больше оптимального времени. Это незначительная задержка, и с учётом того, что альтернативой кабельному подключению является значительно более дорогое оптоволокно, обеспечивающее избыточную для организации пропускную способность, такое решение является подходящим.

### **3.9.2 Обоснование выбора маршрутизатора**

При поиске доступных для покупки в Беларуси маршрутизаторов Allied Telesis было обнаружено всего две модели: AR2050V и AR4050S. При этом, это маршрутизаторы разных поколений, и модель AR4050S имеет значительно большую цену, поэтому приводить сравнение не имеет смысла. Характеристики маршрутизатора AR2050V удовлетворяют требованиям разрабатываемой сети, поэтому была выбрана эта модель.

Маршрутизатор AR2050V поддерживает Gigabit Ethernet. Данное устройство обладает следующими основными характеристиками:

1. 4 Gigabit Ethernet LAN-порта;

2. 1 Gigabit Ethernet WAN-порт;

3. 1 USB-порт и 1 порт для консоли;

4. Поддержка стандарта 802.1Q

# **3.9.3 Обоснование выбора коммутатора**

Компания Allied Telesis предлагает коммутаторы как второго, так и третьего уровней. Так как коммутаторы третьего уровня дороже, чем коммутаторы второго уровня, а бюджет организации ограничен, было решено использовать коммутаторы второго уровня.

Коммутаторы второго уровня делятся на управляемые и неуправляемые. Нам требуются управляемые коммутаторы, которые поддерживают протоколы сетевого уровня, в частности, протокол 802.1Q, так как будет необходимо создать несколько VLANs.

С учётом количества устройств, которые находятся на каждом этаже, было решено выбирать коммутаторы, имеющие шестнадцать портов.

Среди коммутаторов, представленных на сайте Allied Telesis, под описанные выше требования подходят коммутаторы, представленные в таблице 3.7.

Таблица 3.7 – Сравнение коммутаторов

|  |  |  |
| --- | --- | --- |
| Коммутатор | AT-GS950/16PS | AT-GS916M |
| Цена | ≈800$ | ≈290$ |
| Количество портов | 16 x Gbe | 16 x Gbe |
| Пропускная способность | 56 Гбит/с | 48 Гбит/с |
| Скорость пересылки пакетов | 41,6 Mpps | 35,7 Mpps |
| Поддержка 802.1Q | да | да |
| Поддержка PoE | да | нет |
| Управление | Web GUI (HTTP), CLI | Web GUI (HTTP), CLI |

Так как питание точки доступа осуществляется через PoE, удобно было бы использовать коммутатор модели AT-GS950/16. По функциональным возможностям, обе модели подходят для использования. С учётом того, что сеть организации является бюджетной, и разница в цене двух моделей велика, решено было использовать коммутатор AT-GS916M.

# **3.9.4 Обоснование выбора точки доступа**

По заданию, в разрабатываемой локальной сети необходимо обеспечить возможность подключения пяти мобильных устройств. Для этого понадобится беспроводная точка доступа.

Бюджетные точки доступа Allied Telesis, предназначенные для использования внутри помещений, представлены в таблице 3.8.

Таблица 3.8 – Сравнение точек доступа

|  |  |  |
| --- | --- | --- |
| Точка доступа | TQ1402 | TQ5403 |
| Цена | ≈210 $ | ≈575 $ |
| Частота, Гц | 2,4, 5 | 2,4, 5 |
| Поддерживаемые стандарты IEEE 802.11 | a/b/g/n/ac | a/b/g/n/ac |
| Поддерживаемые стандарты IEEE 802.3 | u/ab/x/at | u/ab/x/at |
| Питание | PoE | PoE, адаптер |
| Максимальная потребляемая мощность от PoE, Вт | 12 | 19 |
| Безопасность | WEP/WPA/WPA2- PSK | WEP/WPA/WPA2- PSK |
| Поддержка VLANs | Да | Да |
| Максимальное пиковое усиление 2,4 ГГц / 5 ГГц, дБи | 1,9 / 3,7 | 3,95 / 4,83 |

Рассматриваемые точки доступа имеют схожие характеристики. Основным отличием является максимальное усиление сигнала антенн. Точка доступа TQ5403 мощнее, но также её цена значительно выше. Точки доступа TQ1402 должно хватить для обеспечения качественной связи в пределах этажа здания организации. Правильность выбора будет проверена в разделе 3.10.

**3.10 Расчёт качества связи беспроводной сети**

Для выбора количества точек доступа необходимо рассчитать покрытие беспроводной сетью всех помещений в организации. Так как межэтажные перекрытия выполнены из железобетона, добиться хорошего уровня сигнала используя одну точку доступа для нескольких этажей не получится, поэтому расчёты будут проводиться в рамках одного этажа.

Будем считать, что соседние здания находятся на расстоянии, достаточном для того, чтобы беспроводные сети, организованные в них, не будут влиять на разрабатываемую сеть.

Для расчёта затухания радиоволн в беспрепятственной воздушной среде используем упрощённую формулу:

(3.1)

где F – частота сигнала в ГГц, D – расстояние в метрах от точки доступа.

Здание имеет квадратную форму. Для минимизации расстояния для всех возможных пользователей, точка размещается в центре этажа, на потолке.

Высоту потолка примем равной 2,5 м, расстояние до стен – 6 м. Рассчитаем расстояние до нижнего угла помещения:

где *l* – длина, *w* – ширина, *h* – высота.

Рассчитаем затухание радиоволн L2,4 для частоты 2,4 ГГц L5 для частоты 5 ГГц по формуле (3.1):

Необходимо учесть затухание сигнала при прохождении конструкционных элементов здания. Внутренние стены состоят из кирпича, максимальное количество препятствующих стен равно двум. Таким образом, затухание радиоволн при прохождении через стены: L2,4 макс. ст. = 2 \* 4,44 = 8,88 дБ. L5 макс. ст. = 2 \* 14,62 = 29,24 дБ.

Согласно документации, мощность излучения точки на частоте 2,4 ГГц составляет 19,78 дБм, на частоте 5 ГГц – 27,31 дБм. Тогда минимальная мощность сигнала *S1* (2.4 ГГц), *S2* (5 ГГц) в самой удаленной точке помещения исходя из мощности передатчика *P2,4* (2.4 ГГц), *P5* (5 ГГц) будет равна:

*S1* = *P2,4 +U2,4* – *L2,4 макс* – *L2,4 макс ст.* = 19,78 дБм +1,9 дБи – 58,98 дБ – 8,88 дБ = – 46,18 дБм.

*S2* = *P5* *+ U5 –* *L5 макс* – *L5 макс ст.*= 27,31 дБм + 3,7 дБи – 65,36 дБ –

29,24 дБ = – 63,59 дБм.

Качество обслуживания беспроводных клиентов напрямую зависит от мощности сигнала в точке обслуживания и может быть оценена по следующей шкале:

* до -30 дБм – идеальный сигнал;
* от -30 до -50 дБм – отличный сигнал;
* от -50 до -60 дБм – комфортный сигнал для большинства задач;
* -67 дБм – минимальный уровень сигнала для HD‑видео и голосовой связи;
* до -70 дБм – слабый сигнал, достаточный для email и легкого интернет-серфинга;
* от -70 до -80 дБм – сигнал нестабильный, возможна передача коротких текстовых сообщений;
* до -90 дБм – сигнала почти нет, пользоваться сетью почти невозможно.

По результатам расчетов получается, что минимальная мощность Wi‑Fi сигнала на этаже при размещении единственной точки доступа в середине этажа будет находиться в диапазоне от -46 дБм до -64 дБм, что обеспечивает комфортный уровень сигнала даже в самых удаленных точках.

## **3.11 Обоснование выбора пассивного сетевого оборудования**

Для коммутаторов, находящихся на нулевом и втором этажах, невозможно выделить отдельную комнату, поэтому из соображений безопасности было решено разместить сетевое оборудование в телекоммуникационные шкафы. Коммутатор, модем и маршрутизатор, находящиеся в отдельной комнате на первом этаже также решено установить в телекоммуникационный шкаф для дополнительной защиты от физического воздействия и удобства их размещения. Подходящие шкафы, выбранные для сравнения, представлены в таблице 3.9.

Таблица 3.9 – Сравнение телекоммуникационных шкафов

|  |  |  |  |
| --- | --- | --- | --- |
| Характеристики | ЦМО ШРН-Э-9.500-9005 | TWT-CBWSF-9U-6x4-GY | ЦМО ШРН-Э-9.500.1 |
| Тип передней двери | Стекло | Металл | Металл |
| Высота, мм | 480 | 480 | 480 |
| Ширина, мм | 600 | 600 | 600 |
| Глубина, мм | 520 | 400 | 520 |
| Вес, кг | 17,64 | 17,34 | 17,28 |
| Цена | 124$ | 167$ | 120$ |

Как видно из таблицы 3.9, один из шкафов имеет стеклянную переднюю дверь. Такой вариант является менее предпочтительным, так как одна из причин использования шкафа – защита сетевого оборудования от физического воздействия. Оставшиеся модели шкафов отличаются размерами и ценой. Также шкаф ЦМО ШРН-Э-9.500.1 предполагает возможность установки вентиляторов в основание или крышу шкафа. Так как эта модель дешевле, имеет большее внутреннее пространство и хорошую вентиляцию, была выбрана она.

## **3.12 Схема адресации**

В задании выдана подсеть 201.68.7.0/25.

Исходя из перечня оборудования, а также ролей пользователей, которые имеют к нему доступ, следует разделить подсеть на 5 подсетей. Одна будет для принтера и стационарных компьютеров сотрудников предприятия. Вторая – для мобильных подключений. Третья подсеть нужна для сервера, четвертая для администрирования, а пятая для системы видеонаблюдения. При этом запретим выход сервера в интернет, а также доступ мобильных подключений к ресурсам предприятия.

Подсеть 201.68.7.0/25 разбита с учетом количества устройств, приходящихся на каждый vlan. Адреса подсетей представлены в таблице 3.10

Для стационарных устройств (8 ПК и 6 принтеров) выбрана подсеть IPv4 201.68.7.0/28, и подсеть FDB1:8C12:131A::/48 для IPv6.

В беспроводной сети 5 мобильных устройств. Для нее выделена подсеть 201.68.7.16/28.

Для системы видеонаблюдения выделена подсеть 201.68.7.32/28, в неё будут входить компьютер охранника, видеорегистратор и камеры.

Для администрирования нужно выделить подсеть, которая будет включать 5 устройств: центральный маршрутизатор, три коммутатора и компьютер администратора. Была выбрана подсеть 201.68.7.48/29.

И для Web-сервера берем подсеть 201.68.7.56/29.

Таблица 3.10 – Схема адресации сетей

|  |  |  |  |
| --- | --- | --- | --- |
| Назначение | VLAN | Адрес подсети | Маска подсети |
| Стационарные подключения | 10 | 201.68.7.0 | 255.255.255.240 |
| FDB1:8C12:131A:1:: | /64 |
| Беспроводная | 20 | 201.68.7.16 | 255.255.255.240 |
| Видеонаблюдения | 30 | 201.68.7.32 | 255.255.255.240 |
| Административная | 40 | 201.68.7.48 | 255.255.255.248 |
| Сервер | 50 | 201.68.7.56 | 255.255.255.248 |

## **3.13 Настройка маршрутизатора**

**3.13.1 Настройка VLAN**

Awplus>enable

Awplus#conf terminal

Awplus(config)#hostname Router

Router (config)#set user admin password dj928lpz21s

Настроим подинтерфейсы для VLAN:

Router (config)#interface gi 0/2

Router (config-if)#interface gi 0/2.1

Router (config-subif)#encapsulation dot1q 10

Router (config-subif)#ip address 201.68.7.1/28

Router (config-subif)#ipv6 address FDB1:8C12:131A:1::1/64

Router (config-subif)#exit

Router (config-if)#interface gi 0/2.2

Router (config-subif)#encapsulation dot1q 20

Router (config-subif)#ip address 201.68.7.17/28

Router (config-subif)#exit

Router (config-if)#interface gi 0/2.3

Router (config-subif)#encapsulation dot1q 30

Router (config-subif)#ip address 201.68.7.33/28

Router (config-subif)#exit

Router (config-if)#interface gi 0/2.4

Router (config-subif)#encapsulation dot1q 40

Router (config-subif)#ip address 201.68.7.49/29

Router (config-subif)#exit

Router (config-if)#interface gi 0/2.5

Router (config-subif)#encapsulation dot1q 50

Router (config-subif)#ip address 201.68.7.57/29

Router (config-subif)#exit

Адреса подинтерфейсов роутера и маски для каждой из подсетей представлены в таблице 3.11.

Таблица 3.11 – Схема адресации маршрутизатора

|  |  |  |
| --- | --- | --- |
| Назначение | IP адрес | Маска подсети |
| Стационарные подключения | 201.68.7.1 | 255.255.255.240 |
| FDB1:8C12:131A:1::1 | /64 |
| Беспроводная | 201.68.7.17 | 255.255.255.240 |
| Видеонаблюдения | 201.68.7.33 | 255.255.255.240 |
| Административная | 201.68.7.49 | 255.255.255.248 |
| Сервер | 201.68.7.57 | 255.255.255.248 |

**3.13.2 Настройка DHCP**

Мобильные устройства выступают как DHCPv4 клиенты, поэтому необходимо настроить DHCPv4 сервер.

Создание пула адресов на подинтерфейсе для vlan 20:

Router(config)#interface gi0/2.20

Router(dhcp-if)#ip dhcp pool wireless

Router(dhcp-if)#network 201.68.7.16/28

Router(dhcp-if)#default-router 201.68.7.17

Запуск DHCPv4 сервера на определённом подинтерфейсе:

Router(config)#interface gi0/2.20

Router(config-if)#ip dhcp server wireless

Так как IP адрес назначается провайдером автоматически, на маршрутизаторе также необходимо настроить DHCPv4 клиент:

Router(config)#interface gi0/1

Router(config-if)#ip address dhcp

**3.13.3 Настройка прокси**

В качестве прокси выберем Smart DNS proxy. Этот сервис предоставляет большое количество серверов и хорошее качество работы.

Для настройки прокси добавим адреса ближайших серверов в список:

Router(config)#ip name-server 54.93.173.153

Router(config)#ip name-server 82.103.129.72

## **3.14 Настройка коммутаторов**

Выдадим адреса устройствам административной подсети в соответствии с таблицей 3.5.

Таблица 3.5 – Адреса устройств для административной подсети.

|  |  |  |
| --- | --- | --- |
| Устройство | IP адрес | Маска подсети |
| Router | 201.68.7.49 | 255.255.255.248 |
| Switch0 | 201.68.7.50 | 255.255.255.248 |
| Switch1 | 201.68.7.51 | 255.255.255.248 |
| Switch2 | 201.68.7.52 | 255.255.255.248 |
| Admin-PC | 201.68.7.53 | 255.255.255.248 |

**3.14.1 Конфигурация коммутатора нулевого этажа**

Awplus>enable

Awplus#conf terminal

Awplus(config)#hostname Switch0

Switch0(config)#set user admin password dj928lpz21s

Создаем VLAN:

Switch0(config)#vlan 10

Switch0(config-vlan)#name user

Switch0(config-vlan)#exit

Switch0(config)#vlan 20

Switch0(config-vlan)#name wireless

Switch0(config-vlan)#exit

Switch0(config)#vlan 40

Switch0(config-vlan)#name management

Switch0(config-vlan)#exit

Switch0 (config)#interface vlan 40

Switch0 (config-if)#ip address 201.68.7.50/29

Switch0(config-vlan)#exit

Switch0(config)#vlan 50

Switch0(config-vlan)#name web-server

Switch0(config-vlan)#exit

Настраиваем порты:

Switch0(config)#interface gi0/1

Switch0(config-if)# switchport mode trunk

Switch0(config-if)# switchport trunk allowed vlan add 10, 20, 40, 50

Switch0(config)#interface gi0/2

Switch0(config-if)# switchport mode access

Switch0(config-if)# switchport access vlan 10

Switch0(config)# interface gi0/3

Switch0(config-if)# switchport mode access

Switch0(config-if)# switchport access vlan 10

Switch0(config)# interface gi0/4

Switch0(config-if)# switchport mode access

Switch0(config-if)# switchport access vlan 20

Switch0(config)# interface gi0/5

Switch0(config-if)# switchport mode access

Switch0(config-if)# switchport access vlan 10

**3.14.2 Конфигурация коммутатора первого этажа**

Awplus>enable

Awplus#conf terminal

Awplus(config)#hostname Switch1

Switch1(config)#set user admin password dj928lpz21s

Создаем VLAN:

Switch1(config)#vlan database

Switch1(config-vlan)#vlan 10 name user state enable

Switch1(config-vlan)#vlan 20 name wireless state enable

Switch1(config-vlan)#vlan 30 name cctv state enable

Switch1(config-vlan)#vlan 40 name management state enable

Switch1(config-vlan)#vlan 50 name web-server state enable

Switch1(config-vlan)#exit

Настраиваем IP-адрес для администрирования:

Switch1 (config-subif)#in vlan 40

Switch1 (config-subif)#ip address 201.68.7.51/2

Настраиваем интерфейсы:

Switch1(config)#interface gi0/1

Switch1(config-if)# no switchport

Switch1(config)# interface gi0/2

Switch1(config-if)# switchport mode access

Switch1(config-if)# switchport access vlan 20

Switch1(config)# interface gi0/3

Switch1(config-if)# switchport mode access

Switch1(config-if)# switchport access vlan 30

Switch1(config)# interface gi0/4

Switch1(config-if)# switchport mode access

Switch1(config-if)# switchport access vlan 30

Switch1(config)# interface gi0/5

Switch1(config-if)# switchport mode access

Switch1(config-if)# switchport access vlan 50

Switch0(config)# interface range gi0/6-7

Switch0(config-if)# switchport mode trunk

Switch0(config-if)# switchport trunk allowed vlan add 10, 20, 40, 50

**3.14.3 Конфигурация коммутатора второго этажа**

Awplus>enable

Awplus#conf terminal

Awplus(config)#hostname Switch2

Switch1(config)#set user admin password dj928lpz21s

Создаем VLAN:

Switch2(config)#vlan database

Switch2(config-vlan)#vlan 10 name user state enable

Switch2(config-vlan)#vlan 20 name wireless state enable

Switch2(config-vlan)#vlan 40 name management state enable

Switch2(config-vlan)#vlan 50 name web-server state enable

Switch2(config-vlan)#exit

Настраиваем IP-адрес для администрирования:

Switch2 (config-subif)#in vlan 40

Switch2 (config-subif)#ip address 201.68.7.53/29

Настраиваем интерфейсы:

Switch2(config)# interface gi0/1

Switch2(config-if)# switchport mode trunk

Switch2(config-if)# switchport trunk allowed vlan add 10, 20, 40, 50

Switch2(config)# interface range gi0/2-12

Switch2(config-if)# switchport mode access

Switch2(config-if)# switchport access vlan 10

Switch2(config)# interface gi0/13

Switch2(config-if)# switchport mode access

Switch2(config-if)# switchport access vlan 20

Switch2(config)# interface gi0/14

Switch2(config-if)# switchport mode access

Switch2(config-if)# switchport access vlan 40

Для защиты порта, к которому подключён ПК администратора, используем port security:

Switch2(config)#interface gi0/14

Switch2(config-if)#switchport port-security

Switch2(config-if)#switchport port-security maximum 1

## **3.15 Настройка ПК**

Для ПК требуется настроить статическую IPv4 и IPv6 маршрутизацию. Адреса ПК представлены в таблице 3.6.

Таблица 3.6 – Адреса ПК.

|  |  |  |
| --- | --- | --- |
| Устройство | IP адрес | Маска подсети |
| Stk-PC1 | 201.68.7.2 | 255.255.255.240 |
| FDB1:8C12:131A:1::2 | /64 |
| Stk-PC2 | 201.68.7.3 | 255.255.255.240 |
| FDB1:8C12:131A:1::3 | /64 |
| Sec-PC | 201.68.7.34 | 255.255.255.240 |
| User-PC1 | 201.68.7.4 | 255.255.255.240 |
| FDB1:8C12:131A:1::4 | /64 |
| User-PC2 | 201.68.7.5 | 255.255.255.240 |
| FDB1:8C12:131A:1::5 | /64 |
| User-PC3 | 201.68.7.6 | 255.255.255.240 |
| FDB1:8C12:131A:1::6 | /64 |
| User-PC4 | 201.68.7.7 | 255.255.255.240 |
| FDB1:8C12:131A:1::7 | /64 |
| User-PC5 | 201.68.7.8 | 255.255.255.240 |
| FDB1:8C12:131A:1::8 | /64 |
| User-PC6 | 201.68.7.9 | 255.255.255.240 |
| FDB1:8C12:131A:1::9 | /64 |
| Admin-PC | 201.68.7.53 | 255.255.255.248 |

Настройка адресов IPv4 и IPv6 на ПК с Windows производиться по следующему алгоритму:

1. Заходим в свойства Ethernet.

2. Выбираем IP версии 4 (TCP/IP), нажимаем кнопку «Свойства». Делаем поле «Использовать следующий IP-адрес», заполняем поля «IP-адрес» и «Маска подсети» соответствующими адресами из таблицы 3.5.

В поле «Основной шлюз» вводим IPv4 адрес центрального маршрутизатора. Окна настройки представлены на рисунке 3.1.

3. Настройка IPv6 аналогична IPv4, только нужно выбрать IP версии 6 (TCP/IP), и в окне настройки ввести IPv6 адреса ПК и маршрутизатора. Окна настройки представлены на рисунке 3.2.



Рисунок 3.1 – Настройка IPv4 на ПК



Рисунок 3.2 – Настройка IPv6 на ПК

## **3.16 Настройка принтера**

Для того, чтобы принтер можно было использовать, его необходимо подключить к локальной сети, а после этого установить драйвер с прилагающегося диска.

Подключение принтера к локальной сети состоит в физическом его подключении посредством Ethernet кабеля и настройке IP адреса. Настроить IP адрес можно с помощью встроенной в принтер консоли, показанной на рисунке 3.3.



Рисунок 3.3 – Консоль принтера

Сначала нужно нажать кнопку «Menu», затем стрелками выбрать раздел «Network Set» и нажать кнопку «ОК». После этого таким же образом выбираем раздел «Wired network setting». Задаём IP адрес и маску подсети. Для этого стрелками выбираем цифры от 0 до 9 и подтверждаем выбор кнопкой «ОК». После того, как последняя цифра маски была введена, ещё раз нажимаем кнопку «ОК» для сохранения и кнопку «Return», чтобы вернуться в предыдущий раздел меню.

Теперь необходимо установить на принтер драйверы, поставляемые в комплекте с принтером на диске. Для этого вставляем диск в дисковод компьютера. После этого на экране появится окно, показанное на рисунке 3.4.



Рисунок 3.4 – Поиск ПО для принтера

Нажимаем на кнопку One-click installation под Wired Network. После этого мы увидим окно со списком всех принтеров в сети. Выбираем IP адрес нужного принтера, после чего начнётся установка драйвера. По завершении установки появится окно, показанное на рисунке 3.5. Нажимаем кнопу «Done» для выхода из программы установки. Принтер готов к использованию.



Рисунок 3.5 – Окно завершения установки драйвера

## **3.17 Настройка web-сервера**

На web-сервере нужно указать адрес 201.68.7.58 и маску 255.255.255.248. В качестве шлюза указать ip адрес маршрутизатора –201.68.7.57. Для этого в директории /etc/network создаём файл interfaces и пишем в него следующие строки:

iface eth0 inet static

address 201.68.7.58

netmask 255.255.255.248

gateway 201.68.7.57

Для создания на сервере веб-сайта, нужно создать отдельную папку в директории /var/www. Создадим папку с именем ovf:

$sudo mkdir /var/www/ovf

В этой папке будут размещаться html файлы со страницами сайта.

Далее нужно создать виртуальный хостинг. Для этого перейдём в директорию с конфигурационными файлами и создадим новую конфигурацию:

$cd /etc/apache2/sites-available/

$sudo cp 000-default.conf ovf.conf

В конфигурационный файл добавим электронную почту администратора, ответственного за сервер, путь к папке с html файлами сервера и имя сервера:

ServerAdmin [myemail@gmail.com](mailto:myemail@gmail.com)

DocumentRoot /var/www/ovf

ServerName ovf.store.by

Теперь нужно активировать хостинг:

$sudo a2ensite ovf.conf

После этого сайт будет доступен по адресу, указанному в конфигурационном файле.

**3.18 Настройка точек беспроводного доступа**

В программное обеспечение маршрутизатора AR2050V входит компонент Vista Manager mini, который позволяет конфигурировать точки доступа, находящиеся в сети. Использовать его можно посредством веб-интерфейса маршрутизатора.

Для использования веб-интерфейса, нужно ввести в строку браузера адрес маршрутизатора, а затем ввести имя пользователя и пароль, настроенные ранее. После этого появится пользовательский интерфейс. В левой части интерфейса находится меню, показанное на рисунке 3.6. Для настройки точек доступа нужно перейти по вкладкам Vista Manager mini -> Wireless -> Wireless Setup -> Access Points.

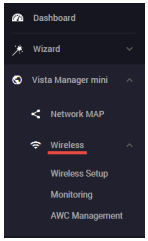


Рисунок 3.6 – Меню веб-интерфейса

Во вкладке Access Points нажмём кнопку Add Access Point, появится форма, показанная на рисунке 3.7.

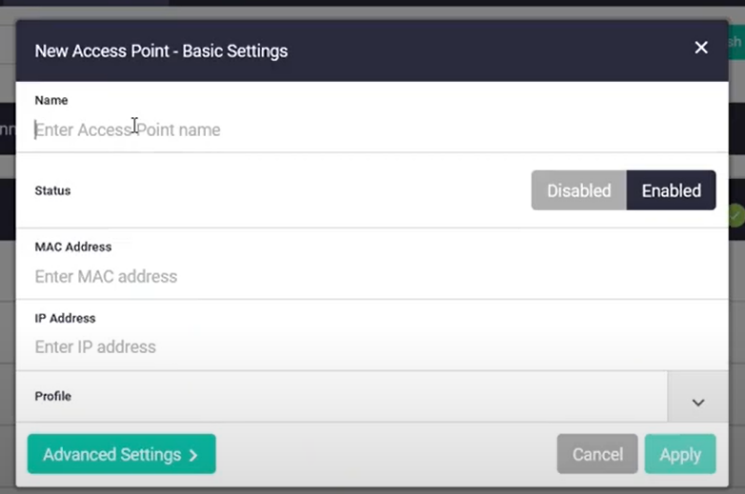


Рисунок 3.7 – Форма добавления точки доступа

В поле Name нужно ввести имя точки доступа. AP0, AP1 и AP2 для точек доступа нулевого, первого и второго этажа соответственно. В поле Status нажать на кнопку Enabled. В поле MAC Address нужно ввести MAC адреса соответствующих точек. В поле IP address ввести следующие адреса: 201.68.7.18 для точки доступа нулевого этажа, 201.68.7.19 для точки доступа первого этажа, 201.68.7.20 для точки доступа второго этажа. После того, как форма была заполнена, нужно нажать кнопку Apply для сохранения данных точки доступа.

После добавления точек доступа, нужно добавить подсеть, в которую они входят. Для этого перейдём во вкладку меню Networks, где нужно нажать кнопку Add Network. Появится форма, показанная на рисунке 3.8.

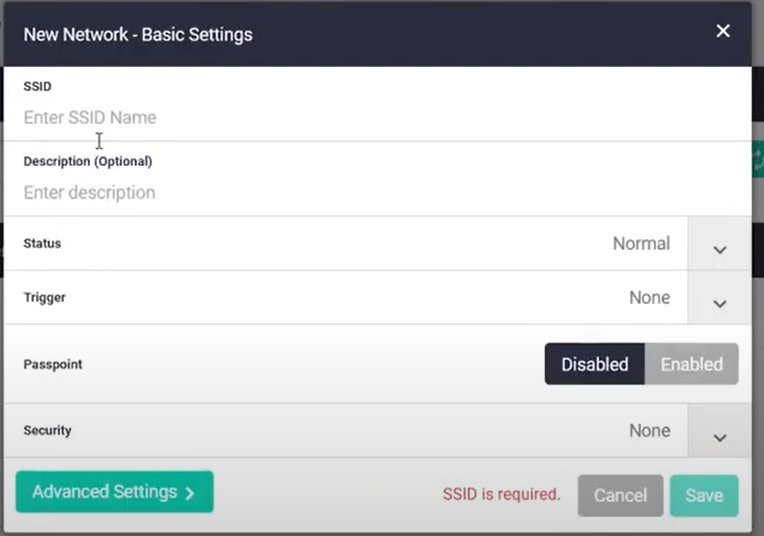


Рисунок 3.8 – Форма добавления подсети

В поле SSID введём название беспроводной сети – Wireless. В поле Security выберем WPA2 и зададим пароль. Остальные поля изменять не требуется. Перейдём в меню Advanced Settings. В поле VLAN ID введём id, назначенное vlan для подсети беспроводных устройств – 20. В поле Maximum Wireless Clients установим значение 5, так как по условию задания нужно обеспечить именно такое количество мобильных подключений. Нажимаем кнопку Save для сохранения изменений.

**3.19 Настройка видеорегистратора** **и камер**

Настройка видеорегистратора осуществляется через WEB интерфейс. По умолчанию установлена учетная запись администратора «admin» и IPv4 адрес по умолчанию «192.168.1.64». При первом доступе к устройству необходимо установить пароль учетной записи администратора для активации устройства. Нажать кнопку «Ok»(см. рис. 3.9).

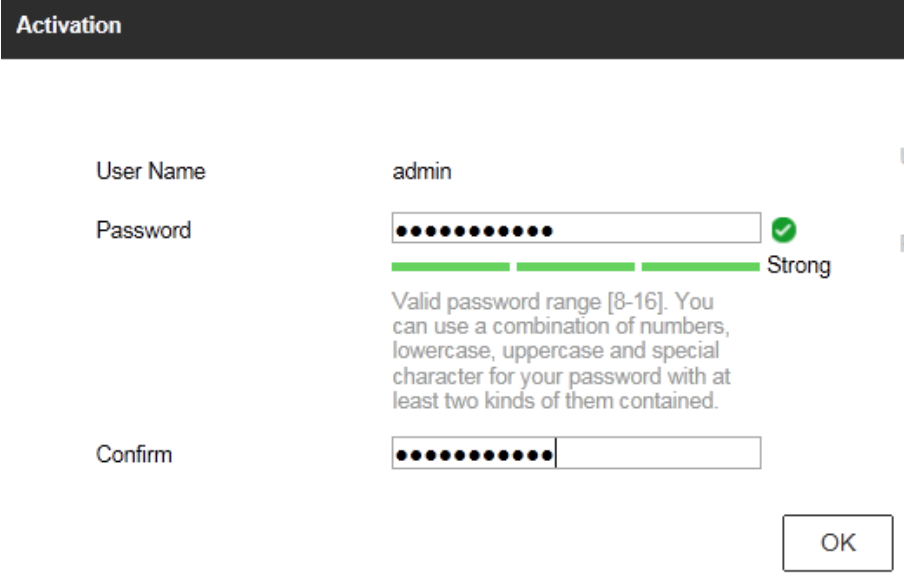


Рисунок 3.9 – Ввод данных для администрирования при первом использовании

Перед использованием устройства в сети необходимо правильно настроить TCP/IP. Доступны как IPv4, так и IPv6. Для этого необходимо зайти в пункт «System → Network → TCP/IP» (см. рис. 3.10).

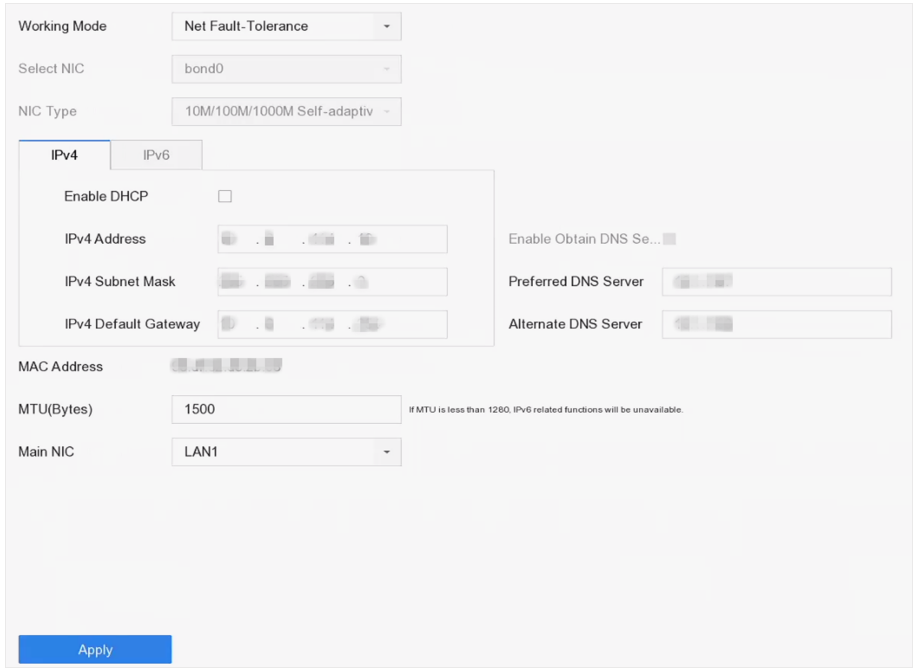


Рисунок 3.10 – Настройка TCP/IP

В пункте «Working Mode» можно выбрать один из режимов работы сетевого адаптера «Net-Fault Tolerance» или «Multi-Address Mode». Режим «Net-Fault Tolerance» (Сетевая отказоустойчивость).

Две сетевые карты используют один и тот же IP-адрес, можно выбрать основную сетевую карту для LAN1 или LAN2. Таким образом, в случае сбоя одной сетевой карты устройство автоматически включит другую резервную сетевую карту, чтобы обеспечить нормальную работу системы.

Режим «Multi-Address Mode» (Многоадресный режим).

Параметры двух сетевых карт можно настроить независимо. Можно выбрать LAN1 или LAN2 в разделе «Select NIC» для настройки параметров. Выберите одну сетевую карту в качестве маршрута по умолчанию. Когда система подключается к экстрасети, данные будут пересылаться по маршруту по умолчанию.

Далее нужно настроить параметры IPv4. В поле IPv4 Address ввести адрес 201.68.7.35, в поле IPv4 Subnet Mask ввести маску 255.255.255.240, в поле IPv4 Default Gateway ввести адрес 201.68.7.33. Нажать «Apply».

Также необходимо добавить камеры через подключение PoE.

Интерфейсы PoE позволяют видеорегистратору безопасно передавать электроэнергию вместе с данными по кабелю Ethernet на подключенные камеры PoE. Устройства поддерживает до восьми камер PoE. Если отключить интерфейс PoE, также возможно подключиться к сетевым онлайн-камерам. Интерфейс PoE поддерживает функцию Plug-and-Play.

Теперь нужно подключить камеры к портам видеорегистратора и настроить их.

Перед использованием каждую камеру необходимо активировать и настроить её IP адрес. Для этого требуется выполнить следующие шаги:

1. Установить на компьютер программу ConfigTool для конфигурации камер Dahua с сайта производителя;

2. Изменить IP-адрес ПК на ту же подсеть, что и устройство, например – 192.168.1.20.

IP-адрес устройства по умолчанию – 192.168.1.108;

3. Запустить программу ConfigTool. Её интерфейс показа на рисунке 3.12;

4. Поставить флаг в поле в левой части строки, описывающей камеру, которую мы хотим активировать. Нажать кнопку Initialize, после чего появится меню, показанное на рисунке 3.13. Ввести и подтвердить пароль, нажать Next. После этого начнётся инициализация камеры, и по её завершении появится окно с соообщением о её завершении. В появившемся окне нажать кнопку Finish, чтобы выйти из меню инициализации;

5. В меню, показанном на рисунке 3.12 поставить флаг в строке, соответствующей настраиваемой камере, нажать кнопку Modify;

6. Появится меню, показанное на рисунке 3.14. Ввести камерам адреса от 201.68.7.36 до 201.68.7.36 и маску 255.255.255.240. В поле Gateway указать адрес 201.68.7.33

4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ

В проектируемой локальной компьютерной сети кабельная система реализована с помощью прокладки витой пары за подвесным потолком. От потолка к информационным розеткам кабель протягивается по стенам, в кабельном коробе. Информационные розетки расположены у пола, в близости от конечных устройств. Между этажами кабели проходят по кабельным шахтам. Кабели системы видеонаблюдения проложены по зданию аналогичным образом.

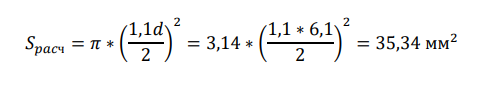
Центральный маршрутизатор, коммутатор и сервер находятся в служебном помещении. Коммутатор и маршрутизатор расположены в телекоммуникационном шкафу, сервер и сетевой видеорегистратор стоят на столе. Точки беспроводного доступа вынесена в коридор и закреплены на потолке, для обеспечения лучшей связи в помещении. Коммутаторы, расположенные на нулевом и втором этажах, помещены в подвесные телекоммуникационные шкафы для того, чтобы обезопасить их от физического воздействия.

В плане здания можно увидеть месторасположение информационных розеток и сетевого оборудования, прокладку кабелей.

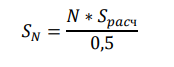
С планами этажей можно ознакомиться в приложениях Г, Д, Е.

**4.1 Обоснование выбора кабельного короба**

Для монтажа кабелей используются кабельные коробы. Перед их выбором, необходимо рассчитать площадь сечения короба. Номинальный диаметр кабеля UTP cat. 5e равен 6,1 мм. При расчёте учтём увеличение диаметра на 10%. Используем следующую формулу:

****

Обычно рассчитывается, что кабели занимают 50% площади поперечного сечения короба. С учётом этого рассчитаем необходимую площадь сечения короба:



Где *SN –* расчётная площадь поперечного сечения короба для N кабелей.

В коробе может находиться от 1 до 8 проводов.

Рассчитав площади по формуле, получим, что для укладки от 1 до 5 проводов требуется короб размерами 25х16, для укладки от 6 до 8 проводов требуется короб размерами 25х25.

Для удобства монтажа, будет использоваться только короб 25х25.

При изучении предлагаемых на рынке кабельных коробов был выбран Кабель-канал 25х25 «ЭЛЕКОР» k38325.

**4.2 Обоснование выбора информационных розеток**

Для подключения устройств к сети необходимо обеспечить доступность устройств к кабелю. Удобно и эстетично организовать доступ позволяет монтаж информационных розеток RJ-45. Хорошим вариантом информационных розеток являются французские SCHNEIDER ELECTRIC AtlasDesign, обеспечивающие доступ к сети.

**4.3 Размещение и монтаж оборудования**

На нулевом этаже устанавливается навесной телекоммуникационный шкаф F1 с коммутатором SW0.

На первом этаже в служебном помещении устанавливается телекоммуникационный шкаф X1 со следующим оборудованием: коммутатор SW1, маршрутизатор R1, модем M1.

В проектируемой ЛКС кабельная система реализована посредством прокладки витой пары в кабельном коробе под фальшпотолком. В помещениях отсутствуют сильные электромагнитные помехи, поэтому можно использовать кабель вида UTP. Исходя из выбранного сетевого оборудования, будет достаточно использовать кабель UTP cat. 5e.

Для подключения оконечного оборудования используются накладные розетки UTP cat. 5e. Информационные розетки устанавливаются на расстоянии 30 см от пола, рядом с местами, где должны находиться оконечные устройства.

Точки доступа закрепляются на потолке посредством монтажного комплекта, прилагающегося к ним. Они подключаются к коммутатору с помощью технологии PoE.

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы была разработана локальная компьютерная сеть для организации, занимающейся торговлей овощами и фруктами. Также были получены практические и теоретические знания, и навыки проектирования локальной вычислительной сети.

Был исследован рынок сетевого оборудования, стандарты и требования к создаваемой системе.

Результатами проектирования являются структурная, функциональная схемы, план этажей здания организации, перечень оборудования и материалов, необходимых для построения и реализации сети. Сюда вошли маршрутизатор, коммутаторы, рабочие станции, принтеры, серверы и пассивное сетевое оборудование. Оборудование, выбранное в данной работе, удовлетворяет всем стандартам качества, надежности.

Использование блоков бесперебойного питания позволило защитить оборудование и пользовательские станции от сильных перепадов напряжения.

Полученная компьютерная сеть будет проста в обслуживании, а также при необходимости ее можно будет масштабировать.

список использованных источников

[1] Сайт производителя сетевого оборудования Allied Telesis [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.alliedtelesis.com/us/en> – Дата доступа: 27.09.2022

[2] Олифер, В. Компьютерные сети. Принципы, технологии, протоколы / В. Олифер, Н. Олифер – Спб: Питер, 2019. – 992 с.

[3] Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – 5-е издание – Санкт-Петербург [и другие]: Питер, Питер Пресс, 2017. – 955 с.

[4] Спецификация маршрутизатора AR2050V [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.alliedtelesis.com/by/en/products/security-appliances/secure-vpn-routers/ar2050v#description-tab> – Дата доступа: 13.10.2022

[5] Спецификация точки беспроводного доступа TQ5403 [Электронный ресурс] – Электронные данные. – Режим доступа: [https://www.alliedtelesis.com/sites/default/files/documents/datasheets/ati-tq5403-ds.pdf](https://www.alliedtelesis.com/sites/default/files/documents/datasheets/ati-tq5403-ds.pdf%20) – Дата доступа: 13.10.2022

[6] Указания по монтажу точки беспроводного доступа TQ5403 [Электронный ресурс] – Электронные данные. – Режим доступа: [https://www.alliedtelesis.com/sites/default/files/documents/installation-guides/ati-tq5403series-ig.pdf](https://www.alliedtelesis.com/sites/default/files/documents/installation-guides/ati-tq5403series-ig.pdf%20) – Дата доступа: 13.10.2022

[7] Информация о подключении камер видеонаблюдения к локальной сети [Электронный ресурс] – Электронные данные. – Режим доступа: [https://www.versitron.com/blog/how-to-configure-nvr-for-ip-camera-on-a-](https://www.versitron.com/blog/how-to-configure-nvr-for-ip-camera-on-a-network)network – Дата доступа: 13.10.2022

[8] Список популярных прокси-серверов для Linux [Электронный ресурс] – Электронные данные. – Режим доступа: [https://losst.pro/luchshie-proksi-servery-](https://losst.pro/luchshie-proksi-servery-linux)linux – Дата доступа: 13.10.2022

[9] Информация о прокси-сервере Squid [Электронный ресурс] – Электронные данные. – Режим доступа: <http://www.squid-cache.org/> – Дата доступа: 13.10.2022

[10] Информация о прокси-сервере Privoxy [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.privoxy.org/> – Дата доступа: 13.10.2022

[11] Информация о прокси-сервере Tinyproxy [Электронный ресурс] – Электронные данные. – Режим доступа: <http://tinyproxy.github.io/> – Дата доступа: 13.10.2022

[12] Различия между DVR и NVR видеорегистраторами [Электронный ресурс] – Электронные данные. – Режим доступа: [https://info.verkada.com/compare/dvr-vs-nvr/#:~:text=A%20DVR%20converts%20analog%20footage,for%20storage%20and%20remote%20viewing.](https://info.verkada.com/compare/dvr-vs-nvr/%23:~:text=A%20DVR%20converts%20analog%20footage,for%20storage%20and%20remote%20viewing.) – Дата доступа: 13.10.2022

[13] Информация о подключении DVR видеорегистраторов к локальной сети [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.cctvcore.com/connect-dvr-lan-basic-network-connection.aspx>– Дата доступа: 13.10.2022

[14] Пользовательское руководство для системы видеонаблюдения Swann SWDVK-845808V [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.manua.ls/swann/swdvk-845808v/manual>– Дата доступа: 04.12.2022

[15] Документация по использованию веб-интерфейса коммутатора AT-GS950/16 [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/gs950_16webs114v110a.pdf>– Дата доступа: 04.12.2022