Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

Дисциплина: Структурная и функциональная организация ЭВМ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовому проекту на тему

Локальная компьютерная сеть

БГУИР КП 1-40 02 01 117 ПЗ

Студент: группы 950501, Лабецкий А. А.

Руководитель:

старший преподаватель каф. ЭВМ Глецевич И. И.

Минск 2022

|  |  |
| --- | --- |
| Вариант | 17 |
| Объект | организация, занимающаяся торговлей овощами и фруктами |
| Форма здания, этажи, суммарная площадь помещений в квадратных метрах | квадратная, 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 | заказчик не уверен |
| Внешняя адресация IPv4, внутренняя адресация IPv4, адресация IPv6 | внешний IPv4-адрес автоматически назначает провайдер, публичная подсеть, взаимодействие в рамках внутренней сети |
| Безопасность | прокси |
| Надежность | защита от сильных перепадов напряжения |
| Финансы | бюджетная сеть |
| Производитель сетевого оборудования | Allied Telesis |
| Дополнительное требование заказчика | нет |

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

Книга Эндрю Таненбаума «Компьютерные сети» [3] предоставила подробный разбор всех аспектов и уровней организации сетей.

На сайте производителя сетевого оборудования Allied Telesis [1] я ознакомился со списком актуальных моделей маршрутизаторов, коммутаторов и точек беспроводного доступа, подходящими для финансов, которые организация готова выделить на создание локальной сети, и с документацией, прилагающейся к оборудованию. Также на этом сайте доступны руководства по установке и настройке оборудования.

Из источника [2] мной была почёрпнута информация об управлении локальными сетями для малого и крупного бизнеса. Также я подробнее узнал о функциях, которые выполняют прокси-серверы, о том, как клиенты должны взаимодействовать с прокси, и о вариантах размещения прокси-сервера в сети.

На сайте [8] я ознакомился со списком наиболее популярных и актуальных прокси-серверов для Linux. Более подробную информацию об особенностях и настройке некоторых из этих серверов я узнал в источниках [9 – 11].

Источник [12] предоставил информацию о различиях между DVR и NVR видеорегистраторами. В источнике [7] содержится информация о подключении NVR-камер видеонаблюдения к локальной сети и особенностях их работы. Из источника [13] я узнал о том, как подключать DVR-видеорегистраторы к локальной сети и взаимодействовать с ними.

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 маршрутизатор, коммутатор, прокси-сервер, 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.

В задании указано, что для обеспечения безопасности требуется использовать прокси. Это значит, что внутренняя сеть организации должна иметь доступ к сети Internet только через прокси-сервер. Прокси сервер находится между маршрутизатором и корневым коммутатором.

3. функциональное проектирование

В рамках данного проекта сеть предприятия будет разделена на 5 виртуальные сети:

1. Виртуальная сеть для стационарных подключений;

2. Виртуальная сеть для мобильных подключений;

3. Виртуальная сеть для администрирования;

4. Виртуальная сеть для web-сервера;

5. Виртуальная сеть для системы видеонаблюдения.

Связь маршрутизатора, коммутаторов, точки беспроводного доступа, web-сервера, принтера, компьютеров и компонентов системы видеонаблюдения будет произведена с помощью кабелей Ethernet.

Для соединения посредством Gigabit Ethernet будет использоваться стандарт 802.3ab 1000BASE-T, определяющий работу передачи данных по неэкранированной витой паре 5e категории.

Оптимальным стандартом для беспроводной сети будет IEEE 802.11n, который имеет значительные преимущества в максимальной скорости передачи данных (до 150 Мбит/c) по сравнению с стандартами 802.11a/g. Данный стандарт имеет обширную зону распространения радиоволн в 100 м. Также стандарт обеспечивает обратную совместимость с устройствами, работающими по стандартам 802.11a/b/g.

Данный раздел сопровождает чертеж схемы СКС функциональной (приложение «Б»).

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

В качестве операционной системы для пользовательских станций выбрана OC Windows 10. На сегодняшний день, Windows 10 является самой популярной операционной системой и достаточно проста в использовании для обычного пользователя, поэтому большинству сотрудников будет удобнее и привычнее работать с этой операционной системой.

## **3.2 Обоснование выбора операционной системы серверов.**

Для прокси-сервера и web-сервера была выбрана операционная система Debian, т.к. она потребляет меньше аппаратных ресурсов, чем современные Windows, и отлично подходит для использования на сервере.

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

По аналогичным причинам, для прокси-сервера был выбран Squid – популярное, производительное и хорошо задокументированное решение, обладающее всем необходимым организации функционалом.

## **3.3 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, была выбрана модель Jet Office 5i8400D8HD1VGALW50. Компьютер удовлетворяет всем вышеперечисленным условиям и имеет среднюю цену порядка 1200 рублей, что приемлемо для бюджетной организации.

Станция обладает следующими характеристиками:

- процессор intel core i5 8400;

- оперативная память DDR4 8 ГБ;

- накопитель HDD 1000 ГБ;

- графический адаптер Intel UHD Graphics 630.

## **3.4 Обоснование выбора web-сервера и прокси сервера**

Требования организации к производительности web-сервера и прокси-сервера схожи, поэтому было решено использовать для них одинаковое аппаратное обеспечение.

Для сервера важно иметь ECC RAM, поэтому в первую очередь нужно выбрать процессор, поддерживающий работу с таким типом памяти. Популярными серверными процессорами с поддержкой ECC RAM являются процессоры Intel Xeon. Для целей организации подойдёт любой процессор из этой серии.

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

При сравнении готовых серверов, представленных на рынке, была выбрана модель Dell POWEREDGE T40.

Станция POWEREDGE T40 обладает следующими характеристиками:

- процессор Intel Xeon E-2224G;

- оперативная память DDR4 ECC 8 ГБ;

- накопитель HDD 1000 ГБ;

- графический адаптер Intel UHD Graphics P630.

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

После исследования рынка принтеров выбор пал на Pantum P3010DW. Он имеет среднюю стоимость $150. Pantum P3010DW является лазерным цветным принтером, печатающим формат A4, что отлично подходит для нужд нашей организации.

Для подключения принтер имеет порт Ehternet, что даёт возможность подключать принтер не к компьютеру, а к сети, предоставляя доступ для удалённого использования всем рабочим станциям внутри сети.

Также имеется возможность подключения по беспроводному интерфейсу WiFi 802.11 b/g/n.

## **3.6 Обоснование выбора системы видеонаблюдения**

При изучении рынка систем видеонаблюдения стало понятно, что с одинаковым успехом можно использовать как систему типа DVR, так и систему типа NVR. При использовании системы любого из этих типов можно добиться одинакового результата, однако NVR камеры значительно дороже как в установке, так и при обслуживании. С учётом того, что сеть по задания характеризуется как бюджетная, такую значительную разницу в цене стоит учесть и использовать DVR камеры. Была выбрана система Swann SWDVK-845808V, состоящая из 8 проводных камер. Накопитель может хранить до 1TB видео-данных. Камеры могут вести запись в качестве 720p или 1080p.

## **3.7 Обоснование выбора активного сетевого оборудования**

Полный перечень оборудования представлен в приложении «В».

### **3.7.1** **Маршрутизатор AT-AR2050V**

Так как по условию задания технология, посредством которой осуществляется выход в интернет, не определена, требуется по своему усмотрению выбрать маршрутизатор производителя Allied Telesis. При этом следует учитывать, что проектируемая сеть в задании характеризуется как бюджетная. В результате изучения каталога имеющегося в продаже оборудования был выбран маршрутизатор AT-AR2050V.

Маршрутизатор AR2050V-10 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

Данное устройство будет являться мостом между коммутатором и сетью провайдера. На нём будет выполняться маршрутизация между виртуальными подсетями организации.

# **3.7.2 Коммутатор AT-GS950/16**

Одним из важнейших критериев для выбора была управляемость коммутатора. AT-GS950/16 является управляемым коммутатором второго уровня, а значит он нам подходит.

Технические характеристики:

- основные порты: 16 Ethernet 10/100/1000 PoE+;

- порты каскадирования: 2 Small Form-Factor Pluggable (SFP) Gigabit Ethernet;

- максимальный размер пакета (MTU): до 10000 байт;

- скорость передачи трафика: 1488 mpps;

- память DRAM: 64 Мб;

- флэш-память: 16 Мб;

- MAC addresses: 8000;

- Available PoE Power: 15.4W PoE.

# **3.7.3 Точка беспроводного доступа TQ5403**

Точка доступа TQ5403отлично подходит для использования в сетях небольшого и среднего размера.

Технические характеристики:

- протоколы WiFi: 802.11a/b/g/n/ac Wave 2;

- технология MIMO: 2x2 MU-MIMO;

- антенны: 2.4GHz 18.79dDm 3.95dBi/ 5GHz 22.13dBm 4.20dBi/ 5GHz 28dBm 4.83dBi;

- протоколы аутентификации WiFi: WPA/WPA2/WPA3;

- память FLASH: 256 Мб;

- объем ОЗУ: 1 Гб;

- габариты: 215 x 215 x 48 мм.

Также TQ5403 имеет два GigabitEthernet интерфейса.

## **3.8 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 3.1

Для стационарных устройств (8 ПК и 6 принтеров) выбрана подсеть IPv4 201.68.7.0/28, и подсеть fc00::/8 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.

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

И для Web-сервера берем подсеть 201.68.7.56/30.

Таблица 3.1 – Схема адресации сетей

|  |  |  |  |
| --- | --- | --- | --- |
| Назначение | VLAN | Адрес подсети | Маска подсети |
| Стационарные подключения | 10 | 201.68.7.0 | 255.255.255.240 |
| fc00:: | /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 | 255.255.255.252 |

## **3.9 Настройка коммутаторов**

Коммутаторы серии GS-950 настраиваются с помощью веб-интерфейса.

Для настройки vlan нужно перейти во вкладку Tagged VLAN, её изначальный вид показан на рисунке 3.1.

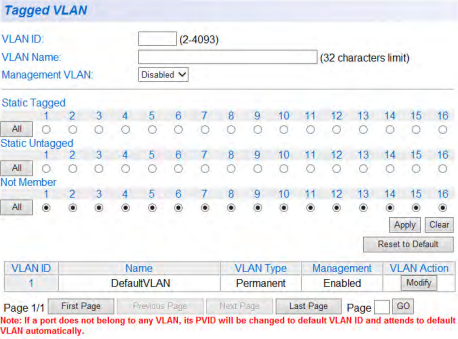


Рисунок 3.1 – вид вкладки Tagged VLAN

Для создания vlan нужно ввести его номер и имя в поля VLAN ID и VLAN Name соответственно, а также выбрать для него нетегированные порты в разделе Static Untagged или тегированные порты в разделе Static Tagged. Поле Management VLAN отвечает за возможность использовать vlan для администрирования. После того, как все параметры vlan настроены, нужно нажать кнопку Apply, чтобы сохранить изменения.

## **3.9.1 Настройка коммутатора этажа 0**

Так, согласно функциональной схеме из приложения Б, создаём пользовательский vlan под номером 10 с именем User и назначаем интерфейсы GigabitEtherner2-3 как нетегированные для этого vlan, интерфейс GigabitEthernet1 как тегированный. Поле Management VLAN установлено в Disabled. Вкладка Tagged VLAN с соответствующими настройками представлена на рисунке 3.2.

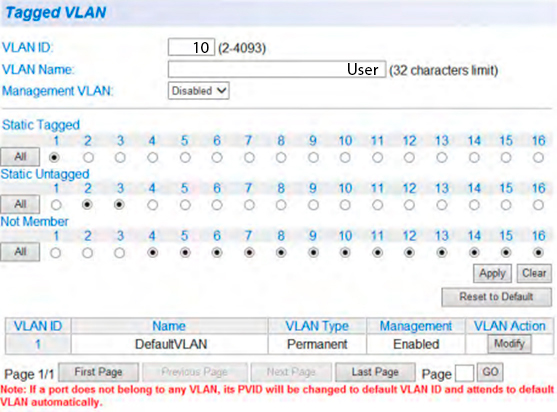


Рисунок 3.2 – Конфигурация vlan 10 коммутатора этажа 0

Создадим vlan 20 с названием Wireless и назначим GigabitEthernet4 нетегированным портом для него для него, интерфейс GigabitEthernet 1 – тегированным. В поле Management VLAN остаётся значение Disabled. Вкладка Tagged VLAN с соответствующей конфигурацией показана на рисунке 3.3.

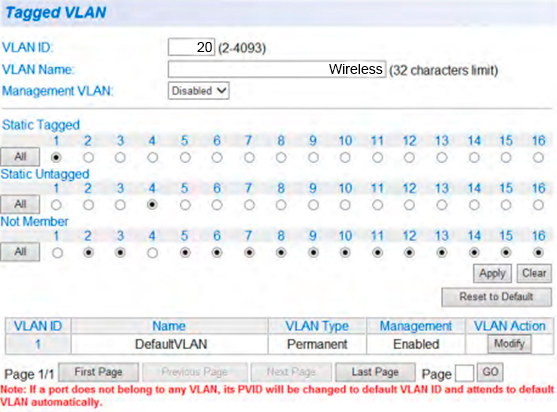


Рисунок 3.3 – Конфигурация vlan 20 коммутатора этажа 0

Создадим vlan 40 с названием Management. Поле Management VLAN нужно установить в значение Enabled, чтобы этот vlan можно было использовать для администрирования. Назначим интерфейс GigabitEthernet1 как тегированный для этого vlan. Вкладка Tagged VLAN с соответствующей конфигурацией показана на рисунке 3.4.

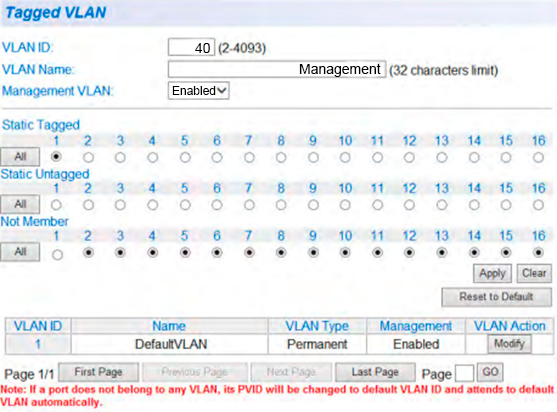


Рисунок 3.4 – Конфигурация vlan 40 коммутатора этажа 0

Создадим vlan 50 с названием WebServer. В поле Management VLAN оставляем значение Disabled. Назначим интерфейс GigabitEthernet1 как тегированный для этого vlan. Вкладка Tagged VLAN с соответствующей конфигурацией показана на рисунке 3.5.

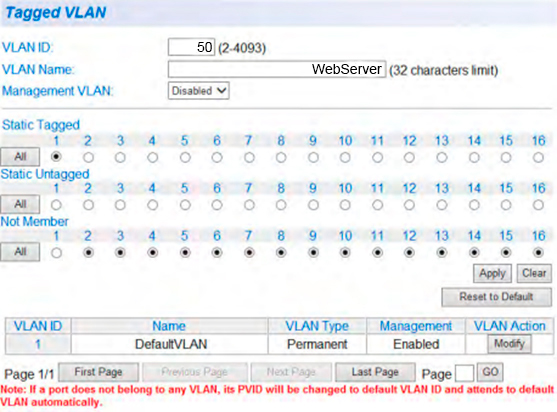


Рисунок 3.5 – Конфигурация vlan 50 коммутатора этажа 0

## **3.9.2 Настройка коммутатора этажа 1**

Создаём vlan под номером 10 с именем User и назначаем интерфейсы GigabitEthernet6-7 как тегированные для этого vlan. Поле Management VLAN установлено в Disabled. Вкладка Tagged VLAN с соответствующими настройками представлена на рисунке 3.6.

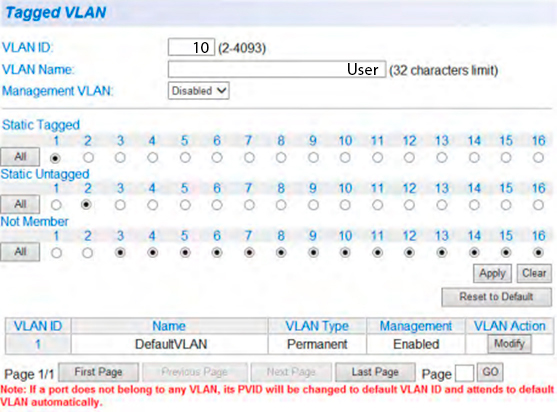


Рисунок 3.6 – Конфигурация vlan 10 коммутатора этажа 1

Создадим vlan 20 с названием Wireless и назначим GigabitEthernet2 нетегированным для него, интерфейсы GigabitEthernet6-7 – тегированными. В поле Management VLAN остаётся значение Disabled. Вкладка Tagged VLAN с соответствующей конфигурацией показана на рисунке 3.7.

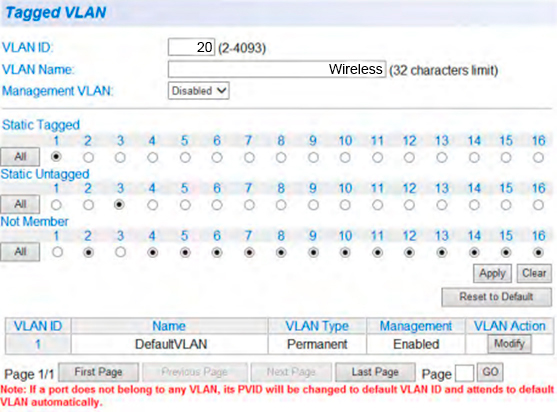


Рисунок 3.7 – Конфигурация vlan 20 коммутатора этажа 1

Создадим vlan 30 с названием CCTV и назначим GigabitEthernet4-5 нетегированными для него. В поле Management VLAN остаётся значение Disabled. Вкладка Tagged VLAN с соответствующей конфигурацией показана на рисунке 3.8.

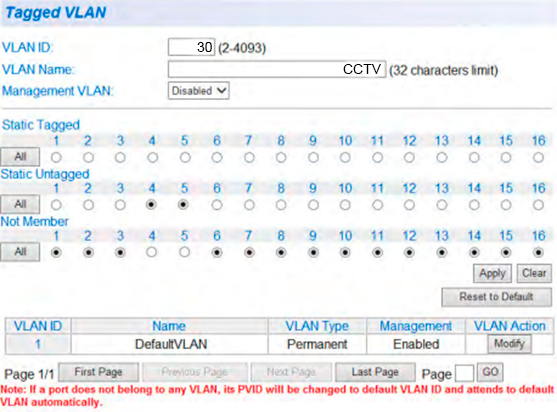


Рисунок 3.8 – Конфигурация vlan 30 коммутатора этажа 1

Создадим vlan 40 с названием Management. Поле Management VLAN нужно установить в значение Enabled, чтобы этот vlan можно было использовать для администрирования. Назначим интерфейсы GigabitEthernet6-7 как тегированные для этого vlan. Вкладка Tagged VLAN с соответствующей конфигурацией показана на рисунке 3.9.

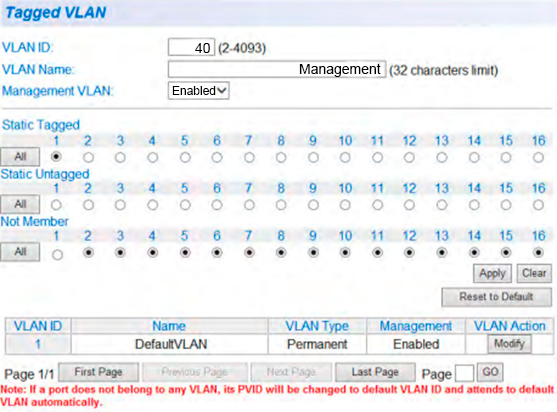


Рисунок 3.9 – Конфигурация vlan 40 коммутатора этажа 1

Создадим vlan 50 с названием WebServer и назначим GigabitEthernet5 нетегированным для него. В поле Management VLAN остаётся значение Disabled. Вкладка Tagged VLAN с соответствующей конфигурацией показана на рисунке 3.10.

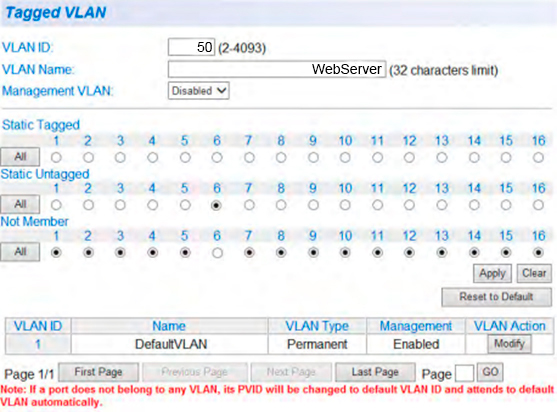


Рисунок 3.10 – Конфигурация vlan 50 коммутатора этажа 1

## **3.9.3 Настройка коммутатора этажа 2**

Создаём vlan под номером 10 с именем User и назначаем интерфейсы GigabitEthernet2-7 как нетегированные для этого vlan, интерфейс GigabitEthernet1 – тегированный. Поле Management VLAN установлено в Disabled. Вкладка Tagged VLAN с соответствующими настройками представлена на рисунке 3.11.

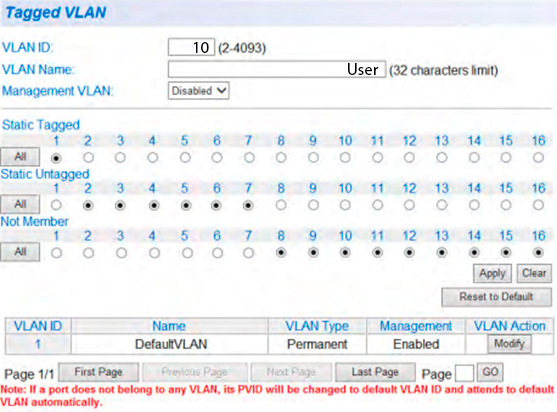


Рисунок 3.11 – Конфигурация vlan 10 коммутатора этажа 2

Создаём vlan под номером 20 с именем Wireless и назначаем интерфейс GigabitEthernet13 как нетегированныq для этого vlan, интерфейс GigabitEthernet1 – тегированный. Поле Management VLAN установлено в Disabled. Вкладка Tagged VLAN с соответствующими настройками представлена на рисунке 3.12.

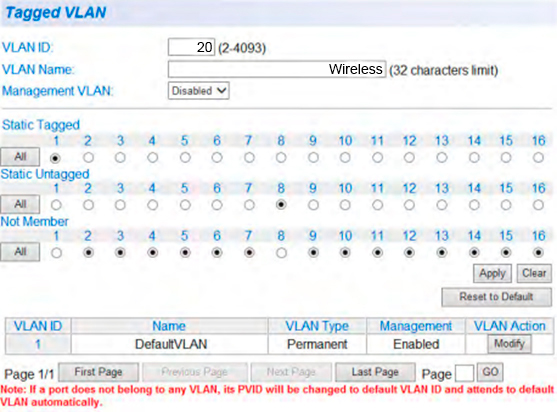


Рисунок 3.12 – Конфигурация vlan 20 коммутатора этажа 2

Создаём vlan под номером 40 с именем Management и назначаем интерфейс GigabitEthernet14 как нетегированный для этого vlan. Поле Management VLAN установлено в Enabled. Вкладка Tagged VLAN с соответствующими настройками представлена на рисунке 3.13.

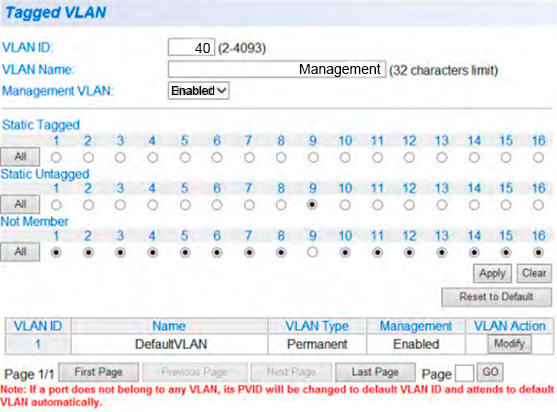


Рисунок 3.13 – Конфигурация vlan 40 коммутатора этажа 2

Создаём vlan под номером 50 с именем WebServer и назначаем интерфейс GigabitEthernet1 как тегированный для этого vlan. Поле Management VLAN установлено в Disabled. Вкладка Tagged VLAN с соответствующими настройками представлена на рисунке 3.14.

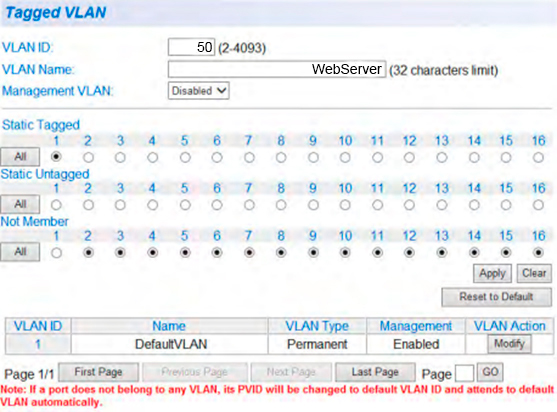


Рисунок 3.14 – Конфигурация vlan 50 коммутатора этажа 2

## **3.10 Настройка маршрутизации между сетями**

На центральном маршрутизаторе разбиваем интерфейс, идущий к коммутатору, на 4 подинтерфейса.

Для подсети с стационарными подключениями прописываем:

Router(config)#int gigabitEthernet 0/0.10

Router(config-if)#encapsulation dot1q 10

Router(config-if)#ip address 80.94.11.1 255.255.255.240

Для подсети с беспроводными подключениями прописываем:

Router(config)#int gigabitEthernet 0/0.20

Router(config-if)#encapsulation dot1q 20

Router(config-if)#ip address 80.94.11.17 255.255.255.240

Для административной подсети прописываем:

Router(config)#int gigabitEthernet 0/0.30

Router(config-if)#encapsulation dot1q 30

Router(config-if)#ip address 80.94.11.33 255.255.255.248

Для подсети с SQL-сервером прописываем:

Router(config)#int gigabitEthernet 0/0.40

Router(config-if)#encapsulation dot1q 40

Router(config-if)#ip address 80.94.11.41 255.255.255.252

IPv4 адреса роутера и маски для каждой из подсетей представлены в таблице 3.2.

Таблица 3.2 – Схема адресации центрального роутера

|  |  |  |
| --- | --- | --- |
| Назначение | IP адрес | Маска подсети |
| Стационарные подключения | 201.68.7.1 | 255.255.255.240 |
| 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 | 255.255.255.252 |

В рамках нашей задаче подсеть предприятия не должна пересекаться с беспроводной. Также эти подсети должны иметь доступ в интернет. Сервер, из соображений безопасности, в интернет выходить не должен. Поэтому для разграничения взаимодействия между подсетями настроим access листы.

Настройка производиться на центральном роутере.

Административный vlan может общаться с кем угодно, поэтому для него ничего не создаем

ACL лист для подсети с PC:

Router(config)#ip access-list standart PCvlan10

Router(config-std-nacl)#deny 80.94.11.16 0.0.0.15

Router(config-std-nacl)#permit any

С помощью deny мы запрещаем общаться с подсетью для беспроводных устройств. С помощью permit разрешает общаться со всем остальными

Привязываем access list к интерфейсу подсети:

Router(config)#int GigabitEthernet 0/0.10

Router(config-if)#ip access-group PCvlan10 out

Параметр out указывает на фильтрацию исходящего трафика.

ACL для беспроводной подсети:

Router(config)#ip access-list standard WiFivlan20

Router(config-std-nacl)#deny 80.94.11.0 0.0.0.15

Router(config-std-nacl)#deny 80.94.11.40 0.0.0.3

Router(config-std-nacl)#permit any

Тут запрещаем взаимодействовать с подсетями стационарных устройств и сервера. Т.е. со всей корпоративной частью предприятия.

Привязываем к интерфейсу.

Router(config)#int GigabitEthernet 0/0.20

Router(config-if)#ip access-group WiFivlan20 out

ACL для подсети с сервером:

Router(config)#ip access-list standard Servervlan40

Router(config-std-nacl)#permit 80.94.11.0 0.0.0.15

Router(config-std-nacl)#permit 80.94.11.32 0.0.0.7

Router(config-std-nacl)#deny any

Тут разрешаем общаться с административной и корпоративной подсетями. Взаимодействие с другими сетями запрещаем. Также привязываем к интерфейсу:

Router(config)#int GigabitEthernet 0/0.40

Router(config-if)#ip access-group Servervlan40 out

Административная же подсеть может взаимодействовать с кем угодно. Поэтому для нее ничего не создаем.

## **3.11 Настройка административной подсети**

Выдадим адреса устройствам в соответствии с таблицей 3.3.

Таблица 3.3 – Адреса устройств для административной подсети.

|  |  |  |
| --- | --- | --- |
| Устройство | IP адрес | Маска подсети |
| Router | 80.94.11.33 | 255.255.255.248 |
| Switch | 80.94.11.34 | 255.255.255.248 |
| Admin-PC | 80.94.11.35 | 255.255.255.248 |

На коммутаторе настроим адрес на vlan 30 интерфейсе.

Switch(config-if)#ip address 80.94.11.34 255.255.255.248

Настроим ssh на роутере и коммутаторе. Для этого выполним следующие команды:

(config)#ip domain-name mine.com

(config)#crypto key generate rsa modulus 1024

(config)#ip ssh version 2

(config)#username admin secret cisco123

(config)#line vty 0 4

(config-line)#login local

(config-line)#transport input ssh

В целях безопасности пропишем Port-security на интерфейсе коммутатора, предназначенном для администратора:

Switch(config-if)#switchport port-security

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

Switch(config-if)#switchport port-security violation restrict

Switch(config-if)#switchport port-security mac-address sticky

## **3.12 Настройка ПК и маршрутизации между ними**

Для ПК требуется настроить статическую IPv4 и IPv6 маршрутизацию. Адреса ПК представлены в таблице 3.3. Сперва включим ipv6 на центральном роутере и зададим ему ipv6 адрес:

Router(config)#ipv6 unicast-routing

Router(config)#int gigabitEthernet 0/0

Router(config-if)#ipv6 address fc00::1/8

Таблица 3.4 – Адреса ПК.

|  |  |  |
| --- | --- | --- |
| Устройство | IP адрес | Маска подсети |
| PC1 | 80.94.11.2 | 255.255.255.240 |
| fc00::2 | /64 |
| PC2 | 80.94.11.3 | 255.255.255.240 |
| fc00::3 | /64 |
| PC3 | 80.94.11.4 | 255.255.255.240 |
| fc00::4 | /64 |
| PC4 | 80.94.11.5 | 255.255.255.240 |
| fc00::5 | /64 |
| PC5 | 80.94.11.6 | 255.255.255.240 |
| fc00::6 | /64 |
| PC6 | 80.94.11.7 | 255.255.255.240 |
| fc00::7 | /64 |
| Admin-PC | 80.94.11.35 | 255.255.255.248 |
| fc00::8 | /64 |

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

## **3.13 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 «Меню», 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 3.3.



Рисунок 3.3 – 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 3.4. Нажимаем кнопу «Done» для выхода из программы установки. Принтер готов к использованию.



Рисунок 3.4 – Окно завершения установки драйвера

## **3.14 Настройка web-сервера**

На компьютере для SQL-сервера нужно будет указать адрес 80.94.11.42 и маску 255.255.255.252 (см. рисунок 3.1). В качестве шлюза указать ip роутера 80.94.11.41.

Обновим базу данных пакетов и установим apache2.

sudo apt update

sudo apt install apache2

## **3.15 Настройка Прокси-сервера**

На компьютере для SQL-сервера нужно будет указать адрес 80.94.11.42 и маску 255.255.255.252 (см. рисунок 3.1). В качестве шлюза указать ip роутера 80.94.11.41.

Запускаем установщик Microsoft SQL Server 2019 Express. Выбираем первый пункт «Новая установка изолированного экземпляра SQL Server или добавление компонентов к существующей установке». Далее принимаем условия пользовательского соглашения. Нажимаем далее до окна «Выбор компонентов». Тут выбираем все, что нужно (см. рисунок 3.4)

## 

Рисунок 3.4 – Выбор компонентов

Нажимаем «Далее», пока не дойдем до окна «Конфигурация SQL сервера». Здесь необходимо указать, от имени какой учетной записи будут работать службы SQL Server).

Идем далее до конца, запускаем установку. Для того что бы с других компьютеров можно было подключиться к установленному северу по сети, необходимо проделать следующие действия. Запустите "Диспетчер конфигурации SQL Server 2019". В разделе «Протоколы SQLEXPRESS» необходимо включить протокол TCP/IP (см. рисунок 3.5).



Рисунок 3.5 – Включение TCP/IP протокола.

После перезапускаем сервис. Далее настроим брандмауэр windows, чтобы он не блокировал соединения. Для этого необходимо запустить Брандмауэр Windows в режиме «Дополнительных параметров».

Первое «Для программы» и указать в качестве программы исполняемый файл Microsoft SQL Server Express. Второе правило следует создать для порта. В разделе протоколов выбрать «UDP» и в значение порта прописать 1434.

**3.16 Настройка точки беспроводного доступа**

Для мобильных устройств адреса из беспроводной сети должны выдаваться автоматически. Поэтому на центральном роутере настраиваем DHCP. Прописываем следующие команды:

Router(config)#ip dhcp pool WiFi

Router(dhcp-config)#network 80.94.11.16 255.255.255.240

Router(dhcp-config)#default-router 80.94.11.17

И исключаем адреса центрального роутера и wifi точки.

Router(config)#ip dhcp excluded-address 80.94.11.17 80.94.11.18

Дальше приступаем к настройке wifi роутера.

Для интерфейса BVI1 задем IP из подсети, предназначенной для смартфонов.

wifi(config)#ip address 80.94.11.18 255.255.255.240

После задаем и настраиваем SSID. Присвоим сети имя WiFi, задействуем авторизацию с помощью WPA, установим ключ сети ciscocisco

wifi(config)#dot11 ssid WiFi

wifi(config-ssid)#authentication open

wifi(config-ssid)#authentication key-management wpa

wifi(config-ssid)#guest-mode

wifi(config-ssid)#wpa-psk ascii ciscocisco

wifi(config-ssid)#exit

Затем настроим радио-интерфейс.

wifi(config)#interface Dot11Radio1

wifi(config-if)#encryption mode ciphers tkip

wifi(config-if)#ssid WiFi

wifi(config-if)#speed basic-54.0 54.0

wifi(config-if)#station-role root access-point

wifi(config-if)#no shutdown

wifi(config-if)#exit

wifi(config)#exit

Для удалённого подключения к точке доступа необходимо ввести адрес 192.168.1.230 в адресной строке браузера.

После этого появится следующее окно, показанное на рисунке Рисунок х.х – потом напишу.



Рисунок х.х – потом напишу

При первом подключении нужно ввести имя пользователя manager и пароль friend.

Тогда появится окно, показанное на Рисунок х.х – потом напишу.



Рисунок х.х – потом напишу\

**3.17 Настройка подключения к Интернету**

В рамках задания подключение идет по VDSL2.0. Для этого необходимо зайти в web-браузер в адресной строке ввести IP-адрес модема (по умолчанию 192.168.1.1). И при переходе на вкладку сеть/WAN и выставить настройки, изображенные на рисунке 3.6.



Рисунок 3.8 – Меню настройки WAN

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.

Помещения организации расположены на трёх этажах здания. Между этажами кабели протянуты по кабельным шахтам.

Центральный маршрутизатор, коммутатор и сервер находятся в служебном помещении. Коммутатор и маршрутизатор имеют крепления на стене, сервер стоит на столе. Точка беспроводного доступа вынесена в коридор, для обеспечения лучшей связи в цехах. Также имеет крепление на стене.

Принтер расположен в кабинете директора на отдельном столе.

В плане монтажа указывается, как и где прокладывать кабель, установка розеток.

Со схемой плана монтажа можно ознакомиться в приложении Г.

В плане здания можно увидеть месторасположение рабочих станций, принтера и сетевого оборудования.

Со схемой плана здания можно ознакомиться в приложении Д.

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 AR2010V [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.alliedtelesis.com/by/en/products/security-appliances/secure-vpn-routers/ar2010v#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