Форма № Н-9.02

Міністерство освіти і науки України

Відокремлений структурний підрозділ «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя»

(повне найменування вищого навчального закладу)

Відділення інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра

(освітньо-професійного ступеня)

на тему: **Розробка проєкту комп'ютерної мережі комп'ютерного клубу "Сталкер"**

Виконав: студент IV курсу, групи КІ-418

Спеціальності 123 Комп'ютерна інженерія

(шифр і назва спеціальності)

_____ Роман ФЕДАК

(ім'я та прізвище)

Керівник Ігор ТХІР

(ім'я та прізвище)

Рецензент _____

(ім'я та прізвище)

Тернопіль – 2025

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ТЕРНОПІЛЬСЬКИЙ ФАХОВИЙ КОЛЕДЖ
ТЕРНОПІЛЬСЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
імені ІВАНА ПУЛЮЯ»

Відділення **інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян**
Циклова комісія **комп'ютерної інженерії**
Освітньо-професійний ступінь **фаховий молодший бакалавр**
Освітньо-професійна програма: **Обслуговування комп'ютерних систем і мереж**
Спеціальність: **123 Комп'ютерна інженерія**
Галузь знань: **12 Інформаційні технології**

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"31" березня 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Федаку Роману Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту комп'ютерної мережі комп'ютерного клубу "Сталкер"**

керівник роботи Тхір Ігор Любомирович
(прізвище, ім'я, по батькові)

Затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя» від 28.03.2025р № 4/9-166а.

2. Строк подання студентом роботи: 13 червня 2025 року.

3. Вихідні дані до роботи: плани приміщень, завдання на проєктування, стандарти ANSI/EIA/TIA 568 - "Commercial Building Telecommunications Wiring Standart" і ANSI/EIA/TIA 569 - "Commercial Building Standart for Telecommunications Pathwais and Spaces

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Загальний розділ. Розробка технічного та робочого проєкту. Спеціальний розділ. Економічний розділ. Охорона праці та безпека життєдіяльності.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
   - план приміщень;
   - фізична топологія мережі;
   - логічна топологія;
   - таблиця IP-адрес;
   - таблиця техніко-економічних показників.
6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Богдана МАРТИНЮК викладач		
Охорона праці та безпека життєдіяльності	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	01.04	
2	Збір і узагальнення інформації	05.05	
3	Написання першого розділу	16.05	
4	Розробка технічного та робочого проекту	23.05	
5	Написання спеціального розділу	30.05	
6	Розрахунок економічної частини	2.06	
7	Написання розділу охорони праці	4.06	
8	Виконання графічної частини	9.06	
9	Оформлення проєкту	11.06	
10	Погодження нормоконтролю	12.06	
11	Попередній захист роботи	13.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 01 квітня 2025 року

Студент _____ Роман ФЕДАК
(підпис) (ім'я та прізвище)

Керівник роботи _____ Ігор ТХІР
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Федак Р.С. Розробка проєкту комп'ютерної мережі комп'ютерного клубу "Сталкер": кваліфікаційна робота на здобуття освітнього ступеня фаховий молодший бакалавр за спеціальністю «123 – Комп'ютерна інженерія». Тернопіль: ВСП «ТФК ТНТУ», 2025. 91с.

Кваліфікаційна робота передбачає розробку проекту комп'ютерної мережі комп'ютерного клубу "Сталкер" згідно стандартів та вимог замовника. В проектовані мережі використано сучасні стандарти Gigabit Ethernet IEEE 802.3ab, IEEE 802.11ac та Ethernet IEEE 802.3q. При цьому реалізовано розподіл мережі на віртуальні підмережі, планування та розподіл адресного простору. Розроблено інструкції з інсталяції та налаштування програмного хабезпечння сервера, активного комутаційного обладнання, шлюзу доступу до мережі Інтернет, віртуальних підмереж та засобів захисту і моніторингу мережі.

Ключові слова: комп'ютерна мережа, файловий сервер, Wi-Fi, маршрутизатор, комутатор, віртуальна мережа, VLAN, антивірус

ANNOTATION

Fedak R.S. Development of a computer network project for the computer club "Stalker": qualification work for obtaining the educational degree of a professional junior bachelor in the specialty "123 – Computer Engineering". Ternopil: VSP "TFK TNTU", 2025. 91 p.

The qualification work involves the development of a computer network project for the computer club "Stalker" according to the standards and requirements of the customer. The designed networks use modern Gigabit Ethernet IEEE 802.3ab, IEEE 802.11ac and Ethernet IEEE 802.3q standards. At the same time, the network is divided into virtual subnetworks, planning and allocation of address space are implemented. Instructions for installing and configuring server software, active switching equipment, Internet access gateway, virtual subnets and network protection and monitoring tools have been developed.

Keywords: computer network, file server, Wi-Fi, router, switch, virtual network, VLAN, antivirus

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

IP (Internet Protocol) – Інтернет-протокол.

LAN (Local Area Network) – локальна мережа.

DNS (Domain Name System) – сервер доменних імен.

DHCP (Dynamic Host Configuration Protocol) – протокол динамічного автоматичного призначення вузлам мережі IP-адрес.

NAT (Network Address Translation) – мережева трансляція адес.

TCP/IP (Transmission Control Protocol/Internet Protocol) – протокол управління передачею/Інтернет протокол.

MAC (Media Access Control) - апаратна адреса ПК.

EIA (Electronic Industries Association) – Асоціація електронної промисловості

HTTP (Hypertext Transfer Protocol) - протокол передачі гіпертексту.

ПК - персональний комп’ютер.

OSI (Open System Interface) – модель з’єднання відкритих систем;

SNMP (Simple Network Management Protocol) – протокол керування мережею;

UTP (Unshielded Twisted Pair) – кабель типу неекранована скручена пара

СКС – структурована кабельна система;

ЛМ – локальна мережа.

ОС – операційна система.

ПК – персональний комп’ютер.

ВСТУП

Інтеграція сучасної комп'ютерної техніки та локальних мереж у повсякденне життя є незаперечною, і приватний сектор активно використовує їх переваги. Застосування цих технологій значно підвищує продуктивність працівників, оскільки кожна затримка в передачі даних може призвести до фінансових втрат. [1].

Локальні мережі являють собою об'єднання комп'ютерів, розташованих на обмеженій території, як правило, в радіусі до 1-2 кілометрів. Хоча існують випадки, коли локальна мережа може охоплювати значно більші відстані, до кількох десятків кілометрів, зазвичай така мережа є комунікаційною системою, що належить одній організації.

Одним із найбільш популярних використання комп’ютерних мереж в побуті стало проведення онлайн-ігор, що послужило поштовхом для розвитку та популяризації комп’ютерних клубів.

Комп'ютерний клуб у своїй сучасній ітерації є більше, ніж просто набір комп'ютерів. В його основі лежить складна комп'ютерна мережа, яка є фундаментом для надання якісних послуг та створення привабливого ігрового середовища.

Кваліфікаційна робота передбачає розробку локальної мережі для комп’ютерного клубу “Сталкер”, який розташовано у місті Чортків, Тернопільської області.

Комп'ютерна мережа є невід'ємною та критично важливою складовою сучасного комп'ютерного клубу. Її якість та функціональність безпосередньо впливають на задоволеність клієнтів, ефективність роботи персоналу та успішність бізнесу в цілому. Інвестиції в надійну та добре спроектовану мережеву інфраструктуру є запорукою конкурентоздатності та привабливості комп'ютерного клубу на ринку розважальних послуг.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Відповідно до тематики у кваліфікаційній роботі комп’ютерного клубу “Сталкер”, який розташовано у місті Чортків, Тернопільської області..

Для вирішення даної задачі потрібно скласти технічне завдання врахувавши всі поставлені до мережі вимоги, проаналізувати план.

Запропонована розробка може бути ефективно використана в локальних мережах організацій різного типу (фірм, підприємств, установ), демонструючи ряд переваг над існуючими аналогами.

До особливостей мережі можна віднести [3]:

- порівняно невеликі затрати на її реалізацію;
- сегментованість локальної мережі з можливістю передачі трафіку між сегментами та налаштування правил фільтрації останнього;
- можливість спільного використання мережевих ресурсів;
- спільне використання мережі Інтернет та централізований захист локальної мережі.

Основною областю застосування комп'ютерної мережі в комп'ютерному клубі є забезпечення функціонування всіх сервісів та послуг, що надаються клубом клієнтам та персоналу:

- забезпечення доступу до ігрових серверів та онлайн-ігор;
- організація локальних багатокористувацьких ігор;
- керування ігровими сесіями та обліковими записами клієнтів;
- забезпечення доступу до інших онлайн-сервісів;
- моніторинг стану комп'ютерів, мережевого обладнання;
- забезпечення роботи адміністративного персоналу;
- надання можливості спільного використання периферійних пристроїв.

1.1.2 Призначення розробки

Проектуючи мережу комп'ютерного клубу “Сталкер”, слід керуватися наступними вимогами, сформульованими замовником:

- об'єднати всі комп'ютери в клубі для спільної гри в багатокористувацькі ігри, участі в локальних турнірах та обміну даними;
- забезпечити високошвидкісне та стабільне підключення до глобальної мережі для завантаження ігор, оновлень, онлайн-змагань та комунікації гравців;
- дозволить адміністраторам контролювати роботу всіх комп'ютерів, встановлювати та оновлювати програмне забезпечення, керувати обліковими записами користувачів та налаштовувати права доступ;
- можливість забезпечення спільного використання принтерів, файлових сховищ та іншого обладнання;
- можливість масштабування мережі шляхом підключення нових вузлів при розширені парку комп’терного клубу;
- швидкість передачі в мережі повинна забезпечувати потреби мультимедійних додатків та онлайн ігор до смуги пропускання каналу;
- передбачити захист обладнання та дані від зовнішніх загроз, забезпечує стабільну роботу всіх елементів мережі для безперебійного ігрового процесу;
- всі витрати на процес розробки проекту та монтажу мережі повинні не перевищувати вказаних замовником.

Комп'ютерний клуб, ефективно використовуючи можливості комп'ютерної мережі, може запропонувати своїм клієнтам:

- високопродуктивні ігрові сесії, завдяки стабільному з'єднанню та потужному обладнанню;
- зручне обслуговування. Швидка авторизація, легкий доступ до ігор та сервісів;
- організацію кіберспортивних заходів;
- створення платформи для спілкування та взаємодії між гравцями;

- додаткові послуги. такі як трансляції ігор, тематичні вечірки, продаж ігрової периферії тощо.

З метою виконання поставлених завдань буде розроблено локальну мережу, фізична топологія якої визначатиме прокладання кабельної системи в коробах різного січення. Тип кабелю, який буде використовуватися, напряму визначається обраним стандартом, що детально розглянуто в розділі 2.1. “Опис та обґрунтування вибору логічного типу та технології мережі”.

Далі в процесі розробки мережі потрібно налаштувати служби локальної мережі та її обладнання.

1.1.3 Вимоги до апаратного і програмного забезпечення

Функціонування будь-якої комп'ютерної мережі забезпечується взаємодією апаратних і програмних засобів. Серед апаратного забезпечення розрізняють активні пристрої, що аналізують і обробляють трафік, та пасивні елементи, які відповідають за передачу сигналів і підключення додаткових компонентів.

Для забезпечення необхідної швидкості передачі мережевого трафіку (не менше 1 Гбіт/с) у проєктованій мережі, пасивне обладнання повинно мати відповідні фізичні характеристики. Для досягнення цієї швидкості необхідно обрати мережеву технологію, яка б гарантувала таку швидкість.Для задоволення цієї вимоги обґрунтованим є використання мережевої технології Gigabit Ethernet.

Відповідно до обраної мережевої технології, активне обладнання мережі, включаючи комутатори робочих груп, сегментуючі комутатори та маршрутизатор, повинно забезпечувати логічну сегментацію, фільтрацію трафіку та підтримку VLAN. Зокрема, комутатори мережі повинні підтримувати стандарти IEEE 802.3ab та IEEE 802.1Q.

У зв'язку з вимогою замовника щодо інтеграції бездротового доступу до мережевих ресурсів, архітектура мережі передбачає наявність безпровідного сегмента, реалізація якого буде здійснена на основі технологічних стандартів Wi-Fi IEEE 802.11ac.

Крім апаратного забезпечення для функціонування мережі використовується програмне забезпечення, до якого відносять операційні системи серверів та робочих станцій та прикладне програмне забезпечення, яке встановлюється враховуючи специфіку діяльності підприємства.

Процес вибору серверної операційної системи передбачає аналіз ряду ключових критеріїв, а саме: вартість ліцензування та підтримки, показники надійності функціонування, рівень безпеки та ефективність механізмів захисту від несанкціонованого доступу (що є першочерговим фактором), а також періодичність випуску оновлень безпеки та функціоналу.

При виборі операційної системи для робочих станцій ключовими критеріями є інтуїтивно зрозумілий інтерфейс та зручність у використанні, оскільки кінцевими користувачами будуть особи, які не мають спеціалізованих знань в адмініструванні, на відміну від серверних ОС, що експлуатуються кваліфікованим персоналом. Додатковою суттєвою вимогою є інтегрована підтримка стеку протоколів TCP/IP, що є фундаментальною технологією для функціонування проектованої мережі.

Згідно вимог замовника також необхідно передбачити безпровідний сегмент для можливості підключення власних пристроїв відвідувачів комп'ютерного клубу до безпровідної мережі із виходом в Інтернет. Для цього слід забезпечити наявність безпровідних точок доступу із підтримкою стандарту IEEE-802.11ac для доступу кінцевих пристроїв із швидкістю не менше 1Гбіт/с.

1.1.4 Вимоги до документації

Правильне, чітке та повне оформлення документації при проєктуванні комп'ютерної підприємства є критично важливим для успішної реалізації, подальшої експлуатації та розвитку мережевої інфраструктури.

Правильно складена документація забезпечить:

- замовнику повне уявлення про те, яка мережа буде створена, її функціональні можливості, архітектуру, використовувані технології та обладнання;

- слугує єдиним джерелом інформації для всіх членів команди розробників, забезпечуючи узгодженість дій та мінімізуючи ризик непорозумінь або помилок під час проєктування та впровадження;

- допомагає швидко виявляти та усувати можливі проблеми на етапі налагодження;

- значно полегшує процес монтажу, підключення та конфігурації мережевого обладнання;

- допомагає новим співробітникам швидко освоїтися з інфраструктурою мережі. У випадку зміни персоналу, якісна документація забезпечує безперервність обслуговування;

- інструкції з експлуатації та діагностики є незамінними для адміністраторів мережі під час щоденного обслуговування, моніторингу працездатності та усунення несправностей;

- забезпечує масштабованості та можливості модернізації. Без якісної документації внесення змін до існуючої мережі може бути складним і ризикованим;

- у випадку інцидентів безпеки, документація може допомогти в аналізі подій та відновленні працездатності;

- допомагає швидко локалізувати проблему та вжити необхідних заходів для її усунення.

Основні види документації, необхідні при проєктуванні комп'ютерної мережі комп’ютерного клубу “Сталкер”:

- технічне завдання (ТЗ), що включає опис цілей проєкту, вимог замовника, функціональних характеристик мережі та обмежень;

- концептуальна схема мережі, яка представляє загальний опис архітектури мережі, основних компонентів та їх взаємодії;

- логічна топологія мережі – детальний опис логічної організації мережі, включаючи IP-адресацію, VLAN, маршрутизацію тощо;

- фізична топологія мережі – схема розміщення обладнання, прокладання кабелів, підключення пристроїв;

- специфікації обладнання та програмного забезпечення, що включають перелік використовуваного обладнання, його характеристики, версії програмного забезпечення, ліцензії;
- детальний графік виконання робіт, етапи проєкту, відповідальні особи;
- інструкції з налаштування мережевого обладнання та програмного забезпечення;
- план тестування та верифікації, що містить опис методів та критеріїв тестування працездатності мережі.
- опис заходів безпеки, правил доступу, процедур резервного копіювання та відновлення.

1.1.5 Техніко-економічні показники

Основні техніко-економічні показники локальної мережі комп'ютерного клубу "Сталкер":

- топологія мережі – гібридна;
- стандарт мережі – Gigabit Ethernet;
- специфікації мережі – IEEE 802.3ac та IEEE-802.11ac;
- операційна система файлового сервера – Ubuntu Linux 25.04;
- технологія доступу до мережі Інтернет – NAT;
- тип маршрутизації між підмережами – статична;
- тип віртуальних підмереж – IEEE 802.1Q;
- тип сервера – файловий, DHCP;
- кількість робочих станцій – 46;
- трудомісткість проектування і інсталяції мереж – до 100 люд/год.
- матеріальні витрати на мережу – до 300 000 грн;
- собівартість мережі – до 350 000 грн;
- повна вартість мережі - до 500 000 грн.

1.1.6 Стадії та етапи розробки

Процес розробки мережі каомп’ютерного клубу складається із наступних етапів [3]:

- ознайомлення з технічним завданням;
- розробка логічної топології мережі;
- розробка фізичної топології мережі;
- налаштування мережевого обладнання комутаторів та VLAN;.
- налаштування маршрутизатора;
- налаштування VPN-тунелю;
- налаштування файлового сервера;
- налаштування програмного забезпечення клієнтів;
- тестування мережі.

1.1.7 Порядок контролю та прийому

На завершальній стадії проєктування комп'ютерної мережі необхідно провести комплексне тестування основних технічних показників з метою верифікації їхньої відповідності встановленим специфікаціям. Для здійснення контролю будуть задіяні апаратні засоби, а саме кабельний тестер, сертифікований відповідно до вимог стандарту 1000 Base-TX, а також відповідне програмне забезпечення.

Процедура введення мережі в експлуатацію та її офіційне приймання здійснюється спеціальною комісією, до складу якої входять уповноважені представники замовника та виконавця, з оформленням відповідної документації (актів прийому-передачі об’єктів).

На завершальному етапі проєктування комп’ютерної мережі проводиться комплексне тестування її ключових технічних показників для підтвердження відповідності заданим вимогам. Це включає тестування пропускної здатності (за допомогою утиліти iperf3), затримки та втрати пакетів (за допомогою ping та

traceroute), якості бездротового сигналу (аналізаторами Wi-Fi), працездатності комутаторів та маршрутизатора, а також перевірку налаштувань VLAN та правил міжмережевого екрану. Для контролю використовуються сертифікований кабельний тестер (стандарт 1000 Base-TX) та спеціалізоване програмне забезпечення для аналізу мережевого трафіку. Всі результати тестування детально протоколюються.

1.2 Постановка задачі на розробку проекту. Характеристика об'єкта розробки мережі

В кваліфікаційній роботі необхідно розробити локальну обчислювальну мережу для комп'ютерного клубу "Сталкер", що знаходиться у місті Чортків, Тернопільскої області.

Комп'ютерний клуб займає площу близько 300 кв.м. Має два основні ігрових зали (основний та VIP), рецепцію, зону очікування, приміщення власника клубу, бухгалтера, адміністраторів та менеджерів.

Основна аудиторія – молодь віком 14-25 років, студенти та школярі, а також аматори кіберспорту. VIP-зона орієнтована на більш досвідчених гравців та проведення невеликих турнірів.

Клуб працює щоденно з 10:00 до 22:00. У вихідні та святкові дні можливе продовження роботи до 23:00. Пікове навантаження спостерігається у вечірній час та у вихідні.

В основному залі розміщено 32 ігрових ПК, у VIP-зоні – 10 більш потужних ПК. На рецепції використовується 2 адміністративних ПК. Окремі ПК розташовано в кімнаті власника клубу та бухгалтера.

Окрема VIP-зона на 10 ПК, обладнана більш потужним залізом та окремою системою кондиціонування.

На території клубу є міні-бар з напоями та снеками. Для оплати використовується POS-термінал, який також потребує підключення до мережі.

Більшість ПК в основному залі мають середні характеристики (Intel Core i5, GeForce GTX 1650, 16GB RAM, HDD). ПК у VIP-зоні – високі характеристики (Intel Core i7, GeForce RTX 3060, 32GB RAM, SSD). Операційна система – Windows 11. Встановлено набір популярних ігор.

При розробці мережі необхідно забезпечити стабільну роботу мережі при одночасному підключенні до 42 ігрових ПК та до 10 гостьових пристроїв через Wi-Fi.

Потрібен високошвидкісний та стабільний інтернет-канал з пропускною здатністю не менше 1 Гбіт/с для забезпечення комфортної гри та завантаження оновлень. Низький пінг є критично важливим.

Локальна мережа повинна забезпечувати швидкість передачі даних не менше 1 Гбіт/с між ПК для можливих локальних ігор та швидкого обміну даними з майбутніми серверами.

Обов'язкове забезпечення стабільного та швидкого Wi-Fi для відвідувачів у зоні очікування та, можливо, у VIP-зоні (окрема гостьова мережа).

Необхідно забезпечити захист від зовнішніх кіберзагроз, запобігти несанкціонованому доступу до адміністративних ресурсів та ізолювати клієнтську мережу від гостьової. Розглянути можливість впровадження міжмережевого екрану.

Мережа повинна працювати без збоїв під час пікових навантажень. Розглянути можливість резервування ключових елементів.

Мережа повинна мати можливість для подальшого розширення при збільшенні кількості ПК або впровадженні нових сервісів.

Потрібне підключення POS-термінала до мережі, а також майбутньої системи обліку відвідувань.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис та обґрунтування вибору логічного типу та технології мережі

Згідно із завданням дипломної роботи, мережа ігрового клубу буде використовувати провідне фізичне середовище за технологією Ethernet та включатиме безпровідний сегмент Wi-Fi.

Для ігрового комп'ютерного клубу, де критично важливі стабільність, низька затримка (ping) та висока пропускна здатність, ключовим є використання провідних технологій. Безпровідний сегмент є доповненням, але не основою для ігрових станцій.

Назва Ethernet походить від слів "Ether" (ефір) та "Net" (мережа), що вказує на різноманітність потенційних середовищ для передачі даних. Ця технологія передбачає використання системи керування доступом до середовища (MAC), яка дозволяє підключеним мережевим пристроям спільно використовувати одне середовище передачі.

В основі Ethernet лежить принцип множинного доступу з контролем несучої та виявленням колізій (CSMA/CD). "Множинний доступ" означає, що декілька користувачів або пристроїв можуть взаємодіяти з одним ресурсом, наприклад, одним файлом або пристроєм. Протоколи CSMA/CD працюють за принципом:

- прослуховування кабелю перед початком передачі;
- виявлення колізій (коли дві системи починають передачу одночасно);
- ініціалізація повторних передач після виявлення колізії, з випадковою затримкою.

Це означає, що абонентська система може почати передачу, лише якщо в мережі немає інших активних передач. Якщо ж під час передачі виявляється паралельна передача, система припиняє свою роботу та спробує повторити її пізніше. Це досягається завдяки виявленню несучої (Carrier Sense) перед початком передачі та виявленню колізій (Collision Detection) під час передачі.

Технології Ethernet охоплюють фізичний та канальний рівні OSI-моделі та стандартизовані групою IEEE 802.3. Залежно від швидкості передачі, існують різні модифікації: Ethernet, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, 40 Gigabit Ethernet та 100 Gigabit Ethernet.

Для ігрового комп'ютерного клубу, де критично важливі стабільність, низька затримка (ping) та висока пропускна здатність не менше 1 Гбіт/с, абсолютний мінімум для кожної ігрової станції оптимальним вибором буде Gigabit Ethernet.

Технологія Gigabit Ethernet передбачає три типи середовища передачі сигналів Ethernet зі швидкістю 100 Мбіт/с [3]:

- 1000BASE-SX – використовує багатомодове оптоволокно для передачі на короткі відстані (до 550 м) з використанням короткохвильових лазерів (850 нм);

- 1000BASE-LX – використовує одномодове або багатомодове оптоволокно для передачі на довші відстані (до 5 км для одномодового) з використанням довгохвильових лазерів (1300 нм);

- 1000BASE-CX – використовує спеціальні екрановані мідні кабелі Twinax на дуже короткі відстані (до 25 м), зазвичай для з'єднання обладнання в межах однієї стійки;

- IEEE 802.3ab (1000BASE-T) – цей стандарт є найбільш поширеним варіантом Gigabit Ethernet. Він дозволяє передавати дані зі швидкістю 1 Гбіт/с по стандартних кабелях на основі крученої пари.

Для побудови мереж Gigabit Ethernet на невеликі відстані (до 100 метрів) в межах офісу або будівлі, найекономнішим варіантом є використання кабелю крученої пари.

Існують дві основні специфікації для передачі 1 Гбіт/с по міді: 1000BASE-T та 1000BASE-TX:

- 1000BASE-TX вимагає використання кабелів Cat-6 або Cat-7;

- 1000BASE-T є більш гнучким і дозволяє використовувати дешевші кабелі категорій Cat-5, Cat-5e та Cat-6.

З огляду на економічну доцільність, специфікація 1000BASE-T є більш прийнятним вибором для такого типу мереж.

Безпровідний сегмент (Wi-Fi) є доповненням, оскільки не підходить для безпосередньої гри, але є важливим для інших цілей у клубі:

- для відвідувачів, щоб вони могли підключити свої смартфони, планшети або ноутбуки для серфінгу в Інтернет, доступу до соцмереж, стрімінгу тощо;
- для адміністративного персоналу: підключення принтерів, POS-терміналів, робочих планшетів адміністраторів;
- для VR-зон, оскільки деякі VR-системи можуть вимагати стабільного Wi-Fi з низькою затримкою (наприклад, Wi-Fi 6/6E) для бездротової передачі зображення з ПК на шолом.

Рекомендовані технології Wi-Fi 6 (802.11ax) – це поточний стандарт, який забезпечує вищу швидкість, меншу затримку та кращу продуктивність у середовищах з великою кількістю підключених пристроїв, що ідеально для ігрового клубу.

Для ігрового комп'ютерного клубу, основою мережі повинна бути провідна інфраструктура на базі Gigabit Ethernet для ігрових ПК, з можливим використанням 10 Gigabit Ethernet для серверної та магістральної мережі. Wi-Fi 6/6E буде чудовим доповненням для відвідувачів та адміністративних потреб.

Кожна комп'ютерна мережа має логічну та фізичну топології.

Фізична топологія показує, як саме робочі станції з'єднані між собою за допомогою певного виду зв'язку.

Логічна топологія визначає набір правил, які керують взаємодією між робочими станціями в мережі. Недотримання цих правил призведе до порушення роботи всієї мережі.

Фізична топологія мережі описує, як комп'ютери та інші пристрої фізично з'єднані між собою за допомогою кабелів або бездротових зв'язків. Вибір топології впливає на вартість, надійність, продуктивність та простоту обслуговування мережі. Розгляньмо основні типи фізичних топологій:

- шина (Bus). У цій топології всі пристрої підключаються до одного центрального кабелю (шини). Дані, що надсилаються одним пристроєм, поширюються по всій шині, і кожен пристрій "слухає", чи не призначені дані йому. На кінцях кабелю встановлюються термінатори для поглинання сигналу та запобігання його відбиванню. Таку мережу легко монтувати та розширювати, додаючи пристрої до шини. Вимагає менше кабелю, ніж інші топології. Основні недоліком є низька надійність – пошкодження центрального кабелю або одного з термінаторів призводить до виходу з ладу всієї мережі. Також обмежена кількість пристроїв. Зі збільшенням кількості пристроїв зростає ймовірність колізій (зіткнень даних), що знижує продуктивність мережі;

- зірка (Star). Всі пристрої підключаються до центрального мережевого пристрою, такого як комутатор (switch) або концентратор (hub). Коли один пристрій надсилає дані, вони спочатку проходять через центральний пристрій, який потім пересилає їх до пристроя-призначення. Вихід з ладу одного кабелю або пристрою не впливає на роботу решти мережі. Лише пристрій, який від'єднався, втрачає зв'язок. Легко локалізувати проблему, оскільки несправність, як правило, стосується лише одного з'єднання або пристрою. Додати новий пристрій дуже просто, достатньо підключити його до вільного порту на центральному комутаторі. Комутатор дозволяє одночасно передавати дані між кількома парами пристроїв, що значно збільшує пропускну здатність мережі. Основними недоліками більша вартість, адже вимагає значно більше кабелю, оскільки кожен пристрій має окреме з'єднання до центру. Вихід з ладу центрального комутатора або концентратора призводить до зупинки роботи всієї мережі. Комутатори можуть бути дорогими, особливо керовані та високошвидкісні моделі.

- кільце (Ring). Кожен пристрій підключається до двох сусідніх пристроїв, формуючи замкнуте коло. Дані передаються по кільцю в одному напрямку (або в обох, у випадку подвійного кільця) від одного пристрою до іншого, поки не досягнуть місця призначення. Кожен пристрій отримує рівний доступ до мережі, оскільки дані передаються по черзі. Добре підходить для оптичних волокон:

Часто використовується в оптоволоконних мережах на великих відстанях. Основним недоліком є низька відмовостійкість. Якщо кабель розривається або один пристрій виходить з ладу (у простому кільці), це призводить до розриву всього кільця та зупинки роботи мережі. Подвійне кільце вирішує цю проблему, але збільшує вартість. Додавання нового пристрою вимагає розриву кільця та тимчасової зупинки мережі. Як і в шині, визначити місце несправності може бути важко;

- сітка (Mesh). У повній сітковій топології кожен пристрій підключається безпосередньо до кожного іншого пристрою в мережі. Це забезпечує максимальну відмовостійкість та надлишковість. Існують також часткові сіткові топології, де не всі пристрої з'єднані між собою. Основною перевагою є висока відмовостійкість/надлишковість. Якщо один шлях відмовляє, дані можуть бути передані іншим шляхом. Це забезпечує надзвичайно високу надійність. Кількість каналів зв'язку дуже велика. З точки зору безпеки складніше перехопити дані, оскільки є багато шляхів передачі. Оснвоний недолік – винятково висока вартість. Вимагає величезної кількості кабелів та портів (кількість з'єднань зростає експоненційно з кількістю пристроїв). Монтаж та конфігурація такої мережі дуже складні. Практично не використовується для локальних мереж;

- дерево (Tree) / Розширена зірка (Extended Star). Це ієрархічна топологія, яка по суті є розширеною версією топології "зірка". Кілька зіркових топологій підключаються до центральної "кореневої" шини або центрального комутатора вищого рівня. Основна перевага – легко розширювати, додаючи нові "зірки" або гілки до існуючої структури. Простота пошуку несправностей шляхом ізоляції проблем на окремих гілках.

- комбінування переваг шини та зірки. Можливість використання різних типів кабелів та пристроїв на різних рівнях. Основний недолік – залежність від центрального сегмента. Вихід з ладу центрального кабелю або комутатора на вищому рівні може паралізувати значну частину мережі. Дещо складнішае встановлення, аніж проста зірка.

Для ігрового комп'ютерного клубу найоптимальнішою фізичною топологією буде "Розширена зірка". Вона забезпечує високу надійність, легкість масштабування та простоту керування, що є критично важливим для стабільної роботи багатьох ігрових станцій.

При цьому, для логічного поділу мережі та враховуючи територіальне розташування кінцевих вузлів пропонується об’єднати окремими комутаторами робочих груп комп’ютери залу для VIP-клієнтів та окрема для основного залу, ПК адміністраторів, керівника і касирів. Також до другого комутатора буде під’єднано безпровідні точки доступу. Топологічна схема з’єднання мережі комп’ютерного клубу представлена на рисунку 2.1.

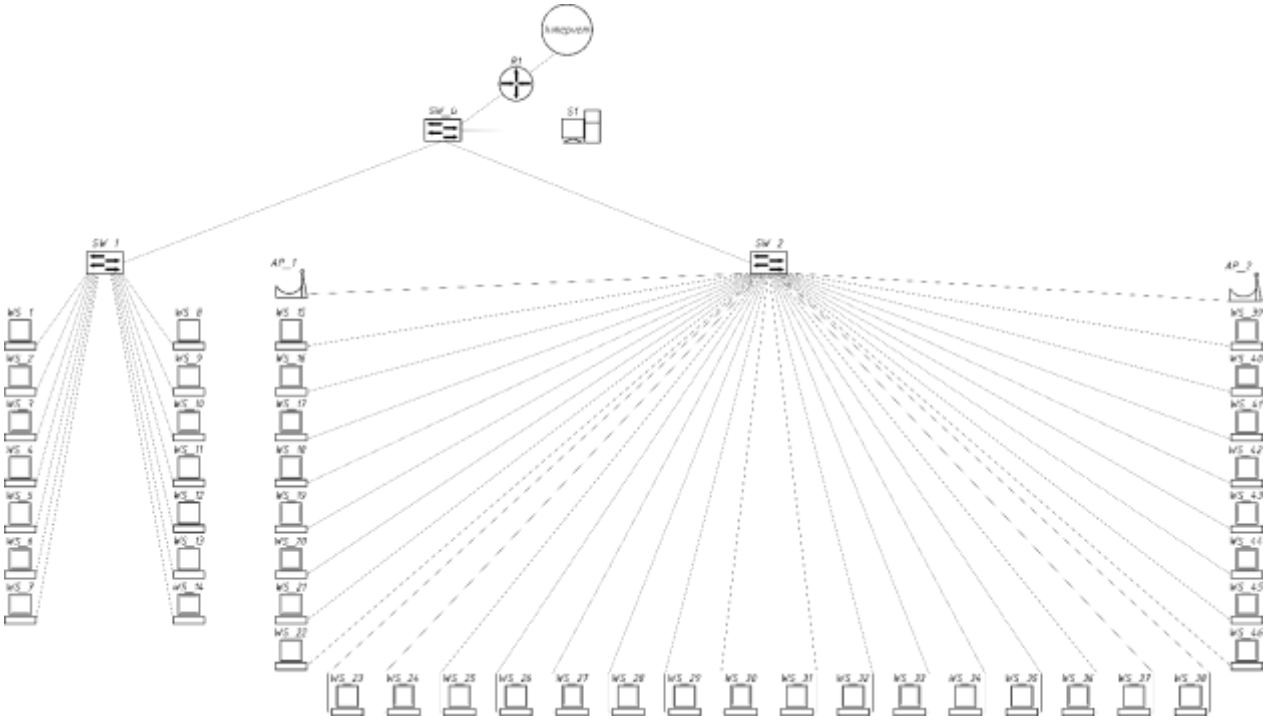

Рисунок 2.1 – Логічна топологія мережі комп’ютерного клуюу “Сталкер”

2.2 Розробка схеми фізичного розташування кабелів та вузлів

Технічне завдання даного кваліфікаційної роботи полягає у розробці комп'ютерної мережі комп’ютерного кдубу, який розташований в частині одного поверхову будівлі із 6-и окремих кімнат та офісного залу для відвідувачів із

перегородками, загальною площею 360 м^2. При цьому довжина приміщення становить 30 м і ширина – 12 м. План будівлі представлено на рисунку 2.2.

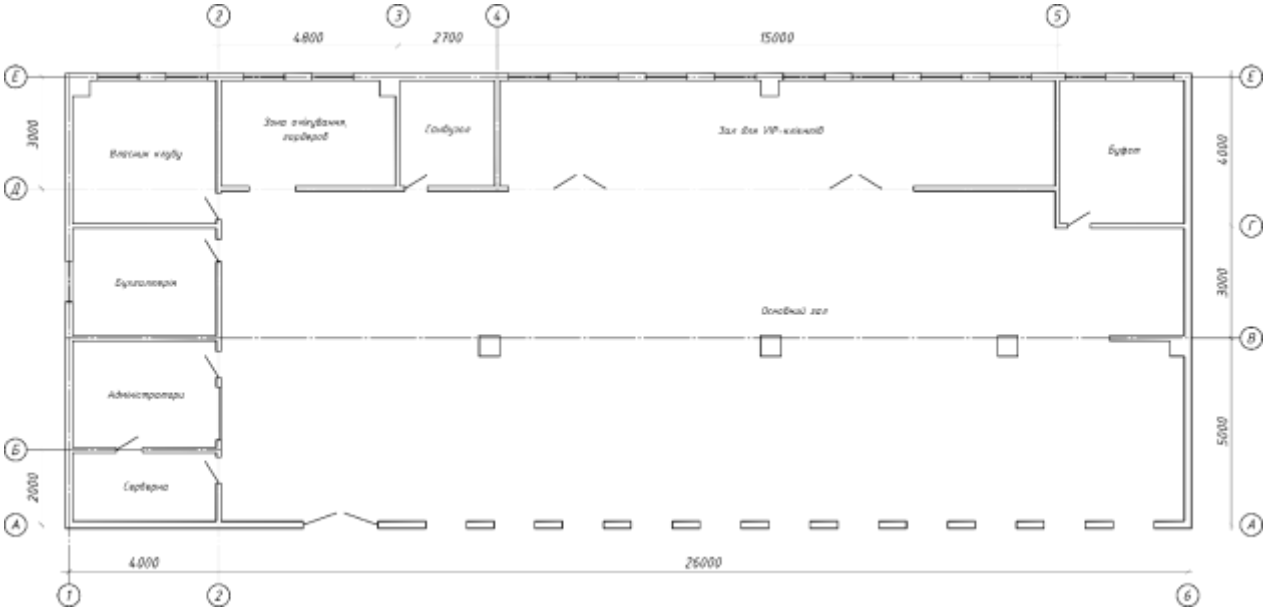

Рисунок 2.2 – План приміщення комп’ютерного клубу

У будівлі потрібно об'єднати в мережу 46 робочих комп'ютерів та окремо виділити одну кімнату під серверну і там розташувати центральне активне мережеве обладнання разом із сервером мережі. Отже, разом із сервером загальна кількість вузлів у мережі становить 47 комп'ютер. Найбільш оптимальним є розташування серверної у кімнаті зі найменшої площею та приблизно однаковою відстанню до найбільш віддалених об'єктів мережі. Таким приміщенням є кімната №4 із розмірами 2 м на 4 м та розміщенням.

Найбільша кількість вузлів розташована у приміщені із найбільшою площею відповідно до рисунку 2.2 у основному залі клубу. Його площа становить:

$$26\text{м} \times 9\text{ м} - 1\text{м} \times 3{,}5\text{м} = 264 - 8 = 231{,}5\text{ м}^2$$

У цьому приміщенні всього буде розташовано 32 комп’ютери. Визначимо, яка площа повинна бути відведена на таку кількість комп’ютерної техніки згідно із рекомендаціями [4]. Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями, затверджених наказом Мінсоцполітики № 207 від 14.02.2018). Відповідно до цих вимого площа приміщення на одне робоче місце повинна становити не менше 6м^2, а об’єм 20 м^3:

$$32 \text{ ПК} \times 6 \text{ м}^2 = 192 \text{ м}^2 < 231{,}5 \text{ м}^2$$

Проведемо перевірку відповідності державним санітарним правилами ДСанПіН 3.3.2.007-98, щодо об'єму приміщення, враховуючи, висота поверху у даному приміщені становить 4м:

$$32 \text{ ПК} \times 20 \text{ м}^3 = 640 \text{ м}^3 < 231{,}5 \text{ м}^2 \times 3{,}2 \text{ м} = 740{,}8 \text{ м}^3$$

Отже, приміщення залу обслуговування клієнтів цілком задовольняє вимогам ДСанПіН 3.3.2.007-98, щодо розміщення в ньому 32 комп'ютерів.

Перевіримо, відповідність інших приміщень санітарним нормам. Для цього необхідно зіставити і розрахувати площі і об'єми необхідні для кожної кімнати, враховуючи кількість ПК, які необхідно розмістити в кімнатах. Відповідно до технічного завдання практичної роботи розподіл робочих станцій по приміщеннях офісу представлено у таблиці 2.1.

Таблиця 2.1 – Параметри приміщень для розміщення кінцевих вузлів

Підрозділ	Кількість робочих місць	S, $м^2$	V, $м^3$
Власник клубу	1	16	56
Бухгалтерія	1	12	42
Адміністратори	2	12	42
Серверна	1	8	28
Зал для VIP-клієнтів	10	60	210
Зал для клієнтів	32	231,5	740,8

Площа і об'єм розраховуються за формулами:

$$S = A \times B, \text{ м}^2 \quad (2.1),$$

$$V = A \times B \times C, \text{ м}^3 \quad (2.2),$$

де А – довжина, В – ширина , С – висота, яка для всіх кімнат однакова і як вже повідомлялось вище дорівнює 3,2 м. Значення ширини і довжини кожної кімнати представлені на плані приміщення, зображеному на рисунку 2.1. Результати розрахунків представлені в таблиці 2.2.

Таблиця 2.2 – Порівняння реальної площі та об’єму приміщень комп’ютерного клубу “Сталкер”із необхідними згідно вимог

Підрозділ	Площі приміщень		Згідно вимог	
	S, м^2	V, м^3	S, м^2	V, м^3
Власник клубу	16	56	6	20
Бухгалтерія	12	42	6	20
Адміністратори	12	42	12	40
Серверна	8	28	4	20
Зал для VIP-клієнтів	60	210	60	200
Зал для клієнтів	231,5	740,8	192	640

Отже, всі запропоновані приміщення будівлі відповідають санітарним вимогам і цілком підходить для проектування мережі згідно із технічного завдання кваліфікаційної роботи.

На рисунку 2.3 представлено розташування робочих станцій та сервера мережі відповідно до технічного завдання. Кожен пристрій буде розташовано на відстані 50 см від стіни. При цьому, вузли нумеруються позначкоюWS (скорочення WorkStation) і числом – порядковий номер ПК, розділеними символом "_".

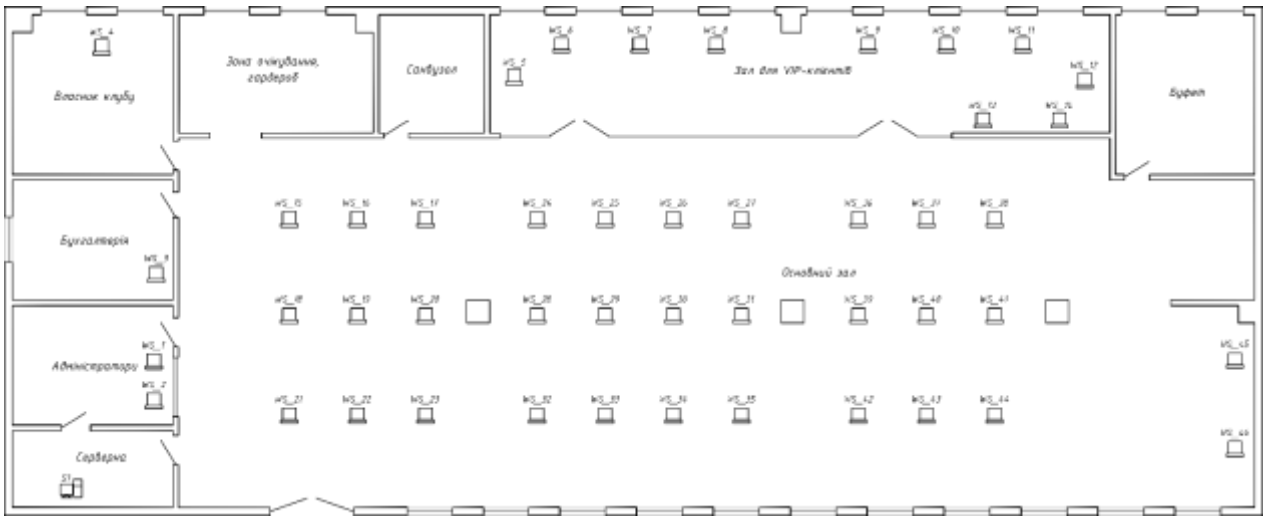

Рисунок 2.3 – Розташування кінцевих вузлів мережі в будівлі комп’ютерного клубу “Сталкер”

Як вже відзначалось мережу слід розділити на логічні сегменти. Також для забезпечення максимальної ефективної швидкості передачі та комутації для VIP-клієнтів необхідно відділити логічну групу пристроїв залу VIP-клієнтів окремим комутатором Sw_1 (див. рис. 2.4).

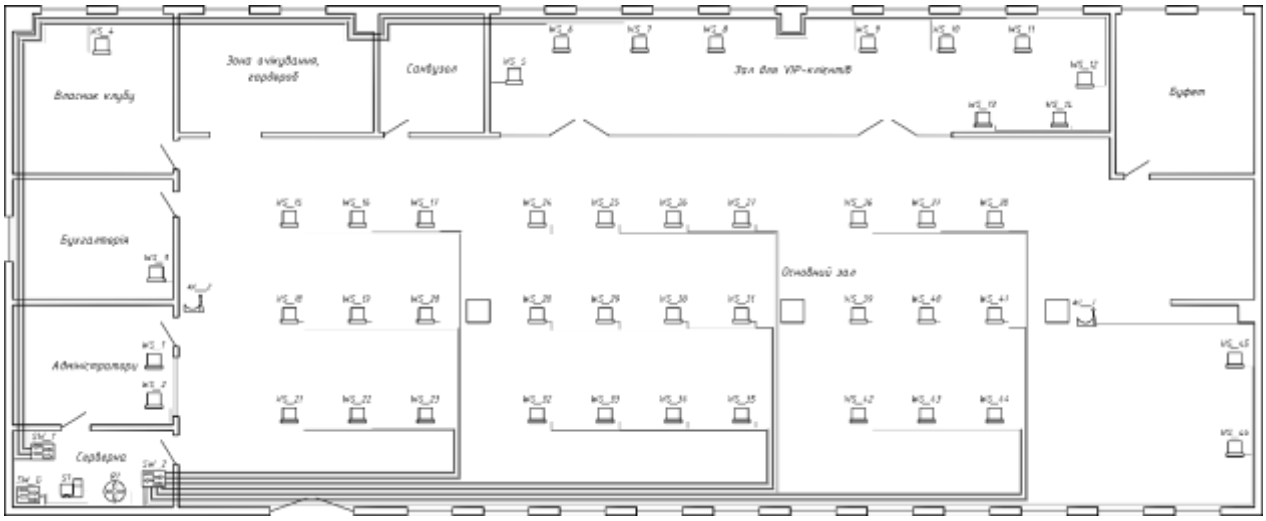

Рисунок 2.4 – Схема фізичного розташування кабелів та вузлів мережі комп’ютерного клубу “Сталкер”

За територіальним принципом до цього ж комутатора необхідно під’єднати робочі станції розташовані в приміщені власника клубу, бухгалтерії та адміністраторів.

Враховуючи параметри розмірів приміщення комп’ютерного клубу, які дозволяють забезпечити допустиму довжину кабеля сегменту мережі та з міркувань кращої безпеки мережевого обладнання усі пристрої активного мережевого обладнання будуть розміщені

До комутатора Sw_2 відповідно необхідно під’єднати комп’ютери основного залу комп’ютерного клубу в кількості 32 (див. рис. 2.4).

Згідно ієрархічної топології обидва сегментуючі комутатори робочих груп Sw_1 та Sw_2 необхідно під’єднати до головного комутатора Sw_G (див. рис. 2.4), який буде здійснювати комутацію та маршрутизацію між підмережами. Для забезпечення кращою швидкості комутації в поєднанні із маршрутизацією

між VLAN вирішено використати для маршрутизації комутатор третього рівня. Для з'єднання між сегментуючими та головним комутаторами, як вже відмічалось в розділі 2.1 слід використати більш швидкісну топологію 10 Gigabit Ethernet. Також, данку технологію рекомендується використати для під'єднаня севреру мережі. Тому сервер буде під'єднано до окремого порту головного комутатора та виділено в окрему віртуальні підмережу.

В серверній кімнаті (див. рис. 2.4) також слід розмістити сервер мережі, під'єднаний до головного комутатора SW_G та маршрутизатор, який буде виконувати функцію шлюзу доступу до Інтернет із мережі комп'ютерного клубу "Сталкер".

Для забезпечення можливості безпровідного доступу до мережі гостей комп'ютерного клубу із мобільних пристроїв (власних ноутбуків, смартфонів, планшетів та ін.) в приміщені основного залу слід розмістити дві точки безпровідного доступу в протилежних кінцях залу (див. рис. 2.4) для забезпечення повного та надійного покриття усієї площі приміщення клубу. Точки доступу також повинні забезпечити з'єднання із POS-терміналами.

Точки доступу слід під'єднати до комутатора Sw_1 (див. рис. 2.4).

2.3 Обґрунтування вибору комунікаційного обладнання

2.3.1 Обґрунтування вибору пасивного мережевого обладнання

Кабель є основним компонентом структурованих кабельних систем, його головна функція – передача електричних або оптичних сигналів між пристроями. Існує безліч видів кабелів з різним функціональним призначенням, розрахованих на експлуатацію в різних умовах.

При виборі кабелю слід враховувати тип мережі, її топологію, а також відповідність стандартам, що відображено в маркуванні кабелю. Сьогодні переважна більшість мереж проектується з використанням неекранованої крученої пари (UTP) та волоконно-оптичних кабелів.

Вибір кабельної системи має ґрунтуватися на вимогах замовника, обраній технології мережі, а також на вартості та можливості подальшої модернізації. Для мережі комп'ютерного клубу "Сталкер", враховуючи обрану технологію Gigabit Ethernet, можна використовувати два типи кабелю крученої пари: категорії 5e або 6.

Для під'єднання комутаторів робочих груп та сервера до головного комутатора вибрано технологію 10 Gigabit Ethernets стандарту 10GBASE-T (IEEE 802.3an). Також даний стандарт слід використати для під'єднання головного комутатора та маршрутизатора.

Кабель категорія 6 (Cat6) може підтримувати 10GBASE-T, але тільки на коротких відстанях, до 55 метрів. На практиці, це може бути навіть менше (37 метрів), залежно від якості кабелю та рівня перехресних перешкод (Alien Crosstalk) від сусідніх кабелів. Враховуючи, що все активне мережеве обладнання буде розміщено в серверній кімнаті, то довжина кабеля не буде перевищувати 5 м (для під'єднання сервера інші сегменти до 2 м), то використання кабель категорія 6 (Cat6) цілком виправдано.

Крім того, замовник вимагає наявності безпровідного доступу до мережевих ресурсів. Тому, для бездротового сегмента проєктується мережа, що використовуватиме стандарт Wi-Fi IEEE 802.11ac, який також підтримує швидкість до 1 Гбіт/с.

З метою мінімізації витрат на розробку мережі та викорситання одного типу кабеля усіх сегментів мережі , в якості основного фізичного середовища передачі даних обрано кабель категорії Cat 6.

Оскільки клуб знаходиться у громадському місці багатолюдному приміщенні готелю, рекомендовано використовувати кабелі з оболонкою LSZH. У разі пожежі такі кабелі виділяють менше диму та не містять галогенів, які утворюють токсичні гази

Для структурованої кабельно системи вирішено вибрати кабель КПВонг-HF-ВП (250) 42X (U/UTP-cat.6 LSOH) виробництва "Одескабель". Його конструктивні особливості включають [12]:

– струмопровідна жила: мідний м'який провідник;

– ізоляція: LSZH;

– діаметр кабеля: 1,05 мм.;

– діаметр: 0,57 мм (23 AWG);

– температурний діапазон під час монтажу від -10 °С до +60 °С;

– температурний діапазон під час експлуатації: від -20 °С до +60 °С;

– радіус вигину не менше 4 зовнішніх діаметрів кабелю;

– відповідність вимогам: EN 50173-1:2002, ISO/IEC 11801:2002, ANSI/TIA/EIA-568-B.2-1-2002, IEC 61156-5:2002.

Для підключення локальної мережі до глобальної мережі Інтернет (у якості магістрального каналу) було обрано оптоволоконний кабель ОПТ-24А4 виробництва "Південкабель". Цей кабель має такі конструктивні особливості [13]:

– тип оптичного волокна: одномодовий з розширеним діапазоном хвиль;

– кількість волокон – 24;

– діаметр кабеля: 10х19±0.5 мм.

Кабелі будуть під’єднувтаись до мережевих розеток.

Найчастіше для офісів, житлових приміщень, комп'ютерних клубів використовуються розетки для прихованої установки (вбудовані в стіну). Вони встановлюються в спеціальні монтажні коробки (підрозетники) у стіні, забезпечуючи естетичний вигляд. Характеристики розеток для прихованої установки Cablexpert RJ-45, 6 cat, (NCAC—HS—SMB2) представлено в таблиці 2.3.

Таблиця 2.3 – Розетка з екраном Cablexpert RJ-45, 6 cat, прихованої установки (NCAC—HS—SMB2) [17]

Характеристика	Значення
Тип розетки	Прихованої утсановки
Матеріал	пластик
Габарити	50х50х30мм

Для підключення комп'ютерів до кабелів, прокладених під підлогою, в основному залі (див. рис. 2.4) використовуються спеціальні підлогові розетки (лючки). Вони встановлюються безпосередньо в підлогу та можуть бути прихованими (висувними) або стаціонарними. Для проектованої мережі вибрано модуль Keystone RJ45 Cat.6 UTP Panduit NetKey NK688MB чорного кольору.

Спеціалізовані підлогові лючки ("підлоговий лючок" або "Floor Box" для офісних або комерційних приміщень) самі по собі не є "розетками" в чистому вигляді, а є корпусом для встановлення модулів Keystone.

Для проектованої мережі потрібно 30 комплектів підлогових розеток для підключення комп’ютерів основного залу (див. рис. 2.4). Решту пристроїв будуть підключатись настінними розетками для прихованої установки.

Для під’єднання мережевого кабелю тип скручена пара використовуються мережеві роз’єми (конектори) стандарту 8P8C (ще називають RJ45). Для даної мережі прийнято рішення використати конектори ATCOM RJ45 CAT.5t UTP 8P8C.

Для встановлення зв'язку маршрутизатора з провайдером послуг Інтернет за допомогою оптичних каналів, необхідно придбати оптичний конектор SC одномодового типу (Single-mode) з діаметром 3 мм.

Ринок мережевого обладнання пропонує великий асортимент вже готовий з’єднувальних кабелів різноманітної довжини. У даній мережі достатньо буде застосування патч-кордів довжиною 1,5 м. Випадку вибрано патч-корд 1м RJ-45 CCA ATCOM.

Для організації та кросування мережевих з'єднань будуть використані 24-портові патч-панелі Panduit категорії 6 (19-дюймові). Ці панелі легко монтуються в серверну шафу або стійку. Вони оснащені конекторами RJ-45, які не потребують спеціальних інструментів для підключення завдяки механізму автоматичного прорізання ізоляції провідників. У комплект поставки входять кріпильні елементи та хомути Colring. Самі патч-панелі повністю відповідають стандарту EIA/TIA 568 B.2-1 [14].

Проведемо розрахунок довжини кабельного з’єднання відповідно до схеми локальної обчислювальної мережі з розташуванням її на плані приміщення представленої на додатку А розрахуємо необхідні довжини кабелів між окремими мережевими вузлами. Результати розрахунків представлені в таблиці Б.1 додатку Б.

Для розміщення мережевого обладнання в серверній буде використано шафу комутаційну висотою 22U, габарити – 600х600х1196мм. Комутаційна шафа містить патч-панелі, маршрутизатор, головний комутатор, комутатори робочих груп Sw_1, Sw_3 та Sw_4, кабельні організатори. В якості моделі вибрано Ipcom CH-4U 600X600 [14] (див. рис. 2.5).

Рисунок 2.5 – Шафа комутаційна серверна Ipcom CH-4U 600X600

Повний перелік пасивного мережевого обладнання пресдтавлено в таблиці 2.4.

Таблиця 2.4 – Вибір пасивного мережевого обладнання для ЛОМ (шафи, патчпанелі, кабельорганайзери)

Назва	Тип	Розмір	Габарит	Кількість, шт
Шафа монтажна Ipcom CH-4U 600X600	Підлогова	600х600	22U	1
Патч панель 1U 24 порта кат. 5E 19"	Стійкова	19"	1U	1

2.3.2 Обґрунтування вибору активного мережевого обладнання

Проектована мережа комп'ютерного клубу "Сталкер" включатиме наступні активні комунікаційні компоненти: головний комутатор, комутатори робочих груп, маршрутизатор та безпровідні точки доступу. Ця конфігурація реалізує топологію розширеної зірки.

Головний комутатор, розташований у серверній кімнаті, виконуватиме роль центрального вузла. Він об'єднуватиме всі пристрої мережі, підключені через сегментуючі комутатори робочих груп. Безпосередньо до головного комутатора також буде під'єднано маршрутизатор, що забезпечує доступ до мережі Інтернет.

Комутатори робочих груп (сегментуючі) створять окремі сегменти мережі, виступаючи як центри зірок у загальній топології розширеної зірки. Кожен із цих комутаторів буде з'єднаний з головним комутатором. Всього в мережі буде використано чотири комутатори робочих груп та один головний комутатор.

Безпровідні точки доступу забезпечують розширення провідної мережі на безпровідні мобільні пристрої клієнтів клубу та для підключення POS-терміналів.

При виборі комутаторів для робочих груп головне – забезпечити достатню кількість портів і відповідну пропускну здатність. Комутатор має мати достатньо інтерфейсів для підключення всіх пристроїв у мережевому сегменті, а також один додатковий порт для з'єднання з головним комутатором.

Згідно з вимогами, кожному користувачу мережі потрібна пропускна здатність не менше 1000 Мбіт/с. Це означає, що порти комутатора мають відповідати стандарту Gigabit Ethernet.

Однак, лінія зв'язку з головним комутатором (UpLink порт) потребує вищої пропускної здатності, щоб сукупно забезпечити потреби всіх робочих станцій. Тому комутатор має підтримувати щонайменше один інтерфейс зі швидкістю 10 Гбіт/с, що відповідає стандарту 10Gigabit Ethernet. Зазвичай, комутатори мають спеціалізований UpLink порт саме для такого типу з'єднання, що дозволяє

підключатися до маршрутизатора або іншого вищого за рівнем пристрою в мережевій структурі, як-от головний комутатор у даному випадку.

Для того щоб комутатор ефективно справлявся з трафіком усіх підключених до нього користувачів, його загальна пропускна здатність має бути достатньою. Щоб розрахувати це значення, необхідно врахувати потребу кожного користувача в пропускній здатності та подвоїти її, оскільки передача даних відбувається в дуплексному режимі (одночасно в обох напрямках).

Наприклад, до комутатора Sw_2 підключається найбільша кількість пристроїв: 32 комп'ютери із основної зали і 2 безпровідні точки доступу. Разом це 34 кінцевих вузли. Таким чином, комутатор має забезпечувати пропускну здатність, розраховану за формулою:

1000 Мбіт/с x 34 вузлів x 2 = 68 000 Мбіт/с = 68 Гбіт/с

Отже, пропускна спроможність комутатора повинна бути не менше 68 Гбіт/с.

Враховуючи ці критерії відбору для робочих груп клієнтів основної зали, Wi-Fi-мережі POS-терміналів та гостьової Wi-Fi мережі вибрано комутатор Cisco SG350X-48MP-K9-EU. Зовнішній вигляд якого представлено на рисунку 2.6.

Рисунок 2.6 – Комутатор для сегментів мережі Cisco SG350X-48MP-K9-EU

Ця модель, має 48 портів Gigabit Ethernet для підключення кінцевих вузлів., також має 4 порти 10 Gigabit Ethernet, з яких 2 є комбінованими (10GBASE-T/SFP+) і 2 є SFP+. Комбіновані порти 10GBASE-T/SFP+ означають, що ви можете використовувати або мідний кабель (RJ45) для 10 Гбіт/с з'єднання, або вставити SFP+ модуль для оптоволоконного з'єднання. Пропускна здатність 176 Гбіт/с, що перевищує розраховану мінімальну необхідну 68 Гбіт/с. Повний

перелік технічних характеристик комутатора Cisco SG350X-48MP-K9-EU представлено у таблиці 2.5 [15].

Таблиця 2.5 – Характеристики комутатора Cisco SG350X-48MP-K9-EU

Характеристика	Значення
Тип пристрою	Комутатор другого рівня L2
Порти LAN	48 x 10/100/1000 Мбіт/с PoE+
Порти Uplink	2 x 10G SFP+, 2 x 10G Combo (RJ45/SFP+)
Пропускна здатність	176 Гбіт/с
Швидкість обробки пакетів	130,94 млн пакетів/сек
Буфер пам’яті	16 Мб
Підтримка VLAN	4096
QoS	Так
Функції безпеки	802.1X, ACL, DHCP Snooping, DoS захист
Розмір, мм	440 x 350 x 44
Вага, кг	5б28
Підтримка PoE	IEEE 802.3af/at (PoE+)
Загальний бюджет PoE	740 Вт

В загальному для мережі потрібно придбати 2 комутатори робочих груп Cisco SG350X-48MP-K9-EU.

Для з'єднання мережевих сегментів, а саме залу обслуговування VIP-клієнтів та підмережі адміністраторів, нам знадобиться комутатор. Він має забезпечити 14 портів стандарту Gigabit Ethernet для підключення кінцевих пристроїв (згідно зі схемою логічної топології, див. рис. 2.1), а також один Uplink порт стандарту 10 Gigabit Ethernet для зв'язку з головним комутатором або маршрутизатором.

З метою уніфікації обладнання та спрощення керування, вирішено використовувати однакові моделі комутаторів для обох цих сегментів.

Отже, розрахуємо необхідну загальну пропускну здатність для такого комутатора:

1000 Мбіт/с х 14 вузлів х 2 = 28000 Мбіт/с = 28 Гбіт/с

Комутатор Cisco SG350X-48MP-K9-EU задовольняє цю пропускну здатність (таблиця 2.5), отже його можна використовувати як сегментуючий комутатор у всіх сегментах мережі.

При виборі головного комутатора будемо керутися тими ж основними критеріями, що й раніше. Згідно зі схемою фізичної топології мережі (див. рис. 2.4), до цього комутатора підключаються: два сегментуючі комутатори, сервер та маршрутизатор.

Таким чином, сумарно потрібно 4 інтерфейси. Важливо, що пропускна здатність Uplink портів сегментуючих комутаторів становить 10 Гбіт/с, тому LAN порти головного комутатора, до яких вони підключаються, також мають забезпечувати таку ж пропускну здатність (10 Гбіт/с).

Для визначення необхідної пропускної здатності головного комутатора, ми повинні врахувати загальну кількість усіх кінцевих вузлів мережі. Завданням передбачено 49 пристроїв (46 робочих станцій, 2 безпровідні точки доступу та один сервер).

Отже, пропускну здатність комутатора розраховуємо, множачи кількість користувачів на їхні індивідуальні потреби в пропускній здатності та на два (для врахування дуплексної передачі) плюс пропускну здатність для сервера 10 Гбіт/с:

1000 Мбіт/с х 48 вузлів х 2 + 10000 Мбіт/с х 2 = 116 000 Мбіт/с = 116 Гбіт/с

Щоб оптимізувати мережевий трафік та підвищити безпеку, ми плануємо розділити мережу на логічні сегменти за допомогою VLAN. Для реалізації такої функціональності, головний комутатор має підтримувати керування рівня 3 (L3). Це дозволить йому маршрутизувати трафік між різними VLAN-ми, що є ключовим для ефективного та захищеного мережевого середовища. Найкращий варіант для вимо даної мережі бууде комутатор C9200CX-8UXG-2X-E, зовнішній вигляд якого представлено на рисунку 2.7.

Рисунок 2.7 – Головний комутатор C9200CX-8UXG-2X-E

Цей комутатор обладнаний 4 портами 10G Ethernet (Multigigabit) RJ45 PoE+ та 4 портами 1G Ethernet RJ45 PoE+. Тобто, є 4 необхідні вбудовані 10G RJ45 порти. Додатково має 2 порти 10G SFP+ для оптичного Uplink. Комутаційна здатність 128 Гбіт/с. перевищує потрібну 116 Гбіт/с.

Цей комутатор дозволяє зберегти простоту традиційної комутації локальних мереж і при цьому розгорнути інтелектуальні мережеві послуги, такі як QoS, обмеження швидкості передачі даних, списки контролю доступу (ACL), управління мультимовленням та високопродуктивна IP-маршрутизація. Завдяки технології Cisco Express Forwarding (CEF) серія Catalyst 3560-CX забезпечує високопродуктивну маршрутизацію трафіку IP [16].

Повний перелік технічних характеристик комутатора C9200CX-8UXG-2X-E представлено у таблиці 2.6 [17].

Таблиця 2.6 – Характеристики комутатора C9200CX-8UXG-2X-E

Характеристика	Значення
1	2
Тип пристрою	Комутатор третього рівня L3
Порти LAN	4 x Gigabit Ethernet (RJ-45 1000 Мбіт/с) 4 x 10 Gigabit Ethernet (RJ-45 10000 Мбіт/с)
Порти Uplink	2x 10 Gigabit Ethernet (SFP+ 10000 Мбіт/с)
Тип Uplink портів	2 x 10G SFP+
Пропускна здатність	128 Гбіт/с
Продуктивність маршрутизації	95,23 Mpps

Продовження таблиці 2.6

1	2
Пам'ять	DRAM 512 МБ / Flash 128 Мб
Підтримка протоколів	IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z
Кількість VLAN	32000
Міжмережевий екран	Присутній
Розмір, мм	269 x 244 x 44
Вага	3,18 кг
Живлення	230 В, 35,2 Вт

Оскільки маршрутизатор забезпечуватиме підключення локальної мережі до Інтернет-провайдера за допомогою оптоволоконного кабелю, ключовим критерієм його вибору є наявність SFP-модуля.

З урахуванням цих вимог, було прийнято рішення обрати маршрутизатор Cisco ISR4221/K9. Його зовнішній вигляд представлений на рисунку 2.8.

Рисунок 2.8 – Зовнішній вигляд маршрутизатора Cisco ISR4221/K9

Цей маршрутизатор оснащений двома SFP-портами та двома Gigabit Ethernet LAN-портами (RJ-45). Для подальшого розширення можливостей він має два додаткові слоти для інтерфейсних модулів NIM.

Пристрій вирізняється високою продуктивністю, забезпечуючи швидкість передачі даних до 10 Гбіт/с. Він обладнаний 4 ГБ оперативної пам'яті, яку можна розширити до 16 ГБ, та має 4 ГБ вбудованої флеш-пам'яті для зберігання даних.

Маршрутизатор підтримує VPN-сервіси та широкий спектр мережевих протоколів, включаючи NAT, RIP v1/v2, OSPF, EIGRP, BGP, PBR та PfR. Він також повністю підтримує роботу з адресацією як IPv4, так і IPv6.

Характеристики маршрутизатора представлено в таблиці 2.7 [17].

Таблиця 2.7 – Розподіл комп'ютерів по приміщеннях офісу

Характеристика	Значення
1	2
Серія продукту	4000
Модель продукту	4221
Кількість вбудованих портів GE SFP	2
Кількість вбудованих портів RJ-45 GE	2
Розмір	43,7 x 32,2 x 25,4 мм
Вага	3,22 кг
Живлення	230 В

Для основної зали комп'ютерного клубу "Сталкер" необхідно розгорнути бездротову мережу за допомогою двох точок доступу. Це оптимальне рішення, адже воно дозволяє пристроям підключатися до Wi-Fi і одночасно мати кабельне з'єднання зі збереженням статичної IP-адреси. Такий підхід усуває потребу в маршрутизаторі чи мості, які б просто розширювали існуючу дротову мережу. Також важливо щоб пристрій підтримував стандарт і пропускну здатність Gigabit Ethernet.

Для цієї мети вирішено обрати TP-LINK EAP225 (див. рис. 2.9). Вона ідеально підходить для невеликих офісів завдяки відмінному поєднанню характеристик і ціни, а також простоті монтажу на стіну чи стелю.

Рисунок 2.9 – Точка доступу TP-LINK EAP225

Цей пристрій має один Gigabit Ethernet порт (RJ45), який підтримує PoE (802.3af/at) для зручного живлення та розміщення. Бездротовий стандарт, що підтримує Wi-Fi 5 (802.11ac), зі швидкістю до 867 Мбіт/с на 5 ГГц та 450 Мбіт/с на 2.4 ГГц.

TP-LINK EAP225 це двосмугова точка доступу, яка забезпечує кращу продуктивність у середовищах з високою щільністю клієнтів. Ідеально підходить для офісів, готелів або комп'ютерних клубів. Також, що важливо EAP225 пропонує відмінний баланс між продуктивністю Wi-Fi 5.

Безпровідна точка доступу TP-Link EAP225 має елегантний дизайн, що нагадує світильник, тому легко впишеться в будь-яке офісне середовище. Ця точка доступу не потребує окремого кабелю живлення, адже підтримує живлення за стандартом PoE (Power over Ethernet). Важливою перевагою EAP225 є підтримка аутентифікації користувачів, що дозволяє ефективно контролювати доступ до мережі.

Адміністратори мережі можуть зручно керувати кількома точками доступу за допомогою програмного забезпечення EAP Controller. Це програмне забезпечення забезпечує централізований контроль над бездротовими мережами.

2.4 Особливості монтажу мережі

Розгортання локальної мережі для комп'ютерного клубу "Сталкер" буде виконано в кілька етапів. Необхідно дотримуватися всіх встановлених стандартів і врахувати особливості планування приміщень. Загальну структуру та

взаємозв'язки всіх вузлів мережі можна знайти на схемах рисунку 2.4. Для створення локальної мережі обрано неекрановану кручену пару категорії 6.

Щоб відповідати стандартному обмеженню у 100 метрів між кінцевим пристроєм та мережевим комутатором, довжина основних кабельних сегментів (від розетки до патч-панелі) не повинна перевищувати 90 метрів. Це залишає 10 метрів для використання коротких патч-кордів: один для з'єднання розетки з робочою станцією, а інший – для підключення патч-панелі до комутатора. Згідно аналізу таблиці Б.1, додатку Б можна зробити висновок, що всі сегменти мережі цілком відповідають цій вимозі.

Кабельні сегменти всередині кімнат будуть прокладені в настінних кабельних коробах розміром 50х40 мм і підключені до мережевих розеток RJ-45. Ці розетки будуть встановлені на зручній висоті, що відповідає рівню робочого столу користувача.

У приміщені основної зали для комп’ютерів розміщених посередині зали (загальна кількість 30 ПК), прокладання буде здійснено під підлоговим покриттям, де використовується фальшпідлога. Прокладання під підлогою має свої специфічні вимоги та норми. В Україні ці вимоги регулюються низкою нормативних документів, зокрема ПУЕ (Правила улаштування електроустановок), ДБН В.2.5-56:2014 (Державні будівельні норми), а також відповідні стандарти (ДСТУ EN 50085-2-2:2015:).

Кабелі повинні мати відповідні показники пожежної безпеки (наприклад, не поширювати горіння, мати низьке димоутворення та токсичність продуктів горіння), особливо у місцях масового перебування людей. Це маркування LSZH (Low Smoke Zero Halogen) або відповідне.

Лотки повинні бути металевими (перфоровані або неперфоровані) або ПВХ. Вони забезпечують вентиляцію, захист від механічних пошкоджень та зручність обслуговування. У зв’язку із потенційним ризиком пошкодження гризунами, необхідно передбачити додатковий захист (металеві лотки, броньовані кабелі або кабелепроводи). В даному випадку буде вибрано металічні лотки.

Кабелепроводи повинні бути надійно закріплені до конструкцій опор фальшпідлоги, щоб уникнути провисання, зміщення та механічного навантаження на них.

Необхідно дотримуватися мінімально допустимих радіусів вигину кабелів, щоб не пошкодити жили та ізоляцію, що може призвести до погіршення характеристик або виходу з ладу. Для витої пари це зазвичай 4-8 зовнішніх діаметрів кабелю.

Усі кабелі повинні бути чітко промарковані на кінцях та через певні проміжки (зазвичай не більше 5-10 метрів), вказуючи їхнє призначення та місце призначення. Це спрощує обслуговування, діагностику та подальші зміни.

У місцях перетину стін, колон або інших перешкод кабелі повинні бути захищені за допомогою ПВХ труб або інших захисних елементів, що запобігають механічним пошкодженням під час монтажу та експлуатації.

В основній залі комп'ютерного клубу використовуються підлогові розетки. За допомогою спеціального інструменту (коронки або пили) у плиті фальшпідлоги вирізається отвір відповідного діаметру/розміру для монтажного лючка розетки. Краї отвору мають бути чистими та рівними. Кінець кабелю виводиться через трубу до місця встановлення лючка з необхідним запасом для подальшого монтажу.

Встановлюється монтажний лючок підлогової розетки у підготовлений отвір і надійно закріплюється (зазвичай гвинтами або спеціальними затискачами). Кабель зачищається, і його жили розкладаються та підключаються до відповідних контактів модуля RJ45 відповідно до обраної схеми (T568A/B). Залишки жил обрізаються. Модуль RJ45 встановлюється у рамку лючка [8].

Кабелі, що ведуть до бездротових точок доступу, будуть інтегровані у підвісні гофровані лотки з внутрішньою розділювальною перегородкою, розташовані над підвісною стелею.

Для захисту кабелю та забезпечення безпеки прокладання, перетин стін виконуватиметься через ПВХ трубки діаметром 16 мм. Розташування та

необхідні діаметри отворів детально вказані на монтажній схемі кабельних мереж (див. рис. 2.4).

З метою ефективної організації та впорядкування всіх мережевих кабелів, все активне мережеве обладнання в серверній буде розміщено у комутаційній шафі, де також будуть задіяні патч-панелі та відповідні патч-корди.

Лотки мають бути надійно закріплені до конструкцій стелі, дотримуючись безпечних інтервалів та відстаней від інших комунікацій.

Для перетину кабелями стін обов'язково використовуються ПВХ трубки діаметром 16 мм. Це забезпечує захист кабелю від гострих країв стін, вологи та механічних впливів, а також дозволяє за потреби легше замінити кабель.

Отвори для цих трубок повинні бути просвердлені строго відповідного діаметру у місцях, що позначені на монтажній схемі кабельних мереж (додаток В), для точного та безпечного прокладання.

Мережеві розетки 8P8C встановлюються біля робочих місць користувачів, переважно на стіні. Розетки проєктуються на рівні робочого столу користувача комп'ютера для максимальної зручності підключення та мінімізації ризику пошкодження кабелів.

Кабелі повинні бути правильно обтиснуті та підключені до розетки згідно з обраним стандартом (наприклад, T568B), що забезпечує роботу мережі [8].

Після завершення прокладання кабельних систем та монтажу розеток, необхідно перейти до встановлення та підключення активного мережевого обладнання в комутаційних шафах.

Спочатку буде виконано монтаж патч-панелей Panduit (19 дюймів, 24 порти, категорія 6) у комутаційних шафах. До цих патч-панелей будуть підключені всі прокладені кабельні сегменти, використовуючи конектори з автоматичним прорізанням ізоляції провідників для забезпечення надійного контакту.

Далі в комутаційні шафи буде встановлено таке обладнання: маршрутизатор (Cisco ISR4221/K9), головний комутатор Sw_G (Cisco C9200CX-8UXG-2X-E), два сегментуючих комутатори Sw_1 та Sw_2 (Cisco SG350X-48MP-K9-EU) та блок безперебійного живлення, для забезпечення стабільної роботи обладнання.

Для впорядкування та акуратного укладання всіх мережевих кабелів слід використати кабельні організатори.

Наступний крок передбачає повну комутацію кабельних систем та підключення всіх мережевих пристроїв. Це включає:

- з'єднання патч-панелей з комутаторами. Порти патч-панелей будуть підключені до відповідних портів комутаторів за допомогою патч-кордів;

- підключення сегментуючих комутаторів. Всі комутатори сегментів будуть під'єднані до центрального комутатора;

- з'єднання центрального комутатора з маршрутизатором. Це забезпечить маршрутизацію між VLAN та доступ до Інтернету.

- підключення сервера. Сервер буде під'єднано до окремого порту маршрутизатора;

- підключення до провайдера. На маршрутизатор буде встановлено одномодовий оптичний конектор SC (3 мм) для зв'язку з інтернет-провайдером.

- розміщення точки доступу. Бездротова точка доступу TP-LINK EAP110 буде розміщена на стелі в приміщенні оснвоної зали, використовуючи живлення PoE (Power over Ethernet)

Дотримання цих детальних вимог до прокладання кабелів — це ключ до створення надійної, високопродуктивної та легко керованої мережевої інфраструктури комп'ютерного клубу "Сталкер".

2.5 Планування IP-адресації пристроїв

Для локальної мережі комп’ютерного клуюу вирішено виділити приватну IP-адресу класу C 192.168.0.0/24.

Щоб локалізувати мережевий трафік і зменшити навантаження на головний комутатор, а також підвищити загальну безпеку мережі, ми вирішили розділити її на віртуальні підмережі (VLAN). Відповідно, план адресації всіх пристроїв буде розроблятися з урахуванням цієї нової підмережевої структури.

Необхідно розділити дві окремі підмережі для клієнтів (Clients) та VIP-клієнтів (Vip) комп’ютерного клубу. Також в окрему підмережу слід об’єднати комп’ютери власника клубу, бухгалтера, адміністраторів клубу (Adm). Також окрема підмережа буде виділена для POS-терміналів, які підключаються через бузпровідну мережу Wi-Fi (Pos). Та ще одна підмережа для безпровідного підключення мобільних пристроїв відвідувачів клубу (Guest). Окрему підмереже також слід виділити для підключення севера (Serers).

Для комп'ютерного клубу "Сталкер" критично важливо забезпечити надійну та безпечну роботу POS-терміналів (Point of Sale), оскільки вони є серцем фінансових операцій. Ми виділимо ці термінали в окрему віртуальну підмережу (VLAN), що підключатиметься через бездротову мережу Wi-Fi. Таке рішення має кілька значних переваг:

- створення окремого VLAN для POS-терміналів гарантує, що їхній трафік буде повністю ізольований від інших сегментів мережі (наприклад, клієнтського Wi-Fi або адміністративної мережі). Це значно підвищує безпеку, мінімізуючи ризики несанкціонованого доступу чи перехоплення конфіденційних платіжних даних;

- L3-комутатор (Cisco C9200CX-8UXG-2X-E) буде налаштований з чіткими правилами фаєрволу. Це означає, що доступ до POS-терміналів буде дозволено лише з необхідних джерел (наприклад, банківських шлюзів, серверів обліку) та лише за певними портами. Весь інший трафік буде блокуватися.

Для підключення POS-терміналів вирішено зарезервувати 10 IP-адрес, а для гостьової Wi-Fi мережі 42 IP-алреси, щоб забезпечити максимально можливу кількістю відвідувачів додатковим безпровідним каналом з’єднання.

Для ефективнішого використання адресного простору та з метою економії вирішено застосувати маски змінної довжини (VLSM). Це дозволить оптимізувати розподіл IP-адрес, використовуючи безокласову адресацію (CIDR).

При розробці плану адресації, будуть призначатися маски змінної довжини для підмереж, починаючи з тих, що потребують найбільшої кількості вузлів. Такий підхід допоможе уникнути перекриття адресних просторів та забезпечити

гнучкість. Спочатку слід визначити необхідну кількість IP-адрес для кожної мережі з урахуванням кількості комп'ютерів, а також додаючи по одній IP-адресі для шлюзу до зовнішньої мережі.

Загальна кількість вузлів у мережі становить 49 для підключень по кабелю та 52 для бездротових пристроїв. Детальний перелік підмереж з необхідною кількістю IP-адрес наведено в Таблиці 2.8.

Розпочнемо з найбільшої підмережі – Guests, яка потребує 43 адреси. Щоб забезпечити цю кількість, потрібен мінімальний блок адрес із 64 адресами.

Таблиця 2.8 – Необхідна кількість IP-адрес в підмережах

Clients	Vip	Adm	Pos	Guests	Servers
32+1=33	10+1=11	4+1=5	10+1=11	42+1=43	1+1=2

Для цього обчислюємо останній октет маски підмережі: 256−64=192. Таким чином, маска підмережі буде 255.255.255.192. Це означає, що в останньому октеті маски підмережі шість старших бітів відведено для мережевої частини адреси.

Отже, адреса підмережі Guests буде 192.168.0.0/26. Доступний адресний простір для вузлів у цій підмережі становитиме від 192.168.0.1 до 192.168.0.62, а широкомовна адреса буде 192.168.0.63.

Наступною за необхідною кількістю IP-адрес є підмережа Clients кількістю 33 адреси. Для забезпечення їх кількості, теж потрібен мінімальний блок із 64 адресами.

Обчислюємо останній октет маски підмережі: 256-64=192. Таким чином, маска підмережі буде 255.255.255.192. Це означає, що в останньому октеті маски підмережі шість старших бітів відведено для мережевої частини адреси.

Отже, адреса підмережі Clients буде 192.168.0.64/26. Доступний адресний простір для вузлів у цій підмережі становитиме від 192.168.0.65 до 192.168.0.126, а широкомовна адреса буде 192.168.0.127.

Подібним чином визначаються адресний простір та маска для інших підмереж. Результати розрахунків розподілу на підмережі представлені в таблиці 2.9.

Відповідно до таблиці 2.9 всього вільних адрес в мережі – 55, що дозволить в майбутньому розширити мережу. Також залишились невикористані мережні адреси в діапазоні 192.168.0.172 до 192.168.0.254.

Для безпосереднього призначення IP-адрес кінцевим пристроям введемо правило, що у кожній підмережі остання адреса буде призначена шлюзу, тобто віртуальному інтерфейсу головного комутатора через який буде здійснюватися маршрутизація між віртуальними мережами.

Таблиця 2.9 – Планування IP-адрес для підмереж

Назва підме-режі	Кіль-кість вузлів	Обчислення останнього октету	Доступ-на к-сть адрес	Адреса підмережі	Діапазон адрес для вузлів	Широкосм угова адреса
Guests	43	256-64 =192	62 (вільно 19)	192.168.0.0/ 26	192.168.0.1— 192.168.0.62	192.168.0.63
Clients	33	256-64 =192	62 (вільно 29)	192.168.0.64/ 26	192.168.0.65— 192.168.0.126	192.168.0.127
Vip	11	256-16 =240	14 (вільно 3)	192.168.0.128/ 28	192.168.0.129 —192.168.0.142	192.168.0.143
Pos	11	256-16 =240	14 (вільно 3)	192.168.0.144/ 28	192.168.0.145 —192.168.0.158	192.168.0.159
Adm	5	256-8=248	6 (вільно 1)	192.168.0.160/ 29	192.168.0.161 —192.168.0.166	192.168.0.167
Servers	2	256-4=252	2 (вільно 0)	192.168.0.168/ 30	192.168.0.169 —192.168.0.170	192.168.0.171

2.7 Тестування та налагодження мережі

Тестування та налагодження мережі є критично важливим етапом після фізичного розгортання та початкового налаштування. Його мета — переконатися, що мережа працює стабільно, ефективно та відповідає всім проектним вимогам. Для комп'ютерного клубу, де стабільність і швидкість з'єднання є ключовими, це особливо актуально.

Першим етапом тестування є перевірка кабельної системи, яка виконується спочатку як візуальний огляд цілісності, а після того тестування електричних з’єднань в кабелях.

Використання професійних кабельних тестерів (наприклад, Fluke Networks CableAnalyzer) для перевірки кожної лінії крученої пари (RJ45) на відповідність стандартам Категорії 6. Це включає перевірку:

- довжини кабелю. Переконатися, що довжина не перевищує 90 метрів до патч-панелі;
- цілісності проводів. Відсутність обривів або коротких замикань;
- схеми розводки. Перевірка відповідності стандартам T568A/B;
- перехресних наведень (Crosstalk). Вимірювання NEXT (Near-End Crosstalk) та FEXT (Far-End Crosstalk);
- затухання (Attenuation). Перевірка ослаблення сигналу в кабелі;
- повернення втрат (Return Loss). Вимірювання відбиття сигналу.

Для SFP/SFP+ з'єднань (наприклад, маршрутизатора до провайдера), перевірка рівня оптичного сигналу (Tx/Rx power) за допомогою оптичного тестера або вбудованих функцій обладнання. Перевірка цілісності оптичних волокон.

Налагодження та тестування мережевого обладнання

- завантаження конфігурацій на маршрутизатор (Cisco ISR4221/K9), головний комутатор (Cisco C9200CX-8UXG-2X-E) та сегментуючі комутатори (Cisco SG350X-48MP-K9-EU);

- перевірка коректності створення та призначення VLAN (для клієнтів, VIP, адміністрації, POS-терміналів, гостьового Wi-Fi) на всіх комутаторах.

Тестування маршрутизації:

- перевірка зв'язку між пристроями в різних VLAN через маршрутизатор. Використання команд ping, traceroute;

- перевірка виходу в Інтернет з усіх підмереж. Тестування NAT.

Тестування сервісів та бзепеки:

- перевірка коректності видачі IP-адрес DHCP-сервером та роботи DNS-серверів;

- перевірка пріоритизації трафіку для критичних сервісів (наприклад, POS-терміналів), якщо налаштована.

Тестування бездротової мережі (Wi-Fi):

- перевірка покриття та потужності сигналу. Використання спеціалізованих програм для аналізу Wi-Fi (наприклад, InSSIDer, Ekahau Site Survey) для визначення рівня сигналу (RSSI), перешкод та "мертвих зон" у приміщенні;

- тестування роумінгу. Перевірка безшовного переключення клієнтських пристроїв між точками доступу (для двох EAP110) без розриву з'єднання;

- тестування SSID та безпеки. Перевірка доступності всіх налаштованих SSID (для POS-терміналів, гостьової мережі), коректності налаштувань безпеки (WPA2-Enterprise/PSK, WPA3);

- перевірка роботи аутентифікації користувачів;

- тестування ізоляції клієнтів. Переконатися, що клієнти гостьової мережі ізольовані один від одного та від інших сегментів мережі.

Тестування сервісів та безпеки

- тестування POS-терміналів. Перевірка стабільності та швидкості проведення транзакцій;

- тестування фаєрволу та правил доступу. Перевірка коректності блокування небажаного трафіку та дозволу необхідного (наприклад, доступ до POS-терміналів лише з визначених джерел);

- навантажувальне тестування. Симуляція навантаження на мережу (наприклад, одночасне підключення багатьох клієнтів, активний трафік) для оцінки продуктивності та виявлення потенційних "вузьких місць".

Останній етап – це моніторинг та документування, який включає:

- налаштування системи моніторингу (SNMP, NetFlow) для відстеження стану мережевих пристроїв, завантаження каналів, помилок та інших важливих показників у реальному часі;

- створення детальних звітів про результати тестування, виявлені проблеми та їх вирішення. Оновлення мережевої документації (схем, конфігурацій) відповідно до фінальних налаштувань.

Цей комплексний підхід до тестування та налагодження забезпечить високу надійність та продуктивність мережі комп'ютерного клубу, що є критично важливим для його успішної роботи.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування програмного забезпечення серверів

Цей розділ містить інструкції щодо налаштування ключового програмного забезпечення серверів, необхідного для функціонування мережі комп'ютерного клубу "Сталкер". Ефективна конфігурація цих служб забезпечить стабільну роботу клієнтських машин, централізоване управління та безпеку.

Для комп'ютерного клубу критично важливо мати централізовану систему управління робочими станціями. Прикладами такого ПЗ є "Сам себе администратор" (SSA), "SmartShell", "GameClass" або подібні.

Спочатку необхідно встановити операційну систему сервера. Для комп’ютернго клубу рекомендується серверна операційна система на платформі Windows. В даному випадку буде використано ОС Microsoft Windows Server 2022.

Часто ігрове програмне забезпечення використовує базу даних (наприклад, MS SQL Server, MySQL). Необхідно провести її встановлення та початкову конфігурацію, створити користувача з необхідними правами доступу.

Далі необхідно відкрити необхідні порти на фаєрволі сервера для взаємодії з клієнтськими машинами та адміністративними клієнтами.

Для централізованого управління обліковими записами, правами доступу та політиками безпеки в адміністративній мережі слід встановити "Active Directory Domain Services.

Щоб розгорнути контролер домену, спочатку потрібно встановити на сервері ролі DNS-сервера та Active Directory Domain Services.

Для цього виконайте такі кроки:

- відкрити Server Manager (рсиунок 3.1);
- перейти на вкладку Manage та обрати пункт Add Roles and Features;
- у першому вікні Майстра встановлення ролі та служби натиснути Next;
- у вікні Installation Type вибрати Role-based or feature-based installation;

- у наступному вікні, Select a server from the server pool, обрати потрібний сервер зі списку та натиснути Next;

- у четвертому вікні Майстра обрати ролі для встановлення на вибраний сервер. У нашому випадку, зі списку достатньо вибрати DNS Server та Active Directory Domain Services (див. рис. 3.1).

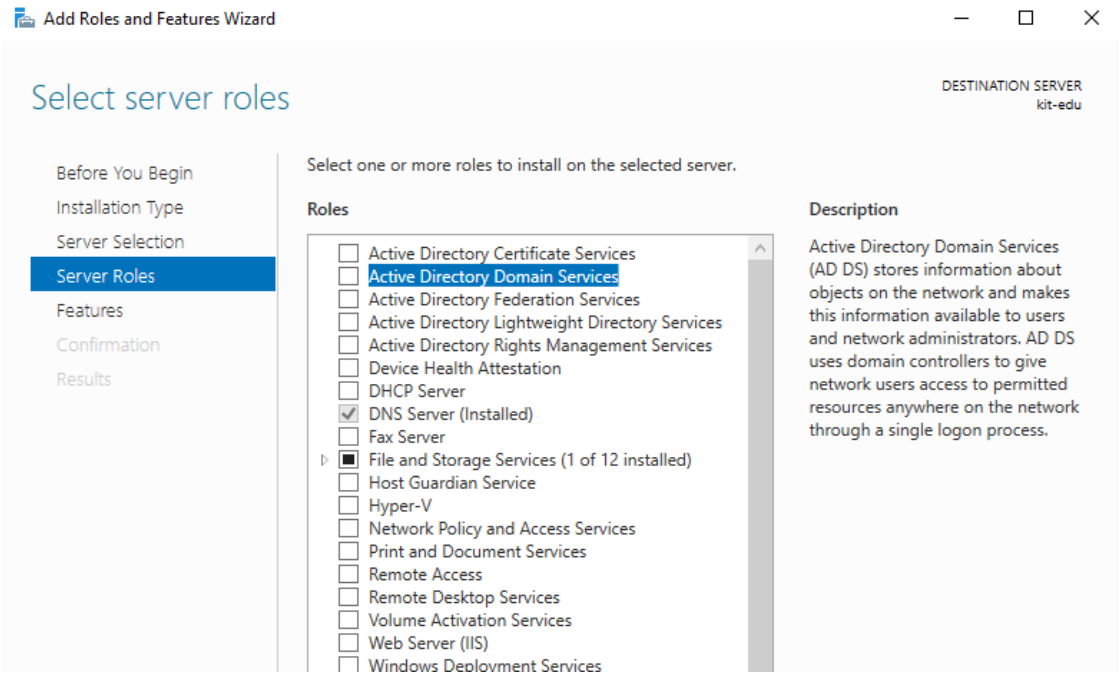

Рисунок 3.1 – Вибір ролей для встановлення

- після натискання Next з'явиться додаткове вікно з ієрархічним списком компонентів для встановлення. Перевіривши його, натиснути Add;

- далі відкриється інформаційне вікно, де слід натиснути Next. Після цього з'явиться останнє вікно, в якому натиснути Install. Розпочнеться процес встановлення.

Після завершення встановлення ролі Active Directory Domain Services необхідно налаштувати її та підвищити цей сервер до доменного контролера. Для цього у вікні Server Manager необхідно натиснути на піктограму прапорця з жовтим трикутником та оберіть опцію Promote this server to a domain controller (див. рис. 3.2).

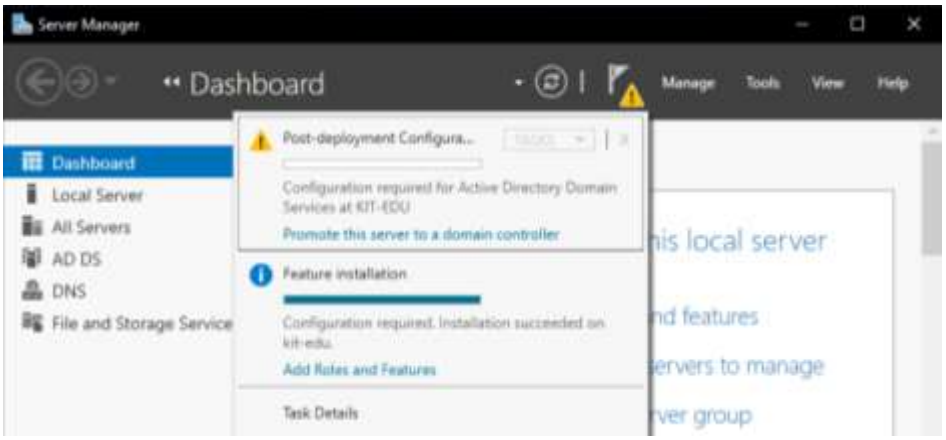

Рисунок 3.2 – Підвищення ролі сервера до доменного контролера

Відкриється перше вікно (див. рис. 3.3), де для створення нового лісу доменів потрібно вибрати опцію Add a new forest та в полі Root domain name вказати назву кореневого домену – stalker.chortkiv.net.

Рисунок 3.3– Створення нового лісу доменів

У наступному вікні, в розділі Type the Directory Services Restore Mode (DSRM) password, потрібно двічі ввести надійний пароль для режиму відновлення служб каталогів. Тут також слід обрати функціональні рівні для кореневого домену: Forest functional level (Режим роботи лісу) та Domain functional level (Режим роботи домену). Крім того, обов'язково відмітьте опції для підключення DNS-сервера (Domain Name System (DNS) server) та глобального каталогу доменних імен (Global Catalog (GC)).

У подальшому вікні є можливість налаштувати делегування служби DNS іншим серверам за допомогою опції Create DNS delegation (Створити делегування DNS). У даному випадку, не потрібно активувати цю опцію.

У третьому вікні Additional Options слід вказати NetBIOS-ім'я для старих комп'ютерних систем, що працюють під Windows NT. Це ім'я не повинно повторюватися з іншими NetBIOS-іменами і має містити до п'ятнадцяти символів. Оскільки ім'я “stalker.chortkiv.net" вже використовується самим сервером, обрано "stalkerchortkiv ".

У вікні Path можна вказати папки для зберігання журналів транзакцій бази даних та загального доступу SYSVOL. За замовчуванням вони зберігаються у підкаталогах C:\Windows\.

У п'ятому вікні необхідно матимете можливість перевірити всі налаштування, зроблені на попередніх етапах. Шосте вікно відобразить вимоги та інформацію про подальші зміни на сервері. Після цього натисніть кнопку Install. Після розгортання конфігурації Active Directory Domain Services сервер автоматично перезавантажиться.

Після успішного розгортання доменного контролера необхідно додати до домену користувачів та групи користувачів.

Для цього необхідно перейти до Server Manager, у пункті меню Tools обрати підпункт Active Directory Users and Computers. Відкриється вікно, де можна переглянути список вбудованих облікових записів користувачів та груп домену. Для додавання нових об'єктів необхідно вибрати в меню Actions пункт New, а потім Group (для створення групи) або User (для створення користувача).

Відкривається вікно (див. рис. 3.4), де відображається список вбудованих облікових записів користувачів та груп домену. При цьому необхідно відмітити опція "Domain Local" для області дії облікового запису (локально в домені) та "Security" для типу групи (група безпеки). В полі First Name слід вказати ім'я користувача, а в полі User logon name – його логін при входженні в систему. Після заповнення цих полів натискається кнопка Next.

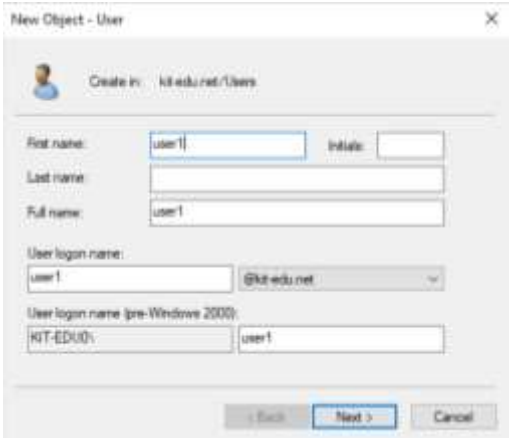

Рисунок 3.4 – Створення користувача домену

У наступному вікні вводиться пароль облікового запису користувача. При цьому відмічаються дві опції: User must change password at next logon (щоб користувач був змушений змінити пароль при першому вході в систему) та Account is disabled (для блокування даного облікового запису). В останньому вікні натискається кнопка Finish.

3.2 Інструкції з налаштування активного комутаційного обладнання

3.2.1 Інструкції з налаштування маршрутизатора доступу до Інтернет

Для налаштування маршрутизатора доступу до Інтернету в мережі комп'ютерного клубу "Сталкер", необхідно виконати низку кроків. Цей маршрутизатор буде виконувати функції прикордонного пристрою (edge router), забезпечуючи вихід у глобальну мережу, маршрутизацію між VLAN, NAT, а також базовий захист.

Спочатку слід ввімкнути маршрутизатор, підключитись до консольного порту маршрутизатора за допомогою консольного кабелю (RJ45) та програми-терміналу (PuTTY, Tera Term).

Перейти у привілейований режим та режим глобальної конфігурації [5]:

Router> enable

Router# configure terminal

Ввести м'я пристрою:

Router(config)# hostname R1

Встановлення паролів:

R1(config)# enable secret <пароль>

R1(config)# line console 0

R1(config-line)# password <пароль>

R1(config-line)# login

R1(config-line)# exit

R1(config)# line vty 0 4 // Для Telnet/SSH

R1(config-line)# password YourVTYPassword

R1(config-line)# login

R1(config-line)# transport input ssh // Рекомендовано SSH замість Telnet

R1(config-line)# exit

R1(config)# service password-encryption // Шифрування паролів у конфігурації

Створення користувача для SSH (якщо вибрали SSH):

R1(config)# username admin privilege 15 secret YourAdminSSHPassword

R1(config)# ip domain name stalkerclub.local // Важливо для SSH

R1(config)# crypto key generate rsa // Генеруємо RSA ключі для SSH

Вимкнення пошуку DNS (для прискорення роботи):

R1# no ip domain lookup

Далі необхідно налаштувати WAN-інтерфейс. Для цього слід вибрати інтерфейс, який буде підключатися до провайдера і ввести команди [5]:

R1(config)# interface GigabitEthernet 0/0/0

R1(config-if)# description WAN_ISP_Connection

R1(config-if)# ip address 174.125.245.65 255.255.255.252

R1(config-if)# no shutdown

R1(config-if)# exit

В даному випадку використано IP-адресу 174.125.245.65 підмережі провайдера 174.125.245.64/30.

Інший інтерфейс буде підключено до головного комутатора (наприклад, Cisco C9200CX-8UXG-2X-E). Він буде налаштований як access для під'єднання головного комутатора до нього. Для цього необхідно створити ще одну віртуальну підмережу із двох Ip-адрес для з'єднання із головним комутатором третього рівня.

Враховуючи дані таблиці 2.9 вільні адреси адресного простору локальної мережі починаються від адреси 192.168.0.172. Саме цю адресу слід призначити даній підмережі. Враховуючи, що мережа буде складатись із двох IP-адрес, то для неї буде виділено маску 255.255.255.252. Отже адреса підмережі між головним комутатором та маршрутизатором буде 192.168.0.172/30. Для інтерфейсу маршрутизатора буде виділено адресу 192.168.0.173/30, а для віртуального інтерфейсу комутатора – 192.168.0.174/30.

Отже, для налаштування LAN-інтерфейсу (підключення до головного комутатора) необхідно ввести наступні команди [5]:

R1config)# interface GigabitEthernet 0/0/1

R1(config-if)# description LAN_To_Core_Switch

R1(config-if)# ip address 192.168.0.174 255.255.255.252

R1(config-if)# no shutdown

R1(config-if)# exit

Далі необхідно налаштувтаи статичний маршруту за замовчуванням (Default Route). Це маршрут, який вказує, куди відправляти трафік, якщо немає більш специфічного маршруту. Це буде IP-адреса шлюзу провайдера.

R1(config)# ip route 0.0.0.0 0.0.0.0 174.125.245.66

Також потрібно налаштувати статичну маршрутизацію від маршрутизатора до підмереж, вказавши IP-адреси та маски підмережі із таблиці 2.9 та в якості інтерфейсу доступу адресу віртуального інтерфейсу головного комутатора 192.168..0.173/30. Отже, команди будуть мати вигляд:

R1(config)# ip route 192.168.0.0 255.255.255.128 192.168.0.173

R1(config)# ip route 192.168.0.64 255.255.255.192 192.168.0.173

R1(config)# ip route 192.168.0.128 255.255.255.192 192.168.0.173

R1(config)# ip route 192.168.0.144 255.255.255.240 192.168.0.173

R1(config)# ip route 192.168.0.160 255.255.255.248 192.168.0.173

R1(config)# ip route 192.168.0.168 255.255.255.252 192.168.0.173

Далі необхідно налаштувати NAT (Network Address Translation). Який дозволяє всім внутрішнім пристроям використовувати одну (або декілька) публічних IP-адрес для виходу в Інтернет. Визначення внутрішніх та зовнішніх інтерфейсів [5]:

R1(config)# interface GigabitEthernet 0/0/0

R1(config-if)# ip nat outside

R1(config-if)# exit

R1(config)# interface GigabitEthernet 0/0/1

R1(config-if)# ip nat inside

R1(config-if)# exit

Створення ACL для визначення трафіку, що підлягає NAT [5]:

R1(config)# access-list 1 permit 192.168.0.0 0.0.0.255

Застосування NAT (PAT - Port Address Translation):

R1(config)# ip nat inside source list 1 interface GigabitEthernet 0/0/0 overload

Збереження конфігурації:

R1(config)# end

R1# write memory

3.2.2 Інструкції з налаштування комутаторів та створення віртуальних підмереж

Після налаштування маршрутизатора необхідно перейти до налаштування комутаторів, створення VLAN та маршрутизації між ними. Почнемо із комутаторів окремих сегментів мережі.

Налаштування цих комутаторів передбачає конфігурацію їхніх імен, інтерфейсів для підключення до відповідних VLAN та встановлення параметрів безпеки із застосуванням паролів аутентифікації.

Спочатку буде налаштовано комутатор Sw_1, розташований у серверній. Для цього необхідно підключитися до комутатора через консольне з'єднання. Після підключення автоматично відбувається вхід у користувацький режим комутатора. Для того, щоб задати ім'я пристрою, необхідно ввести наступні команди [5]:

Switch>enable

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname Sw_1

Sw_1(config)#

Для встановлення захисту комутаторів слід ввести такі ж команди як для парольного захисту маршрутизатора, описані в розділі 3.2.1.

Для створення віртуальних мереж VLAN на комутаторі потрібно увійти в режим глобального конфігурування комутатора Sw_1 і ввести команду vlan <номер>, де номер створюваної мережі. Після цього слід вказати назву мережі командою name <назва>. Назви та імена підмереж представлено у таблиці 3.1.

Таблиця 3.1 – Назви та номери підмереж VLAN

Кімната	Під'єднано до комутатора	Назва VLAN	Номер VLAN
Власник клубу	Sw_1	Adm	11
Бухгалтер	Sw_1	Adm	11
Адміністратори	Sw_1	Adm	11
Зал обслуговування VIP клієнтів	Sw_1	Vip	12
Оснвоний зал	Sw_2	Clients	13
Підмережа POS-терміналів	Sw_2	Pos	14
Гостьова Wi-Fi	Sw_2	Guests	15
Сервер	Sw_G	Servers	16
З'єднання комутатор-маршрутиз.	Sw_G	Routers	17

Отже, для створення підмереж потрібно вказати наступні команди [4]:

Sw_1(config)#vlan 11

Sw_1(config-vlan)#name Adm

Sw_1(config)#vlan 12

Sw_1(config-vlan)#name Vip

Sw_1(config)#vlan 13

Sw_1(config-vlan)#name Clients

Sw_1(config)#vlan 14

Sw_1(config-vlan)#name Pos

Sw_1(config)#vlan 15

Sw_1(config-vlan)#name Guests

Sw_1(config)#vlan 16

Sw_1(config-vlan)#name Servers

Sw_1(config-vlan)#exit

Наступним кроком є вибір і налаштування типів портів комутатора, які братимуть участь у функціонуванні VLAN.

Інтерфейси, до яких безпосередньо підключені кінцеві пристрої (комп'ютери) в певній VLAN, необхідно визначити як access-порти. Це пов'язано з тим, що вони працюють з нетегованим трафіком, призначеним лише для цієї конкретної VLAN.

Натомість, порти, що з'єднують комутатори між собою, а також ті, що підключають мережу до маршрутизатора, слід визначити як trunk-порти. Вони призначені для передачі тегованих пакетів з усіх VLAN одночасно, забезпечуючи зв'язок між різними сегментами мережі.

Для налаштування інтерфейсів комутатора Sw_1 необхідно в режимі глобальної конфігурації налаштувати порти GigabitEthernet, до яких підключені комп'ютери віртуальних підмереж 11 та 12.

Відповідно до схеми топології, представленою на рисунку 2.1, комп'ютери під'єднані наступним чином:

- інтерфейси gig0/1, gig0/2, gig0/3 та gig0/4 належать підмережі Adm;
- інтерфейси від gig0/5 до gig0/14 належать підмережі Vip.

Необхідно ввести команди для налаштування інтерфейсів комутатора:

Sw_1(config)#interface range gig0/1-4

Sw_1(config-range-if)#description Administyrators

Sw_1(config-range-if)#switchport mode access

Sw_1(config-range-if)#switchport access vlan 11

Sw_1(config-range-if)#exit

Sw_1(config)# interface range gig0/5-14

Sw_1(config-range-if)#description VIP-zone

Sw_1(config-range-if)#switchport mode access

Sw_1(config-range-if)#switchport access vlan 12

Sw_1(config-range-if)#exit

При цьому команда description є необов’язковою, вона встановлює опис призначення інтерфейсу і полегшує роботу адміністартору під час обслуговування мережі [5].

Ще одним етапом налаштування VLAN на цьому комутаторі є призначення uplink порту транкового типу:

Sw_1(config)#interface TenGigabitEthernet1/0/1

Sw_1(config-if)#description SW_Global

Sw_1(config-if)#switchport mode trunk

Sw_1(config-if)# switchport trunk allowed vlan 11,12

Sw_1(config-if)#exit

Для налаштування інтерфейсів комутатора Sw_2 необхідно в режимі глобальної конфігурації налаштувати порти GigabitEthernet, до яких підключені комп'ютери віртуальних підмереж 13, 14, 15.

Відповідно до схеми топології, представленою на рисунку 2.1, комп'ютери під'єднані наступним чином:

- інтерфейси від gig0/1 до gig0/32 належать підмережі Clients;
- інтерфейс gig0/33 належать підмережі Pos;
- інтерфейс gig0/34 належать підмережі Guests.

Отже, відповідно до цього слід ввести команди для налаштування інтерфейсів комутатора [4]:

Sw_2(config)#interface range gig0/1-32

Sw_2(config-range-if)#description Game_Zal

Sw_2(config-range-if)#switchport mode access

Sw_2(config-range-if)#switchport access vlan 13

Sw_2(config-range-if)#exit

Sw_2(config)#interface gig0/33

Sw_2(config-if)#description POS_Termanals

Sw_2(config-if)#switchport mode access

Sw_2(config-if)#switchport access vlan 14

Sw_2(config-if)#exit

Sw_2(config)#interface gig0/34

Sw_2(config-if)#description Guests

Sw_2(config-if)#switchport mode access

Sw_2(config-if)#switchport access vlan 15

Sw_2(config-if)#exit

Ще одним етапом налаштування VLAN на цьому комутаторі є призначення uplink порту транкового типу:

Sw_2(config)#interface TenGigabitEthernet1/0/1

Sw_2(config-if)#description SW_Global

Sw_2(config-if)#switchport mode trunk

Sw_2(config-if)# switchport trunk allowed vlan 13,14,15

Sw_2(config-if)#exit

Після налаштування сегментуючих комутаторів слід перейти до налаштування конфігурації головного комутатора. Для цього необхідно підключитися до комутатора через консольне з'єднання. Після підключення автоматично відбувається вхід у користувацький режим комутатора. Для того, щоб задати ім'я пристрою, необхідно ввести наступні команди [5]:

Switch>enable

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname Sw_G

Sw_G(config)#

Для встановлення захисту головного комутатора слід ввести такі ж команди як для парольного захисту маршрутизатора, описані в розділі 3.2.1.

Далі на головному комутаторі потрібно перевести усі порти в транковий режим, крім інтерфейсу TenGigabitEthernet1/0/4, який буде використовуватись для підключення віртуальної підмережі сервера та інтерфейсу TenGigabitEthernet1/0/3 який буде підключено до маршрутизатора. Їх слід перевести в режим access. Для цього вводимо наступні команди:

Sw_G(config)#interface range TenGigabitEthernet1/0/1-TenGigabitEthernet1/0/2

Sw_G(config-range-if)# switchport mode trunk

Sw_G(config-range-if)#interface TenGigabitEthernet1/0/1

Sw_G(config-if)# switchport trunk allowed vlan 11,12

Sw_G(config-if)#interface TenGigabitEthernet1/0/2

Sw_G(config-if)# switchport trunk allowed vlan 13,14,15

Sw_G(config-if)#exit

Sw_G(config)#interface range TenGigabitEthernet1/0/3-TenGigabitEthernet1/0/4

Sw_G(config-range-if)# switchport mode access

Sw_G(config-range-if)#interface TenGigabitEthernet1/0/3

Sw_G(config-if)#switchport access vlan 17

Sw_G(config-range-if)#interface TenGigabitEthernet1/0/4

Sw_G(config-if)#switchport access vlan 16

Після цього на головному комутаторі третього рівня потрібно включити режим маршрутизації командою:

Sw_G(config)#ip routing

Далі потрібно створити віртуальні VLAN-порти і призначити їм IP-адреси шлюзів, які прийнято останню IP-адресу хоста підмереж (див. таблицю 2.9).

Для цього необхідно ввести наступні команди:

Sw_G(config)#interface vlan11

Sw_G(config-if)#ip address 192.168.0.166 255.255.255.248

Sw_G(config-if)#interface vlan12

Sw_G(config-if)#ip address 192.168.0.142 255.255.255.240

Sw_G(config-if)#interface vlan13

Sw_G(config-if)#ip address 192.168.0.126 255.255.255.192

Sw_G(config-if)#interface vlan14

Sw_G(config-if)#ip address 192.168.0.158 255.255.255.240

Sw_G(config-if)#interface vlan15

Sw_G(config-if)#ip address 192.168.0.62 255.255.255.192

Sw_G(config-if)#interface vlan16

Sw_G(config-if)#ip address 192.168.0.170 255.255.255.252

Sw_G(config-if)#interface vlan17

Sw_G(config-if)#ip address 192.168.0.173 255.255.255.252

Sw_G(config-if)#exit

Далі необхідно налаштувтаи статичний маршруту за замовчуванням (Default Route). Це маршрут, який вказує, куди відправляти трафік, якщо немає більш специфічного маршруту. Це буде IP-адреса внутрішнього інттерфейсу маршрутизатора (192.168.0.174):

Sw_G(config)# ip route 0.0.0.0 0.0.0.0 192.168.0.174

Також потрібно налаштувати статичну маршрутизацію

3.3 Інструкція з використання тестових наборів та тестових програм

Ця інструкція надає вичерпні рекомендації щодо використання апаратних і програмних засобів для діагностики.

Тестування мережі – це систематичний процес перевірки її функціональності, продуктивності та надійності. Він охоплює кілька ключових етапів:

- фізичний рівень – перевірка цілісності та якості кабелів, конекторів, оптичних ліній;

- логічний рівень – діагностика IP-адресації, маршрутизації, коректності роботи VLAN, DNS та DHCP;

- продуктивність – оцінка реальної пропускної здатності, затримки (latency) та втрат пакетів (packet loss);

- безпека – перевірка ефективності фаєрволів, правил доступу та функціонування VPN-з'єднань.

Для всебічного тестування мережі "Сталкер" знадобиться наступний апаратні та програмні інструменти.

Для забезпечення стабільної роботи клубу, необхідно провести наступні тестові сценарії.

Тестування підключення клієнтських ПК:

- перевірити зв'язок (ping) з кожного клієнтського ПК до шлюзу його VLAN, потім до маршрутизатора, до файлового/ігрового сервера та до Інтернету;

- використати iPerf3 для вимірювання пропускної здатності між клієнтськими ПК та ігровим сервером для оцінки швидкості завантаження ігор.

Тестування Wi-Fi мереж (POS-термінали, гості) [3]:

- перевірити успішне підключення POS-терміналів до їхнього спеціалізованого SSID, а також стабільність та швидкість проведення транзакцій;

- протестувати гостьову Wi-Fi мережу: переконатися в ізоляції клієнтів один від одного та від внутрішніх сегментів мережі, а також у коректності обмежень швидкості (якщо такі налаштовані);

- застосувати аналізатори Wi-Fi для перевірки якості покриття та рівня сигналу у всіх ігрових зонах та зонах очікування.

Для тестування між-VLAN маршрутизації необхідно виконати ping або traceroute між пристроями, що належать до різних VLAN (наприклад, з адміністративного ПК до клієнтського, або до POS-терміналу), щоб підтвердити коректність налаштування маршрутизації.

Тестування доступу до Інтернету:

- перевірити швидкість Інтернет-з'єднання з різних VLAN за допомогою онлайн-сервісів або iPerf3 до зовнішнього тестового сервера;

- підтвердити коректну роботу NAT, забезпечуючи вихід у глобальну мережу.

Тестування безпеки:

- спробувати отримати доступ до адміністративних ресурсів або сегментів мережі з клієнтських ПК; ці спроби мають бути заблоковані фаєрволом;

- перевірити коректність застосованих правил фаєрволу на маршрутизаторі та комутаторах;

- провести тестування VPN-з'єднання (якщо така функція використовується для віддаленого доступу або безпечного зв'язку).

Документування та регулярний моніторинг

- вести детальний журнал тестування, вказуючи дату, час, виконавця, використані інструменти, опис тесту, результат (PASS/FAIL), деталі виявлених проблем та дії з їх усунення. Зберігати всі згенеровані тестовим обладнанням звіти (наприклад, сертифікати кабельних ліній);

- налаштувати систему моніторингу мережі (наприклад, на базі SNMP/NetFlow) для постійного відстеження стану мережевих пристроїв, завантаження каналів, виявлення помилок та аномалій у реальному часі. Це дозволить проактивно реагувати на потенційні проблеми.

Комплексний підхід до тестування та налагодження, описаний у цій інструкції, є запорукою створення стабільної, високопродуктивної та безпечної мережі, що критично важливо для успішної роботи комп'ютерного клубу "Сталкер".

3.4 Інструкції з налаштування засобів захисту мережі

Безпека мережі є пріоритетною для комп'ютерного клубу "Сталкер", оскільки вона захищає від несанкціонованого доступу, кібератак, витоків даних та забезпечує стабільну роботу всіх сервісів. Ці інструкції описують налаштування ключових засобів захисту.

Маршрутизатор є першим рубежем захисту, оскільки через нього проходить весь зовнішній трафік. На ньому слід налаштутвиа фаєрвол, ввівши наступні команди:

R1(config)# ip access-list extended WAN_IN_ACL

Дозволити відповіді на встановлені з'єднання:

R1(config-ext-nacl)# permit tcp any any established

R1(config-ext-nacl)# permit udp any any established

R1(config-ext-nacl)# permit icmp any any echo-reply

R1(config-ext-nacl)# remark --- Дозволити DNS трафік ---

R1(config-ext-nacl)# permit udp any any eq domain // DNS

R1(config-ext-nacl)# permit tcp any any eq domain

Блокувати приватні IP ззовні:

R1(config-ext-nacl)# deny ip 10.0.0.0 0.255.255.255 any

R1(config-ext-nacl)# deny ip 172.16.0.0 0.15.255.255 any

R1(config-ext-nacl)# deny ip 192.168.0.0 0.0.255.255 any

Явно блокувати весь інший трафік та логувати:

R1(config-ext-nacl)# deny ip any any log

R1(config-ext-nacl)# exit

Призначення ACL спсику інтерфейсу:

R1(config)# interface TenGigabitEthernet 0/0/0

R1(config-if)# ip access-group WAN_IN_ACL in

R1(config-if)# exit

На головному комутаторі встановити контроль доступу між різними віртуальними підмережами (VLAN). Наприклад, адміністративна VLAN має доступ до всіх, клієнтська VLAN не має доступу до POS-терміналів:

Sw_G(config)# ip access-list extended CLIENTS_TO_OTHER_VLAN_ACL

Дозволити клієнтам доступ до Інтернету:

Sw_G(config-ext-nacl)# permit ip 192.168.0.0 0.0.0.255 any

Блокувати доступ клієнтів до адміністарторів та VLAN POS-терміналів:

Sw_G(config-ext-nacl)# deny ip 192.168.0.163 0.0.0.7

Sw_G(config-ext-nacl)# deny ip 192.168.0.144 0.0.0.15

Sw_G(config-ext-nacl)# permit ip any any // Дозволити інший трафік

Sw_G(config-ext-nacl)# exit

Призначення ACL інтферйссам:

Sw_G(config)# interface Vlan13

Sw_G(config-if)# ip access-group CLIENTS_TO_OTHER_VLAN_ACL in //

Sw_G(config-if)# interface Vlan15

Sw_G(config-if)# ip access-group CLIENTS_TO_OTHER_VLAN_ACL in //

Sw_G(config-if)# exit

Захист безпровідної мережі:

- використовувати WPA2-PSK з окремим паролем, або портал авторизації (Captive Portal);

- приховування SSID для POS-мережі (тобто, вони не будуть транслюватися публічно), щоб ускладнити їх виявлення сторонніми особами. Гостьову мережу зазвичай залишають видимою;

- для гостьової Wi-Fi мережі (через Omada Controller) налаштувати обмеження швидкості (Bandwidth Control) для кожного клієнта, щоб запобігти надмірному споживанню трафіку та забезпечити справедливий розподіл ресурсів.

Дотримання цих інструкцій забезпечить комплексний та багаторівневий захист мережевої інфраструктури комп'ютерного клубу "Сталкер" від більшості типових кіберзагроз та внутрішніх ризиків.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини дипломного проекту є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки проекту комп'ютерної мережі комп'ютерного клубу «Сталкер» і прийняття рішення про її подальше впровадження в роботу.

4.1 Визначення стадій техпроцесу та загальної тривалості проведення НДР

Для визначення загальної тривалості проведення НДР доцільно дані витрат часу по окремих операціях технологічного процесу звести у таблицю. Виконавцями стадій технологічного процесу будуть: керівник проекту, інженер, технік. В таблиці 4.1 наводяться стадії технологічного процесу та середній час їх виконання.

Таблиця 4.1 – Середній час виконання НДР та стадії технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
2.	Робота з клієнтом	керівник	4
3.	Проектування мережі	інженер	28
4.	Монтаж мережі	технік	20
5.	Вибір операційної системи	інженер	1
6.	Встановлення та налаштування ПЗ	інженер	6
6.	Остаточне налаштування системи	інженер	7
7.	Здача проекту	Керівник	7
Разом			73

Загальний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі для комп'ютерного клубу «Сталкер» становить 73 годин.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Оплата праці – це грошовий вираз вартості та ціни робочої сили, який виступає у формі будь-якого заробітку, та виплаченого власником підприємства працівникові за виконану роботу.

Заробітна плата працівника залежить від кінцевих результатів роботи даного підприємства, та регулюється податками і максимальними розмірами не обмежується.

Основна заробітна плата розраховується за формулою:

$$З_{осн} = Т_с \cdot К_г, \quad (4.1)$$

де Тс – тарифна ставка, грн.;

Кг – кількість відпрацьованих годин.

Основна заробітна плата становить:

1. Керівник проекту: $З_{осн1} = 120 \cdot 11 = 1320$ грн.;
2. Інженер: $З_{осн2} = 90 \cdot 42 = 3780$ грн.;
3. Технік: $З_{осн3} = 60 \cdot 20 = 1200$ грн.

Сумарна основна заробітна плата становить:

$$З_{осн} = 1320 + 3780 + 1200 = 6300 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати та обчислюється за формулою 4.2:

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \quad (4.2)$$

де $К_{допл.}$ – коефіцієнт додаткових виплат працівникам: 0,1–0,15.

Отже, додаткова заробітна плата по категоріях працівників становить:

1. Керівник проекту: $З_{дод1} = 1320 \cdot 0,12 = 158,4$ грн.;

2. Інженер: $З_{дод2} = 3780 \cdot 0,12 = 453,6$ грн.;

3. Технік: $З_{дод3} = 1200 \cdot 0,12 = 144$ грн.

Сумарна додаткова заробітна плата становить:

$$З_{дод} = 158,4 + 453,6 + 144 = 756 грн.$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п} = З_{осн} + З_{дод} \quad (4.3)$$

Отже, загальні витрати на оплату праці становлять:

$$В_{о.п} = 6300 + 756 = 7056 \text{ грн.}$$

Відрахування на соціальні заходи становлять 22%. Отже, сума відрахувань на соціальні заходи буде обчислюватися за формулою 4.4:

$$В_{с.з.} = ФОП * 0.22 \quad (4.4)$$

де ФОП – фонд оплати праці, грн.

$$В_{с.з.} = 7056 \cdot 0,22 = 1552,32 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2:

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додатк. Зароб. Плата, грн.	Нарахув. На ФОП, грн.	Всього витрати на оплату праці, грн.
		Тариф. Ставка, грн.	К-сть відпр. Год.	Факт. Нарах. з/пл., грн.			
1	Керівник проекту	120	12	1320	158,4	-	-
2	Інженер	90	42	3780	453,6	-	-
3	Технік	60	20	1200	144	-	-
Разом				6300	756	1552,32	8608,32

Загальні витрати на оплату праці становлять 8608,32 грн.

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються за формулою 4.5 як добуток кількості витрачених матеріалів та їх ціни:

$$\text{МВі} = q_i * p_i \quad (4.5)$$

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 4.6:

$$\text{З м. в.} = \Sigma\ \text{МВі} \quad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Кількість	Ціна, грн.	Сума, грн.
1	2	3	4	5	6
1	Комутаційна шафа Ipcom CH-4U 600X600	шт.	1	3240	3240
2	Патч панель 1U 24 порта кат. 5E 19"	шт.	1	1200	1200
3	Розетка RJ-45 (категорія 6)	шт.	15	105	1575
4	Розетка підлогова Panduit NetKey NK688MB (категорія 6)	шт	30	195	5850
5	Роз’єм 8P8C (пачка 100 шт)	шт.	1	522	522
6	Короб (середня ціна для різного січення)	м.	102	105	10710
7	Короб підлоговий	м.	66	195	12870
8	Гофрований лоток	м.	5	112	560
9	Кабель UTP (кат. 6) (бухта)	шт.	4	5260	21040
10	Патчкорди (кат. 6)	шт.	47	52	2444
11	Кабель опотоволоконний	м.	3	23	69
12	Комутатор робочих груп Cisco SG350X-48MP-K9-EU	шт.	2	46592	93124
13	Головний комутатор C9200CX-8UXG-2X-E	шт.	1	76334	76334

Продовження таблиці 4.3

1	2	3	4	5	6
14	Маршрутизатора Cisco ISR4221/K9	шт.	1	34325	34325
15	Безпровідна точка доступу TP-LINK EAP225	шт	2	2999	2999
Разом:					266862

Загальна сума матеріальних витрат становить 266862 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою 4.7:

$$З_е = W * T * S \quad (4.7)$$

де W – необхідна потужність, кВт; Т – кількість годин роботи обладнання; S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 40 години, споживана потужність – 0,6 кВт/год., вартість 1 кВт електроенергії – 7 грн. Тому витрати на електроенергію будуть становити:

$$З_е = 0,6 \cdot 40 \cdot 7 = 103,68 \text{ грн.}$$

4.5 Визначення транспортних затрат

Транспортні витрати слід прогнозувати у розмірі 8-10 % від загальної суми матеріальних затрат. Транспортні витрати розраховуються за формулою 4.8.

$$Т_В = З\ м.в. * 0.08..0.1 \quad (4.8)$$

де $Т_В$ – транспортні витрати.

Отже, транспортні витрати будуть становити:

$$Т_В = 266862 \cdot 0,09 = 18273,24 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Мінімально допустимі строки їх використання 2 роки. Для визначення амортизаційних відрахувань застосовуємо формулу 4.9:

$$А = \frac{Б_В * Н_А}{100\%} * Т \quad (4.9)$$

де А – амортизаційні відрахування за звітний період, грн. $Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.; $Н_А$ – норма амортизації, %? Т – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 10 год., балансова вартість ПК - 26500 грн., тому, то амортизаційні відрахування становлять:

$$A = \frac{26500 \cdot 0,04}{150} \cdot 10 = 70,67 \text{ грн}$$

4.7 Обчислення накладних витрат

Накладні витрати - це витрати, не пов'язані безпосередньо з технологічним процесом виготовлення продукції, а утворюються під впливом певних умов роботи по організації, управлінню та обслуговуванню виробництва.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20 – 60 % від суми основної та додаткової заробітної плати працівників, обчислюються за формулою 4.10.

$$Н_в = В_{о.п.} * 0.2 \dots 0.6 \quad (4.10)$$

де $Н_В$ – накладні витрати.

$$Н_в = 7056 * 0.5 = 3528$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Кошторис витрат являє собою зведений план усіх витрат підприємства на майбутній період виробничо-фінансової діяльності.

Результати проведених вище розрахунків зведемо у таблиці 4.4, де зазначено наступні види витрат: витрати на оплату праці, відрахування на соціальні заходи, матеріальні витрати, витрати на електроенергію, транспортні витрати, амортизаційні відрахування, накладні витрати.

Таблиця 4.4 – Кошторис витрат НДР

Зміст витрат	Сума, грн.	в % до загального
Витрати на оплату праці (основну і додаткову заробітну плату)	7056	2,37
Відрахування на соціальні заходи	1552,32	0,52
Матеріальні витрати	266862	89,67
Витрати на електроенергію	103,68	0,03
Транспортні витрати	18273,24	6,14
Амортизаційні відрахування	213	0,07
Накладні витрати	3528	1,19
Собівартість	297588,24	100

Собівартість ($С_в$) НДР розрахуємо за формулою 4.11:

$$С_в = В_{о.п.} + В_{с.п.} + З_{м.в.} + З_е + Т_в + А + Н_в \quad (4.11)$$

Собівартість дорівнює $С_В$ = 297588,24 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = \frac{С_в \cdot (1 + Р_{рен}) + К \cdot В_{ні}}{К} \cdot (1 + ПДВ) \quad (4.12)$$

де $P_{рен.}$ – рівень рентабельності;

Ц = 297588,24 · (1+0,3) · (1+0,2) = 464 237,65 грн.

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Для визначення ефективності продукту розраховують чисту теперішню вартість (ЧТВ), можна визначити за формулою 4.13 та термін окупності ($T_{ОК}$), який можна визначити за формулою 4.14.

$$ЧТВ = -K_В + \sum_{i=1}^{t} \frac{Г_в}{(1+i)^t} \geq 0, \quad (4.13)$$

де $К_В$ – затрати на проект;

$Г_п$ – грошовий потік за t – ий рік;

t – відповідний рік проекту;

i - величина дисконтної ставки (10…15%).

Якщо ЧТВ ≥ 0, то проект може бути рекомендований до впровадження.

$$ЧТВ = -297588,24 + \frac{272180,00}{(1+0,1)} + \frac{272180,00}{(1+0,1)^2} = 174790,3 \text{ грн}$$

Термін окупності визначається за формулою:

$$T_{ОК} = T_{ПВ} + \frac{H_В}{Г_{ПР}}, \quad (4.14)$$

де $Т_{ПВ}$ – період до повного відшкодування витрат, років;

$Н_В$ – невідшкодовані витрати на початок року, грн.;

$Г_{ПР}$ – грошовий потік на початок року, грн.

$$T_{ОК} = 1 + \frac{50151,88}{272180,00} = 1,2$$

Всі дані розрахунків внесемо в зведену таблицю 4.5 техніко-економічних показників.

Таблиця 4.5 - Техніко-економічні показники розробки програми

№ п/п	Показник	Значення
1	2	3
1.	Собівартість, грн.	297588,24
2.	Плановий прибуток, грн.	166648,8
3.	Ціна, грн.	464 237,65
4.	Чиста теперішня вартість, грн.	174790,3
5.	Термін окупності, рік	1,2

Загальна вартість розробленого проекту мережі для комп’ютерного клубу “Сталкер” становить 464 237,65 грн. Проводити проектні роботи варто і вкладені кошти окупляться за 1,2 року.

.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

5.1 Пожежна безпека приміщення комп’ютерного клубу “Сталкер”

Пожежна безпека в приміщенні комп'ютерного клубу “Сталкер” є надзвичайно важливою, враховуючи значне скупчення людей, наявність великої кількості електрообладнання та горючих матеріалів (меблі, оздоблення, папір тощо). Дотримання правил пожежної безпеки допоможе запобігти виникненню пожежі, мінімізувати її наслідки та забезпечити безпечну евакуацію людей у разі її виникнення.

На організаційному рівні в комп'ютерного клубу “Сталкер” проведено наступні заходи пожежної безпеки:

– розроблено та затверджено інструкцію з пожежної безпеки, де визначено обов'язки працівників та відвідувачів щодо забезпечення пожежної безпеки, порядок дій у разі виникнення пожежі, правила користування первинними засобами пожежогасіння;

– наказом керівника призначено працівника відповідального за забезпечення пожежної безпеки в клубі, який проводить інструктажі, навчання та контроль за дотриманням правил;

– проводяться протипожежних інструктажі:

- первинний інструктаж – з новими працівниками перед допуском до роботи,
- повторний інструктаж – періодично (не рідше одного разу на рік, а для робіт підвищеної пожежної небезпеки – раз на півріччя),
- позаплановий інструктаж – при зміні технологічного процесу, введенні нових правил, після пожеж або нещасних випадків,
- цільовий інструктаж – перед виконанням разових робіт підвищеної пожежної небезпеки;

– проводяться навчання працівників діям у разі пожежі – практичні тренування з евакуації та користування первинними засобами пожежогасіння;

– розроблено та розміщено на видних місцях в кожному приміщенні плани евакуації;

– ведеться журнал реєстрації інструктажів, журнал перевірок первинних засобів пожежогасіння.

Також в комп'ютерному клубі “Сталкер” організовано наступні технічні заходи пожежної безпеки:

– забезпечено приміщення первинними засобами пожежогасіння:

- порошкові вогнегасники, відповідно до площі приміщення та класу пожежної небезпеки. Вогнегасники сертифіковані, мати пломби та проходити періодичні перевірки. Вони розміщені у легкодоступних видних місцях,
- пожежний щит укомплектований пожежним інструментом (лопата, лом, багор, відро), покривалом протипожежним;

– облаштовано систему автоматичної пожежної сигналізації для своєчасного виявлення пожежі на ранній стадії та оповіщення про неї;

– облаштування системи оповіщення про пожежу та управління евакуацією для своєчасного інформування людей про пожежу та організації безпечної евакуації.

Також в комп'ютерному клубі “Сталкер” передбачені заходи електробезпеки:

– регулярно перевіряється ізоляція проводів, надійність з'єднань, справність розеток та вимикачів, щоб не допускати використання саморобних електроприладів та подовжувачів низької якості;

– встановлення автоматичні вимикачі (автомати) відповідного номіналу для захисту від короткого замикання та перевантаження;

– для захисту від ураження електричним струмом у разі пошкодження ізоляції реалізовано заземлення (занулення) електрообладнання;

На випадок надзвичайної ситуації передбачені евакуаційні шляхи, які є вільно доступними і не захаращені меблями та іншими перешкодами. Напрямок

евакуаційних шляхів вказується фотолюмінесцентними знаками, що вказують напрямок руху до евакуаційних виходів.

Двері евакуаційних виходів відчиняються за напрямком руху евакуації та не мають замків, які не можуть бути відчинені зсередини без ключа.

Дерев'яні конструкції, текстильні матеріали оброблено спеціальними вогнезахисними речовинами.

В комп'ютерному клубі “Сталкер” передбачені також наступні режимні заходи:

– заборонено використання саморобних або несправних електронагрівальних приладів;

– заборонено паління у невідведених місцях: Обладнано спеціальні місця для куріння із попільничками та знаками;

– обмежено кількості горючих матеріалів у приміщенні, та передбачене їх спеціалізоване правильне зберігання;

– регулярне прибирання приміщення від пилу та горючого сміття;

– огляд приміщення після закінчення роботи на предмет вимкнення електрообладнання, освітлення.

На випадок виникнення пожежі створення інструкції із алгоритмом дій [2]:

– негайно повідомити про пожежу до Служби порятунку за номером 101. Чітко назвати адресу, місце виникнення пожежі, що горить, наявність загрози для людей;

– увімкнути систему оповіщення про пожежу;

– організувати евакуацію людей з приміщення. Спокійно направляти відвідувачів до евакуаційних виходів згідно з планом евакуації. Допомагати дітям та особам з обмеженими можливостями;

– за можливості, розпочати гасіння пожежі первинними засобами пожежогасіння (вогнегасниками) до прибуття пожежних підрозділів;

– при гасінні електрообладнання, переконатися, що воно знеструмлене;

– перекрити подачу електроенергії (за необхідності та безпеки);

– зустріти пожежно-рятувальні підрозділи та надати їм необхідну інформацію про осередок пожежі та обстановку.

5.2 Заходи і засоби захисту від шуму

Шум у комп'ютерному клубі може створювати дискомфорт для відвідувачів та працівників, призводити до втоми, зниження концентрації уваги, а при тривалому впливі – до проблем зі слухом та нервовою системою. Тому впровадження ефективних заходів і засобів захисту від шуму є важливим аспектом забезпечення безпечних та комфортних умов перебування.

Джерела шуму в комп'ютерному клубі:

– комп'ютерне обладнання: вентилятори системних блоків, відеокарт, блоків живлення, жорстких дисків;

– системи охолодження та вентиляції: робота кондиціонерів, вентиляторів припливно-витяжної вентиляції;

– периферійні пристрої: клавіатури (особливо механічні), миші (клацання), колонки (звук гри, музики, спілкування);

– відвідувачі: голосна розмова, крики, емоційні вигуки під час гри, стукіт по клавіатурі та миші;

– зовнішні джерела: шум з вулиці, сусідніх приміщень.

Основні заходи та засоби захисту від шуму можна поділити на [1]:

– архітектурно-планувальні та будівельні рішення;

– технічні засоби зниження шуму від обладнання;

– організаційні та поведінкові заходи;

– засоби індивідуального захисту (для працівників).

До архітектурно-планувальних та будівельних рішень можна віднести [1]:

– звукоізоляція приміщення, яке включає використання звукоізоляційних матеріалів для стін (мінеральна вата, акустичні панелі, гіпсокартонні системи з заповненням), підвісні акустичні стелі, звукоізоляційні плити, звукоізоляційні

підкладки під підлогові покриття (ламінат, лінолеум, ковролін). Крім цього, встановлення якісних склопакетів з підвищеною звукоізоляцією, ущільнення дверних та віконних прорізів;

– розташування обладнання. Розміщення найбільш шумного обладнання (серверні шафи, потужні ігрові ПК) в окремих, звукоізольованих приміщеннях;

– раціональне розміщення комп'ютерних столів для мінімізації прямого поширення звуку між робочими місцями;

– акустичне оздоблення приміщення, шляхом використання звукопоглинаючих матеріалів на стінах та стелі (акустичні панелі, перфоровані панелі, м'які оббивні матеріали).

– застосування елементів інтер'єру, що поглинають звук (м'які меблі, штори, килими).

Технічні засоби зниження шуму від обладнання [6]:

– використання малошумного комп'ютерного обладнання, що включає вибір системних блоків з низьким рівнем шуму вентиляторів (великі повільно обертові вентилятори, рідинні системи охолодження). Використання безвентиляторних відеокарт або моделей з ефективними та тихими системами охолодження;

– застосування блоків живлення з низьким рівнем шуму вентиляторів.

– використання твердотільних накопичувачів (SSD) замість традиційних жорстких дисків (HDD), які є джерелом вібрації та шуму;

– антивібраційні елементи: встановлення системних блоків на антивібраційні підставки, використання антивібраційних кріплень для вентиляторів та жорстких дисків всередині корпусу;

– зниження шуму від периферійних пристроїв: використання тихих клавіатур (мембранних або механічних з демпферами), безшумних або малошумних мишей, регулювання гучності акустичних систем до комфортного рівня;

– регулярне очищення вентиляторів від пилу, змащування рухомих частин для запобігання зайвому шуму;

– звукоізоляційні кожухи. Для особливо шумного обладнання (наприклад, серверів) можуть використовуватися спеціальні звукоізоляційні кожухи.

Організаційні та поведінкові заходи [1]:

– встановлення обмежень на максимальну гучність звуку в навушниках та акустичних системах;

– контроль за рівнем шуму від відвідувачів, шляхом проведення роз'яснювальних бесід з відвідувачами щодо необхідності дотримання тиші;

– за можливості, створення окремих зон для різних видів діяльності (тихі ігрові зони, зони для спілкування), що дозволить локалізувати шум;

– оптимізація режиму роботи клубу, враховуючи час найбільшого навантаження та можливий піковий шум;

– заохочення відвідувачів до використання навушників для індивідуального прослуховування звуку.

– встановлення інформаційних табличок. Розміщення нагадувань про необхідність дотримання тиші.

Засоби індивідуального захисту (для працівників) [6]:

– беруші – індивідуальні вкладиші для вух, що знижують рівень шуму, що потрапляє до слухового каналу;

– навушники протишумові – повнорозмірні навушники, які забезпечують більш високий рівень шумопоглинання, ніж беруші;

Вибір конкретних заходів та засобів захисту залежить від [6]:

– рівня шуму. Проведення вимірювань рівня шуму в різних зонах клубу для визначення необхідних заходів;

– бюджету. Вартість різних звукоізоляційних та акустичних матеріалів може варіюватися;

– дизайну приміщення: Заходи повинні гармонійно вписуватися в загальний дизайн клубу;

– специфіки діяльності. Врахування особливостей використання комп'ютерів та поведінки відвідувачів.

Комплексний підхід, що включає архітектурно-планувальні, технічні, організаційні та індивідуальні засоби захисту, дозволить створити в комп'ютерному клубі акустично комфортне середовище, що позитивно вплине на самопочуття та продуктивність як відвідувачів, так і працівників. Регулярний контроль за рівнем шуму та ефективністю впроваджених заходів є запорукою підтримання оптимальних акустичних умов.

5.3 Системний підхід у безпеці життєдіяльності

Системний підхід у безпеці життєдіяльності розглядає людину, навколишнє середовище та небезпеки як взаємопов'язані елементи складної системи. Замість ізольованого вивчення окремих факторів ризику, системний підхід аналізує всю систему "людина - середовище - небезпека" в її цілісності, враховуючи взаємодію між її компонентами.

Основні принципи системного підходу в БЖД [2]:

– цілісність. Система розглядається як єдине ціле, де зміни в одному елементі впливають на інші елементи та на систему в цілому. Небезпека не існує ізольовано, а є результатом взаємодії людини та середовища;

– ієрархічність. Система БЖД має багаторівневу структуру. Людина є підсистемою суспільства, яке, в свою чергу, є частиною біосфери. Небезпеки також можуть мати різний рівень впливу (індивідуальний, груповий, суспільний);

– структурність. Кожен елемент системи має свою структуру та виконує певні функції. Розуміння структури елементів (організму людини, виробничого процесу, природного явища) допомагає ідентифікувати потенційні джерела небезпек та вразливі місця;

– функціональність. Кожен елемент системи виконує певні функції, спрямовані на досягнення мети системи (виживання, розвиток, виробництво).

Порушення функцій одного елемента може призвести до виникнення небезпечної ситуації;

– взаємозв'язок та взаємодія. Елементи системи постійно взаємодіють між собою. Характер цих взаємодій може бути причиною виникнення небезпек або фактором, що сприяє їх запобіганню чи мінімізації наслідків;

– динамічність. Система БЖД є динамічною і постійно змінюється під впливом внутрішніх та зовнішніх факторів. Небезпеки також можуть виникати, розвиватися та зникати;

– ймовірністьний характер. Виникнення небезпек та їх наслідки часто мають ймовірнісний характер. Системний підхід враховує можливість виникнення небезпечних подій та оцінює їх вірогідність;

– керованість. Система БЖД піддається управлінню. За допомогою цілеспрямованих дій можна впливати на окремі елементи та їх взаємодію з метою підвищення рівня безпеки.

Застосування системного підходу в БЖД передбачає [6]:

– ідентифікація елементів системи. Визначення основних компонентів системи "людина - середовище - небезпека" в конкретній ситуації. Наприклад, на виробництві це можуть бути працівник, обладнання, технологічний процес, виробниче середовище, потенційні небезпечні фактори;

– аналіз взаємозв'язків та взаємодії між елементами. Вивчення того, як різні елементи системи впливають один на одного та як ці взаємодії можуть призвести до виникнення небезпечних ситуацій. Наприклад, аналіз впливу шуму від обладнання на стан працівника та його працездатність;

– виявлення потенційних небезпек. Ідентифікація можливих джерел небезпек на кожному рівні системи та аналіз їх характеристик (причини виникнення, можливі наслідки);

– оцінка ризиків. Визначення ймовірності виникнення небезпечних подій та потенційної тяжкості їх наслідків. Це дозволяє пріоритезувати заходи безпеки;

– розробка та впровадження заходів безпеки. На основі аналізу ризиків розробляються комплексні заходи, спрямовані на запобігання виникненню небезпек, зменшення їх впливу або ліквідацію наслідків. Ці заходи можуть бути технічними, організаційними, медико-профілактичними, навчальними і інше;

– моніторинг та контроль. Постійне спостереження за станом системи, виявлення нових небезпек та оцінка ефективності впроваджених заходів безпеки;

– удосконалення системи. На основі результатів моніторингу та контролю проводиться постійне вдосконалення системи безпеки життєдіяльності з метою підвищення її надійності та ефективності.

Переваги системного підходу в безпеці життєдіяльності [6]:

– комплексне бачення проблеми. Дозволяє враховувати всі фактори, що впливають на безпеку життєдіяльності;

– виявлення прихованих небезпек. Аналіз взаємодій між елементами системи допомагає виявити неявні ризики;

– розробка ефективних заходів. Комплексний підхід дозволяє розробляти більш дієві та системні заходи безпеки, спрямовані на усунення причин небезпек, а не лише на боротьбу з їх наслідками;

– прогнозування небезпечних ситуацій. Аналіз динаміки системи дозволяє прогнозувати можливі небезпечні сценарії;

– оптимізація ресурсів. Системний підхід допомагає ефективно розподіляти ресурси на заходи безпеки з урахуванням пріоритетності ризиків;

– підвищення культури безпеки. Сприяє формуванню у працівників розуміння взаємозв'язку між їх діями та рівнем безпеки.

Приклади застосування системного підходу в безпеці життєдіяльності [1]:

– на виробництві. Аналіз технологічного процесу як системи, виявлення небезпечних операцій, оцінка ризиків, розробка комплексних заходів безпеки (технічне переоснащення, навчання персоналу, використання ЗІЗ, контроль за дотриманням правил);

– у транспорті. Розгляд системи "водій - транспортний засіб - дорожнє середовище", аналіз факторів, що призводять до ДТП, розробка заходів (підготовка водіїв, технічний стан транспорту, організація дорожнього руху).

– у побут. Аналіз системи "людина - житло - побутові прилади", виявлення потенційних небезпек (електробезпека, пожежна безпека, газобезпека), розробка заходів (правила експлуатації приладів, встановлення детекторів диму та газу);

– у екологічній безпеці. Розгляд екосистеми як складної системи, аналіз впливу антропогенних факторів, розробка заходів щодо запобігання забрудненню та відновлення навколишнього середовища.

Таким чином, системний підхід є фундаментальним принципом сучасної безпеки життєдіяльності, що дозволяє комплексно та ефективно вирішувати проблеми забезпечення безпеки на всіх рівнях – від індивідуального до глобального..

ВИСНОВКИ

Результатом кваліфікаційної роботи є розроблений проект локальної мережі рекламного комп'ютерного клубу «Сталкер». Основні технічні характеристики розробленого проекту локальної мережі:

- фізична топологія – «гібридна»;
- технології використані для розробки мережі - IEEE 802.3ab, IEEE 802.11ac, IEEE 802.1Q;
- маршрутизатор-шлюз – Cisco ISR4221/K9;
- головний комутатор – Cisco C9200CX-8UXG-2X-E
- комутатори робочих груп – Cisco SG350X-48MP-K9-EU;
- безпровідна точка доступу – TP-LINK EAP225
- стек протоколів локальної мережі - TCP/IP версії 4.

В кваліфікаційній роботі спроектовано логічну та фізичну топологію мережі. Підібрано відповідне апаратне та програмне забезпечення. При виборі апаратного забезпечення (активного) враховано можливість масштабування локальної мережі в майбутньому.

Описано процедуру налаштування активного комутаційного обладнання. Розроблено інструкцію з тестування та налагодження мережі.

Логічна та фізична топології локальної мережі подано в графічній частині.

В економічній частині зроблено розрахунком повної вартості робіт по проектуванню, встановленню і запуску в експлуатацію мережі. Отримана вартість мережі є в межах запропонованої замовником.

Останній розділ роботи описує питання охорони праці, та техніки безпеки, які є важливими для безпечної праці користувачів комп'ютерної техніки

ПЕРЕЛІК ПОСИЛАНЬ

1. Атаманчук П. С., Мендерецький В. В., Панчук О. П. Чорна О. Г. Основи охорони праці. Навч. посіб. – К.: Центр учбової літератури, 2011. – 224 с.

2. Бедрій Я.І., Основи охорони праці : навчальний посібник для студентів вищих навчальних закладів / Я.І. Бедрій. Вид. 4-те переробл. і допов. — Тернопіль : Навчальна книга – Богдан, 2014. – 240 с.

3. Буров Є., Митник М. Комп'ютерні мережі.(у 2-х томах) Львів, Магнолія, 2018.

4. Єфіменко А. А. Основи побудови локальних комп'ютерних мереж Ethernet на базі керованих комутаторів компанії Cisco : навчальний посібник. – Житомир : Житомирська політехніка, 2021. – 116 с.

5. Комп'ютерні мережі / О. Д. Азаров, С. М. Захарченко, О. В. Кадук, М. М. Орлова, В. П. Тарасенко // Навчальний посібник. – Вінниця: ВНТУ, 2013./МОНУ (Лист №1/11 – 8260 від 15.05 2013 р.) - 500 с.

6. Жидецький В.Ц. Охорона праці користувачів комп'ютерів. Навчальний посібник. – Вид. 2-ге., доп. – Львів.: Афіша, 2000. – 176с.

7. Комп'ютерні мережі / О. Д. Азаров, С. М. Захарченко, О. В. Кадук, М. М. Орлова, В. П. Тарасенко // Навчальний посібник. – Вінниця: ВНТУ, 2013./МОНУ (Лист №1/11 – 8260 від 15.05 2013 р.) – 500 с.

8. Методичні вказівки до виконання дипломного проекту зі спеціальності 5.091504 «Обслуговування комп′ютерних та інтелектуальних систем та мереж» напрямок "Обслуговування технічних засобів комп'ютерних систем і мереж"

9. Технології захисту локальних мереж на основі обладнання CISCO : навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки, 2021. – 188 с.

10.Базові поняття мережевих технологій. URL: http://um.co.ua/8/8-17/8-1748.html. Дата доступу: 5.06.2024.

11.App.Diagrams сайт для створення схем URL: https://app.diagrams.net.

(Дата звернення: 14.05.2024)

12.Одескабель Cat.6 URL: https://odeskabel.com/ua/products/katalog-lan/lan-kabeli-kategorii-6/uutp-4pr-indoor.html. (Дата звернення: 16.05.2024)

13.Південкабель ОПТ-24А4 URL: https://www.yuzhcable.info/edata/mrr/501001090120072144/lang/en. (Дата звернення: 16.05.2024)

14. СЕРВЕРНА ШАФА CH-22U 600X600 ПЕРФОРАЦІЯ RAL9005 [електронний ресурс] – Режим доступу: https://ipcom.ua/uk/servernyj-shkaf-ipcom-sn-22u-600h600-perforacyya-ral9005

15.Комутатор Cisco SB SG350X-48MP-K9 [електронний ресурс]. Доступно: https://xn--h1aemkx.com.ua/kommutator-cisco-sb-sg350x-48mp-k9-eu.

16. Комутатор Cisco C9200CX-8UXG-2X-E [електронний ресурс]. Доступно: https://stack-systems.com.ua/ru/kommutator-cisco-c9200cx-8uxg-2x-e?srsltid=AfmBOopgUga2lqrl0E_vk-uiv8W8zyJ6ueFChR52PNaXcn7udQ_0ssTa.

17. Маршрутизатор Cisco ISR4221/K9 [електронний ресурс] – Доступно: https://stack-systems.com.ua/marshrutizator-cisco-isr4221-k9.

18.КПВ-ВП (250) URL: https://lantorg.com/products/odeskabel-kpv-vp-250-4h2h057-utp---cat6-vnutrenniy- korobka-305m/. (Дата звернення: 19.05.2024)

Додатки

Додаток А. План будівлі комп’ютерного клубу “Сталкер”