

Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

Дисциплина: Аппаратное обеспечение компьютерных сетей

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к курсовому проекту
на тему
ЛОКАЛЬНАЯ КОМПЬЮТЕРНАЯ СЕТЬ,
ВАРИАНТ 17

БГУИР КП 1–40 02 01 01 017 ПЗ

Студент:

М.А. Михайловский

Руководитель:

И.И. Глецевич

МИНСК 2023

Вариант	17
Объект	организация, занимающаяся торговлей овощами и фруктами
Форма здания, этажи, суммарная площадь помещений в квадратных метрах	прямоугольная (с соотношением сторон 1:2), 0-2, 430
Количество стационарных пользователей (ПК), количество стационарных подключений, количество мобильных подключений	10, 10, 5
Сервисы (дополнительные подключения)	web-сервер для внутреннего и внешнего использования
Прочее оконечное оборудование (дополнительные подключения)	принтеры, видеонаблюдение
Подключение к Internet	условный заказчик не уверен
Внешняя адресация IPv4, внутренняя адресация IPv4, адресация IPv6	внешний IPv4-адрес автоматически назначает провайдер, публичная подсеть, взаимодействие в рамках внутренней сети - использовать одну из подходящих подсетей из своего варианта лабораторных работ (если возможно), взаимодействие в рамках внутренней сети
Безопасность	прокси
Надежность	защита от сильных перепадов напряжения
Финансы	бюджетная сеть
Производитель сетевого оборудования	Allied Telesis
Дополнительные требования заказчика	нет

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
1 ОБЗОР ЛИТЕРАТУРЫ	5
1.1 Allied Telesis.....	5
1.2 Видеонаблюдение	6
2 РАЗРАБОТКА СТРУКТУРНОЙ СХЕМЫ	8
3 РАЗРАБОТКА ФУНКЦИОНАЛЬНОЙ СХЕМЫ	9
3.1 Обоснование выбора типа подключения к Internet	9
3.2 Обоснование выбора оборудования для защиты от сильных перепадов напряжения	9
3.3 Обоснование выбора пользовательской операционной системы	10
3.4 Обоснование выбора операционной системы web-сервера.....	11
3.5 Обоснование выбора пользовательских станций	11
3.6 Обоснование выбора web-сервера.....	12
3.7 Обоснование выбора чёрно-белого принтера A4	13
3.8 Обоснование выбора компонентов системы видеонаблюдения	13
3.9 Обоснование выбора кабельного модема.....	14
3.10 Обоснование выбора маршрутизатора.....	14
3.11 Обоснование выбора коммутатора.....	14
3.12 Обоснование выбора точки доступа	15
3.13 Расчёт качества связи беспроводной сети	16
3.14 Обоснование выбора телекоммуникационных шкафов.....	18
3.15 Схема адресации.....	18
3.16 Настройка маршрутизатора.....	19
3.17 Настройка коммутаторов.....	21
3.18 Настройка ПК	23
3.19 Настройка web-сервера.....	24
3.20 Настройка точек беспроводного доступа	25
3.21 Настройка видеорегистратора и камер	26
3.22 Настройка принтеров.....	27
4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ	28
4.1 Обоснование выбора кабельного короба.....	28
4.2 Обоснование выбора информационных розеток	29
4.3 Размещение и монтаж оборудования	29
ЗАКЛЮЧЕНИЕ	30
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	31
ПРИЛОЖЕНИЕ А	33
ПРИЛОЖЕНИЕ Б.....	34
ПРИЛОЖЕНИЕ В	35
ПРИЛОЖЕНИЕ Г.....	36
ПРИЛОЖЕНИЕ Д	37

ВВЕДЕНИЕ

Локальные компьютерные сети (ЛКС) являются неотъемлемой частью современной организации, обеспечивая эффективное взаимодействие между стационарными пользователями и обеспечивая доступ к информационным ресурсам. В рамках данного курсового проекта рассматривается задача проектирования ЛКС для организации, специализирующейся на торговле овощами и фруктами.

Организация расположена в прямоугольном здании, на трех этажах, включая подвал. Каждый этаж имеет суммарную площадь 430 квадратных метров. Необходимо обеспечить 10 стационарных пользователей, 10 стационарных подключений и 5 мобильных подключений на все здание. Кроме того, необходимо разместить дополнительное оконечное оборудование, такое как принтеры и системы видеонаблюдения.

Важным аспектом проектирования является подключение к сети интернет, где условный заказчик выражает неопределенность относительно выбора провайдера. Внешняя адресация IPv4 предполагается автоматически назначаемой провайдером, в то время как внутренняя адресация IPv4 будет использовать публичную подсеть. IPv6 будет применяться для внутренних коммуникаций в рамках собственной сети.

Основными требованиями заказчика являются надежность сети с защитой от сильных перепадов напряжения и ориентация на бюджетную составляющую. Для реализации проекта будет использовано сетевое оборудование от компании Allied Telesis, обеспечивающее высокую степень надежности и производительности.

Цель проекта: разработка локальной компьютерной сети для организации, занимающейся торговлей овощами и фруктами.

Задачи проекта:

1. Изучение материала по заданию на проект до начала выполнения проекта, как и дальнейшее изучение технологий по ходу выполнения проекта;
2. Разработка общей структуры сети, структурной схемы;
3. Выбор конкретных устройств, обоснование их выбора, описание настройки устройств, составление функциональной схемы;
4. Разработка структурированной кабельной системы, составление её схемы.

1 ОБЗОР ЛИТЕРАТУРЫ

1.1 Allied Telesis

Allied Telesis - это мировой поставщик сетевых решений, который предлагает широкий спектр продуктов и технологий для построения современных сетей.

Allied Telesis предлагает широкий спектр сетевых коммутаторов, включая устройства для малых, средних и крупных предприятий.

Коммутаторы Allied Telesis поддерживают разные скорости (от Fast Ethernet до 10 Gigabit Ethernet и более) и различные форм-факторы. Они предоставляют возможности управления сетью, включая виртуализацию, балансировку нагрузки и многое другое. Например, Allied Telesis AT-X510-28GPX предназначен для предприятий и имеет 28 портов, включая порты Gigabit Ethernet и 10 Gigabit Ethernet. Он обладает высокой производительностью и поддерживает функции управления сетью и безопасности.

Компания предлагает маршрутизаторы для организаций и провайдеров услуг. Эти маршрутизаторы обеспечивают высокую производительность и надежность, поддерживая разные технологии маршрутизации и виртуальных сетей. Например, Allied Telesis AT-AR2010V предоставляет маршрутизацию и управление сетью для организаций. Он может поддерживать множество интерфейсов, включая Ethernet и WAN-интерфейсы, и обеспечивает безопасную связь.

Allied Telesis предоставляет решения для беспроводных сетей, включая беспроводные точки доступа и контроллеры. Эти решения позволяют создавать масштабируемые и безопасные беспроводные инфраструктуры. Например, Allied Telesis AT-TQ2450.

Компания предлагает средства для обеспечения безопасности сетей, включая межсетевые экраны, системы обнаружения вторжений и антивирусные решения.

Allied Telesis предоставляет инструменты и программное обеспечение для управления сетью, мониторинга и диагностики сетевой инфраструктуры.

Компания предлагает продукты, способствующие оптимизации трафика и улучшению производительности сети.

Allied Telesis разрабатывает системы видеонаблюдения, которые позволяют организациям обеспечивать безопасность и мониторинг важных объектов. Например, Allied Telesis AR425S предоставляет возможность мониторинга и записи видеопотока с помощью сетевых камер. Она поддерживает разные методы хранения данных и обеспечивает безопасность объектов наблюдения.

Компания активно работает над инновациями, такими как Software-Defined Networking (SDN), Internet of Things (IoT) и другими, чтобы помочь организациям адаптироваться к современным требованиям сетевых

технологий.

Продукты Allied Telesis предназначены для широкого спектра рынков, включая корпоративные сети, образование, здравоохранение, государственные учреждения и другие, и они ориентированы на обеспечение надежной, безопасной и эффективной работы сетей.

1.2 Видеонаблюдение

В соответствии с заданием требуется установить систему видеонаблюдения в здании организации. Перед началом проектирования этой системы необходимо ознакомиться с основными задачами, правилами построения и различными типами систем.

Основные задачи системы видеонаблюдения включают мониторинг, обнаружение и идентификацию. Видеокамеры передают изображение оператору в режиме реального времени, и данные должны храниться на запоминающих устройствах определенное время. Чтобы выбрать подходящую систему наблюдения, необходимо иметь план территории или помещения, знать их размеры и архитектурные особенности, такие как наличие колонн, выступов и ниш. Затем определяются места размещения камер, их количество и технические характеристики.

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

Принцип аналогового видеонаблюдения состоит в следующем: аналоговая видеокамера принимает входной видеосигнал, обрабатывает его и отправляет в аналоговом виде на видеорегистратор. Аналоговое видеонаблюдение имеет разрешение не более двух мегапикселей, что является существенным недостатком. Кроме того, для аналоговой системы требуется прямое соединение камеры с видеорегистратором, что может привести к увеличению длины кабельных линий, а также сигнал в такой системе менее защищен от помех. Главные преимущества аналоговой системы: низкая цена, простота установки и универсальность оборудования.

Цифровое видеонаблюдение использует протокол TCP/IP по сети Ethernet для передачи сигнала от видеокамеры к видеорегистратору. Оцифровка сигнала осуществляется на самой видеокамере, которая преобразует сигнал для передачи по сети Ethernet. Сетевые видеорегистраторы (NVR) предназначены для работы в IP-системах видеонаблюдения. В отличие от обычных цифровых видеорегистраторов (DVR), NVR получают видеоданные уже в сжатом виде. Одной из особенностей NVR является то, что они могут работать только с определенным списком моделей IP-видеокамер, интегрированных в программное обеспечение видеорегистратора. Некоторые устройства могут работать автономно без дополнительного оборудования, в то время как для других необходим видеорегистратор.

К преимуществам IP-систем видеонаблюдения можно отнести

следующее:

1. Возможность использования высокого разрешения видеокамер.
2. Гибкость в построении архитектуры и масштабируемости.
3. Возможность подключения удаленных видеокамер через Интернет.
4. Наличие функций видеоаналитики на видеокамерах.

К недостаткам IP-систем видеонаблюдения можно отнести следующее:

1. Более высокая стоимость оборудования по сравнению с аналоговыми системами.
2. Требуется наличие сетевой инфраструктуры для передачи данных.
3. Возможность уязвимости системы к кибератакам.

Для проектирования и установки систем видеонаблюдения на объектах общественной безопасности и местах массового скопления людей применяются определенные требования ТНПА. Эти требования накладывают определенные условия на системы IP-видеонаблюдения.

Существуют несколько вариантов интеграции IP камер системы видеонаблюдения в ЛКС предприятия. Например, камеры могут быть подключены к ЛКС как независимые устройства в сети. Это самый простой, но не самый эффективный вариант, так как управление и контроль доступа к видеопотоку затруднены. Кроме того, необходимо решить вопросы с питанием камер и организацией хранилища для сохраненных видеоданных.

Второй вариант интеграции предусматривает установку специального коммутатора в локальной сети для подключения камер, а также доступ к существующему или специально созданному файловому серверу. Это хорошее решение для систем видеонаблюдения с большим количеством камер и высокими требованиями к объему хранилища для файлов.

Третий вариант – размещение видеорегистратора в ЛКС. Это устройство объединяет функции коммутатора и специализированного файлового сервера для просмотра, записи и хранения видеопотоков от IP камер.

2 РАЗРАБОТКА СТРУКТУРНОЙ СХЕМЫ

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 прямоугольной формы с соотношением сторон 1:2 на трёх этажах: подвал, первый этаж и второй этаж. Общая площадь помещений каждого этажа составляет 430 квадратных метров.

В подвале находится складское помещение, где хранятся продаваемые овощи и фрукты, различные хозяйственные помещения, кабинет заведующего складом. В кабинете установлены две пользовательские станции и принтер. В складском помещении установлены две камеры видеонаблюдения.

На первом этаже расположены торговый зал, кабинет охраны и комната с сетевым оборудованием. В кабинете охраны установлена одна пользовательская станция. В комнате с сетевым оборудованием находятся модем, web-сервер, коммутатор, маршрутизатор, сетевой видеорегистратор. В торговом зале установлены четыре камеры видеонаблюдения и беспроводная точка доступа.

На втором этаже находятся кабинет директора организации, кабинет секретаря, бухгалтерия, кабинет отдела кадров, кабинет маркетолога, кабинет администратора сети. В кабинетах начальника организации, секретаря, администратора сети, маркетолога, отдела кадров расположено по одной пользовательской станции. В бухгалтерии находятся две пользовательские станции и принтер. В кабинете директора также есть принтер.

В подвале и на втором этаже находится по одному коммутатору, к которым подключается оконечное оборудование этих этажей.

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

3 РАЗРАБОТКА ФУНКЦИОНАЛЬНОЙ СХЕМЫ

3.1 Обоснование выбора типа подключения к Internet

Условный заказчик не уверен насчёт выбора типа подключения к интернету, поэтому придётся выбрать оптимальный способ исходя из прочих условий и требований.

Разрабатываемая сеть является бюджетной, поэтому разумно было бы выбрать наиболее дешевый и простой способ подключения. Наиболее простым и дешевым способом подключения среди тех, что были представлены в задании других вариантов, является ADSL2+ через витую пару.

ADSL2+ использует уже существующую инфраструктуру телефонной сети и витую пару для передачи данных. В большинстве случаев провайдеры могут предоставить ADSL-подключение по низкой стоимости, поскольку они уже имеют инфраструктуру и линии для телефонной связи. Однако, скорость и доступность ADSL2+ могут существенно различаться в зависимости от расстояния до центральной станции провайдера.

Тем не менее ADSL2+ имеет крайне низкую скорость передачи данных. В то же время DOCSIS может иметь примерно сопоставимую стоимость услуг, при этом предоставляя куда более высокие показатели скорости передачи данных и надёжности, поэтому был выбран именно этот вариант подключения к интернету.

3.2 Обоснование выбора оборудования для защиты от сильных перепадов напряжения

Для защиты оборудования от значительных изменений в напряжении можно использовать различные устройства, такие как реле контроля напряжения, стабилизаторы напряжения и источники бесперебойного питания (ИБП). В среднем, реле является более доступным по цене вариантом по сравнению со стабилизаторами и ИБП, однако оно отключает приборы от сети при превышении установленного порогового значения напряжения. Такое решение не подходит для нашей организации, так как частые отключения рабочих станций и сетевого оборудования приведут к снижению производительности сотрудников. Более предпочтительным вариантом является использование стабилизатора напряжения, который обеспечивает стабильное напряжение в сети и предотвращает отключение приборов при изменениях напряжения. ИБП также обеспечивает стабилизацию напряжения, не отключая приборы от сети, и обеспечивает им некоторое время автономной работы в случае отключения электропитания. Это особенно полезно, так как сотрудники имеют время для сохранения данных, из-за потери которых может возникнуть ущерб для организации. Общая потребляемая мощность пользовательских станций и мониторов не

превышает 400 Вт. С учетом этого, минимально допустимая мощность для ИБП должна быть не менее 600 Вт. В таблице 3.1 приведены характеристики ИБП, которые соответствуют указанным требованиям.

Таблица 3.1 – Сравнение источников бесперебойного питания

Характеристики	Powerman Smart Sine 1000	Powercom Raptor RPT-1000AP 1000VA	Kiper Power A1500 USB (1500VA/900W)
Мощность, Вт	700	600	900
Полная мощность, ВА	1000	1000	1500
Время зарядки, ч	8	4	4
Цена	682 BYN	256 BYN	407 BYN

Из таблицы 3.1 видно, что источник питания Powercom Raptor RPT-1000AP 1000VA соответствует указанным требованиям, при этом является наиболее дешевым среди отобранных вариантов. Поэтому для бюджетной сети он является наилучшим выбором.

3.3 Обоснование выбора пользовательской операционной системы

На сегодняшний день самыми популярными операционными системами являются Windows, MacOS и Linux.

MacOS предназначена только для устройств Apple, которые отличаются высокой стоимостью. Учитывая, что наша сеть ориентирована на бюджетные решения, а производительность устройств Apple излишне для офисных задач, использование MacOS нецелесообразно и следует от него отказаться.

Большинство дистрибутивов Linux распространяются бесплатно и совместимы с большинством процессоров Intel, выпущенных за последние 30 лет. Учитывая, что персональные компьютеры будут использоваться для работы с офисным программным обеспечением, мы рассматриваем только операционные системы с графическим интерфейсом. Среди популярных дистрибутивов Linux с графической оболочкой наиболее часто используются Ubuntu, Fedora и Mint. Они подходят для офисных работников, но стоит помнить, что наиболее распространенной операционной системой, которую обычные пользователи используют дома и в офисах, является Windows.

Сотрудники организации могут столкнуться с трудностями при знакомстве с незнакомой операционной системой, что отразится на их производительности. Поэтому наиболее разумным решением будет использовать операционную систему Windows 10. Таким образом, сотрудники смогут использовать программное обеспечение Microsoft Office,

предоставляющее большую часть необходимого функционала для их работы.

3.4 Обоснование выбора операционной системы web-сервера

Серверы чаще всего работают на операционной системе Linux, которая потребляет меньше аппаратных ресурсов по сравнению с современными версиями Windows и предоставляет широкие возможности опытным пользователям.

Было принято решение использовать дистрибутив Debian, который отличается стабильностью, регулярными обновлениями и поддерживается большим сообществом пользователей.

В качестве веб-сервера был выбран Apache, который является популярным и проверенным решением, а также обладает обширной документацией.

3.5 Обоснование выбора пользовательских станций

Так как рассматриваемая организация, занимается торговлей овощами и фруктами, сотрудники организации не нуждаются в требовательном программном обеспечении. Соответственно они не нуждаются в высокопроизводительном процессоре, видеокарте и большом объеме оперативной памяти. Таким образом можно выделить следующие требования для пользовательских станций:

1. Двухъядерный процессор Intel Pentium G6400 является оптимальным выбором для офисного компьютера в бюджетном ценовом сегменте. Характеристики процессора хватает для комфортной 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 PG6400D8HD05VGALW50	JET OFFICE PG6400D8HD1VGALW50
Процессор	Intel Pentium G6400	Intel Pentium G6400
Оперативная память	DDR4 8 Гб	DDR4 8 Гб
Конфигурация накопителя	HDD 500 Гб	HDD 1000 Гб
Видеокарта	Intel UHD Graphics 610	Intel UHD Graphics 610
Цена	779 BYN	836 BYN

Как видно из таблицы 3.2, станции различаются только объемом накопителя. Станция JET OFFICE PG6400D8HD05VGALW50 дешевле, но объем накопителя у нее в 2 раза меньше, что может вызвать трудности с недостатком свободного места. Кроме того цена различается не столь значительно, поэтому была выбрана станция JET Office PG6400D8HD1VGALW50.

3.6 Обоснование выбора web-сервера

При выборе web-сервера важно обратить внимание на несколько ключевых аспектов.

Производительность является одним из важных факторов. Необходимо оценить способность web-сервера обрабатывать одновременные запросы и выдерживать нагрузку.

Надежность и стабильность работы – ещё один важный аспект. Желательно выбрать web-сервер, который обладает высокой степенью надежности и способен работать стабильно, чтобы минимизировать возможные периоды простоя или сбои в работе вашего веб-сайта или приложения.

Безопасность – ещё один важный аспект, который следует учесть при выборе web-сервера.

Для сравнения были выбраны три сервера. Их характеристики описаны в таблице 3.3.

Таблица 3.3 – Сравнение серверов

Характеристики	Dell PowerEdge R450	Lenovo ThinkSystem SR630 V2	ASUS RS520-E9-RS8 V2 S2
Стандартный объем памяти	128GB (8x16GB)	64GB (2x32GB)	96GB
Тип памяти	DDR4-3200 Registered	DDR4-3200 Registered	DDR4-2933 Registered
Установленные SSD и HDD	SSD 2 x 480GB SATA	SSD - 4x960GB SATA	2x1.92TB SSD + 2x1.2TB SAS 10K HDD
Процессор	Intel Xeon Silver 4309Y 2.8Ghz	Intel Xeon Silver 4314	Intel Xeon 6226R
Порты LAN	2 x GbE	2 x GbE	2 x GbE
Цена	1096 BYN	1086 BYN	1128 BYN

Сервер Lenovo ThinkSystem SR630 V2 является самым дешевым, поэтому был выбран именно он.

3.7 Обоснование выбора чёрно-белого принтера А4

Для удовлетворения потребностей сотрудников в печати рабочих документов, важно обеспечить быструю и качественную печать. В связи с этим, следует выбирать лазерные принтеры, так как они обладают более высокой скоростью печати по сравнению со струйными принтерами и обеспечивают отличное качество печати текстовых документов. Для сравнительного анализа были рассмотрены 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	368 BYN	785 BYN	340 BYN

Из таблицы 3.4 видно, что принтер Pantum P2507 является наиболее дешевым, при этом имеет вполне достаточную скорость печати, поэтому именно он и был выбран.

3.8 Обоснование выбора компонентов системы видеонаблюдения

Для полного охвата важных зон в здании, необходимо установить 6 камер в систему видеонаблюдения.

При анализе доступных видеорегистраторов было выяснено, что подходящей моделью для бюджетного решения является HIKVISION Standart DS-7608NI-K2. Этот видеорегистратор позволяет подключить 6 камер через использование витой пары. Сравнить его с другими моделями, поддерживающими такое же количество камер, не имеет смысла, поскольку эти модели находятся в высоком ценовом сегменте и не обладают заметными преимуществами.

Для сравнения были выбраны камеры, представленные в таблице 3.5.

Таблица 3.5 – Сравнение камер

Характеристики	IP-камера Dahua DH-IPC-HDW3841EMP-AS-0280B	Dahua DH-IPC-HFW2831SP-S-0360B-S2
Разрешение	8 МП	8МП
Корпус	купольная	уличная
Подсветка	ИК	ИК
Цена	785 BYN	500 BYN

Представленные камеры имеют схожие характеристики, и хотя

купольный корпус вероятно был бы предпочтительнее, так как направление объектива для злоумышленника было бы не столь очевидно, модель Dahua DH-IPC-HFW2831SP-S-0360B-S2 значительно дешевле, потому выбрана именно она.

3.9 Обоснование выбора кабельного модема

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	112 BYN	148 BYN

Как видно из таблицы 3.6, модем D-Link DCM-301 является более дешевым, поэтому был выбран именно он.

3.10 Обоснование выбора маршрутизатора

На рынке Беларуси среди маршрутизаторов Allied Telesis доступно для покупки всего две модели: AR2050V и AR4050S. Однако, стоит отметить, что рассматриваемые маршрутизаторы принадлежат к разным поколениям и модель AR4050S значительно дороже, поэтому сравнение между ними нецелесообразно. Маршрутизатор AR2050V обладает характеристиками, которые полностью соответствуют требованиям для проекта сети, поэтому именно он был выбран в качестве оптимальной модели.

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.

3.11 Обоснование выбора коммутатора

Allied Telesis предоставляет коммутаторы двух уровней: второго и третьего. В связи с ограниченным бюджетом организации, было принято решение использовать коммутаторы второго уровня, которые являются более

доступными по цене в сравнении с коммутаторами третьего уровня.

Коммутаторы второго уровня могут быть управляемыми и неуправляемыми. В данном случае нам необходимы управляемые коммутаторы, которые поддерживают протоколы сетевого уровня, включая 802.1Q, поскольку планируется создание нескольких VLAN.

Учитывая количество устройств, расположенных на каждом этаже, было принято решение выбрать коммутаторы с шестнадцатью портами.

На сайте Allied Telesis были проанализированы доступные коммутаторы, и согласно указанным требованиям, наиболее подходящие модели представлены в таблице 3.7.

Таблица 3.7 – Сравнение коммутаторов

Коммутатор	AT-GS950/16PS	AT-GS916M
Цена	2047 BYN	940 BYN
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

Учитывая, что питание точки доступа осуществляется через технологию Power over Ethernet (PoE), было бы удобно использовать коммутатор модели AT-GS950/16, который поддерживает эту функциональность. Обе модели коммутаторов имеют подходящий функционал для наших потребностей.

Однако, учитывая бюджетные ограничения организации и большую разницу в цене между двумя моделями, было решено остановиться на коммутаторе AT-GS916M в качестве оптимального варианта.

3.12 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	700 BYN	2000 BYN
Частота, Гц	2, 4, 5	2, 4, 5

Продолжение таблицы 3.8

1	2	3
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 VLAN	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.

3.13 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 влияли на разрабатываемую сеть.

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

$$L = 32,44 + 20 \lg(F) + 20 \lg(D), \text{ дБ}, \quad (3.1)$$

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

Здание имеет прямоугольную форму с соотношением сторон 1:2. Для минимизации расстояния для всех возможных пользователей, точка размещается в центре этажа, на потолке.

Высоту потолка примем равной 2,5 м, расстояние до стен – 14 м и 7 м.

Рассчитаем расстояние до нижнего угла помещения:

$$D = \sqrt{l^2 + w^2 + h^2} = \sqrt{2,5^2 + 14^2 + 7^2} = 15,85 \text{ м}, \quad (3.2)$$

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

Рассчитаем затухание радиоволн $L_{2,4}$ для частоты 2,4 ГГц L_5 для частоты 5 ГГц по формуле (3.1):

$$L_{2,4 \text{ макс}} = 32,44 + 20 \lg(2,4) + 20 \lg(15,85) = 64,05 \text{ дБ}; \quad (3.3)$$

$$L_{5 \text{ макс}} = 32,44 + 20 \lg(5) + 20 \lg(15,85) = 70,42 \text{ дБ.}; \quad (3.4)$$

Необходимо учесть затухание сигнала при прохождении конструктивных элементов здания. Внутренние стены состоят из кирпича, максимальное количество препятствующих стен равно двум. Таким образом, затухание радиоволн при прохождении через стены: $L_{2,4 \text{ макс. ст.}} = 2 * 4,44 = 8,88 \text{ дБ}$. $L_{5 \text{ макс. ст.}} = 2 * 14,62 = 29,24 \text{ дБ}$.

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 S_1 (2,4 ГГц), S_2 (5 ГГц) в самой удаленной точке помещения исходя из мощности передатчика $P_{2,4}$ (2,4 ГГц), P_5 (5 ГГц) будет равна:

$$S_1 = P_{2,4} + U_{2,4} - L_{2,4 \text{ макс}} - L_{2,4 \text{ макс ст.}} = 19,78 \text{ дБм} + 1,9 \text{ дБи} - 64,05 \text{ дБ} - 8,88 \text{ дБ} = -52,25 \text{ дБм.}; \quad (3.5)$$

$$S_2 = P_5 + U_5 - L_{5 \text{ макс}} - L_{5 \text{ макс ст.}} = 27,31 \text{ дБм} + 3,7 \text{ дБи} - 70,42 \text{ дБ} - 29,24 \text{ дБ} = -68,65 \text{ дБм.} \quad (3.6)$$

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 -52 дБм до -69 дБм, что обеспечивает достаточный уровень сигнала даже в самых удаленных точках.

3.14 Обоснование выбора телекоммуникационных шкафов

Из-за отсутствия отдельной комнаты для коммутаторов на нулевом и втором этажах, для обеспечения безопасности было принято решение разместить сетевое оборудование в телекоммуникационных шкафах. Также, для обеспечения дополнительной защиты от физического воздействия и для удобства размещения, коммутатор, модем и маршрутизатор, находящиеся в отдельной комнате на первом этаже, также были установлены в телекоммуникационный шкаф. В таблице 3.9 приведены соответствующие шкафы, выбранные для сравнения.

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	355 BYN	451 BYN	336 BYN

Эти модели шкафов отличаются своими размерами и стоимостью. Кроме того, шкаф ЦМО ШРН-Э-9.500.1 предоставляет опцию установки вентиляторов в основание или крышу. Учитывая более низкую цену, большее внутреннее пространство и хорошую вентиляцию, было решено выбрать эту модель.

3.15 Схема адресации

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 199.182.111.0/25 разбита с учетом количества устройств,

приходящихся на каждый vlan. Адреса подсетей представлены в таблице 3.10

Для стационарных устройств (8 ПК и 7 принтеров) выбрана подсеть IPv4 199.182.111.0/27, и подсеть 2001:0DB8:1234::/48 для IPv6.

В беспроводной сети 5 мобильных устройств. Для нее выделена подсеть 199.182.111.32/28.

Для системы видеонаблюдения выделена подсеть 199.182.111.48/28, 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 199.182.111.64/29.

Для Web-сервера взята подсеть 199.182.111.72/29.

Таблица 3.10 – Схема адресации сетей

Назначение	VLAN	Адрес подсети	Маска подсети/ Префикс
Стационарные подключения	10	199.182.111.0	255.255.255.224
		fd00:65cf:34ad:10::	/64
Беспроводная	20	199.182.111.32	255.255.255.240
Видеонаблюдения	30	199.182.111.48	255.255.255.240
Административная	40	199.182.111.64	255.255.255.248
Сервер	50	199.182.111.72	255.255.255.248

3.16 Настройка маршрутизатора

3.16.1 Настройка VLAN

```
Awplus>enable
Awplus#conf terminal
Awplus(config)#hostname Router
Router (config)#set user admin password ab3542zp79s
```

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 199.182.111.1/27
Router (config-subif)#ipv6 address fd00:65cf:34ad:10::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 199.182.111.33/28
Router (config-subif)#exit
```

```
Router (config-if)#interface gi 0/2.3
Router (config-subif)#encapsulation dot1q 30
Router (config-subif)#ip address 199.182.111.49/28
```

```

Router (config-subif)#exit

Router (config-if)#interface gi 0/2.4
Router (config-subif)#encapsulation dot1q 40
Router (config-subif)#ip address 199.182.111.65/29
Router (config-subif)#exit

Router (config-if)#interface gi 0/2.5
Router (config-subif)#encapsulation dot1q 50
Router (config-subif)#ip address 199.182.111.73/29
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	199.182.111.1	255.255.255.224
	fd00:65cf:34ad:10::1	/64
Беспроводная	199.182.111.33	255.255.255.240
Видеонаблюдения	199.182.111.49	255.255.255.240
Административная	199.182.111.65	255.255.255.248
Сервер	199.182.111.73	255.255.255.248

3.16.2 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 199.182.111.32/28
Router(dhcp-if)#default-router 199.182.111.33

```

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

```

3.16.3 Настройка прокси

В качестве прокси был выбран 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 46.246.29.69
```

3.17 Настройка коммутаторов

Выдадим адреса устройствам административной подсети в соответствии с таблицей 3.12.

Таблица 3.12 – Адреса устройств для административной подсети.

Устройство	IP адрес	Маска подсети
Router	199.182.111.66	255.255.255.248
Switch0	199.182.111.67	255.255.255.248
Switch1	199.182.111.68	255.255.255.248
Switch2	199.182.111.69	255.255.255.248
Admin-PC	199.182.111.70	255.255.255.248

3.17.1 Настройка коммутатора подвала

```
Awplus>enable
Awplus#conf terminal
Awplus(config)#hostname Switch0
Switch0(config)#set user admin password ab3542zp79s
```

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 administration
Switch0(config-vlan)#exit
Switch0 (config)#interface vlan 40
Switch0 (config-if)#ip address 199.182.111.67/29
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
```

3.17.2 Настройка коммутатора первого этажа

```
Awplus>enable
Awplus#conf terminal
Awplus(config)#hostname Switch1
Switch1(config)#set user admin password ab3542zp79s
```

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 video state enable
Switch1(config-vlan)#vlan 40 name administration 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 199.182.111.68/29
```

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
Switch1(config)#interface range gi0/6-7
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#switchport trunk allowed vlan add 10,20,40,50
```

3.17.3 Настройка коммутатора второго этажа

```
Awplus>enable
Awplus#conf terminal
Awplus(config)#hostname Switch2
Switch2(config)#set user admin password ab3542zp79s
```

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 administration 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 199.182.111.69/29
```

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 gi0/2-7
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 10
Switch2(config)#interface gi0/8
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
```

3.18 Настройка ПК

Для ПК требуется настроить статическую IPv4 и IPv6 маршрутизацию. Адреса ПК представлены в таблице 3.13.

Таблица 3.13 – Адреса ПК.

Устройство	IP адрес	Маска подсети
Storage-PC1	199.182.111.2	255.255.255.224
	fd00:65cf:34ad:10::2	/64

Продолжение таблицы 3.13

1	2	3
Storage-PC2	199.182.111.3	255.255.255.224
	fd00:65cf:34ad:10::3	/64
Sec-PC	199.182.111.51	255.255.255.240
User-PC1	199.182.111.4	255.255.255.224
	fd00:65cf:34ad:10::4	/64
User-PC2	199.182.111.5	255.255.255.224
	fd00:65cf:34ad:10::5	/64
User-PC3	199.182.111.6	255.255.255.224
	fd00:65cf:34ad:10::6	/64
User-PC4	199.182.111.7	255.255.255.224
	fd00:65cf:34ad:10::7	/64
User-PC5	199.182.111.8	255.255.255.224
	fd00:65cf:34ad:10::8	/64
User-PC6	199.182.111.9	255.255.255.224
	fd00:65cf:34ad:10::9	/64
Admin-PC	199.182.111.70	255.255.255.248

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

1. Зайти в свойства Ethernet.
2. Выбрать IP версии 4 (TCP/IP), нажать кнопку «Свойства». Выбрать поле «Использовать следующий IP-адрес», заполнить поля «IP-адрес» и «Маска подсети» соответствующими адресами из таблицы 3.13.

В поле «Основной шлюз» ввести IPv4 адрес центрального маршрутизатора.

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

3.19 Настройка web-сервера

На web-сервере нужно указать адрес 199.182.111.74 и маску 255.255.255.248. В качестве шлюза указать ip адрес маршрутизатора – 199.182.111.73. Для этого в директории /etc/network нужно создать файл interfaces и написать в него следующие строки:

```
iface eth0 inet static
address 199.182.111.74
netmask 255.255.255.248
gateway 199.182.111.73
```

Для создания на сервере веб-сайта, нужно создать отдельную папку в директории /var/www. Создание папки 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 нужно перейти в директорию с конфигурационными файлами и создать новую конфигурацию:

```
$cd /etc/apache2/sites-available/  
$sudo cp 000-default.conf ovf.conf
```

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

```
ServerAdmin 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.

3.20 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, ввести имя пользователя и пароль. Для настройки точек доступа нужно перейти по вкладкам Vista Manager mini -> Wireless -> Wireless Setup -> Access Points.

Во вкладке Access Points нужно нажать кнопку Add Access Point.

В появившейся форме в поле Name нужно ввести имя точки доступа. В поле Status нажать на кнопку Enabled. В поле MAC Address нужно ввести MAC адреса соответствующих точек. В поле IP address ввести следующий адрес: 199.182.111.34. 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 нужно перейти во вкладку меню Networks, где нужно нажать кнопку Add Network.

В появившейся форме в поле SSID нужно найти название

беспроводной сети – Wireless. В поле Security нужно выбрать WPA2 и задать пароль. Остальные поля изменять не требуется. Затем нужно перейти в меню Advanced Settings. В поле VLAN ID нужно ввести 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. Наконец, нужно нажать кнопку Save для сохранения изменений.

3.21 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».

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»

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. Нужно выбрать 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 нужно ввести адрес 199.182.111.52, в поле IPv4 Subnet Mask ввести маску 255.255.255.240, в поле IPv4 Default Gateway ввести адрес 199.182.111.49. 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. Устройство 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 – 199.182.111.51.
3. Запустить программу ConfigTool.
4. Поставить флаг в поле в левой части строки, описывающей камеру, которую нужно активировать. Нажать кнопку Initialize, после чего появится новое меню. Ввести и подтвердить пароль, нажать Next. После этого начнётся инициализация камеры, и по её завершении появится окно с сообщением о ее завершении. В появившемся окне нужно нажать кнопку Finish, чтобы выйти из меню инициализации;
5. В предыдущем меню поставить флаг в строке, соответствующей настраиваемой камере, нажать кнопку Modify;
6. Появится новое меню. В нем нужно ввести камерам адреса от 199.182.111.53 до 199.182.111.58 и маску 255.255.255.240. В поле Gateway указать адрес 199.182.111.49.

3.22 Настройка принтеров

Вначале нужно подключить принтер к компьютеру, используя USB-кабель типа A-B, подключить один конец к порту USB на задней панели принтера Pantum P2507, а другой конец подключить к свободному порту USB компьютера.

Далее нужно включить принтер и установить драйверы.

Нужно перейти на официальный веб-сайт Pantum или использовать диск, поставляемый с принтером, чтобы загрузить последние версии драйверов для модели Pantum P2507.

Затем нужно запустить установочный файл драйверов и следовать инструкциям на экране, чтобы установить драйверы на компьютер.

После завершения установки драйверов принтера Pantum P2507 может потребоваться некоторое время для завершения процесса и инициализации принтера.

Следует убедиться, что принтер Pantum P2507 успешно подключен к компьютеру, путем проверки наличия нового устройства в списке установленных принтеров на вашем компьютере.

Чтобы убедиться, что принтер Pantum P2507 правильно настроен и работает, можно выполнить печать тестовой страницы. Это можно сделать, выбрав опцию "Печать тестовой страницы" в настройках принтера на компьютере или используя кнопки на самом принтере.

4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ

В проектируемой локальной компьютерной сети, система кабельной инфраструктуры будет реализована путем укладки витой пары, которая будет проходить под подвесным потолком. Кабели будут протягиваться по стенам и проходить через кабельные короба, чтобы достичь информационных розеток, расположенных у пола рядом с конечными устройствами. Кабели между этажами будут проходить по кабельным шахтам. Также, кабели системы видеонаблюдения будут проложены по зданию аналогичным способом.

Центральные сетевые устройства, включая маршрутизатор, коммутатор и сервер, будут размещены в отдельном служебном помещении. Коммутатор и маршрутизатор будут установлены в телекоммуникационном шкафу, а сервер и сетевой видеорегистратор будут размещены на столе. Точка беспроводного доступа будет закреплена на потолке для обеспечения лучшего беспроводного соединения в помещении. Коммутаторы, расположенные в подвале и на втором этаже, будут помещены в подвесные телекоммуникационные шкафы, чтобы защитить их от физических воздействий.

На плане здания отображено расположение информационных розеток, сетевого оборудования и прокладки кабелей.

С планом этажей можно ознакомиться в приложении Г.

4.1 Обоснование выбора кабельного короба

Для монтажа кабелей используются кабельные коробки. 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:

$$S_{\text{расч}} = \pi \cdot \left(\frac{1,1d}{2}\right)^2 = 3,14 \cdot \left(\frac{1,1 \cdot 6,1}{2}\right)^2 = 35,34 \text{ мм}^2, \quad (4.1)$$

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

$$S_N = \frac{N \cdot S_{\text{расч}}}{0,5}, \quad (4.2)$$

где S_N – 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 обеспечения подключения устройств к сети необходимо предоставить доступ к кабелю. Удобным и эстетичным решением для этой цели является установка информационных розеток RJ-45. В качестве хорошего варианта информационных розеток можно использовать французскую модель SCHNEIDER ELECTRIC AtlasDesign, которая обеспечивает удобный доступ к сети.

4.3 Размещение и монтаж оборудования

В подвале будет установлен внешний телекоммуникационный шкаф F1, в котором будет размещен коммутатор SW0.

На первом этаже, в специально предназначенном помещении, будет установлен телекоммуникационный шкаф X1, в котором будет размещено следующее оборудование: коммутатор SW1, маршрутизатор R1 и модем M1.

На втором этаже будет установлен внешний телекоммуникационный шкаф F2, в котором будет размещен коммутатор SW2.

В проектируемой локальной компьютерной сети кабельная система будет реализована путем прокладки витой пары в кабельном коробе, который будет расположен под фальшпотолком. Помещения не подвержены сильным электромагнитным помехам, поэтому для кабельной системы можно использовать витую пару UTP. Учитывая выбранное сетевое оборудование, будет достаточно использовать кабель UTP категории 5е.

Для подключения конечного оборудования будут использоваться наружные розетки UTP категории 5е. Информационные розетки будут установлены на высоте 30 см от пола рядом с местами, где будут находиться конечные устройства.

Точка доступа будет закреплена на потолке с помощью монтажного комплекта, поставляемого в комплекте. Она будет подключена к коммутатору с использованием технологии PoE.

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы была разработана локальная компьютерная сеть для компании, специализирующейся на торговле овощами и фруктами. В процессе работы были получены как практические, так и теоретические знания и навыки в области проектирования локальных компьютерных сетей.

Был проведен анализ рынка сетевого оборудования, изучены стандарты и требования, которым должна соответствовать создаваемая система, проведено сравнение множества различных вариантов сетевого и оконечного оборудования различных категорий. В результате проектирования были разработаны структурная схема сети, функциональная схема сети, а также план этажей здания компании.

Был составлен перечень необходимого оборудования и материалов, включающий маршрутизатор, коммутаторы, рабочие станции, принтеры, сервер и пассивное сетевое оборудование. Вся выбранная в работе техника соответствует высоким стандартам качества и надежности.

Для защиты оборудования и пользовательских станций от сильных перепадов напряжения было решено использовать блоки бесперебойного питания.

Была реализована система видеонаблюдения для обеспечения сохранности и безопасности продаваемой продукции и персонала организации.

Так как проектировалась бюджетная сеть, оборудование выбиралось с учётом ценового сегмента, при этом решения не выбирались по принципу выбора самого дешёвого. Выбор оборудования рационально обоснован, некоторые решения являются не самыми бюджетными, однако без них сеть была бы нерациональной.

Для разграничения трафика использовалась технология VLAN. Разграничение производилось по типу и характеру подключений.

Полученная компьютерная сеть будет легко обслуживаться, а также ее можно будет расширять и масштабировать при необходимости.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- [1] Сайт производителя сетевого оборудования Allied Telesis [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.alliedtelesis.com/us/en> – Дата доступа: 25.09.2023
- [2] 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.> – Дата доступа: 25.09.2023
- [3] Сайт производителя технологии DOCSIS [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.cablelabs.com/technologies/docsis-4-0-technology> – Дата доступа: 22.10.2023
- [4] Каталог сетевого оборудования [Электронный ресурс] – Электронные данные. – Режим доступа: <https://server-x.by/> – Дата доступа: 22.10.2023
- [5] 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: 01.11.2023
- [6] Указания по монтажу точки беспроводного доступа TQ1402 [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.alliedtelesis.com/sites/default/files/documents/installation-guides/ati-tq1402series-ig.pdf> – Дата доступа: 01.11.2023
- [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-network> – Дата доступа: 11.11.2023
- [8] Список популярных прокси-серверов для Linux [Электронный ресурс] – Электронные данные. – Режим доступа: <https://losst.pro/luchshie-proksi-servery-linux> – Дата доступа: 18.11.2023
- [9] Информация о прокси-сервере Squid [Электронный ресурс] – Электронные данные. – Режим доступа: <http://www.squid-cache.org/> – Дата доступа: 18.11.2023
- [10] Информация о прокси-сервере Privoxy [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.privoxy.org/> – Дата доступа: 18.11.2023
- [11] Информация о прокси-сервере Tinyproxy [Электронный ресурс] – Электронные данные. – Режим доступа: <http://tinyproxy.github.io/> – Дата доступа: 18.11.2023
- [12] 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: 18.11.2023

[13] Пользовательское руководство для системы видеонаблюдения Swann SWDVK-845808V [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.manua.ls/swann/swdvk-845808v/manual> – Дата доступа: 18.11.2023

[14] Техническое руководство к интерфейсу командной строки оборудования Allied Telesis [Электронный ресурс] – Электронные данные. – Режим доступа: https://www.alliedtelesis.com/sites/default/files/documents/getting-started-guides/getting_started_aw_feature_overview_guide.pdf – Дата доступа: 25.11.2023

[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: 25.11.2023

[16] Каталог принтеров [Электронный ресурс] – Электронные данные. – Режим доступа: <https://5element.by/catalog/291-printery?tab=product&q=%D0%BF%D1%80%D0%B8%D0%BD%D1%82%D0%B5%D1%80> – Дата доступа: 18.11.2023

[17] Каталог камер [Электронный ресурс] – Электронные данные. – Режим доступа: <https://catalog.onliner.by/ipcamera/dahua/hfw2831sps0360bs> – Дата доступа: 18.11.2023

[18] Каталог телекоммуникационных шкафов [Электронный ресурс] – Электронные данные. – Режим доступа: <https://datastream.by/shkaf-antivandalnyj-penalnogo-tipa-9u-twt-cbwsf-9u-6x4-gy/> – Дата доступа: 18.11.2023

[19] Настройка Smart DNS Proxy [Электронный ресурс] – Электронные данные. – Режим доступа: <https://support.smartdnsproxy.com/article/30-general-router-dns-setup-for-smart-dns-proxy> – Дата доступа: 25.11.2023

[20] Каталог компьютеров [Электронный ресурс] – Электронные данные. – Режим доступа: <https://itmarket.by/> – Дата доступа: 18.11.2023

ПРИЛОЖЕНИЕ А
(Обязательное)

Схема СКС структурная

ПРИЛОЖЕНИЕ Б
(Обязательное)

Схема СКС функциональная

ПРИЛОЖЕНИЕ В
(Обязательное)

План этажа. Схема монтажная

ПРИЛОЖЕНИЕ Г
(Обязательное)

Перечень оборудования, изделий и материалов

ПРИЛОЖЕНИЕ Д
(Обязательное)

Ведомость документов