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-кваліфікаційний рівень)

на тему: Розробка проєкту комп'ютерної мережі туристичної компанії "Трайдент"

Виконав: студент(ка) IV курсу, групи КІ-418ск
Спеціальності **123 «Комп'ютерна інженерія»**
(шифр і назва напряму підготовки, спеціальності)

Павло ХАЛАК
(ім'я та прізвище)

Керівник Людмила ЦИМБАЛЮК
(ім'я та прізвище)

Рецензент
(ім'я та прізвище)

Тернопіль – 2024

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
"03" квітня 2024 року

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

_____Халаку Павлу Руслановичу_____
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи __ Розробка проєкту комп'ютерної мережі туристичної компанії "Трайдент"

керівник роботи __Цимбалюк Людмила Володимирівна
(прізвище, ім'я, по батькові)

Затверджені наказом ВСП «Тернопільський фаховий коледж ТНТУ імені Івана Пулюя» від 02.04.2024 р №4/9-157.

2. Строк подання студентом роботи: 17 червня 2024 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, техніка безпеки та екологічні вимоги.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
- плани 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, техніка безпеки та екологічні вимоги	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	04.04	
2	Збір і узагальнення інформації	13.05	
3	Написання першого розділу	20.05	
4	Розробка технічного та робочого проекту	27.05	
5	Написання спеціального розділу	3.06	
6	Розрахунок економічної частини	5.06	
7	Написання розділу охорони праці	7.06	
8	Виконання графічної частини	10.06	
9	Оформлення проекту	12.06	
10	Погодження нормоконтролю	14.06	
11	Попередній захист роботи	17.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 04 квітня 2024 року

Студент _____ Павло ХАЛАК
(підпис) (ім'я та прізвище)

Керівник роботи _____ Людмила ЦИМБАЛЮК
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Павло ХАЛАК. Розробка проєкту комп’ютерної мережі туристичної компанії «Трайдент»: кваліфікаційна робота на здобуття освітнього ступеня фаховий молодший бакалавр, за спеціальністю 123 Комп’ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2023. 83 с.

Кваліфікаційна робота фахового молодшого бакалавра присвячена розробці локальної комп’ютерної мережі для туристичної компанії "Трайдент".

В результаті аналізу комунікаційних потреб компанії «Трайдент» було сформовано технічне завдання на проектування локальної комп’ютерної мережі. Визначено топологію та архітектуру мережі, а також перелік необхідних вузлів. Проведено порівняльний аналіз і обрано моделі обладнання: комутаторів для ядра мережі та рівня доступу, файрволу, точок доступу, мережевих принтерів, серверів. Організовано та налаштовано поділ мережі на віртуальні підмережі. Обрано операційні системи для серверів та робочих станцій.

Розроблено логічну та фізичну топології мережі. Наведено інструкції з налаштування комутаційного устаткування локальної мережі, конфігурації файволу для організації доступу до Інтернет та моніторингу і діагностики мережі.

Ключові слова: локальна комп’ютерна мережа, активне мережеве обладнання, пасивне мережеве обладнання, віртуальні підмережі, комутатор, файрвол, точка доступу, сервер.

ЗМІСТ

ВСТУП

Сучасний розвиток суспільства невід'ємно пов'язаний із впровадженням інформаційних технологій у різні сфери діяльності. Комп'ютерні мережі стали фундаментом для ефективного обміну інформацією, забезпечуючи можливість зберігання, обробки та передачі даних. В умовах зростаючої цифровізації персональні комп'ютери та інші пристрої комунікації є невід'ємною частиною повсякденного життя, що підвищує важливість належної організації та безпеки інформаційних систем.

Локальні комп'ютерні мережі надають численні переваги, включаючи можливість спільного використання ресурсів, таких як принтери та сервери, що значно знижує накладні витрати та підвищує ефективність роботи компанії. Крім того, мережі дозволяють централізовано управляти комп'ютерним обладнанням і забезпечувати безпечний доступ до даних, що зменшує ризики втрати інформації та несанкціонованого доступу [1].

Правильне проектування мережі передбачає використання відкритих, кросплатформенних технологій, що забезпечує гнучкість і масштабованість мережевих рішень. Це дозволяє адаптуватися до швидкозмінних технологічних вимог і забезпечувати безперервність бізнес-процесів [2].

Метою цієї кваліфікаційної роботи є розробка комплексного проекту локальної комп'ютерної мережі для туристичної компанії «Трайдент». У результаті роботи буде створена документація, яка детально описує процеси проектування, впровадження та тестування мережі, що забезпечить її ефективне функціонування та відповідність сучасним стандартам безпеки та продуктивності.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Тема кваліфікаційної роботи: Розробка проєкту комп’ютерної мережі туристичної компанії «Трайдент».

Проєкт призначений для створення та впровадження локальної комп’ютерної мережі в офісних приміщеннях туристичної компанії «Трайдент» з метою забезпечення ефективної роботи співробітників та обслуговування клієнтів компанії.

1.1.2 Призначення розробки

Основним призначенням розробки є створення сучасної, надійної та безпечної комп’ютерної мережі, яка забезпечить безперебійний обмін інформацією між різними відділами компанії, доступ до Інтернету, захист даних та підтримку мережевих сервісів, таких як електронна пошта, CRM-система, бронювання турів та інші бізнес-додатки.

1.1.3 Вимоги до апаратного і програмного забезпечення

Для функціонування локальної комп’ютерної мережі туристичної компанії «Трайдент» потрібно вибрати та налаштувати таке апаратне забезпечення:

– маршрутизатор з підтримкою оптоволоконного підключення;

– міжмережевий екран (Firewall) з підтримкою VPN, IPS, фільтрації веб-контенту та антишкідливого ПЗ;

– керований комутатор рівня L2+ або L3 (Core Switch) з підтримкою VLAN;

– проміжні комутатори для підключення кінцевих пристроїв;

– сервери: файловий сервер, сервер баз даних, сервер електронної пошти, сервер резервного копіювання;

– мережеві принтери;

– точки доступу Wi-Fi з підтримкою WPA3;

– комп’ютери, ноутбуки та інші кінцеві пристрої для співробітників;

Щодо програмного забезпечення, то потрібно вибрати та налаштувати:

– операційні системи серверів;

– системи управління базами даних;

– програмне забезпечення для електронної пошти;

– CRM-система для управління взаємовідносинами з клієнтами;

– програмне забезпечення для резервного копіювання та відновлення даних;

– антивірусне програмне забезпечення.

1.1.4 Вимоги до документації

Документація по супроводу проектованої локальної мережі повинна включати [3]:

– технічну документацію на апаратне забезпечення;

– інструкції з налаштування та експлуатації мережевого обладнання;

– схеми мережі та плани розташування обладнання;

– документацію на програмне забезпечення та інструкції з його використання;

– політики безпеки та процедури резервного копіювання;

– посібники користувача для співробітників компанії.

1.1.5 Техніко-економічні показники

Впровадження локальної комп'ютерної мережі туристичної компанії «Трайдент» дозволить оптимізувати техніко-економічні показники її роботи, а саме забезпечить:

– зниження витрат на управління мережевими ресурсами та обслуговування;

– підвищення ефективності роботи співробітників за рахунок надійного і швидкого доступу до інформаційних ресурсів;

– безперервність бізнес-процесів за рахунок високої надійності мережі;

– зменшення часу на вирішення технічних проблем завдяки централізованому управлінню та моніторингу мережі.

1.1.6 Стадії та етапи розробки

Процес планування, проектування та розгортання локальної комп'ютерної мережі туристичної компанії «Трайдент» повинен включати такі етапи:

1. Аналіз вимог та проектування, який включає [3]:

– вивчення вимог бізнесу та технічних потреб;

– проектування мережевої інфраструктури та складання технічного завдання.

2. Підготовка специфікацій та закупівля необхідного обладнання та програмного забезпечення.

3. Монтаж та налаштування обладнання, який передбачає

– встановлення мережевого обладнання та кабельної інфраструктури.

– налаштування маршрутизаторів, комутаторів, міжмережевих

екранів та серверів.

4. Інсталяція та налаштування програмного забезпечення:

– встановлення операційних систем та серверного програмного забезпечення;

– налаштування CRM-системи, системи резервного копіювання та інших бізнес-додатків;

5. Тестування та перевірка:

– тестування мережі на предмет продуктивності, надійності та безпеки;

– виправлення виявлених проблем та недоліків.

6. Впровадження та навчання:

– введення мережі в експлуатацію;

– навчання персоналу використанню нових систем та процедур.

1.1.7 Порядок контролю та прийому

Порядок контролю та прийому повинен передбачати такі стадії та етапи:

– проміжні перевірки на кожному етапі розробки для виявлення та виправлення помилок;

– фінальне тестування всієї мережі перед введенням в експлуатацію;

– приймальні випробування з боку замовника для підтвердження відповідності мережі технічному завданню;

– документоване затвердження результатів тестування та приймання мережі;

– регулярний моніторинг та технічна підтримка після введення в експлуатацію з метою забезпечення безперебійної роботи проектованої локальної комп’ютерної мережі.

1.2 Постановка задачі на розробку проекту. Характеристика організації, для якої створюється проект мережі

Туристична компанія «Трайдент» потребує розробки сучасної, надійної та масштабованої комп'ютерної мережі, яка забезпечить ефективну роботу всіх підрозділів компанії. Основними задачами розробки та провадження проекту локальної мережі є:

– забезпечення безперебійного обміну інформацією між різними відділами компанії;

– підключення всіх робочих місць до мережевої інфраструктури;

– забезпечення надійного та швидкого доступу до Інтернету для всіх співробітників;

– реалізація мережевої безпеки з використанням міжмережевого екрану (Firewall) та інших засобів захисту;

– підтримка мережевих сервісів, таких як електронна пошта, CRM-система, системи бронювання та обслуговування клієнтів;

– впровадження системи резервного копіювання для захисту критичних даних;

– підготовка та надання технічної документації для управління та обслуговування мережі;

– навчання персоналу щодо використання нової інфраструктури.

Туристична компанія «Трайдент» є динамічною організацією, що спеціалізується на наданні широкого спектра туристичних послуг. Компанія має на меті забезпечити своїм клієнтам найкращий досвід планування та проведення подорожей, включаючи бронювання турів, організацію подорожей, консультації та підтримку клієнтів.

Структура компанії включає наступні підрозділи:

1. Адміністративний підрозділ, до якого входять:

– відділ кадрів (HR);

– відділ юридичного супроводу

2. Фінансово-економічний підрозділ, до якого входять:

– відділ фінансів;

– бухгалтерія.

3. Відділ підтримки і обслуговування клієнтів, до якого входять:

– відділ обслуговування клієнтів;

– відділ бронювання.

4. Відділ маркетингу і продажів, до якого входять:

– відділ маркетингу;

– відділ продажів.

5. Операційний підрозділ, до якого входять:

– відділ організації турів;

– відділ логістики.

6. Підрозділ розвитку та управління якістю, до якого входять:

– відділ досліджень та розвитку (R&D);

– відділ управління якістю.

7. IT-підрозділ, тобто відділ інформаційних технологій (IT)

Характеристики організації:

– кількість працівників: до 50 осіб, розподілених між різними відділами;

– головний офіс знаходиться в місті з розвиненою інфраструктурою та доступом до високошвидкісного Інтернету;

– основні напрямки діяльності: продаж турів, організація корпоративних та індивідуальних подорожей, бронювання квитків і готелів, надання консультаційних послуг, логістичне забезпечення подорожей.

Основні вимоги до мережі компанії «Трайдент»:

– висока надійність та доступність мережевих ресурсів;

– захист конфіденційної інформації клієнтів та фінансових даних;

– гнучкість і можливість масштабування мережі для підтримки

майбутнього зростання компанії;

– простота управління та моніторингу мережі;

– підтримка різноманітних мережевих сервісів та додатків, необхідних для щоденної роботи компанії.

Проектування мережі повинно враховувати ці вимоги та забезпечувати ефективну роботу всіх підрозділів компанії «Трайдент», що сприятиме підвищенню продуктивності працівників та рівня обслуговування клієнтів.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис та обґрунтування вибору логічного типу мережі

Компанія «Трайдент» має головний офіс із кількістю працівників до 50 осіб, динамічно розподілених між різними відділами. Логічна мережа для цієї компанії буде побудована за схемою локальної обчислювальної мережі. Логічна структура мережі відображає спосіб організації та взаємодії між різними пристроями в мережі [5].

Основними компонентами логічної мережі «Трайдент»:

– вузли (Nodes), тобто робочі станції, сервери, принтери та інші мережеві пристрої;

– комунікаційне середовище (Medium), для організації якого передбачено використання комутаторів (switches) та маршрутизаторів (routers) для з'єднання вузлів.

Для мережі туристичної компанії «Трайдент» обрана ієрархічна архітектура на основі зіркової топології з використанням керованих комутаторів на кожному рівні. Така архітектура дозволяє [6]:

– забезпечити високу надійність та безпеку мережі, коли відмова одного пристрою не впливає на всю мережу, а використання міжмережевого екрану (Firewall) підвищує рівень безпеки;

– забезпечити масштабованість мережі, тобто легке додавання нових пристроїв та сегментів мережі без значних змін в існуючій інфраструктурі.

– оптимізувати продуктивність мережі за рахунок розподілу навантаження між різними рівнями мережі, що дозволяє уникнути заторів та забезпечити швидкий доступ до ресурсів.

– забезпечити простоту управління та моніторингу за рахунок централізованого управління мережевими ресурсами, що дозволяє швидко виявляти та виправляти проблеми.

Таким чином, обрана топологія та архітектура найкраще відповідають вимогам та специфікаціям туристичної компанії «Трайдент», забезпечуючи необхідний рівень надійності, продуктивності та безпеки.

В якості протоколів передачі даних було прийнято рішення використовувати стандартні мережеві протоколи, такі як Ethernet для локальної мережі та TCP/IP для взаємодії з Інтернетом.

Логічна структура мережі типу "зірка" забезпечує легкість додавання нових пристроїв без значного впливу на існуючу мережу. Це важливо для компанії «Трайдент», оскільки кількість працівників може зростати, а також можуть додаватися нові відділи або пристрої.

У разі виходу з ладу одного з пристроїв (наприклад окремої робочої станції), інші пристрої продовжуватимуть функціонувати, що мінімізує час простою та підвищує надійність мережі.

Логічна мережа, побудована за типом "зірка", дозволяє зменшити затримки при передачі даних, оскільки кожен вузол має пряме з'єднання з центральним комутатором. Це особливо важливо для забезпечення високої швидкості роботи в умовах інтенсивного використання мережевих ресурсів.

Центральна точка управління дозволяє легше контролювати мережевий трафік, реалізовувати політики безпеки та виявляти потенційні загрози. Використання віртуальних локальних мереж (VLAN) дозволяє сегментувати мережу, що підвищує безпеку даних і знижує ризик несанкціонованого доступу.

Використання комутаторів замість більш складних та дорогих мережевих пристроїв знижує загальні витрати на побудову та обслуговування мережі. Це робить мережу економічно вигідною та доступною для компанії "Трайдент".

Використання маршрутизаторів дозволяє забезпечити надійний доступ до Інтернету, а також інтеграцію з віддаленими офісами або філіями компанії «Трайдент». Це забезпечує безперервну та ефективну комунікацію між

працівниками.

Враховуючи наведені аргументи, логічний тип мережі компанії «Трайдент» буде побудований за схемою локальної обчислювальної мережі з використанням топології "зірка". Це забезпечить високу продуктивність, надійність, безпеку та гнучкість мережі, що відповідає потребам компанії та сприяє її ефективній роботі та розвитку.

2.2 Розробка схеми фізичного розташування кабелів та вузлів

2.2.1 Типи кабельних з’єднань та їх прокладка

Для побудови локальної комп'ютерної мережі туристичної компанії «Трайдент» використовуються різні типи кабельних з'єднань, зокрема, мідні кабелі категорії 6 (Cat 6) для підключення робочих станцій, комутаторів та мережевих принтерів, а також оптоволоконні кабелі для підключення до провайдера Інтернету. Розглянемо типів кабелів та рекомендації щодо їх прокладки.

Мідні кабелі категорії 6 (Cat 6) будуть використовуватися для підключення робочих станцій, комутаторів рівня доступу (SW_2, SW_3), мережевих принтерів та точок доступу Wi-Fi.

Такий тип кабелю забезпечує високошвидкісну передачу даних до 10 Гбіт/с на відстані до 55 метрів та 1 Гбіт/с на відстані до 100 метрів, має відмінну стійкість до електромагнітних перешкод.

Оптоволоконні кабелі будуть використовуватися для підключення основного комутатора (SW_1) до провайдера Інтернету через файрвол, а також для з'єднання віддалених комутаторів, якщо відстань перевищує можливості мідних кабелів.

Даний тип кабелю забезпечує передачу даних на великі відстані без втрати якості сигналу, стійкі до електромагнітних перешкод та зовнішніх

впливів.

Мідні кабелі Cat 6 повинні бути прокладені так, щоб забезпечити мінімальну довжину та уникнути зайвих поворотів, що знижують якість сигналу [7]. Рекомендується прокладати кабелі в кабельних каналах або лотках для захисту від механічних пошкоджень.

Кабелі прокладаються від серверної кімнати до розподільчих вузлів (SW_2, SW_3), а потім до робочих станцій, мережевих принтерів та точок доступу Wi-Fi. Необхідно дотримуватися рекомендованої відстані між кабелями і джерелами електромагнітних перешкод (наприклад, силові кабелі).

Всі кабелі повинні бути чітко промарковані з обох кінців для полегшення ідентифікації та обслуговування.

Оптоволоконні кабелі повинні бути прокладені з урахуванням мінімальної кількості вигинів та перегинів для збереження цілісності сигналу. Рекомендується використовувати спеціальні захисні кожухи та канали для прокладки [8].

Кабель від провайдера Інтернету прокладається до файрволу у серверній кімнаті. При необхідності підключення віддалених комутаторів також використовується оптоволоконний кабель.

Всі оптоволоконні кабелі повинні бути чітко промарковані для уникнення плутанини та полегшення обслуговування.

Прокладка кабельних сегментів повинна здійснюватися з дотриманням загальних рекомендацій:

– для організації кабельних систем повинні використовуватися органайзери (короби чи кабельні лотки), які дозволили б підтримувати порядок і полегшели обслуговування мережі;

– всі кабелі повинні бути захищені від механічних пошкоджень та стороннього доступу;

– при прокладці кабелів у закритих просторах слід забезпечити

достатню вентиляцію для уникнення перегріву.

Прокладка кабелів повинна виконуватися з урахуванням всіх технічних вимог та стандартів для забезпечення надійної та ефективної роботи мережі туристичної компанії «Трайдент».

2.2.2 Будова вузлів та необхідність їх застосування

Фізична топологія мережі туристичної компанії «Трайдент» являє собою структуру, в якій кабелі та мережеві вузли (робочі станції, сервери, комутатори, точки доступу та принтери) розташовані у відповідності до логічної топології та потреб організації. Основні елементи фізичної топології включають комутатори рівня доступу (SW_1, SW_2, SW_3), основний комутатор (SW_1), сервери (S_1, S_2), точки доступу (AP_1, AP_2, AP_3) та мережеві принтери (PR_1 - PR_7).

Сервери (S_1, S_2) розміщені у спеціально обладнаній серверній кімнаті, яка забезпечує належні умови для безперебійної роботи серверів (контроль температури, вологості, безперебійне живлення). Сервери підключені безпосередньо до основного комутатора (SW_1) для забезпечення максимальної швидкості та надійності передачі даних. В цьому ж приміщення буде встановлений основний комутатор (SW_1).

Основний комутатор (SW_1) буде встановлений у серверній кімнаті для забезпечення централізованого управління мережею.

Файрвол (Firewall) буде розташований у серверній кімнаті між провайдером і основним комутатором. Він забезпечуватиме захист внутрішньої мережі від зовнішніх загроз та здійснюватиме управління міжмережевим трафіком.

Розглянемо кількісний розподіл робочих станцій по відділах компанії:

– у відділі кадрів (HR) буде встановлено 2 робочі станції (WS_1, WS_2);

– у відділі юридичного супроводу буде встановлено 2 робочі станції (WS_3, WS_4);

– у відділі фінансів буде встановлено 4 робочі станції (WS_5 - WS_8);

– у бухгалтерія буде встановлено 3 робочі станції (WS_9 - WS_11);

– у відділі обслуговування клієнтів буде встановлено 4 робочі станції (WS_12 - WS_15);

– у відділ бронювання буде встановлено 3 робочі станції (WS_16 - WS_18);

– у відділ маркетингу буде встановлено 3 робочі станції (WS_19 - WS_21);

– у відділ продажів буде встановлено 4 робочі станції (WS_22 - WS_25);

– у відділі організації турів буде встановлено 3 робочі станції (WS_26 - WS_28);

– у відділі логістики буде встановлено 2 робочі станції (WS_29, WS_30);

– у відділі управління якістю: 2 робочі станції (WS_31, WS_32);

– у відділі досліджень та розвитку (R&D) буде встановлено 2 робочі станції (WS_33, WS_34);

– у відділі інформаційних технологій (IT) буде встановлено 2 робочі станції (WS_35, WS_36).

Розміщення мережевих принтерів наступне :

– PR_1 встановлений у відділі обслуговування клієнтів та відділ бронювання;

– PR_2 встановлений у відділі організації турів та відділ логістики;

– PR_3 встановлений у відділі кадрів та відділ юридичного супроводу;

– PR_4 встановлений у відділі фінансів та бухгалтерія;

– PR_5 встановлений у відділі маркетингу та відділ продажів;

– PR_6 встановлений у відділі управління якістю та відділ досліджень та розвитку;

– PR_7 встановлений у відділі інформаційних технологій.

Точки доступу Wi-Fi (AP) розміщені по наступних принципах:

– AP_1 покриває зону відпочинку та кабінети найближчих відділів (відділ кадрів, юридичного супроводу, фінансів, бухгалтерії);

– AP_2 покриває зону маркетингу, продажів, обслуговування клієнтів та бронювання;

– AP_3 покриває відділи організації турів, логістики, управління якістю, досліджень та розвитку, IT.

Розподільчі вузли (комутатори) будуть встановлені так:

– SW_1 (Core switch) - у серверній кімнаті, де знаходяться сервери. Виконує роль основного комутатора, до якого підключені всі інші комутатори рівня доступу та сервери;

– SW_2, SW_3 (Access switches) - в приміщеннях, де є найбільша концентрація робочих станцій. Наприклад, SW_2 розташований ближче до відділів продажів, маркетингу, обслуговування клієнтів та бронювання, тоді як SW_3 покриває відділи організації турів, юридичного супроводу, IT та фінансів.

Отже мережеві вузли туристичної компанії «Трайдент» розміщені у відповідності до їх функціональних потреб та з урахуванням зручності доступу та ефективного використання ресурсів. Сервери знаходяться у серверній кімнаті, що забезпечує належні умови для їх безперебійної роботи. Робочі станції розподілені по кабінетах відділів, забезпечуючи оптимальну продуктивність кожного підрозділу. Мережеві принтери розташовані у стратегічних місцях для зручності користування, а точки доступу Wi-Fi забезпечують надійне покриття бездротовим зв'язком у всіх необхідних зонах. Комутатори рівня доступу розміщені в місцях з найбільшою концентрацією робочих станцій для забезпечення максимальної ефективності

мережі. Файрвол, розташований у серверній кімнаті, забезпечує надійний та захищений доступ до Інтернету для всієї компанії.

2.3 Обґрунтування вибору обладнання для мережі

2.3.1 Вибір пасивного обладнання мережі

Пасивне обладнання є фундаментальною частиною будь-якої комп'ютерної мережі, оскільки забезпечує фізичну інфраструктуру для передачі даних. Для побудови надійної та ефективної мережі туристичної компанії "Трайдент" було вибрано пасивне обладнання, яке відповідає сучасним стандартам і вимогам. Ключовими компонентами пасивного мережевого обладнання є:

– кабельні системи;
– роз'єми та конектори;
– патч-панелі;
– кабельні органайзери та канали;
– кабельні шафи та стійки.

До кабельних сисем належать мідні кабелі та оптоволоконні кабелі.

Мідні кабелі (див. рис. 2.1) категорії 6 (Cat 6) будуть використовуватися для підключення робочих станцій, комутаторів, мережевих принтерів та точок доступу Wi-Fi.

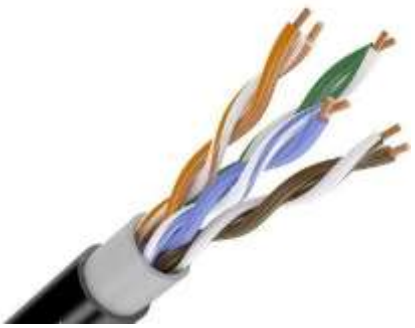

Рисунок 2.1 - Мідний кабель категорії 6 (Cat 6)

Даний тип кабелю забезпечує пропускну здатність до 10 Гбіт/с на відстані до 55 метрів і 1 Гбіт/с на відстані до 100 метрів. Має високу стійкість до електромагнітних перешкод завдяки щільному екрануванню.

Мідні кабелі Cat 6 є оптимальними для внутрішньої кабельної інфраструктури через їх високу швидкість передачі даних та надійність.

Оптоволоконні кабелі в проектованій мережі будуть використовуватися для підключення основного комутатора (SW_1) до провайдера Інтернету через файрвол, а також для з'єднання віддалених комутаторів, якщо відстань перевищує можливості мідних кабелів.

Даний тип кабелю забезпечує передачу даних на великі відстані без втрат якості сигналу. Оптоволокно стійке до зовнішніх впливів та електромагнітних завад.

Рисунок 2.2 - Оптоволоконний типу OM3

Для туристичної компанії «Трайдент» рекомендується використовувати оптоволоконний кабель (див. рис. 2.2) типу OM3 (відомий також як лазерно-оптимізоване багатомодове волокно) для підключення до провайдера Інтернету та для міжвіддалених з'єднань в межах будівлі.

Технічні характеристики оптоволоконного кабелю:

– тип волокна: багатомодове (Multi-Mode);
– діаметр сердечника: 50 мікрометрів;

– довжина хвилі: 850 нм та 1300 нм;

– пропускна здатність: підтримує швидкість передачі до 10 Гбіт/с на відстані до 300 метрів, та 40 Гбіт/с або 100 Гбіт/с на коротших відстанях з використанням відповідного обладнання;

– стандарт: Відповідає стандартам ISO/IEC 11801 та TIA-568-C.3

Використання такого типу кабелю забезпечує підтримку високошвидкісних з'єднань, що критично важливо для основного підключення до Інтернету та внутрішніх мережевих з'єднань;

Даний тип кабелю сумісний з сучасним мережевим обладнанням, таким як комутатори та маршрутизатори з підтримкою 10GBASE-SR, 40GBASE-SR4 та 100GBASE-SR10 та має високу стійкість до електромагнітних перешкод, що забезпечує стабільну роботу навіть у середовищах з високим рівнем електромагнітного випромінювання.

Хоча OM3 кабель дорожчий за деякі інші типи багатомодових волокон, він забезпечує значно більшу пропускну здатність та дозволяє будувати масштабовані мережі з урахуванням майбутніх потреб [9].

Щодо використання оптоволокна в мережі "Трайдент", то цей тип кабелю буде використаний для:

– основного підключення до Інтернету, тобто підключення файволу до провайдера Інтернету;

– з'єднання між комутаторами в різних частинах будівлі, де використання мідних кабелів недоцільне через великі відстані.

Таким чином, оптоволоконний кабель OM3 є оптимальним вибором для мережі туристичної компанії «Трайдент», забезпечуючи високу швидкість передачі даних, надійність та готовність до майбутнього розширення мережевої інфраструктури.

Щодо роз'єми та конекторів, то в проектованій мережі туристичної компанії «Трайдент» будуть використані RJ45 конектори для Cat 6 (див. рис. 2.3). Ці конектори будуть використовуватися для завершення мідних кабелів.

Даний тип конектора має високу надійність контактів та відповідає стандартам TIA/EIA-568-B, що забезпечує сумісність та стабільну роботу.

Рисунок 2.3 – Конектор RJ45 для Cat 6

Також в мережі будуть використані SC/LC конектори для завершення оптоволоконних кабелів (див. рис. 2.4). Цей тип конектора має низький коефіцієнт втрат сигналу, високу точність з'єднань, що забезпечує стабільну та якісну передачу даних.

Рисунок 2.4– Конектор SC/LC для завершення оптоволоконних кабелів

Отже SC/LC конектори забезпечують надійне та швидке з'єднання оптоволоконних кабелів, що є критично важливим для високошвидкісної передачі даних.

Патч-панелі для Cat 6 (див. рис. 2.5) використовуються для організації та управління з'єднаннями мідних кабелів у серверній кімнаті та розподільчих вузлах. Відповідність стандартам Cat 6 забезпечує високошвидкісну передачу даних, зручність у монтажі та обслуговуванні. Патч-панелі дозволяють організувати кабельну систему таким чином, щоб

забезпечити легкий доступ до з'єднань та зменшити ризик виникнення помилок під час експлуатації.

Рисунок 2.5 - Патч-панель для Cat 6

Кабельні органайзери та канали в проектованій мережі будуть використовуватися для підтримання порядку в кабельних системах, що забезпечує зручність у обслуговуванні та зменшує ризик пошкодження кабелів. Як правило вони міцні, легкі у використанні, з можливістю маркування кабелів. Таким чином органайзери допомагають уникнути плутанини кабелів, що сприяє підвищенню ефективності роботи мережі та зручності у обслуговуванні.

Кабельні канали (див. рис. 2.6) в мережі туристичної компанії «Трайдент» будуть використовуватися для прокладки кабелів по приміщеннях, забезпечуючи їх захист від механічних пошкоджень та електромагнітних перешкод. Як правило вони виготовлені з негорючих матеріалів, легко монтуються, дозволяють приховати кабелі. Кабельні канали забезпечують безпеку кабельної системи та естетичний вигляд приміщень.

Рисунок 2.6 - Кабельні канали

Щодо кабельних шаф та стійок, то в проектованій мережі будуть використані 19-дюймові серверні шафи (див. рис. 2.7) для розміщення серверів, комутаторів, патч-панелей та іншого мережевого обладнання. Такий тип обладнання має вентиляцію, можливість закривання на ключ для забезпечення безпеки, підтримка органайзерів та патч-панелей. Серверні шафи забезпечують зручний доступ до обладнання, підтримують порядок та сприяють охолодженню обладнання.

Рисунок 2.7 - Серверна шафа

Отже вибір пасивного обладнання для мережі туристичної компанії «Трайдент» базується на вимогах до швидкості, надійності та безпеки передачі даних. Мідні та оптоволоконні кабелі, разом із відповідними роз'ємами, патч-панелями, кабельними органайзерами та шафами, забезпечують оптимальні умови для стабільної роботи мережі та зручність в обслуговуванні.

2.3.2 Вибір активного обладнання мережі

Активне мережеве обладнання є ключовою частиною мережевої інфраструктури, оскільки воно забезпечує передачу, маршрутизацію та управління даними. Для побудови надійної, швидкої та безпечної мережі туристичної компанії "Трайдент" потрібно обрати наступне активне обладнання:

– основний комутатор (Core Switch);
– проміжні комутатори (Access Switches);
– файрвол (Firewall);
– безпровідні точки доступу (Wi-Fi Access Points);
– сервери;
– мережеві принтери.

Основний комутатор (Core Switch), позначений на топологіях SW_1, розміщений у відділі інформаційних технологій (IT). Забезпечує централізоване управління трафіком і виконує маршрутизацію між підмережами. Тобто SW_1 виконує функції комутації та маршрутизації між різними підмережами, забезпечуючи централізоване управління трафіком.

Для вибору моделі комутатора SW_1, який буде виконувати роль основного комутатора (Core Switch), розглянемо порівняльну таблицю 2.1 з кількома моделями керованих L3 комутаторів.

Таблиця 2.1 – Порівняльна таблиця для вибору моделі комутатора SW_1

Критерії	Cisco Catalyst 9300 Series	HP Aruba 3810M Series	Juniper EX3400 Series
1	2	3	4
Модель	C9300-24T-A	JL428A	EX3400-24T

Критерії	Cisco Catalyst 9300 Series	HP Aruba 3810M Series	Juniper EX3400 Series
1	2	3	4
Кількість портів	24 x 1G, 4 x 10G SFP+	24 x 1G, 4 x 10G SFP+	24 x 1G, 4 x 10G SFP+
Пропускна здатність (Gbps)	240	272	256
Функціональність Layer 3	OSPF, BGP, ISIS, RIP, EIGRP	OSPF, BGP, RIP	OSPF, BGP, RIP, EIGRP
Підтримка VLAN	Так	Так	Так

Продовження таблиці 2.1

1	2	3	4
Підтримка PoE	Так (до 437W на порт)	Так (до 600W на порт)	Так (до 100W на порт)
QoS (Quality of Service)	Так	Так	Так
Підтримка стекування	Так	Так	Так
Ціна, грн	152000	133000	50820

В результаті порівняння очевидними видаються такі висновки:

Cisco Catalyst 9300 Series має певні переваги: потужну Layer 3 функціональність з підтримкою різних протоколів маршрутизації, велика підтримку PoE, надійність і високу якість обслуговування (QoS). Недоліком такого вибору є висока ціна.

HP Aruba 3810M Series має переваги: відмінну пропускну здатність, велику підтримка PoE, хорошу Layer 3 функціональність. Недоліком HP Aruba 3810M Series є дещо вища ціна порівняно з Juniper EX3400.

Щодо Juniper EX3400 Series (див. рис. 2.8), то перевагами його є: найнижча ціна з трьох, хороша Layer 3 функціональність, підтримка QoS та VLAN, підтримка PoE. Слабкою стороною є дещо менша потужність PoE порівняно з Cisco і HP Aruba.

Рисунок 2.8 – Комутатор Juniper EX3400-24T

Отже на основі аналізу, для туристичної компанії «Трайдент» в якості основного L3-комутатора доцільним буде вибрати Juniper EX3400 Series. Він забезпечує всі необхідні функціональності, включаючи підтримку Layer 3 протоколів, QoS, VLAN, та PoE, при цьому має найнижчу ціну з трьох розглянутих моделей. Це дозволяє забезпечити необхідну продуктивність і функціональність мережі, зберігаючи бюджет компанії [12]. Детальніші характеристико мутатора подані в додатку А квалффікаційної роботи.

Проведемо порівняльний аналіз та вибір проміжних комутаторів (SW_2 та SW_3). Основними критеріями для порівняння є:

– наявність відповідної кількості 1G портів;

– підтримка VLAN.

Для вибору комутаторів рівня доступу розглянемо таблицю 2.2 з порівняльними характеристиками керованих L2 комутаторів.

Таблиця 2.2 – Вибір моделі L2-керовних комутаторів (SW_2 та SW_3)

Критерії	Cisco Catalyst 2960-X Series	HP Aruba 2530 Series	Juniper EX2300 Series
1	2	3	4
Модель	WS-C2960X-24TS-L	JL357A	EX2300-24T
Кількість портів	24 x 1G, 4 x 1G SFP	24 x 1G, 4 x 1G SFP	24 x 1G, 4 x 10G SFP+
Пропускна здатність (Gbps)	216	56	128
Функціональність Layer 2	STP, RSTP, MSTP, IGMP Snooping	STP, RSTP, MSTP, IGMP	STP, RSTP, MSTP, IGMP Snooping
Підтримка VLAN	Так	Так	Так
Підтримка PoE	Так (370W)	Так (144W)	Так (370W)
QoS	Так	Так	Так

Продовження таблиці 2.2

1	2	3	4
Підтримка стекування	Так	Ні	Так
Ціна, грн	95000	30244	68400

В результаті порівняльного аналізу вибір було зупинено на моделі Juniper EX2300-24T (див. рис. 2.9). Перевагами даної моделі є висока пропускна здатність, повна підтримка функціональності Layer 2, підтримка PoE з високою потужністю. До недоліків можна віднести дещо вищу ціну порівняно з HP Aruba, однак нижчу ніж у Cisco.

Рисунок 2.9 – Комутатор Juniper EX2300-24T

Таким чином на основі аналізу, для використання в якості проміжних комутаторів SW_2 та SW_3 доцільно вибрати Juniper EX2300 Series. Він забезпечує всі необхідні функціональності, включаючи підтримку Layer 2 протоколів, QoS, VLAN, та PoE, при цьому має високу пропускну здатність і підтримує стекування. Цей вибір дозволяє забезпечити надійну та ефективну роботу мережі, залишаючись в рамках розумного бюджету [13]. Детальніші характеистики моделі Juniper EX2300-24T подані в додатку Б кваліфікаційної роботи.

Перейдемо до вибору моделі файрволу (Firewall), основним функціональним призначенням якого є захист мережі від зовнішніх загроз, здійснює контроль доступу до мережі.

Критеріями для вибору є:

– пропускна здатність до 10 Гбіт/с;
– підтримка IPS, VPN, антивірусного захисту;
– висока продуктивність та низька затримка.

Розглянемо порівняльну таблицю 2.3 з кількома моделями файволів.

Таблиця 2.3 – Вибір файрволу

Критерії	Cisco ASA 5506-X	Fortinet FortiGate 60E	Palo Alto PA-220
Пропускна здатність (Gbps)	0.75	1	0.5
VPN пропускна здатність (Mbps)	100	75	100
Макс. кількість користувачів	50	100	50
Підтримка SSL VPN	Так	Так	Так
Підтримка IPSec VPN	Так	Так	Так
Ціна, грн.	23000	19880	22500

В результаті порівняння було обрано модель файрволу Fortinet FortiGate 60E (див рис. 2.10). Він пропонує найкращу пропускну здатність і максимальну кількість користувачів за найнижчою ціною. Тобто Fortinet FortiGate 60F поєднує в собі функціональність та високу продуктивність, забезпечуючи надійний захист мережі "Трайдент". Детальні характеристики файрволу подані в додатку В кваліфікаційної роботи.

Рисунок 2. 10 – Файрвол Fortinet FortiGate 60F

Виберемо модель точок доступу, які будуть забезпечувати бездротове покриття у приміщеннях компанії.

Основними критеріями для вибору є:

– підтримка стандартів 802.11ac.

– двочастотний режим (2.4 ГГц та 5 ГГц).

– висока пропускна здатність та покриття.

Розглянемо порівняльну таблицю 2.4 з кількома моделями точок безпровідного доступу.

Таблиця 2.4 – Вибір точки доступу (Wi-Fi Access Points)

Критерії	Ubiquiti UniFi AP AC Pro	Cisco Aironet 1832i	Aruba Instant On AP22
Частотний діапазон	2.4GHz / 5GHz	2.4GHz / 5GHz	2.4GHz / 5GHz
Пропускна здатність (Mbps)	1300	867	1200
Макс. кількість клієнтів	200	200	200
Підтримка PoE	Так	Так	Так
Ціна, грн	4940	11400	5700

В результаті порівняння було обрано точку доступу Ubiquiti UniFi AP AC Pro. Вона забезпечує високу швидкість бездротового з'єднання, легке управління та масштабованість.

Виберемо серверне обладнання для проектованої мережі. У інформаційно-технічному відділі компанії «Трайдент» буде встановлено два сервери (позначені S_1 та S_2).

Сервер S_1 виконуватиме ролі:

– DNS-сервера;

– веб-сервера;

– поштового сервера.

Сервер S_2 виконуватиме ролі:

– файл-сервера;

– buckup –сервера.

Розглянемо порівняльну таблицю 2.5 для вибору сервера S_1.

Таблиця 2.5 – Вибір серверного обладнання

Критерії	Dell PowerEdge R540	HPE ProLiant DL360 Gen10	Lenovo ThinkSystem SR530
Процесор	Intel Xeon Silver 4210	Intel Xeon Silver 4210	Intel Xeon Silver 4210
Оперативна пам'ять (GB)	32	32	32
Зберігання даних (TB)	2	2	2
Підтримка RAID	Так	Так	Так
Ціна, грн.	171000	182400	159600

За підсумками порівняння було обрано модель сервера Lenovo ThinkSystem SR530 (див. рис. 2.11), яка пропонує всі необхідні функціональності за найнижчою ціною.

Рисунок 2.11 – Сервер Lenovo ThinkSystem SR530

Ключові характеристики Lenovo ThinkSystem SR530:

– підтримка процесорів Intel Xeon Scalable;

– до 1.5 ТБ оперативної пам'яті;

– можливість встановлення до 4 жорстких дисків.

Сервер Lenovo ThinkSystem SR530 забезпечує високу продуктивність,

надійність та гнучкість у налаштуванні, що дозволяє виконувати різні мережеві завдання.

В якості сервера S_2 було прийнято рішення вибрати модель сервера Synology RackStation RS3617xs+ (див. рис. 2.12), який забезпечує централізоване зберігання та управління даними.

Рисунок 2.12 – NAS Synology RackStation RS3617xs+

Ключові характеристики Synology RackStation RS3617xs+:

– підтримка до 12 дисків.
– підтримка RAID для захисту даних.
– висока пропускна здатність.

Synology RackStation RS3617xs+ забезпечують надійне зберігання даних, легке управління та високу продуктивність.

Виберемо модель мережевого принтера. Для цього розглянемо порівняльну таблицю 2.6.

Таблиця 2.6 – Вибір моделі мережевого принтера

Критерії	HP LaserJet Pro MFP M428fdw	Brother MFC-L8900CDW	Canon imageCLASS MF743Cdw
1	2	3	4
Технологія друку	Лазер	Лазер	Лазер
Швидкість друку (ppm)	40	33	28

Продовження таблиці 2.6

1	2	3	4
Двосторонній друк	Так	Так	Так
Підключення	Ethernet, Wi-Fi	Ethernet, Wi-Fi	Ethernet, Wi-Fi
Ціна	15200	22800	19000

За результатами аналізу порівняльної таблиці було прийнято рішення вибрати для проектованої мереже модуль мережевого принтера HP LaserJet Pro MFP M428fdw. Дана модель пропонує високу швидкість друку та весь необхідний функціонал за найнижчою ціною.

Виберемо блоки безперебійного живлення (UPS), які потрібно встановити у кожній серверній шафі проектованої мережі. При такому виборі слід враховувати кілька важливих факторів: потужність кожної серверної шафи, час автономної роботи, розширюваність, тип батарей та можливість моніторингу. Для такої мережі доцільно розглянути моделі UPS, які забезпечать надійний захист та стабільну роботу обладнання.

Критеріями порівняння блоків безперебійного живлення (UPS) будуть:

– модель;
– потужність (VA/W);
– час автономної роботи (за половинного навантаження);
– тип батарей;
– розширюваність батарей;
– порти для підключення;
– мережевий моніторинг;
– ціна.

Розглянемо порівняльну таблицю 2.7 з кількома моделями блоків безперебійного живлення (UPS), які можна було б встановити у серверних шафах компанії «Трайдент».

Таблиця 2.7 – Вибір моделі блоків безперебійного живлення

Критерії	APC Smart-UPS SRT 3000VA (SRT3000RMXLA)	Eaton 9PX 3000VA (9PX3000RTN)	Vertiv Liebert GXT4 3000VA (GXT4-3000RT120)
Потужність (VA/W)	3000VA / 2700W	3000VA / 2700W	3000VA / 2700W
Час автономної роботи	10 хв (за половинного навантаження)	11 хв (за половинного навантаження)	12 хв (за половинного навантаження)
Тип батарей	Змінні внутрішні батареї	Змінні внутрішні батареї	Змінні внутрішні батареї
Розширюваність батарей	Так	Так	Так
Порти для підключення	8 x NEMA 5-15R, 2 x NEMA 5-20R	8 x NEMA 5-15R, 2 x NEMA 5-20R	8 x NEMA 5-15R, 2 x NEMA 5-20R
Мережевий моніторинг	Так (через SmartSlot)	Так	Так
Ціна, грн	83600	57210	79800

В результаті порівняльного аналізу було обрано модель безперебійого живлення Eaton 9PX 3000VA (9PX3000RTN).

Дана модель пропонує довгий час автономної роботи, можливість розширення батарей, мережевий моніторинг і при цьому має найкраще співвідношення ціна/якість серед розглянутих моделей. Це забезпечить надійний захист для трьох серверних шаф в мережі туристичної компанії "Трайдент".

Зведемо все вибране пасивне та активне мережеве обладнання у окрему підсумкову таблицю 2.8.

Таблиця 2.8 – Перелік вибраного мережевого обладнання

Назва	Позн.	Модель	Одиниці вим.	Кількість	Вартість, грн / одиницю
1	2	3	4	5	6
Кабель мідний	-	Cat 6 (бухта 305 м)	шт.	2	1740
Конектор	-	RJ-45 cat 6	шт.	200	4
Кабель оптичний	-	CMS-U-BQ(BN)H 8F G50/125 OM3	м.	86	81
Конектор SC / LC	-	Фаст-конектор SC/UPC	шт.	12	31
Трансивер	-	SFP+ 10G 300m 850nm DOM LC (SFP-10G-SR)	шт.	6	590
Короб	-	40*25*2м	шт.	120	25
Органайзер для кабеля		1U	шт.	3	164
Серверна шафа	-	6U	шт.	2	3970
Серверна шафа	-	9U	шт.	1	5355
Патч-панель	-	RJ45 cat6 24 port	шт.	3	1215
Комутатор (Core)	SW_1	Juniper EX3400-24T	шт.	1	50820
Комутатор (проміжний)	SW_2, SW_3	Juniper EX2300-24T	шт.	2	30244
Файрвол	FW_1	Fortinet FortiGate 60E	шт.	1	19880

Продовження таблиці 2.8

1	2	3	4	5	6
Точка доступу	AP_1 – AP_3	Ubiquiti UniFi AP AC Pro	шт.	3	4940
Сервер	S_1	Lenovo ThinkSystem SR530	шт.	1	159600
Сервер	S_2	Synology RackStation RS3617xs+	шт.	1	132450
Мережевий принтер	PR_1 – PR_7	HP LaserJet Pro MFP M428fdw	шт.	7	15200
Блок безпереб. живлення	-	Eaton 9PX 3000VA	шт.	3	57210

Активне мережеве обладнання, обране для мережі туристичної компанії "Трайдент", забезпечує необхідний рівень продуктивності, надійності та безпеки. Вибрані моделі комутаторів, точок доступу, файрволу, серверів та систем зберігання даних відповідають сучасним стандартам та забезпечують стабільну роботу мережі з можливістю масштабування у майбутньому. Особливо важливим є те, що основний комутатор (SW_1) буде виконувати функції маршрутизації між підмережами, що значно спрощує архітектуру та підвищує ефективність роботи мережі.

2.4 Особливості монтажу мережі

Монтаж комп’ютерної мережі туристичної компанії «Трайдент» включає кілька ключових етапів, кожен з яких потребує особливої уваги для забезпечення надійності, ефективності та безпеки мережевої інфраструктури.

На етапі підготовчих робіт потрібно виконати:

– огляд приміщень, тобто аналіз планування офісу для визначення

оптимальних місць прокладки кабелів і встановлення мережевого обладнання;

– проектування траси кабелів, тобто визначення шляхів прокладки кабелів з урахуванням мінімізації перешкод та забезпечення естетичності.

На етапі прокладки кабелів потрібно виконати:

– власне прокладку кабелів в кабель-каналах або підвісних стелях для зменшення впливу зовнішніх факторів. Особлива увага на даному етапі приділяється дотриманню мінімальних радіусів згину та захисту від механічних пошкоджень.

– маркування кабелів відповідно до їх призначення для полегшення подальшого обслуговування.

На етапі встановлення мережевого обладнання потрібно:

– установити три серверні шафи у виділених технічних зонах для розміщення активного та пасивного обладнання;

– встановити комутатори SW_1 (центральний), SW_2 та SW_3 (проміжні) у відповідних шафах з забезпеченням резервного живлення;

– підключити сервери та робочі станції до центрального комутатора та робочих станцій до проміжних комутаторів.

Далі потрібно провести установку спеціального обладнання:

– встановити файрвола у центральній серверній шафі для забезпечення захисту мережі;

– розмістити точки доступу у стратегічних місцях для забезпечення оптимального покриття бездротової мережі.

Після цього потрібно провести тестування та налаштування мережі, тобто:

– виконати тестування всіх кабельних з'єднань на відповідність стандартам і виявлення можливих проблем;

– налаштувати конфігурацію комутаторів, файрвола та інших мережевих пристроїв для забезпечення оптимальної роботи мережі.

– провести комплексне тестування мережі для перевірки її працездатності, продуктивності та безпеки.

Монтаж мережі туристичної компанії «Трайдент» включає ретельне планування, професійне виконання робіт з прокладки кабелів та встановлення обладнання, а також всебічне тестування та налаштування для забезпечення надійної та безперебійної роботи мережевої інфраструктури.

2.5 Обґрунтування вибору операційних систем та програмного забезпечення для серверів та робочих станцій в мережі

Сервер S_1 (модель Lenovo ThinkSystem SR530) обраний для виконання ролей: DNS-сервера, веб-сервера та поштового сервера. Для забезпечення надійності, безпеки та ефективного функціонування цих ролей будемо виберемо операційні системи та програмне забезпечення.

В якості операційної системи обрано Ubuntu Server 22.04 LTS. Це популярна серверна операційна система з довгостроковою підтримкою, що забезпечує стабільність та безпеку. Вона широко підтримується спільнотою та має великий набір пакетів для різних серверних ролей.

Для роботи DNS-сервер встановимо BIND (Berkeley Internet Name Domain) - один з найпоширеніших DNS-серверів у світі, забезпечує надійне та масштабоване вирішення DNS-запитів.

Для роботи веб-сервер встановимо Apache HTTP Server - популярний веб-сервер з відкритим вихідним кодом, що забезпечує високу продуктивність та надійність, а також Nginx, який буде використаний як зворотний проксі-сервер для покращення продуктивності та безпеки.

Для роботи поштового сервера встановимо Postfix - надійний та продуктивний поштовий сервер, який використовується для надсилання та отримання електронної пошти.

Також на сервері встановимо:

– SpamAssassin - інструмент для фільтрації спаму;

– ClamAV - антивірусне програмне забезпечення для сканування вхідної та вихідної пошти.

Сервер S_2 (модель Synology RackStation RS3617xs+) обраний для виконання ролей файл-сервера та backup-сервера. Цей сервер має вбудовану операційну систему та програмне забезпечення від Synology, яке оптимізоване для цих завдань. Операційна система Synology DiskStation Manager (DSM) - пропрієтарна операційна система від Synology, яка забезпечує зручний веб-інтерфейс та широкий набір функціональних можливостей для управління файлами та резервним копіюванням.

Для роботи файл-сервера буде використано:

– File Station - інструмент для управління файлами через веб-інтерфейс.

– SMB/AFP/NFS - підтримка різних протоколів доступу до файлів для забезпечення сумісності з різними операційними системами.

Для роботи Backup-сервер використаємо інфстументи:

– Hyper Backup - для резервного копіювання даних з різних пристроїв та збереження їх на сервері Synology.

– Snapshot Replication - для забезпечення високої надійності даних шляхом створення моментальних знімків.

Для робочих станцій компанії «Трайдент» слід вибрати операційні системи та програмне забезпечення, що забезпечують стабільну та безпечну роботу співробітників.

В якості операційних систем робочих станцій в компанії використовуються:

– Windows 10 Pro - популярна операційна система для бізнес-користувачів, яка забезпечує сумісність з більшістю бізнес-додатків та має вбудовані засоби безпеки.

– Ubuntu 22.04 LTS - вільна операційна система з довгостроковою

підтримкою, яка є стабільною та надійною альтернативою для робочих станцій, особливо для технічних спеціалістів.

Програмне забезпечення, яке використовується для робочих станцій:

– Microsoft Office 365 - пакет офісних програм для продуктивної роботи з документами, таблицями та презентаціями.

– Mozilla Firefox/Google Chrome - веб-браузери для безпечного та швидкого перегляду Інтернету.

– Antivirus Software - для забезпечення безпеки робочих станцій від вірусів та шкідливого ПЗ.

– Slack/Microsoft Teams - інструменти для комунікації та співпраці в команді.

– VLC Media Player - для відтворення мультимедійних файлів.

– Adobe Acrobat Reader - для перегляду та управління PDF-документами.

Таким чином обрані операційні системи та програмне забезпечення для серверів та робочих станцій забезпечують надійну, стабільну та безпечну роботу всієї мережі туристичної компанії «Трайдент». Вони відповідають вимогам сучасного бізнесу та сприяють підвищенню продуктивності та ефективності роботи співробітників.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкція з налаштування активного комутаційного обладнання

Одним з ключових етапів налаштування активного комутаційного обладнання є налаштування поділу прокованої мережі на підмережі (VLAN). Це забезпечить підвищену безпеку, ефективне управління трафіком і оптимізацію роботи мережевих ресурсів туристичної компанії «Трайдент». Основні принципи поділу мережі включають ізоляцію критичних сегментів, покращення контролю доступу і забезпечення масштабованості мережі.

Поділ на підмережі дозволить:

– обмежити доступу до критичних сегментів мережі та мінімізути ризики внутрішніх загроз;

– спростити управління мережею за рахунок розподілу різних функціональних відділів у окремі підмережі;

– легко додавати нові відділи чи пристроїв без порушення існуючої структури;

– зменшити кількість широкомовних повідомлень та підвищення швидкості обміну даними.

При поділі проектованої мережі на підмережі важливо дотримуватися таких принципів:

– функціональної ізоляції, згідно якої кожен відділ або група відділів, що виконують схожі функції, отримують окрему підмережу;

– ізоляції критичних ресурсів, тобто сервери, файрвол та інші критичні ресурси розміщуються в окремих підмережах з обмеженим доступом;

– планування зростання, тобто проектування підмереж повинно здійснюватися з урахуванням майбутнього розширення мережі.

Розглянувши основні цілі та принципи поділу мережі туристичної компанії «Трайдент» на підмережі, було прийнято рішення налаштувати підмережі у відповідності до описаних її підрозділів. Характеристики яких описані в таблиці 3.1.

Таблиця 3.1 – Підмережі проектованої мережі

Підрозділ	Підмережа	Функції
Адміністративний підрозділ	192.168.10.0/24	Управління кадрами (HR), юридична підтримка
Фінансово-економічний підрозділ	192.168.20.0/24	Фінансове управління, бухгалтерія
Відділ підтримки і обслуговування клієнтів	192.168.30.0/24	Обслуговування клієнтів, бронювання турів
Відділ маркетингу і продажів	192.168.40.0/24	Маркетинг, реклама, продажі
Операційний підрозділ	192.168.50.0/24	Організація турів, логістика
Підрозділ розвитку та управління якістю	192.168.60.0/24	Дослідження та розвиток (R&D), управління якістю
IT-підрозділ	192.168.70.0/24	Підтримка IT інфраструктури, управління мережевими ресурсами
Серверна підмережа	192.168.80.0/24	DNS-сервер, веб-сервер, поштовий сервер, файл-сервер, backup-сервер
WiFi працівників	192.168.90.0/24	Безпроводовий доступ до мережевих ресурсів компанії для працівників
Гостьова мережа	192.168.100.0/24	Доступ до Інтернету для гостей і

Підрозділ	Підмережа	Функції
		відвідувачів

Таблиця IP-адрес подана в графічній частині кваліфікаційної роботи.

Отже наразі визначено IP-адрес для кожної підмережі з використанням приватних адрес (RFC 1918). Далі потрібно налаштувати VLAN для кожної підмережі для сегментації трафіку на фізичних комутаторах. Після цього скористатися функціональністю керованого комутатора L3 для маршрутизації між підмережами з використанням VLAN. На заключному етапі налаштування потрібно сконфігурувати файрвол для контролю доступу між підмережами та забезпечення безпеки критичних ресурсів.

Перейдемо до налаштування підмереж на комутаторах рівня доступу SW_2 та SW_3, а також на центральному L3 комутаторі SW_1.

Перед початком налаштування потрібно переконатися, що наявний доступ до консолі управління комутаторів та адміністраторські права.

1. Налаштування підмереж на комутаторах рівня доступу SW_2 та SW_3

Підключаємося до комутатора через консольний кабель або через мережевий доступ (SSH/HTTP).

Створюємо VLAN для підмереж.

Для кожної підмережі створіть на обох комутаторах створюємо окремий VLAN. Для цього вводимо команди:

```
enable
configure terminal
vlan 10
name Admin_HR_Legal
exit
vlan 20
name Finance_Accounting
exit
```

vlan 30

name Customer_Service_Booking

exit

vlan 40

name Marketing_Sales

exit

vlan 50

name Tours_Organization_Logistics

exit

vlan 60

name R&D_Quality_Management

exit

vlan 70

name IT_Department

exit

vlan 80

name Servers

exit

vlan 90

name Employees_WiFi

exit

vlan 100

name Guest_WiFi

exit

Визначаємо порти, які будуть належати кожній VLAN.

Для комутатора SW_2:

interface range fa0/1-8

switchport mode access

switchport access vlan 30

exit

interface range fa0/9-17

switchport mode access

switchport access vlan 40

exit

Визначаємо транковий порт:

interface fa0/24

switchport mode trunk

exit

Для комутатора SW_3:

interface range fa0/1-5

switchport mode access

switchport access vlan 60

exit

interface range fa0/6-11

switchport mode access

switchport access vlan 20

exit

Визначаємо транковий порт:

interface fa0/24

switchport mode trunk

exit

2. Налаштування центрального L3 комутатора SW_1

Підключаємося до комутатора через консольний кабель або через мережевий доступ (SSH/HTTP).

Створюємо VLAN, аналогічні до тих, що на комутаторах рівня доступу.

enable

configure terminal

vlan 10

```
name Admin_HR_Legal
exit
vlan 20
name Finance_Accounting
exit
vlan 30
name Customer_Service_Booking
exit
vlan 40
name Marketing_Sales
exit
vlan 50
name Tours_Organization_Logistics
exit
vlan 60
name R&D_Quality_Management
exit
vlan 70
name IT_Department
exit
vlan 80
name Servers
exit
vlan 90
name Employees_WiFi
exit
vlan 100
name Guest_WiFi
exit
```

Включаємо у сконфігуровані підмережі відповідні порти комутатора

Для комутатора SW_1

```
interface range fa0/1-5
switchport mode access
switchport access vlan 10
exit
interface range fa0/6-9
switchport mode access
switchport access vlan 70
exit
interface range fa0/10-15
switchport mode access
switchport access vlan 50
exit
interface range fa0/16-18
switchport mode access
switchport access vlan 80
exit
interface range fa0/19-20
switchport mode access
switchport access vlan 90
exit
interface fa0/21
switchport mode access
switchport access vlan 100
exit
```

Налаштовуємо віртуальні інтерфейси SVI для маршрутизації між VLAN, тобто створюємо віртуальний інтерфейс SVI (Switch Virtual Interface) для кожної VLAN та призначаємо йому IP-адресу.

```
interface vlan 10
ip address 192.168.10.200 255.255.255.0
exit
interface vlan 20
ip address 192.168.20.200 255.255.255.0
exit
interface vlan 30
ip address 192.168.30.200 255.255.255.0
exit
interface vlan 40
ip address 192.168.40.200 255.255.255.0
exit
interface vlan 50
ip address 192.168.50.200 255.255.255.0
exit
interface vlan 60
ip address 192.168.60.200 255.255.255.0
exit
interface vlan 70
ip address 192.168.70.200 255.255.255.0
exit
interface vlan 80
ip address 192.168.80.200 255.255.255.0
exit
interface vlan 90
ip address 192.168.90.200 255.255.255.0
exit
interface vlan 100
ip address 192.168.100.200 255.255.255.0
```

exit

Налаштовуємо маршрутизації між VLAN, тобто умикаємо маршрутизацію на комутаторі і переконуємося, що вона активована.

ip routing

Підключаємо комутатори рівня доступу SW_2 та SW_3 до центрального комутатора SW_1 через trunk-порти.

Налаштовуємо режим їх роботи

interface gig0/23

switchport mode trunk

switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100

exit

interface gig0/24

switchport mode trunk

switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100

exit

Після виконання цих кроків в проектованій мережі буде налаштовано поділ її на підмережі з можливістю маршрутизації між ними. Це забезпечить ефективне управління трафіком, підвищену безпеку і масштабованість мережі туристичної компанії «Трайдент».

3.2 Інструкція з налаштування доступу до Інтернет та захисту мережі

Підключення до провайдера послуг Інтернет буде здійснюватися засобами файрволу. Для цього потрібно виконати ряд кроків:

Крок 1. Підключення файрволу.

Підключаємо WAN-порт файрволу FortiGate 60E до оптоволоконної лінії провайдера.

Підключаємо LAN-порт файрволу FortiGate 60E до core switch SW_1, а

саме до 18-го порта.

Крок 2. Підключаємося до файрволу через консоль. Тобто підключаємо консольний кабель до порту консолі на FortiGate 60E і до відповідного порту на комп'ютері.

Відкриваємо термінальну програму (наприклад, PuTTY) і встановлюємо такі параметри підключення:

Speed: 9600

Data bits: 8

Stop bits: 1

Parity: None

Flow control: None

Запускаємо сесію, натиснувши "Open" в PuTTY.

Вводимо ім'я користувача (за замовчуванням: admin) і натискаємо Enter.

Залишаємо поле пароля порожнім і натискаємо Enter (за замовчуванням, пароля немає).

Крок 3. Налаштування WAN-інтерфейсу

Для налаштування WAN-інтерфейсу (отримуємо IP-адресу від провайдера динамічно) вводимо наступні команди у консолі:

```
config system interface
edit port1
set mode dhcp
set allowaccess ping http https ssh
next
end
```

Крок 4. Налаштування LAN-інтерфейсу

Для налаштування LAN-інтерфейсу вводимо наступні команди у консолі:

```
config system interface
```

edit port2

set ip 192.168.80.3 255.255.255.0

set allowaccess ping http https ssh

next

end

Крок 5. Налаштування NAT.

Для налаштування NAT вводимо наступні команди у консолі:

config firewall policy

edit 1

set name "Allow-Internet"

set srcintf "port2"

set dstintf "port1"

set srcaddr "all"

set dstaddr "all"

set action accept

set schedule "always"

set service "ALL"

set nat enable

next

end

Крок 6. Налаштування політик безпеки.

Створюємо правила доступу для локальних підмереж і Інтернету. Наприклад:

config firewall policy

edit 2

set name "Allow-LAN"

set srcintf "port2"

set dstintf "port1"

set srcaddr "all"

set dstaddr "all"

set action accept

set schedule "always"

set service "ALL"

next

end

Створюємо зони безпеки:

config system zone

edit "LAN"

set interface "port2"

next

edit "WAN"

set interface "port1"

next

end

Крок 7. Перевірка налаштувань.

Перевіряємо підключення шляхом підключення комп'ютера до LAN-сегмента мережі. Тестуємо правила файрволу, переконуємося, що вони працюють відповідно до очікувань.

Крок 8. Завершуємо налаштувань. Зберігаємо конфігурацію. Створюємо резервну копію конфігурації:

execute backup config ftp <server_ip> <username> <password> <path>

3.3 Інструкція з тестування та моніторингу мережі

Для моніторингу проектованої мережі можна скористатися відповідними інструментами. Для цього потрібно встановити програмне забезпечення для моніторингу мережі, яке дозволить відстежувати стан мережевих пристроїв, трафік мережі та інші параметри. Для цього можна

скористатися популярними інструментами Nagios та Zabbix. Тобто потрібно налаштувати ці інструменти для моніторингу мережі з використанням SNMP (Simple Network Management Protocol) для отримання інформації від комутаторів SW_1, SW_2 та SW_3.

Для перевірка з'єднання між комутаторами можна скористатися такими інструментами як ping або traceroute. Наприклад можна запустити ping-запити до IP-адрес кожної робочої станції проектованої мережі та перевірити час відповіді, щоб визначити наявність затримок або втрат пакетів.

Для моніторингу трафіку на комутаторах можна використовувати можливості комутаторів Juniper EX3400-24T та Juniper EX2300-24T. Команди моніторингу, такі як show interfaces, дозволять переглянути статистики по кожному порту та виявити будь-яких аномалії чи перевантажень.

У випадку виявлення проблем з мережевим трафіком, можна скористатися інструментом аналізу Wireshark для перехоплення та аналізу пакетів у реальному часі.

Для підтримання оптимального режиму роботи мережі потрібно планувати регулярні тести мережі для виявлення проблем та попередження їх перед появою. Для цього можуть використовуватися автоматизовані інструменти для проведення тестів, такі як сканування портів, тестування пропускної здатності та інші, щоб забезпечити ефективність та надійність мережі.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини дипломного проекту є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності проектування комп'ютерної мережі туристичної компанії «Трайдент» і прийняття рішення щодо її подальшого розвитку та впровадження або ж недоцільність проведення відповідної розробки.

Для розрахунку вартості НДР необхідно виконати наступні етапи:

– описати технологічний процес розробки із зазначенням трудомісткості кожної операції;

– визначити суму витрат на оплату праці основного і допоміжного персоналу, включаючи відрахування на соціальні заходи;

– визначити суму матеріальних затрат;

– обчислити витрати на електроенергію для науково-виробничих цілей;

– розрахувати транспортні витрати;

– нарахувати суму амортизаційних відрахувань;

– визначити суму накладних витрат;

– скласти кошторис та визначити собівартість НДР;

– розрахувати ціну НДР;

– визначити економічну ефективність та термін окупності продукту.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Для визначення загальної тривалості проведення НДР доцільно дані витрат часу по операціях технологічного процесу звести у таблицю 4.1.

Таблиця 4.1 - Середній час виконання НДР та стадії (операції) технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Підготовка	Керівник	7
2	Розробка проекту мережі	Керівник	23
3	Монтаж кабелів та розеток	Лаборант	5
4	Налаштування активного комутаційного обладнання	Технік	5
5	Інсталяція та налаштування серверів	Технік	5
6	Тестування мережі	Технік	2
Р а з о м		–	47

До виконавців, у залежності від змісту виконуваної роботи, можна віднести: керівника проекту, інженера, лаборанта, консультанта, техніка.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України “Про оплату праці” заробітна плата – це “винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу”.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов'язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

Основна заробітна плата розраховується за формулою:

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

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

$$З_{осн.} = 100*30+60*5+80*12=4260 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

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

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

$$З_{дод.} = 4260*0,15=639,00 \text{ грн.}$$

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

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

$$В_{о.п.} = 4260+639,00=4899,00 \text{ грн.}$$

Крім того, слід визначити відрахування на заробітну плату:

– єдиний соціальний внесок – 22 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.} = ФОП \cdot 0,22, \quad (4.4)$$

де $ФОП$ – фонд оплати праці, грн.

$$В_{с.з.} = 4899*0,22=1077,78 \text{ грн.}$$

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.			Додаткова заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на оплату праці, грн. 6=3+4+5
		Тарифна ставка, грн.	К-сть відпрацьов. год.	Фактично нарах. з/пл., грн.			
1	Керівник проекту	100	30	3000,00	450,00	-	-
2	Лаборант	60	5	300,00	45,00	-	-
3	Технік	80	12	960,00	144,00	-	-
	Разом	-	-	4260,00	639,00	1077,78	5976,78

4.3 Розрахунок матеріальних витрат

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

$$M_{Bi} = q_i \cdot p_i \,, \tag{4.5}$$

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \Sigma M_{Bi} \tag{4.6}$$

$З_{м.в.}$=3480+800+6966+372+3540+3000+492+7940+5355+3645+50820+60488+
+9880+14820+159600+132450+106400+171630= 740060,00 грн.

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Факт. витр. матеріалів	Ціна 1-ці, грн.	Заг. сума витрат, грн.
1	Кабель мідний Cat6 (бухта 305м)	шт	2	1740	3480
2	Конектор RJ-45 cat 6	шт.	200	4	800
3	Кабель оптичний CMS-U-BQ(BN)H 8F G50/125 OM3	м.	86	81	6966
4	Фаст-конектор SC/UPC	шт.	12	31	372
5	Тринсивер SFP+ 10G 300m 850nm DOM LC (SFP-10G-SR)	шт.	6	590	3540
6	Короб 40*25*2м	шт.	120	25	3000
7	Органайзер для кабеля1U	шт.	3	164	492
8	Серверна шафа 6U	шт.	2	3970	7940
9	Серверна шафа 9U	шт.	1	5355	5355
10	Патч-панель RJ45 cat6 24 port	шт.	3	1215	3645
11	Комутатор Juniper EX3400-24T	шт.	1	50820	50820
12	Комутатор Juniper EX2300-24T	шт.	2	30244	60488
13	Файрвол Fortinet FortiGate 60E	шт.	1	19880	19880
14	Точка доступу Ubiquiti UniFi AP AC Pro	шт.	3	4940	14820
15	Сервер Lenovo ThinkSystem SR530	шт.	1	159600	159600
16	NAS Synology RackStation RS3617xs+	шт.	1	132450	132450
17	Принтер HP LaserJet Pro MFP M428fdw	шт.	7	15200	106400
18	ДБЖ Eaton 9PX 3000VA	шт.	3	57210	171630
	ВСЬОГО				740060

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$З_е = W \cdot T \cdot S, \quad (4.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Для комп'ютера: $W = 0{,}5$ кВт.

$$З_е = 0{,}5*23*7 = 30{,}50 \text{грн.}$$

4.5 Визначення транспортних затрат

Транспортні витрати слід прогнозувати у розмірі 8–10 % від загальної суми матеріальних затрат.

$$Т_в = З_{м.в.} \cdot 0{,}08 \ldots 0{,}1, \quad (4.8)$$

де $Т_В$ – транспортні витрати.

$$Т_в = 740060*0{,}08 = 59204{,}80 \text{ грн}$$

4.6 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$А = \frac{Б_В \cdot Н_А}{100\%}, \quad (4.9)$$

де $А$ – амортизаційні відрахування за звітний період, грн.;

$Б_В$ – балансова вартість групи основних фондів на початок

звітного періоду, грн.;

H_A – норма амортизації, %.

Для проектування даної комп'ютерної мережі використовується один комп'ютер (вартість якого становить 34099 грн.), який працює 23 години.

$$A= 34099*0,04*23/150=209,14 \text{ грн.}$$

4.7 Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління та створення необхідних умов праці.

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

$$H_в=B_{о.п.} \cdot 0,2 \ldots 0,6, \quad (4.10)$$

де H_B – накладні витрати.

$$H_B=4899*0,4=1959,60 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 4.4.

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці	4899	0,61
Відрахування на соціальні заходи	1077,78	0,13
Матеріальні витрати	740060	91,66
Витрати на електроенергію	30,5	0,00
Транспортні витрати	59204,8	7,33
Амортизаційні відрахування	209,14	0,03
Накладні витрати	1959,6	0,24
Собівартість	807440,82	100,00

Собівартість ($С_В$) НДР розрахуємо за формулою:

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

$С_в$=4899+1077,78+740060+30,5+59204,8+209,14+1959,6=

=807440,82 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

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

де $Р_{рен.}$ – рівень рентабельності, 30 %;

$К$ – кількість замовлень, од. ;

$В_{і.н.}$ – вартість носія інформації, грн. ;

$ПДВ$ – ставка податку на додану вартість, (20 %).

$Ц$=807440,82*(1+0,23)*(1+0,2)= 1191782,65 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) і термін окупності ($Т_{ОК}$).

$$ЧТВ = -К_В + \sum_{i=1}^{t} \frac{Г_П}{(1+i)^t}, \quad (4.13)$$

де $К_В$ – затрати на проект;

$Г_п$ – грошовий потік за t – ий рік;

t – відповідний рік проекту;

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

$ЧТВ$ = –807440,82+749033,33/(1+0,15)+ 749033,33/$(1+0,15)^2$ =492534,38 грн.

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

Термін окупності визначається за формулою:

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

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

$H_{В}$ – невідшкодовані витрати на початок року, грн.;

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

$$T_{ОК}=1+126501,43/749033,33=1,2$$

Результати розрахунків основних економічних показників зведені у таблицю 4.5.

Таблиця 4.5 - Економічні показники НДР

№ п/п	Показник	Значення
1.	Собівартість, грн.	807440,82
2.	Плановий прибуток, грн.	384341,83
3.	Ціна, грн.	1191782,65
4.	Чиста теперішня вартість, грн	492534,38
5.	Термін окупності, рік	1,2

Згідно параметрів, поданих у попередній таблиці, можна зробити висновок, що при терміні окупності – 1,2 року проводити роботи по впровадженню даної мережі є доцільним та економічно вигідним.

5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

Однією з характерних рис сучасного суспільного розвитку є збільшення кількості сфер діяльності, де застосовуються інформаційні технології. Персональні комп'ютери стали широко поширеними. Проте їхнє використання загострило питання збереження індивідуального та суспільного здоров'я, вимагаючи вдосконалення наявних та створення нових методів організації робочих місць, а також проведення профілактичних заходів для запобігання негативним наслідкам впливу ПК на здоров'я користувачів.

5.1 Засоби оповіщення про загорання або пожежу в туристичній компанії «Трайдент»

Для туристичної компанії "Трайдент" важливо забезпечити максимальний рівень безпеки клієнтів у всіх своїх об'єктах. Основною метою системи оповіщення є інформування людей у будівлі про пожежу або іншу надзвичайну ситуацію та координація їхньої евакуації. Ці системи можуть бути автономними або інтегрованими в загальну систему безпеки об'єкта.

Системи оповіщення повинні відповідати встановленим нормативним вимогам. Норми пожежної безпеки передбачають п'ять типів систем оповіщення та управління евакуацією (СОУЕ) залежно від характеристик будівлі та кількості людей у ній.

Типи систем оповіщення [16]:

1. Перший тип використовує звукові та світлові сигнали (світловий миготливий сигнал, таблички "Вихід") і має одну лінію оповіщення.

2. Другий тип додає світлові таблички напрямку руху та має дві або більше ліній оповіщення, які працюють незалежно.

3. Третій тип включає мовні оповіщення разом зі звуковими та світловими, з кількома незалежними лініями оповіщення.

4. Четвертий тип має аналогічні функції, як і третій, але забезпечує зв’язок з диспетчерською.

5. П’ятий тип повністю автоматизований, забезпечує кілька варіантів евакуації та зв’язок з диспетчерською.

Типи управління системами [16]:

– автоматичне, коли система активується сигналом від автоматичних установок пожежної сигналізації або пожежогасіння.

– напівавтоматичне, коли система активується диспетчером при отриманні сигналу від цих установок.

Типи систем оповіщення [16]:

– централізовані системи мають центральний блок управління, можуть працювати в автоматичному або напівавтоматичному режимі, передаючи екстрені повідомлення з мікрофонної консолі.

– локальні системи складаються з мовного процесора, підсилювача та гучномовців і автоматично транслюють записані повідомлення при отриманні сигналу тривоги.

Для туристичної компанії "Трайдент" важливо, щоб системи оповіщення були встановлені у всіх приміщеннях, включаючи опалювані та неопалювані зони, а також вибухонебезпечні ділянки. Системи поділяються на основні (сповіщувачі, блоки управління, підсилювачі, звукові пристрої, евакуаційні знаки) та додаткові (блоки резервного живлення, джерела сигналу).

Технічні вимоги включають передачу електричних сигналів на сповіщувачі, контроль справності ліній зв'язку, автоматичне перемикання живлення з основного на резервне та захист від несанкціонованого доступу. Також передбачені ручне відключення звукової сигналізації при збереженні світлової, коригування алгоритму оповіщення та дистанційне відкривання

евакуаційних виходів.

Конструктивно системи оповіщення можна поділити на аналогові та цифрові. У цифрових системах обробка та передача аудіоінформації здійснюється в цифровому вигляді, що значно покращує якість сигналів. Це дозволяє передавати кілька повідомлень одночасно в одній лінії, поєднувати кілька автономних систем і централізовано ними керувати.

Альтернативою провідним системам є бездротові системи оповіщення, що спрощують монтаж і забезпечують живучість системи завдяки бездротовому зв’язку між центральним блоком та оповіщувачами.

У штатному режимі системи оповіщення можуть використовуватися для передачі фонової музики або мовних оголошень, що дозволяє контролювати працездатність ліній оповіщення та мовних сповіщувачів. Допускається суміщення систем оповіщення та управління евакуацією (СОУЕ) з радіотрансляційною мережею будівлі, при цьому пріоритет повинен бути наданий сигналам СОУЕ. Мовні сповіщувачі не повинні мати регулятора гучності і повинні підключатися до мережі без роз’ємних пристроїв.

Згідно з Нормами Пожежної Безпеки (НПБ), прилади керування оповіщувачами повинні забезпечувати [16]:

– передачу електричних сигналів на сповіщувачі;

– контроль справності лінії зв’язку з оповіщувачами;

– автоматичне перемикання електроживлення з основного джерела на резервне і назад без видачі хибних сигналів. Час роботи від резервного джерела в черговому режимі повинен бути не менше 24 годин, у тривожному режимі - не менше 1 години;

– захист органів управління від несанкціонованого доступу сторонніх осіб.

– контроль стану резервного джерела живлення;

– ручне відключення звукової сигналізації при збереженні світлової.

Відключення звукової сигналізації повинно супроводжуватися світловою індикацією;

– можливість коригування алгоритму оповіщення;

– ручний та автоматичний контроль працездатності вузлів і блоків приладів;

– дистанційне відкривання дверей або додаткових евакуаційних виходів.

Кабелі і проведення систем оповіщення та управління евакуацією повинні зберігати працездатність в умовах пожежі протягом часу, необхідного для повної евакуації людей у безпечну зону.

У штатному режимі системи оповіщення туристичної компанії "Трайдент" можуть використовуватися для передачі фонової музики або мовних оголошень, що дозволяє контролювати працездатність системи. Пріоритет сигналів СОУЕ завжди повинен бути вищим за радіотрансляцію, а мовні сповіщувачі повинні підключатися без роз'ємних пристроїв і не мати регуляторів гучності.

Компанія "Трайдент" прагне забезпечити найвищі стандарти безпеки для своїх клієнтів, використовуючи передові технології оповіщення та управління евакуацією.

5.2 Відповідальність керівника та працівників туристичної компанії щодо порушення вимог з охорони праці

Відповідно до статті 44 Закону України «Про охорону праці», за порушення законів та інших нормативно-правових актів щодо охорони праці, а також за створення перешкод у діяльності посадових осіб органів державного нагляду за охороною праці, винні особи несуть дисциплінарну, адміністративну, матеріальну та кримінальну відповідальність згідно із законодавством [17].

Керівник туристичної компанії "Трайдент" несе відповідальність за забезпечення дотримання вимог з охорони праці на всіх рівнях організації. Він зобов’язаний створити безпечні умови праці, розробити та впровадити відповідні інструкції та процедури, забезпечити їх дотримання працівниками, а також проводити регулярні навчання та інструктажі.

Працівники компанії повинні виконувати свої обов’язки відповідно до встановлених правил та інструкцій з охорони праці, брати участь у навчаннях і тренінгах, дотримуватися правил безпеки на робочому місці та негайно повідомляти керівництво про будь-які порушення чи небезпечні ситуації.

Притягнення до адміністративної відповідальності посадових осіб і працівників за порушення законів та інших нормативно-правових актів з охорони праці здійснюється відповідно до Кодексу України про адміністративні правопорушення (КУАП). Зокрема, стаття 231 КУАП передбачає, що центральний орган виконавчої влади, який реалізує державну політику у сфері охорони праці, розглядає справи про порушення законодавства про охорону праці, безпечне ведення робіт, зберігання, використання та облік вибухових матеріалів, а також невиконання законних вимог посадових осіб цього органу.

Інші статті КУАП, які регламентують відповідальність за порушення вимог з охорони праці, включають [17]:

– частину 5 статті 41 (відповідальність за порушення вимог законодавства про охорону праці);

– частину 6 статті 41 (відповідальність за порушення порядку повідомлення про нещасний випадок на виробництві);

– статтю 47 (відповідальність за самовільне користування надрами);

– статтю 57 (відповідальність за порушення вимог щодо охорони надр);

– статтю 93 (відповідальність за порушення вимог безпечного ведення робіт);

– статтю 94 (відповідальність за порушення вимог щодо зберігання та

обліку вибухових матеріалів);

– статтю 188-4 (відповідальність за невиконання законних вимог органів нагляду за охороною праці).

Кримінальна відповідальність за порушення вимог з охорони праці передбачена Кримінальним кодексом України. Зокрема:

– стаття 271 (порушення вимог законодавства про охорону праці);

– стаття 272 (порушення правил безпеки під час виконання робіт з підвищеною небезпекою);

– стаття 273 (порушення правил безпеки на вибухонебезпечних підприємствах).

Керівник туристичної компанії "Трайдент" може притягнути працівників, які допустили порушення правил, інструкцій чи норм з охорони праці, до дисциплінарної або матеріальної відповідальності. Це включає заходи від догани до звільнення, а також відшкодування збитків, завданих компанії через порушення.

5.3 Захист від ІЧ випромінювання

Інфрачервоне (ІЧ) випромінювання є невидимою частиною електромагнітного спектру, що випромінюється сонцем [18]. Хоча ІЧ випромінювання не є настільки небезпечним, як ультрафіолетове випромінювання, воно може мати негативний вплив на здоров'я людини при тривалому або інтенсивному впливі.

Короткохвильові інфрачервоні хвилі проникають на кілька сантиметрів в шкіру, викликаючи нагрівання внутрішніх органів. Вони не тільки викликають дискомфорт, але й можуть завдати шкоди здоров'ю. При тривалому впливі відчувається інтенсивне тепло, головний біль, запаморочення та нудота. Короткохвильові промені особливо небезпечні для очей, їх довготривалий вплив може спричинити катаракту. Також короткохвильове ІЧ випромінювання може викликати тепловий удар.

Довгохвильові інфрачервоні промені при потраплянні на шкіру викликають відчуття тепла. Вони не тільки безпечні, але й корисні для здоров'я, сприяючи підвищенню імунітету і прискоренню регенерації клітин. Прикладом джерела довгохвильового ІЧ випромінювання є сільська піч, відома своїми лікувальними властивостями.

До джерел ІЧ випромінювання належать: сонце, інфрачервоні лампи, сауни та обігрівачі. Інфрачервоні обігрівачі стають все популярнішими через їх економічність, особливо в умовах зростання тарифів на опалення. При виборі інфрачервоного опалення слід враховувати характеристики приміщення, яке потребує обігріву.

В туристичній компанії "Трайдент" особливо увагу приділяють безпеці та комфорту клієнтів, тому рекомендують звернути увагу на інфрачервоні обігрівачі, які стають все популярнішими через їх економічність, особливо в умовах зростання тарифів на опалення. При виборі інфрачервоного опалення під час подорожей або у місцях проживання слід враховувати характеристики приміщення, яке потребує обігріву.

Короткохвильові обігрівачі підходять для використання на відкритих майданчиках та у холодних виробничих приміщеннях з великим об'ємом. Довгохвильові інфрачервоні обігрівачі ідеальні для опалення квартир, приватних будинків, офісів, кафе. Однак вони не підходять для приміщень з тонкими стінами, які не зберігають тепло.

Туристична компанія "Трайдент" приділяє особливу увагу захисту своїх клієнтів і працівників від потенційних ризиків, пов'язаних з ІЧ випромінюванням, особливо під час подорожей до сонячних регіонів.

ІЧ випромінювання може викликати тепловий стрес і опіки шкіри, якщо на нього тривалий час впливає. Тривале перебування під впливом інтенсивного ІЧ випромінювання може також спричинити зневоднення і тепловий удар.

Туристична компанія "Трайдент" рекомендує наступні заходи для

захисту від ІЧ випромінювання [18]:

– використання захисного одягу. Легкий, світлого кольору, довгий одеяг допомагає відбивати сонячне випромінювання і захищає шкіру від перегріву;

– капелюхи та окуляри. Носіння широкополих капелюхів і сонцезахисних окулярів з УФ-фільтром допомагає захистити обличчя і очі від сонячних променів;

– сонцезахисні креми. Використання кремів з високим фактором захисту від сонця (SPF) знижує ризик опіків та інших шкірних ушкоджень;

– перебування у тіні. Планування активностей на відкритому повітрі у ранкові або вечірні години, коли сонце менш інтенсивне, а також забезпечення можливості перебування у тіні протягом дня;

– регулярні перерви та зволоження. Під час екскурсій або інших активностей на свіжому повітрі важливо регулярно робити перерви у тіні і пити достатню кількість води, щоб уникнути зневоднення.

Компанія "Трайдент" забезпечує своїх клієнтів і працівників необхідною інформацією щодо захисту від ІЧ випромінювання. До початку подорожі клієнти отримують інформаційні матеріали, що містять рекомендації щодо захисту від сонця та ІЧ випромінювання. Гіди і супроводжуючі працівники також проводять інструктажі перед початком екскурсій і активностей на відкритому повітрі.

Для додаткового захисту під час подорожей туристична компанія "Трайдент" використовує сучасні технічні засоби, такі як мобільні намети та парасолі для створення тіньових зон під час зупинок на екскурсіях. Також автобуси і транспортні засоби компанії обладнані спеціальними віконними плівками, що блокують ІЧ випромінювання.

Туристична компанія "Трайдент" приділяє значну увагу забезпеченню безпеки своїх клієнтів і працівників, включаючи захист від ІЧ випромінювання. Дотримання вищезазначених заходів допомагає

мінімізувати ризики для здоров'я і забезпечує комфортне і безпечне перебування на сонці під час подорожей.

ВИСНОВКИ

У першому розділі пояснювальної записки кваліфікаційної роботи сформульовано технічне завдання та описано стан комп'ютеризації відділів туристичної компанії «Трайдент».

У другому розділі обрано топологію мережі. Прийнято рішення будувати мережу на основі комбінованої топології. У цьому розділі підібрано пасивне та активне комутаційне обладнання. Для середовища передачі даних обрано кабель вита пара категорії 6. Центральним вузлом мережі призначено керований комутатор рівня L3 Juniper EX3400-24T. Модель комутаторів рівня доступу - керований комутатор L2 Juniper EX2300-24T. В якості точок доступу використано моделі Ubiquiti UniFi AP AC Pro. Файрвол - модель Fortinet FortiGate 60E.

У цьому ж розділі розглянуто особливості розподілу адресного простору підмереж, характеристики вузлів мережі та особливості монтажу кабельної частини мережі. За результатами другого розділу було розроблено логічну та фізичну топології мережі, які представлені на окремих плакатах у графічній частині кваліфікаційної роботи.

У третьому розділі наведено інструкцію з налаштування активного комутаційного обладнання, інструкції з налаштування доступу до Інтернет, а також описані методи моніторингу та тестування мережі.

У четвертому розділі обчислено вартість проектування та введення в експлуатацію мережі.

У п'ятому розділі описано питання охорони праці та техніки безпеки при роботі з обчислювальним обладнанням.

Таким чином, кваліфікаційна робота являє собою комплекс документації щодо проектування та введення в експлуатацію локальної

комп'ютерної мережі туристичної компанії «Трайдент».

ПЕРЕЛІК ПОСИЛАНЬ

1. Гаврилюк С., Андрійчук І. Мережеві технології: основи та інновації. Харків: Ранок, 2021. 480 с.

2. Дорошенко О., Савченко Р. Управління комп'ютерними мережами. Суми: Університетська книга, 2019. 460 с.

3. Жуков В., Коваленко П. Комп'ютерні мережі та безпека даних. Київ: Видавництво КНТ, 2023. 550 с.

4. Костенко А., Чорний С. Мережеві протоколи та технології. Полтава: Оріяна, 2022. 530 с.

5. Кравчук В., Олійник А. Архітектура та організація комп'ютерних мереж. Запоріжжя: ЗНТУ, 2023. 490 с.

6. Куратор Л., Кіндратенко В. Комп'ютерні мережі: теорія та практика. Львів: Палітра, 2022. 520 с.

7. Лавриненко І., Щербак В. Сучасні мережеві технології. Київ: Либідь, 2020. 480 с.

8. Лунтовський А., Мельник І. Комп'ютерні мережі та телекомунікації. Університет «Україна», 2017. 274 с.

9. Мороз В., Сиченко Ю. Мережеві архітектури та їх застосування. Дніпро: Навчальна книга, 2020. 450 с.

10. Степаненко О., Пашков М. Інтернет-протоколи та мережеві рішення. Одеса: Фенікс, 2019. 600 с.

11. Тарасенко М., Волков В. Основи комп'ютерних мереж та їх адміністрування. Вінниця: Поділля, 2021. 510 с.

12. Juniper EX3400-24T: веб-сайт. URL: https://www.juniper.net/us/en/products/switches/ex-series/ex3400-ethernet-switch-datasheet.html (дата звернення: 16.03.2024).

13. GS-4210-24T2S: веб-сайт. URL: https://www.juniper.net/us/en/products/switches/ex-series/ex2300-ethernet-switch-datasheet.html (дата

звернення: 16.03.2024).

14. Оснащення офісних приміщень первинними засобами пожежогасіння: веб-сайт. URL: https://opcb.kpi.ua/?p=3808 (дата звернення: 19.04.2023).

15. Основні причини виробничого травматизму і профзахворюваності та заходи щодо їх попередження: веб-сайт. URL: https://buklib.net/books/27557/ (дата звернення: 19.04.2024).

16. Системи оповіщення та управління евакуацією: веб-сайт. URL: https://www.varta-bezpeka.com.ua/opovishhennja-ta-upravlinnja-evakuacijeju/ (дата звернення: 30.05.2024).

17. Відповідальність посадових осіб та працівників за порушення законодавства про охорону праці: веб-сайт. URL: https://dsp.gov.ua/faq/iaka-vidpovidalnist-posadovykh-osib-ta-pratsivnykiv-za-porushennia-zakonodavstva-pro-okhoronu-pratsi/ (дата звернення: 30.05.2024).

18. Вплив інфрачервоних хвиль на організм людини: веб-сайт. URL: https://teploceramic.ua/ua/vliyanie-infrakrasnogo-izlucheniya-na-organizm.html (дата звернення: 30.05.2024).

ДОДАТКИ

Додаток А – Характеристики комутатора Juniper EX3400-24T

Ethernet-комутатор Juniper Networks® EX3400 із технологією віртуального шасі Juniper Networks надає підприємствам гнучкість і легкість керування, які раніше були доступні лише за допомогою високоякісних комутаторів доступу. EX3400 із фіксованою конфігурацією підтримує низку ключових функцій, зокрема [12]:

– 24-портові та 48-портові моделі з живленням через Ethernet (PoE/PoE+) і без нього призначені для розгортання мереж у кампусах.

– Підтримка хмарної підтримки та забезпечення без дотику (ZTP) для Juniper Mist Wired Assurance

– Варіанти охолодження, оптимізовані для центрів обробки даних, пропонують повітряні потоки як спереду назад, так і ззаду-спереду, що робить EX3400 придатним для розгортання доступу до центрів обробки даних GbE.

– Два резервних джерела живлення, які можна замінити на місці, забезпечують потужність до 920 Вт кожен.

– Доступні чотири порти висхідної лінії зв’язку (SFP/SFP+) малого форм-фактора, що підключаються, для дворежимного (GbE/10GbE) і два порти 40GbE QSFP+.

– Порти висхідної лінії зв’язку можна налаштувати як інтерфейс віртуального шасі та підключити через стандартні оптичні інтерфейси 10GbE/40GbE (порти висхідної лінії зв’язку 40GbE попередньо налаштовані за замовчуванням як порти віртуального шасі).

– Надається повна функціональність рівня 2 з RIP і статичною маршрутизацією.

– Компактний форм-фактор 1 U з глибиною 13,8 дюйма підтримує

гнучкі варіанти розгортання.

– Просте в управлінні рішення включає централізоване оновлення програмного забезпечення.

– Підтримка доступна для такої самої узгодженої модульної реалізації функцій площини керування операційною системою Juniper Networks Junos, яка використовується в усіх інших комутаторах Ethernet Juniper Networks серії EX із фіксованою конфігурацією.

– Надається підтримка рівня 3 (OSPF v2, IGMP v1/v2/v3, PIM, VRRP, BFD, віртуальний маршрутизатор) за допомогою ліцензії на розширені функції (потрібна додаткова ліцензія).

– Доступна підтримка для керування IPv6, включаючи автоматичне налаштування без збереження стану, telnet, SSH, DNS, системний журнал, NTP, ping, traceroute, ACL, статичну маршрутизацію CoS і RIPng.

– Функції маршрутизації IPv6 (OSPFv3, підтримка віртуального маршрутизатора для одноадресної передачі, VRRPv6, PIM, MLDv1/v2) підтримуються за допомогою ліцензії на розширену функцію.

– Підтримка доступна для Border Gateway Protocol (BGP), multiprotocol BGP (MBGP) і Intermediate System-to-Intermediate System (IS-IS) через додаткову ліцензію Advanced Feature.

– Надається можливість енергоефективного Ethernet (EEE).

Додаток Б – Характеристики комутатора Juniper EX2300-24T

Лінійка Ethernet-комутаторів Juniper Networks® EX2300 пропонує компактне, високопродуктивне рішення для підтримки сучасних мережевих доступів з конвергованими середовищами [13].

Кожен комутатор EX2300 включає в себе механізм пересилання пакетів (Packet Forwarding Engine, PFE) на основі ASIC з інтегрованим процесором для постійного забезпечення пересилання з максимальною швидкістю, навіть при активованих всіх функціях управлінського рівня. Заснований на перевірених у реальних умовах технологіях компанії Juniper Networks, PFE забезпечує на комутаторах EX2300 той самий рівень надійності і продуктивності класу операторських мереж, що й маршрутизатори Juniper Networks у найбільших сервіс-провайдерських мережах світу.

Деякі моделі EX2300 також підтримують стандарти Power over Ethernet (PoE) 802.3af Class 3 та 802.3at PoE+, що дозволяє живити мережеві пристрої, такі як телефони, відеокамери, точки доступу WLAN IEEE 802.11ac та відеотелефони в конвергованих мережах. Комутатори EX2300 з підтримкою PoE мають максимальний системний бюджет до 750 ват для надання до 30 ват на окремих портах [13].

У лінійці доступні різні моделі EX2300, включаючи версії з підтримкою мультигігабітних (до 2.5 Гбіт/с) PoE+ доступних портів, що можуть обслуговувати точки доступу IEEE 802.11ac Wave 2 з вищою швидкістю, що дозволяє комутаторам підтримувати більше бездротових користувачів.

Фіксовані Ethernet-комутатори EX2300 забезпечують високу вартість для підприємствових клієнтів, підтримуючи такі ключові технології [13]:

– Технологія Virtual Chassis дозволяє створювати одну логічну пристрійну одиницю з до чотирьох взаємопідключених комутаторів EX2300.

– Гнучкі високошвидкісні з'єднання 1GbE SFP/10GbE SFP+ для

підключення до комутаторів агрегаційного рівня або інших вищезазначених пристроїв.

– До 48 портів 10/100/1000BASE-T доступні з або без підтримки PoE/PoE+.

– Моделі з 24 та 48 мультигігабітними портами підтримують 1GbE/2.5GbE на 8 та 16 портах відповідно.

– Підтримка технології Energy Efficient Ethernet (EEE) на портах 1GbE.

– Повні можливості комутації на рівні Layer 2 та базовий комутації на рівні Layer 3.

– Спрощений підключення та управління з Juniper Mist Wired Assurance.

Додаткові функції включають [13]:

– Комутатори EX2300 з підтримкою PoE можуть одночасно живити до 15.4 ват стандарту 802.3af Class 3 PoE на максимум 48 портах або 30 ват стандарту 802.3at PoE+ на максимум 24 портах, на основі загального системного бюджету до 750 ват.

– Верхні порти можуть бути налаштовані як інтерфейси Virtual Chassis і підключені через стандартні інтерфейси оптики 10GbE (потрібна додаткова ліцензія для Virtual Chassis).

Додаток В – Характеристики файрволу Fortinet FortiGate 60F

Серія FortiGate FortiWiFi 60F поєднує брандмауерні функції, SD-WAN та безпеку в одному пристрої, ідеально підходить для створення мережі, орієнтованої на безпеку, у розподілених підприємствах та для перетворення архітектури WAN будь-якої масштабності.

Серія FortiGate FortiWiFi 60F працює на базі операційної системи FortiOS з першим в галузі єдиною мережевою та безпековою конвергенцією. Ця конвергенція дозволяє підприємствам ефективно захищати динамічні цифрові інфраструктури сьогодення.

Брандмауер наступного покоління FortiGate (NGFW) ідеально поєднується з безпековими службами FortiGuard на основі штучного інтелекту, щоб забезпечити координований, автоматизований захист в реальному часі на всіх випадках використання.

Сімейство 60F побудоване на патентованому SD-WAN-орієнтованому ASIC, що забезпечує неперевершену продуктивність порівняно з традиційними CPU при менших витратах і споживанні енергії. Цей спеціалізований дизайн та вбудований багатоядерний процесор ще більше прискорюють конвергенцію функцій мережі та безпеки в сімействі 60F для оптимізації безпечного з'єднання та користувацького досвіду в розташуваннях філій.

IPS (Intrusion Prevention System), система запобігання вторгненням. IPS виявляє потенційно шкідливий трафік у мережі, аналізує його і намагається заблокувати або відвернути вторгнення або атаки на систему. Вона реагує на виявлені загрози в реальному часі, блокуючи або витіскаючи шкідливий трафік перед тим, як він зможе завдати шкоди мережі чи системам. Продуктивність: 1.4 Gbps

NGFW (Next-Generation Firewall): Це брандмауер нового покоління, який поєднує в собі традиційні функції брандмауера з розширеними

можливостями захисту. NGFW включає в себе функції традиційного брандмауера (такі як контроль доступу на основі правил, NAT, VPN), а також додаткові можливості, такі як інтеграція з IPS, антивірусний сканер, захист від витоку даних, контроль за додатками і т.д. NGFW орієнтований на комплексний захист мережі від різних типів загроз і атак. Продуктивність: 1 Gbps

Захист від загроз: 700 Mbps

Інтерфейси: множина GE RJ45 | Варіанти з внутрішнім сховищем | WiFi варіанти

Порти:

- 1 x USB Port
- 1 x Console Port
- 2 x GE RJ45 WAN Ports
- 1 x GE RJ45 DMZ Port
- 2 x GE RJ45 FortiLink Ports
- 5 x GE RJ45 Internal Ports

Системні характеристики:

- Firewall Throughput (1518 / 512 / 64 byte UDP packets): 10/10/6 Gbps
- Firewall Latency (64 byte UDP packets): 3.3 μs
- Firewall Throughput (Packets Per Second): 9 Mpps
- Concurrent Sessions (TCP): 700 000
- New Sessions/Second (TCP): 35 000
- Firewall Policies: 5000
- IPsec VPN Throughput (512 byte:) 6.5 Gbps
- Gateway-to-Gateway IPsec VPN Tunnels: 200
- Client-to-Gateway IPsec VPN Tunnels: 500
- SSL-VPN Throughput: 900 Mbps
- Concurrent SSL-VPN Users(Recommended Maximum, Tunnel Mode): 200

– SSL Inspection Throughput (IPS, avg. HTTPS): 630 Mbps
– SSL Inspection CPS (IPS, avg. HTTPS): 400
– SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3 55 000
– Application Control Throughput (HTTP 64K) 1.8 Gbps
– CAPWAP Throughput (HTTP 64K): 8 Gbps
– Virtual Domains (Default / Maximum): 10 / 10
– Maximum Number of FortiSwitches Supported: 24
– Maximum Number of FortiAPs (Total / Tunnel Mode): 64 / 32
– Maximum Number of FortiTokens: 500
– High Availability Configurations Active-Active, Active-Passive, Clustering

Розміри:

– Height x Width x Length (inches): 1.5 x 8.5 x 6.3
– Height x Width x Length (mm): 38.5 x 216 x 160 mm
– Weight 2.23 lbs (1.01 kg)
– Form Factor: Desktop