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 компанії "Star way"

Виконав: студент(ка) IV курсу, групи КІ-406ск
Спеціальності **123 «Комп'ютерна інженерія»**
(шифр і назва напряму підготовки, спеціальності)

Станіслав Максим'юк
(ім'я та прізвище)

Керівник Володимир Лісовий
(ім'я та прізвище)

Рецензент
(ім'я та прізвище)

Тернопіль – 2026

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 2026 року

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Максим'юку Станіславу Івановичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Розробка проєкту комп'ютерної мережі компанії "Star way"

керівник роботи Лісовий Володимир Миколайович
(прізвище, ім'я, по батькові)

Затверджені наказом ВСП «Тернопільський фаховий коледж ТНТУ імені Івана Пулюя» від 02.04.2026 р №4/9-157.

2. Строк подання студентом роботи: 17 червня 2026 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 2026 року

Студент _____ Станіслав Максим'юк
(підпис) (ім'я та прізвище)

Керівник роботи _____ Володимир Лісовий
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Станіслав Максим’юк**.** Розробка проєкту комп'ютерної мережі компанії «STAR WAY»: кваліфікаційна робота на здобуття освітнього ступеня фаховий молодший бакалавр, за спеціальністю 123 Комп’ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2026. 95 с.

Кваліфікаційна робота фахового молодшого бакалавра присвячена розробці локальної комп’ютерної мережі для маркетингової компанії "STAR WAY ".

В результаті аналізу комунікаційних потреб компанії «STAR WAY » 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, бездротових точок доступу й серверних платформ, 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 програмного міжмережевого екрана iptables/ufw на базі ОС Ubuntu Server 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, програмний міжмережевий екран, iptables, ufw, точка доступу, сервер, VLAN, маршрутизація .

ЗМІСТ

ВСТУП

Сучасний розвиток суспільства нерозривно пов'язаний із активним залученням інформаційних технологій у всі аспекти людської діяльності. Комп'ютерні мережі стали фундаментом для ефективного обміну даними, забезпечуючи зручність у їхньому зберіганні, обробці та передачі [5]. На тлі стрімкої цифровізації персональні комп'ютери та інші засоби комунікації перетворилися на невід'ємну частину нашого повсякденного життя, що ще раз підкреслює необхідність якісного управління та належного захисту інформаційних систем [7].

Локальні комп'ютерні мережі надають широкі можливості, зокрема дозволяють спільно використовувати ресурси, такі як сервери. Це значно знижує витрати та підвищує загальну ефективність роботи компаній [2]. Додатково, подібні мережі забезпечують централізоване управління обладнанням і безпечний доступ до даних, що допомагає мінімізувати ризик втрати інформації та захищати її від несанкціонованого доступу [10].

Правильне проєктування мережі ґрунтується на використанні відкритих і кросплатформних технологій, що забезпечують гнучкість та масштабованість мережевих рішень [6]. Такий підхід дозволяє реагувати на швидкі зміни у сфері технологій, підтримуючи стабільність і безперервність бізнес-процесів [13].

Метою цієї кваліфікаційної роботи є розробка всебічного проєкту локальної комп'ютерної мережі для маркетингової компанії «STAR WAY» [9]. У ході виконання буде створено комплект документації, що детально висвітлює етапи проєктування, впровадження та тестування мережі. Це дозволить забезпечити її стабільну роботу, відповідність сучасним стандартам безпеки та високий рівень продуктивності [12]. Запроєктована мережа об'єднає робочі станції, сервери та бездротові точки доступу, передбачаючи логічний розподіл на віртуальні підмережі згідно зі структурою підрозділів компанії, а також гарантуватиме надійне підключення до Інтернету.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Тема кваліфікаційної роботи: Розробка проєкту комп'ютерної мережі маркетингової компанії «STAR WAY».

Проєкт спрямований на розробку та впровадження локальної комп'ютерної мережі в офісах маркетингової компанії «STAR WAY». Основна мета — підвищення ефективності роботи співробітників, організація спільного доступу до ресурсів та забезпечення безперебійної підтримки цифрових бізнес-процесів компанії.

1.1.2 Призначення розробки

Головна мета розробки полягає у впровадженні сучасної, високонадійної та захищеної комп'ютерної мережі [8]. Вона забезпечить безперебійну взаємодію між відділами компанії, стабільний доступ до Інтернету, ефективний захист даних [11] і підтримку ключових мережевих сервісів, зокрема електронної пошти, CRM-системи, платформ для ведення контекстної реклами, сервісів веб-аналітики, таск-менеджерів та інших бізнес-додатків [4].

1.1.3 Вимоги до апаратного і програмного забезпечення

Для забезпечення роботи локальної комп'ютерної мережі маркетингової компанії «STAR WAY» необхідно підібрати та налаштувати такі апаратні засоби:

– комутатор рівня L3 із підтримкою VLAN для покращення керованості мережі [19], що функціонує на базі сучасних стандартів тегування трафіку [22];

– комутатори рівня L2 для під'єднання кінцевих пристроїв користувачів [18];

– серверна інфраструктура, включаючи основний сервер та сервер додатків на базі надійного заліза [21] під управлінням серверних операційних систем з відкритим кодом [23];

– точки доступу Wi-Fi для мобільних клієнтів [17], оснащені протоколом безпеки WPA3;

– робочі комп'ютери та ноутбуки для співробітників;

– джерело безперебійного живлення для забезпечення стабільної роботи критично важливого обладнання [16].

1.1.4 Вимоги до документації

Документація для супроводу проєктованої локальної мережі повинна містити:

– технічну документацію на апаратне забезпечення мережі;

– інструкції щодо налаштування та експлуатації мережевого обладнання згідно з офіційними керівництвами виробника [20];

– логічну і фізичну схему мережі, а також план розташування обладнання у приміщеннях;

– таблицю IP-адресації вузлів мережі та конфігураційні параметри VLAN;

– документацію на програмне забезпечення серверів разом з детальними інструкціями з налаштування;

– політики безпеки, налаштування списків керування доступом (ACL) і процедури резервного копіювання даних;

– посібники для користувачів, призначені для співробітників компанії.

1.1.5 Техніко-економічні показники

Розгортання локальної комп’ютерної мережі в маркетинговій компанії «STAR WAY» покращить її показники, створюючи умови для отримання переваг:

– зниження витрат на управління мережевими ресурсами та технічне обслуговування через застосування централізованої інфраструктури, побудованої на обладнанні Cisco;

– підвищення продуктивності праці співробітників завдяки швидкому та надійному доступу до інформаційних ресурсів, як-от файлові сервери, CRM-система, хмарні сервіси для роботи з SMM та інструменти для дизайну;

– гарантія безперервності бізнес-процесів завдяки високій надійності мережевих рішень, зокрема, резервному копіюванню даних та використанню джерел безперебійного живлення;

– скорочення часу на усунення технічних збоїв через ефективне управління і цілодобовий моніторинг мережі за допомогою спеціалізованої платформи [24];

– посилення інформаційної безпеки завдяки поділу мережі на віртуальні LAN (VLAN), налаштуванню списків контролю доступу (ACL) та ізоляції гостьової бездротової мережі від корпоративної локальної.

Такі модернізації дозволять компанії значно підняти рівень своєї операційної ефективності та конкурентоспроможності.

1.1.6 Стадії та етапи розробки

Процес планування, розробки та реалізації локальної комп'ютерної мережі для маркетингової компанії «STAR WAY» варто розділити на кілька основних етапів:

1. Аналіз вимог і проектування, який охоплює:

– дослідження бізнес-потреб і технічних вимог усіх структурних підрозділів компанії;

– створення проекту мережевої інфраструктури та формування технічного завдання.

2. Підготовка специфікацій і закупівля необхідного обладнання, програмного забезпечення та додаткових компонентів

3. Монтаж і конфігурація обладнання, що передбачає:

– установку мережевих пристроїв і прокладання кабельної інфраструктури згідно з чинними телекомунікаційними стандартами СКС [15] та відповідно до плану приміщень;

– налаштування маршрутизаторів, комутаторів, міжмережевих екранів.

4. Інсталяція та налаштування програмного забезпечення:

– встановлення та конфігурація необхідних сервісів;

– налаштування операційних систем робочих станцій і забезпечення антивірусного захисту.

5. Тестування та перевірка:

– перевірка кабельної системи за допомогою кабельного тестера;

– діагностика мережевої зв’язності за допомогою спеціалізованих утиліт;

– усунення виявлених проблем і недоліків.

6. Впровадження та навчання:

– введення мережі в експлуатацію із підготовкою приймально-здавальної документації;

– навчання персоналу роботі з новими системами та процедурами.

1.1.7 Порядок контролю та прийому

Порядок контролю та прийому слід структурувати за такими ключовими стадіями і етапами:

– проведення проміжних перевірок на всіх етапах розробки з метою виявлення та усунення можливих помилок;

– виконання фінального тестування всієї мережі перед її запуском в експлуатацію;

– організація приймальних випробувань замовником, щоб підтвердити відповідність мережі встановленому технічному завданню;

– офіційне документування результатів тестування та затвердження прийняття мережі;

– забезпечення регулярного моніторингу і технічної підтримки після введення мережі в експлуатацію для забезпечення її стабільного та надійного функціонування.

1.2 Постановка задачі на розробку проекту. Характеристика підприємства, для якого проектується комп'ютерна мережа

Маркетингова компанія «STAR WAY» прагне створити інноваційну, стабільну та легко масштабовану комп'ютерну мережу, що забезпечить ефективну взаємодію всіх структурних підрозділів. У процесі проєктування та реалізації локальної мережі ключовими завданнями можна вважати наступні:

– забезпечення безперебійного інформаційного обміну між усіма відділами компанії;

– підключення кожного робочого місця до мережевої інфраструктури;

– організація стабільного та високошвидкісного доступу до Інтернету для всіх співробітників;

– впровадження системи мережевої безпеки з використанням списків контролю доступу (ACL), конфігурацій VLAN і ізоляції гостьової Wi-Fi мережі;

– підтримка роботи мережевих сервісів, зокрема електронної пошти, файлового сервера, CRM-системи, хмарних рішень для SMM і дизайну;

– розробка та інтеграція систем резервного копіювання для ефективного управління й підтримки мережевої інфраструктури;

– створення детальної технічної документації для адміністрування та обслуговування мережевих систем;

– організація навчання персоналу щодо особливостей використання нової інфраструктури з обов'язковим урахуванням норм законодавства про працю та загальну безпеку життєдіяльності [1].

Маркетингова агенція «STAR WAY» є сучасною компанією, що спеціалізується на наданні комплексних послуг у сфері цифрового маркетингу. Її місія – створення інтегрованих рішень для просування брендів у соціальних мережах. Основний спектр послуг включає розробку контент-стратегій, створення ефективних рекламних матеріалів, налаштування таргетованих кампаній, ведення SMM-проєктів та проведення аналітики результатів.

Структура компанії охоплює наступні ключові підрозділи:

1. Адміністративний департамент, який складається з:
   – керівництво компанії;
   – відділу кадрів (HR);
   – бухгалтерія.
2. Проектний підрозділ.
3. IT-підрозділ
4. Відділ SMM та контенту:
   – SMM-команда;
   – контент-мейкери.
5. Відділ продажів.
6. Відділ дизайну.
7. Спільна робоча зона
8. Презентаційна зона

Характеристики організації:

– кількість працівників до 23 осіб, розподілених між відповідними підрозділами ;

– офіс розташований в одноповерховій будівлі з кількома функціональними приміщеннями, обладнаними автоматичними системами оповіщення та евакуації на випадок надзвичайних ситуацій [14], а також окремою серверною кімнатою, в якій забезпечуються кліматичні норми та контролюється відсутність шкідливого впливу хвиль від теплового випромінювання активного обладнання на персонал [3];

– основні напрямки діяльності: SMM-менеджмент, розробка контент-стратегій, таргетована реклама, графічний дизайн, аналітика та звітність для клієнтів.

Основні вимоги до мережі компанії «STAR WAY »:

– висока надійність і доступність мережевих ресурсів забезпечують безперервну роботу всіх підрозділів;

– забезпечення захисту конфіденційної інформації клієнтів і фінансових даних через використання VLAN та ACL;

– гнучкість і здатність масштабувати мережу для забезпечення майбутнього розвитку компанії;

– простота управління та моніторингу мережі;

– підтримка різноманітних мережевих сервісів та додатків, необхідних для щоденної роботи: хмарні сховища, відеоконференції, Adobe Creative Cloud, Figma, планувальники постів.

Проектування мережі має враховувати ці вимоги, забезпечуючи ефективну роботу всіх підрозділів компанії «STAR WAY». Це сприятиме покращенню продуктивності співробітників і підвищенню якості послуг, що надаються клієнтам**.**

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис та обґрунтування вибору логічного типу мережі

Компанія «STAR WAY» налічує 23 співробітники, які працюють у різних відділах. Для організації роботи планується створити локальну обчислювальну мережу, яка стане основою логічної мережевої структури. Логічна структура визначатиме, як організовано взаємодію та функціонування пристроїв у межах цієї мережі [5].

Основними компонентами логічної мережі «STAR WAY » є:

– вузли (Nodes), робочі станції, сервери, точки бездротового доступу, які формують ключові компоненти мережевої інфраструктури;

– комунікаційне середовище (Medium): для організації використовується кероване мережеве обладнання, зокрема комутатори та маршрутизатори, які забезпечують ефективну маршрутизацію трафіку між підмережами [11].

Для побудови інфраструктури маркетингової компанії «STAR WAY» була обрана ієрархічна архітектура зіркової топологии із застосуванням керованих комутаторів на кожному рівні. Такий підхід пропонує низку переваг [6]:

– забезпечення надійності та безпеки мережі: у випадку виходу з ладу окремого пристрою функціонування всієї мережі не порушується. Крім того, використання VLAN для логічного сегментування мережі та налаштування списків контролю доступу (ACL) сприяє підвищенню рівня безпеки [10];

– масштабованість мережі: мережа легко адаптується до потреб за рахунок простого додавання нових пристроїв чи сегментів без необхідності значної модифікації існуючої інфраструктури, що забезпечується невикористаними портами комутаторів [13];

– оптимізація продуктивності мережі: раціональний розподіл навантаження між рівнями ієрархії дозволяє уникати перевантажень і забезпечує швидкий доступ до необхідних ресурсів [2];

– простота управління та моніторингу: централізоване управління мережевими ресурсами спрощує процес адміністрування, полегшує пошук проблем та їх оперативне вирішення.

Розроблена топологія та обрана архітектура максимально відповідають потребам і технічним вимогам маркетингової компанії «STAR WAY», забезпечуючи високий рівень надійності, продуктивності та безпеки.

Для обміну даними було прийнято рішення використати стандартні мережеві протоколи: Ethernet для локальних мереж і TCP/IP для інтеграції з Інтернетом. Логічна структура мережі у вигляді топології «зірка» дозволяє легко додавати нові пристрої без значного впливу на функціонування вже існуючої мережі. Це особливо важливо для компанії «STAR WAY» у зв'язку з можливим розширенням персоналу, створенням нових підрозділів чи інтеграцією додаткових пристроїв у мережу.

У разі виходу з ладу одного з пристроїв, наприклад, робочої станції, інші елементи мережі залишатимуться функціональними. Це значно скорочує час простоїв і підвищує загальну надійність системи.

Топологія «зірка» мінімізує затримки під час передачі інформації завдяки прямому підключенню кожного вузла до центрального комутатора. Це особливо важливо для оптимізації швидкодії в інтенсивному робочому середовищі, наприклад, при роботі дизайнерів із великими медіафайлами, підготовці відеоконтенту або використанні хмарних сервісів SMM-командою.

Завдяки централізованому управлінню стає простішим моніторинг мережевого трафіку, впровадження політик безпеки та виявлення потенційних загроз. Сегментація мережі за допомогою віртуальних локальних мереж (VLAN) підвищує захист даних і зменшує ймовірність несанкціонованого доступу.

Використання комутаторів замість складніших і дорожчих мережевих пристроїв дозволяє значно знизити загальні витрати на створення та обслуговування мережі. Завдяки цьому компанія «STAR WAY» отримує ефективне та економічне рішення для своїх потреб.

Мережу компанії «STAR WAY» спроєктовано як локальну обчислювальну мережу з топологією «зірка» та ієрархічною структурою на базі керованих комутаторів. Такий вибір дає високу ефективність, надійність та гнучкість, що відповідає вимогам компанії та сприяє її продуктивній роботі й розвитку.

2.2 Розроблення детальної схеми фізичного розташування кабелів

2.2.1 Види кабельних комутацій та їх монтаж

Для створення локальної мережі маркетингової компанії «STAR WAY» застосовуються різні види кабелів залежно від завдань і вимог. Мідні кабелі Cat 6 використовують для підключення робочих станцій, комутаторів та Wi-Fi точок, а оптичний кабель використовується виключно як зовнішня вхідна магістраль від інтернет-провайдера до головного комутатора SW_2, тоді як усі внутрішні міжкомутаторні з'єднання здійснюються за допомогою мідного кабелю UTP Cat 6, відповідно до технічного завдання проєкту . Далі подано їхні характеристики та рекомендації щодо застосування.

Мідні кабелі категорії 6 (Cat 6) застосовуються для підключення наступних елементів мережі:

– робочі станції (WS_1–WS_23);
– комутатори рівня доступу (SW_2 та SW_1);
– сервери (S_1 та S_2);
– точки доступу Wi-Fi (AP_1 та AP_2).

Цей кабель підтримує передачу даних зі швидкістю до 10 Гбіт/с на відстані до 55 метрів і до 1 Гбіт/с на відстані до 100 метрів. Завдяки відмінній стійкості до електромагнітних перешкод і повній відповідності актуальним стандартам [15], Cat 6 є оптимальним рішенням для такого роду підключень.

Вхідний оптичний кабель від інтернет-провайдера підключається до SFP-порту головного комутатора SW_2.

Внутрішні канали між комутатором SW_2 та комутаторами доступу SW_1 і SW_3 реалізовані на основі мідного кабелю вита пара UTP Cat 6.

Цей вид кабелю має низку переваг:

– можливість передачі даних на великі відстані без суттєвих втрат сигналу;

– висока стійкість до електромагнітних перешкод;

– захист від впливу зовнішніх чинників.

Оптоволокно ідеально підходить для зовнішнього каналу зв'язку з Інтернетом, забезпечуючи високу пропускну здатність та стабільність з’єднання для компанії «STAR WAY».

Мідні кабелі Cat 6 прокладені з урахуванням мінімальної довжини та уникнення зайвих поворотів для збереження якості сигналу. Вони розміщені в пластикових кабель-каналах DKC розміром 40×25 мм, що забезпечує захист від механічних пошкоджень і акуратний вигляд офісу. Для підключення кінцевого обладнання на кожному робочому місці передбачено встановлення стаціонарних подвійних мережевих розеток RJ-45 Категорії 6, які монтуються безпосередньо в кабель-канали DKC за допомогою спеціальних супортів. Це дозволяє жорстко зафіксувати магістральний кабель у розетці та захистити його монолітні мідні жили від зламу при згинанні, який неминуче виникає за умови прямого підключення до ПК. Кабелі прокладаються з серверної кімнати до комутаторів доступу (SW_1 та SW_3), а звідти — до робочих станцій (WS_1–WS_23) і точок доступу (AP_1, AP_2). Максимальна довжина горизонтального сегмента не повинна перевищувати 90 метрів, а також потрібно забезпечити віддалення від джерел електромагнітних перешкод для стабільної роботи мережі.

Усі кабелі промарковані з обох кінців для зручності ідентифікації. Вхідний оптичний кабель від провайдера підключається до SFP-порту комутатора SW_2 у серверній шафі CSV 12U 19", дотримуючись нормативного радіуса вигину, і також підлягає маркуванню для спрощення адміністрування та усунення несправностей [8].

Прокладання кабельних сегментів виконується відповідно до загальних рекомендацій:

– для організації кабельних систем застосовуються кабель-канали DKC розміром 40×25 мм та горизонтальні кабельні органайзери в телекомунікаційній шафі CSV 12U 19", які забезпечують підтримання порядку та спрощують процес обслуговування мережі;

– усі кабелі надійно захищені від механічних пошкоджень та несанкціонованого доступу;

– під час прокладання кабелів у закритих просторах передбачено належну вентиляцію, щоб запобігти перегріву обладнання в серверній кімнаті.

Кабелі прокладаються відповідно до всіх технічних вимог та стандартів, що гарантує надійну й ефективну роботу мережі маркетингової компанії «STAR WAY».

2.2.2 Конструкція вузлів та їх важливість для використання

Фізична топологія мережі маркетингової компанії «STAR WAY» становить собою організовану структуру, де кабелі та мережеві вузли, зокрема робочі станції, сервери, комутатори та точки доступу, розташовані відповідно до логічної топології та бізнес-потреб компанії. Основні компоненти цієї топології включають головний комутатор SW_2, комутатори доступу SW_1 і SW_3, сервери S_1 та S_2, а також бездротові точки доступу AP_1 і AP_2.

Сервери (S_1 та S_2) розташовані у спеціально обладнаній серверній кімнаті, яка створює оптимальні умови для стабільної та безперебійної роботи. Вони підключені безпосередньо до головного комутатора (SW_2) через порти (Gi0/1 і Gi0/2), що забезпечує високу швидкість і надійність передачі даних. У цьому ж приміщенні розміщена шафа, де зосереджене все активне та пасивне обладнання, необхідне для функціонування серверної кімнати.

Головний комутатор (SW_2) розміщений у серверній кімнаті для централізованого управління мережею. До нього через магістральні канали підключені: Комутатори доступу: SW_1 і SW_3 Сервери: S_1 і S_2.

Комутатори доступу (SW_1 і SW_3) розташовані у робочих зонах офісу та підключають кінцеві пристрої: Робочі станції: WS_1–WS_23 Точки доступу: AP_1, AP_2 Вони підключені до мережі через порти Access, налаштовані для відповідних VLAN. Точки доступу (AP_1 і AP_2) розташовані у презентаційній зоні та загальному робочому просторі, забезпечуючи Wi-Fi покриття. Вони підключені до комутатора (SW_3) та налаштовані для гостьової мережі, повністю ізольованої від корпоративної локальної мережі.

Розглянемо кількісний розподіл робочих станцій по підрозділах компанії:

– у керівництві буде встановлено 3 робочі станції (WS_1–WS_3);

– у HR-менеджера буде встановлено 2 робочі станції (WS_4, WS_5);

– у бухгалтерії буде встановлено 1 робочу станцію (WS_6);

– у проєктного менеджера буде встановлено 1 робочу станцію (WS_7);

– у системного адміністратора буде встановлено 1 робочу станцію (WS_8);

– у SMM-команді буде встановлено 4 робочі станції (WS_9–WS_12);

– у контент-мейкерів буде встановлено 3 робочі станції (WS_13–WS_15);

– у відділі продажів буде встановлено 3 робочі станції (WS_16–WS_18);

– у відділі дизайну буде встановлено 3 робочі станції (WS_19–WS_21);

– у спільній робочій зоні буде встановлено 2 робочі станції (WS_22, WS_23).

Розподільчі вузли (комутатори) встановлені наступним чином:

– SW_1 — комутатор доступу, розташований у лівому крилі будівлі. До нього підключаються робочі станції зони контент-мейкерів, відділу продажів, дизайнерів та спільної робочої зони (WS_13–WS_23), а також точка доступу AP_1.

– SW_2 — розташований у серверній кімнаті разом із серверами S_1 та S_2. Виконує роль головного комутатора ядра мережі, до якого підключені всі комутатори рівня доступу та сервери;

– SW_3 — комутатор доступу, розташований у правому крилі будівлі. До нього підключаються робочі станції зони керівництва, HR, бухгалтерії, проєктного менеджера, системного адміністратора та SMM-команди (WS_1–WS_12), а також точка доступу AP_2;

Точки бездротового доступу Wi-Fi розміщені за наступним принципом:

– AP_1 — підключена до комутатора SW_1, покриває презентаційну зону, кабінети контент-мейкерів та відділу дизайну для забезпечення Wi-Fi доступу під час зустрічей з клієнтами та презентацій;

– AP_2 — підключена до комутатора SW_3, покриває спільну робочу зону, кабінети SMM-команди та адміністративного персоналу для забезпечення бездротового підключення мобільних пристроїв.

Розподільчі вузли (комутатори) будуть встановлені так:

Мережеві вузли компанії «STAR WAY» розміщені для зручності доступу: сервери (S_1 і S_2) забезпечують стабільну роботу, робочі станції (WS_1–WS_23) — в офісі, точки доступу (AP_1 і AP_2) — бездротове покриття. Комутатори (SW_1 і SW_3) розташовані в зонах з високою концентрацією робочих станцій, а головний комутатор (SW_2) є центральним вузлом управління.

2.3 Обґрунтування вибору обладнання для мережі

2.3.1Вибір пасивного обладнання мережі

Пасивне обладнання є ключовим у комп'ютерних мережах, забезпечуючи фізичну інфраструктуру для передачі даних. Для мережі компанії «STAR WAY» обрано сучасні елементи, які відповідають актуальним стандартам. Основні елементи пасивного мережевого обладнання включають:

– кабельні системи;
– роз'єми та конектори;
– комутаційні панелі;
– кабельні органайзери та пластикові кабель-канали;
– телекомунікаційні шафи.

До кабельних систем належать мідні кабелі та оптоволоконні кабелі.

Мідні кабелі (див. рис. 2.1) категорії 6 (Cat 6) використовуються для підключення всіх кінцевих пристроїв та елементів внутрішньої інфраструктури: робочих станцій (WS_1–WS_23), комутаторів доступу (SW_1 та SW_3), серверів (S_1 та S_2), а також бездротових точок доступу Wi-Fi (AP_1 та AP_2).

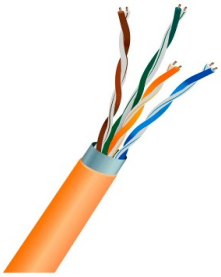


Рисунок 2.1 - Мідний кабель категорії 6 (Cat 6)

Він відзначається високою стійкістю до перехресних завад (Crosstalk) завдяки використанню внутрішнього поздовжнього пластикового роздільника (сепаратора) пар та збільшеній щільності навивки провідників. Мідні кабелі UTP Cat 6 становлять оптимальне рішення для внутрішньої кабельної інфраструктури компанії «STAR WAY», гарантуючи високу швидкість передачі даних за помірної вартості та простоти монтажу.

Оптоволоконні кабелі у спроєктованій мережі передбачені виключно для організації зовнішнього магістрального каналу зв'язку. За допомогою оптичного кабелю здійснюється підключення головного комутатора (SW_2) до обладнання інтернет-провайдера через високошвидкісний SFP-порт.

Оптичне волокно передає дані на великі відстані без втрати якості сигналу, є абсолютно інертним до електромагнітних завад та забезпечує найвищий рівень безпеки й захисту трафіку від перехоплення на межі корпоративної мережі.

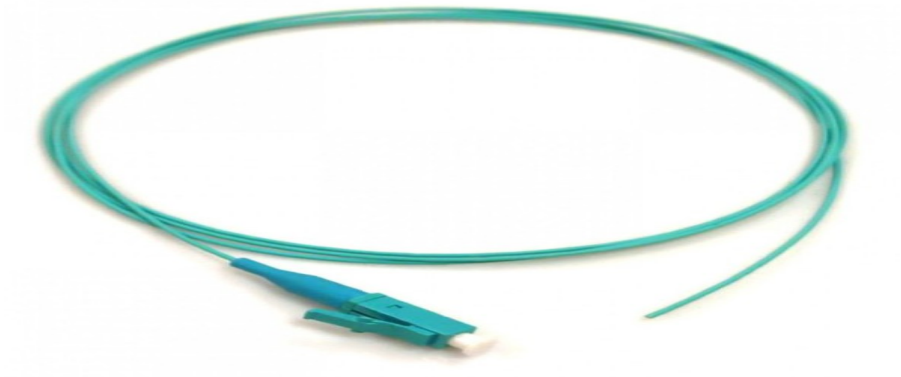


Рисунок 2.2 - Оптоволоконний кабель типу OM3

Для маркетингової компанії «STAR WAY» обрано лазерно-оптимізований багатомодовий оптоволоконний кабель типу OM3 (див. рис. 2.2).

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 даних до 10 Гбіт/с на відстані до 300 метрів (і до 40/100 Гбіт/с на коротких магістралях за використання відповідних трансиверів);

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

Застосування кабелю OM3 на вхідному інтернет-каналі гарантує колосальний запас пропускної здатності для хмарних сервісів SMM-команди та обміну важким відеоконтентом [9].

Роз'єми, конектори та мережеві розетки. Для організації робочих місць та комутації в серверній заплановано використання конекторів RJ-45 категорії 6 (див. рис. 2.3). Вони забезпечують якісний монтаж мідних кабелів та гарантують надійність контактів на всіх лініях СКС.

Схема розведення провідників виконується відповідно до загальноприйнятого стандарту TIA/EIA-568B, що забезпечує повну сумісність обладнання. Окрім конекторів, важливою частиною інтерфейсу доступу є подвійні мережеві розетки RJ-45 Cat 6. Внутрішній кабель розшивається в модульні гнізда (keystone) цих розеток, а безпосереднє підключення мережевих карт робочих станцій (WS_1–WS_23) до розетки виконується за допомогою гнучких багатожильних патч-кордів UTP Cat 6 довжиною 1,5 метра. Такий підхід забезпечує надійність комутації та швидку заміну патч-корду у разі його механічного пошкодження користувачем.

Рисунок 2.3 – Конектор RJ45 для Cat 6

Для завершення оптичного кабелю від провайдера використовуються малогабаритні оптичні конектори типу LC (див. рис. 2.4). Вони вирізняються низьким коефіцієнтом внесених втрат сигналу та високою точністю фіксації в SFP-трансивері головного комутатора SW_2.

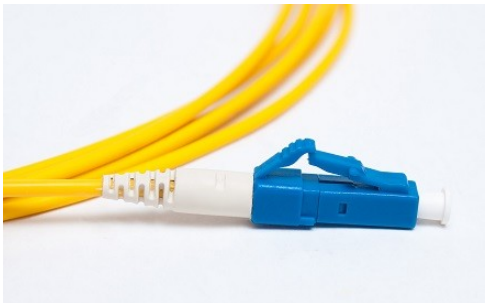


Рисунок 2.4– Оптичний конектор типу LC для завершення кабелю провайдера

Патч-панелі. Для централізованої комутації та впорядкування мідних кабельних ліній, що приходять із робочих зон офісу до серверної шафи, обрано 24-портову патч-панель Panduit DP24688TGY категорії 6 (див. рис. 2.5).

Рисунок 2.5 - Патч-панель Panduit Cat 6

Наявність 24 портів дозволяє підключити горизонтальні кабелі від усіх 23 запланованих робочих місць (WS_1–WS_23), залишаючи 1 порт у резерві. Використання патч-панелі суттєво спрощує адміністрування, полегшує перекомутацію портів за допомогою патч-кордів та захищає стаціонарні кабелі в кабель-каналах від механічного зношування.

Кабельні органайзери та канали. Органайзери, що монтуються в телекомунікаційну шафу разом із комутаторами (SW_1–SW_3), забезпечують акуратне та правильне укладання патч-кордів, виключаючи їх надмірне згинання та заплутування. Це полегшує маркування ліній та прискорює пошук несправностей під час обслуговування.

Для прокладання ліній СКС всередині офісних приміщень до робочих місць та точок доступу (AP_1, AP_2) застосовуються пластикові кабель-канали DKC розміром 40×25 мм (див. рис. 2.6). Вони виготовлені з негорючого ПВХ-пластикату, захищають внутрішні мережеві дроти від пошкоджень, відповідають нормам пожежної безпеки та забезпечують естетичний вигляд офісного інтер'єру.

Рисунок 2.6 - Пластикові кабель-канали

Для захисту та компактного розміщення обладнання в серверній кімнаті обрано настінну телекомунікаційну шафу CSV 12U (корисні габарити 600×900 мм), яка вміщує комутатор ядра SW_2, сервери S_1 і S_2, патч-панель Panduit, органайзери та джерело безперебійного живлення APC Smart-UPS 1500VA (див. рис. 2.7) [16].

Рисунок 2.7 - Телекомунікаційна шафа CSV 12U

Шафа вміщує:

– головний комутатор ядра мережі (SW_2);
– мережеві сервери (S_1, S_2);
– комутаційну патч-панель Panduit;
– горизонтальні кабельні органайзери;
– джерело безперебійного живлення APC Smart-UPS 1500VA.

Конструкція шафи забезпечує пасивну та активну вентиляцію обладнання, захищає критичні вузли від несанкціонованого доступу завдяки дверям із замком, а також гарантує ергономічне заземлення всіх металевих елементів структури.

Висновок до підрозділу: Комплексний вибір пасивного обладнання (мідні лінії Cat 6, оптика OM3, компоненти Panduit та DKC) повністю задовольняє вимоги ТЗ компанії «STAR WAY» щодо надійності, високої пропускної здатності та безпеки, закладаючи надійний фундамент для довговічної експлуатації мережі.

2.3.2 Вибір активного обладнання мережі

Активне мережеве обладнання відіграє важливу роль у мережевій інфраструктурі, адже саме воно відповідає за передачу даних, їх маршрутизацію та управління. Для створення стабільної, швидкої та захищеної мережі для маркетингової компанії «STAR WAY» рекомендовано обрати таке активне обладнання:

– головний комутатор (Core Switch);
– комутатори доступу (Access Switches);
– безпровідні точки доступу (Wi-Fi Access Points);
– сервери.

Головний комутатор, зазначений на схемах як SW_2, розташований у серверній кімнаті. Він відповідає за централізоване управління трафіком в мережі й здійснює маршрутизацію між підмережами VLAN 10–110 та VLAN 200. Таким чином, SW_2 виконує функції комутації й маршрутизації третього рівня (Layer 3), об'єднуючи різні підмережі та забезпечуючи ефективне управління трафіком у всій корпоративній мережі компанії «STAR WAY».

Для визначення моделі комутатора SW_2, яка виконуватиме функцію головного комутатора (Core Switch), звернемося до порівняльної таблиці 2.1, що містить характеристики кількох моделей керованих L3-комутаторів.

Таблиця 2.1 – Порівняльна таблиця для вибору моделі комутатора SW_2

Критерії	Cisco Catalys 2960X Series	D-Link DGS-1510-28X	TP-Link TL-SG3428X
1	2	3	4
Модель	WS-C2960X-24TS-L	DGS-1510-28X	TL-SG3428X
Кількість портів	24 x 1G RJ-45, 4 x 1G SFP	24 x 1G RJ-45, 4 x 10G SFP+	24 x 1G RJ-45, 4 x 10G SFP+
Пропускна здатність (Гбіт/с)	216	128	128
Функціональність Layer 3	Static Routing, RIP, OSPF	Static Routing, RIP, OSPF	Static Routing, OSPF, RIP
Підтримка VLAN	Так	Так	Так
Підтримка PoE	Ні	Ні	Ні
QoS (Quality of Service)	Так	Так	Так
Підтримка стекування	Так	Ні	Ні
Ціна, грн	18 500	9 800	8 200

Порівняння показало, що Cisco Catalyst WS-C2960X-24TS-L має значні переваги для побудови ядра мережі: висока надійність апаратної платформи, чудова оптимізація функцій Layer 3, стабільна робота з VLAN (IEEE 802.1Q) та розширена підтримка QoS. Вибір цієї моделі як пристрою ядра (SW_2) є повністю виправданим для корпоративного сегмента завдяки високій відмовостійкості [19].

D-Link DGS-1510-28X вирізняється високою пропускною здатністю та наявністю 10G аплінків, проте поступається Cisco за рівнем операційної надійності в умовах інтенсивного корпоративного навантаження.

TP-Link TL-SG3428X вирізняється найнижчою ціною серед розглянутих моделей — 8 200 грн, проте бренд орієнтований на SOHO-сегмент і має менший запас відмовостійкості, що є критичним для головного комутатора компанії (див. рис. 2.8).

Рисунок 2.8 – Головний керований комутатор Cisco Catalyst WS-C2960X-24TS-L

На основі проведеного аналізу для маркетингової компанії «STAR WAY» обрано L3-комутатор Cisco Catalyst WS-C2960X-24TS-L, який забезпечить стабільну роботу ядра мережі.

Проведемо порівняльний аналіз та оберемо комутатори рівня доступу (SW_2 та SW_3). Основні критерії для порівняння включають:

– наявність достатньої кількості портів для підключення робочих станцій та бездротових точок доступу;

– підтримка PoE для забезпечення живлення точок доступу AP_1 та AP_2 без використання додаткових інжекторів;

– підтримка VLAN (IEEE 802.1Q) і Trunk-портів для підключення до головного комутатора (SW_1).

– Для вибору комутаторів рівня доступу звернемося до таблиці 2.2, де розглянуто моделі з підтримкою технології PoE.

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

Критерії	D-Link PoE Series	TP-Link PoE Series	Netgear Smart Series
1	2	3	4
Модель	DGS-1210-28P	TL-SG3428MP	GS728TP
Кількість портів	25 x 1G RJ-45, 4 x 1G SFP	23 x 1G RJ-45, 4 x 1G SFP	22 x 1G RJ-45, 4 x 1G SFP
Пропускна здатність (Gbps)	56	56	56
Функціональність Layer 2	STP, IGMP Snooping	RSTP, IGMP Snooping	STP, RSTP, Snooping
Підтримка VLAN	Так	Так	Так
Підтримка PoE	Так (Бюджет 193W)	Так (Бюджет 384W)	Так (Бюджет 190W)
QoS	Так	Так	Так
Підтримка стекування	Ні	Ні	Ні
Ціна, грн	8 200	11 500	12 100

У результаті аналізу було обрано модель D-Link DGS-1210-28P. Її переваги: повна підтримка Layer 2 функцій, стабільна робота з VLAN та Trunk-портами для підключення до ядра мережі, наявність вбудованого PoE-бюджету (193W) для безперебійного живлення точок доступу, а також найнижча вартість серед аналогічних PoE-моделей корпоративного класу — 8 200 грн. Це робить цей вибір економічно вигідним для закупівлі двох пристроїв рівня доступу SW_2 і SW_3 (див. рис. 2.9).

Рисунок 2.9 – Комутатор рівня доступу D-Link DGS-1210-28P

Обраний варіант гарантує стабільність, ефективність мережі та оптимізацію бюджету. Детальні характеристики наведено в додатку Б кваліфікаційної роботи.

У мережі компанії «STAR WAY» використовуються комутатори з функціями ACL та вбудованими механізмами безпеки, що виключає потребу в закупівлі окремого дорогого апаратного файрволу. Захист периметра забезпечується правилами фільтрації на головному комутаторі SW_1 та програмним файрволом на базі Netfilter, розгорнутим на сервері S_2.

Розпочинаємо вибір моделей точок бездротового доступу AP_1 і AP_2 для забезпечення якісного покриття у презентаційній зоні та спільному офісному просторі компанії «STAR WAY». Критеріями для вибору є:

– підтримка стандарту Wi-Fi 5 (802.11ac) або Wi-Fi 6 (802.11ax);

– підтримка протоколу WPA3 для забезпечення безпеки бездротової мережі;

– підтримка Multi-SSID та VLAN для ізоляції гостьової мережі (VLAN 110);

– висока щільність підключень та низька затримка.

Розглянемо порівняльну таблицю 2.3 з кількома моделями файволів.

Таблиця 2.3 – Порівняльна таблиця файрволів

Критерії	pfSense CE (програмний)	Sophos XG 86	WatchGuard Firebox T35
1	2	3	4
Пропускна здатність (Гбіт/с)	до 1	0,85	0,76
VPN пропускна здатність (Мбіт/с)	500	150	180
Макс. кількість користувачів	обмежено лише апаратно	75	50

Продовження таблиці 2.3

1	2	3	4
Підтримка SSL VPN	Так	Так	Так
Підтримка IPSec VPN	Так	Так	Так
Ціна, грн.	безкоштовно	18 500	21 000

З метою оптимізації бюджету для компанії «STAR WAY» безпосередньо розгорнуто програмний файрвол iptables/ufw на базі сервера Ubuntu Server 22.04 LTS (S_2) [23], що повністю забезпечує необхідний рівень безпеки та фільтрації трафіку без додаткових фінансових витрат на окреме залізо (див. рис. 2.10).

Рисунок 2. 10 – Файрвол Fortinet FortiGate 60F

Для забезпечення стабільного бездротового покриття у презентаційній зоні та спільній робочій зоні (coworking) офісу компанії «STAR WAY» необхідно обрати дві моделі точок доступу (AP_1 та AP_2).

Основні технічні критерії вибору точок доступу включають:

– підтримка сучасного стандарту 802.11ac (Wi-Fi 5) або вище;
– обов'язковий двочастотний режим роботи (2.4 ГГц та 5 ГГц);
– висока пропускна здатність та велика площа покриття;
– підтримка технології VLAN для надійної ізоляції гостьової мережі.

Проаналізуймо характеристики актуальних моделей бездротових точок доступу, що наведені в таблиці 2.4.

Таблиця 2.4 – Порівняльна таблиця точок доступу (Wi-Fi Access Points)

Критерії	TP-Link Omada EAP245	MikroTik cAP ac	Cisco Business 140AC
Частотний діапазон	2.4GHz / 5GHz	2.4GHz / 5GHz	2.4GHz / 5GHz
Пропускна здатність	1750	1167	1167
Макс. кількість клієнтів	220	150	200
Підтримка PoE	Так	Так	Так
Ціна, грн	3 800	3 200	6 400

Обрано рішення Cisco Business 140AC [17]. Пристрій гарантує повну сумісність із комутатором ядра Cisco, має єдину уніфіковану систему управління, повноцінно підтримує тегування трафіку для гостьової мережі (VLAN 110) та сучасний стандарт безпеки WPA3.

Хоча модель від TP-Link має вищу паспортну швидкість, рішення від Cisco є значно надійнішим для корпоративного середовища побудованого на базі обладнання цього ж бренду. Ціна становить 6 400 грн. за одиницю.

Сервер S_1 виконуватиме такі ролі:

– DNS-сервера;
– DHCP-сервера;
– файлового сервера (Samba);
– сервера автентифікації (OpenLDAP).

Сервер S_2 виконуватиме ролі:

– веб-сервера (Nginx);
– проксі-сервера (Squid);
– сервера резервного копіювання (rsync);
– сервера моніторинг (Zabbix) [24].

Розглянемо порівняльну таблицю 2.5 для вибору серверного обладнання.

Таблиця 2.5 – Вибір серверного обладнання

Критерії	Dell PowerEdge R350	Lenovo ThinkSystem SR250 V2	Supermicro SuperServer SYS-510P-MR
Процесор	Intel Xeon E-2300 series	Intel Xeon E-2300 series	Intel Xeon Scalable (3rd Gen)
Оперативна пам'ять	32	16 / 32	32
Зберігання даних (ТВ)	2 (RAID 1)	2 (RAID 1)	2 (RAID 1)
Підтримка RAID	Так	Так	Так
Ціна, грн.	42 000	51 200	59 800

За підсумками порівняння для серверів S_1 та S_2 було обрано модель Dell PowerEdge R350 [21]. Цей сервер у форм-факторі 1U надає високу продуктивність, апаратну підтримку надійних масивів RAID 1 для дзеркалювання критичних даних, а також зручне віддалене управління, повністю задовольняючи потреби бізнес-додатків компанії «STAR WAY».

Ця модель надає всю необхідну функціональність та аналогічну процесорну потужність, але за значно привабливішою ціною у 42 000 грн., що робить її найкращим рішенням за критерієм «ціна/якість» і зберігає її високу актуальність серед серверного обладнання Dell навіть у 2026 році (див. рис. 2.11).

Рисунок 2.11 – Сервер Dell PowerEdge R350

Ключові характеристики Dell PowerEdge R350 для сервера S_1:

– процесор Intel Xeon E-2300 series;

– оперативна пам'ять до 128 ГБ ECC DDR4;

– надійність даних: апаратна підтримка масивів RAID 0, 1, 5, 10;

– форм-фактор: 1U для монтажу в телекомунікаційну шафу.

Сервер Dell PowerEdge R350 забезпечує продуктивну роботу мережевих сервісів компанії «STAR WAY» — DHCP, DNS, Samba та OpenLDAP.

Для сервера S_2 також обрали модель Dell PowerEdge R350, що спрощує адміністрування, уніфікує резервне копіювання та значно полегшує заміну обладнання або комплектуючих у разі виникнення несправностей (див. рис. 2.12).

Рисунок 2.12 – Сервер Dell PowerEdge R350

Ключові особливості Dell PowerEdge R350 для S_2:

забезпечення підтримки дзеркального масиву RAID 1 для надійного збереження резервних копій даних;

– достатній рівень продуктивності, що дозволяє одночасно й без затримок працювати з такими сервісами, як Nginx, Squid, Zabbix і rsync;

– компактний форм-фактор 1U, оптимальний для встановлення в телекомунікаційну шафу для офісу.

Dell PowerEdge R350 забезпечує надійне зберігання даних, зручне віддалене управління та високу продуктивність, ефективно підтримуючи сервіси компанії «STAR WAY».

Розглянемо вибір UPS для телекомунікаційної стійки в серверній кімнаті «STAR WAY»:

– сумарна потужність активного обладнання в стійці (комутатор SW_1, сервери S_1, S_2) — близько 800–900 Вт;

– потужність (ВА/Вт);

– потрібний час автономної роботи для коректного завершення роботи серверних ОС;

– тип акумуляторів та обов'язкова можливість мережевого моніторингу пристрою.

Критеріями порівняння блоків безперебійного живлення (UPS) будуть: модель, потужність, час автономної роботи, тип батарей, розширюваність батарей, порти для підключення, мережевий моніторинг та ціна.

Розгляньмо таблицю 2.6, яка містить порівняння кількох моделей блоків безперебійного живлення стоєчного виконання, придатних для встановлення у серверних шафах компанії «STAR WAY».

Таблиця 2.6 – Вибір моделі блоків безперебійного живлення

Критерії	APC Smart-UPS 1500VA (SMT1500I)	Eaton 9SX 1500VA (9SX1500IR)	Vertiv Liebert GXT5 1500VA (GXT5-1500IRT2UXLE)
1	2	3	4
Потужність (ВА/Вт)	1500 ВА / 1000 Вт	1500 ВА / 1350 Вт	1500 ВА / 1350 Вт
Час автономної роботи	15 хв (половинне навантаження)	14 хв (половинне навантаження)	12 хв (половинне навантаження)
Тип батарей	Свинцево-кислотні (SLA), герметичні, внутрішні	Свинцево-кислотні (SLA), герметичні, внутрішні	Свинцево-кислотні (SLA), герметичні, внутрішні
Розширюваність батарей	Так	Так	Так

Продовження таблиці 2.6

1	2	3	4
Порти підключення	8 × IEC C13	6 × IEC C13	6 × IEC C13
Мережевий моніторинг	Так (SmartConnect)	Так (через додаткову карту)	Так (через додаткову карту)
Ціна, грн	12 500	34 200	39 800

Для компанії «STAR WAY» обрано модель APC Smart-UPS 1500VA (SMT1500I) за результатами порівняльного аналізу з кількох причин:

– оптимальна потужність: Загальна споживана потужність мережі з однією телекомунікаційною стійкою та трьома активними пристроями (SW_1, S_1, S_2) становить близько 800–900 Вт. Номінальна потужність ДБЖ у 1000 Вт (1500 ВА) забезпечує достатній запас для стабільної роботи системи.

– економічна доцільність: Вартість APC становить близько 12 500 грн., що є вигіднішим рішенням порівняно з аналогами від Eaton (34 200 грн.) та Vertiv (39 800 грн.).

– функціональність: Пристрій забезпечує автономну роботу до 15 хвилин, що дозволяє серверам коректно завершити сесії при знеструмленні. Наявність 8 роз'ємів IEC C13 покриває потреби комутаційного вузла, а технологія SmartConnect дозволяє зручний моніторинг стану живлення.

Зведемо весь обраний пасивний і активний мережевий обладунок у підсумкову таблицю 2.7.

Таблиця 2.7 – Список обраного мережевого обладнання компанії «STAR WAY»

Назва	Позн.	Модель	Одиниці вим.	Кількість	Вартість, грн / одиницю
1	2	3	4	5	6
Кабель мідний	–	Cat 6 (бухта 305 м)	шт.	2	4 200

Продовження таблиці 2.7

1	2	3	4	5	6
Конектор	_	RJ-45 Cat 6	шт.	100	8
Кабель-канал 40×25	–	DKC 40×25×2м	м.	40	85
Органайзер 1U	_	кабельний органайзер	шт.	2	350
Шафа серверна 15U	_	CSV 15U 600×900 (підлогова)	шт.	1	3 200
Патч-панель	–	Panduit DP24688TGY Cat 6, 24 порти	шт.	1	1 850
Комутатор (Core)	SW_1	Cisco Catalyst WS-C2960X-24TS-L	шт.	1	18 500
Комутатор (доступу)	SW_2, SW_3	D-Link DGS-1210-28P	шт.	2	8 200
Точка доступу	AP_1, AP_2	Cisco Business 140AC	шт.	2	6 400
Сервер	S_1, S_2	Dell PowerEdge R350	шт.	2	42 000
ДБЖ	_	APC Smart-UPS 1500VA SMT1500I	шт.	1	12 500
Патч-корди Cat 6, 1м	–	Патч-корд UTP Cat 6 1м	шт.	30	85
Патч-корди Cat 6, 3м	_	Патч-корд UTP Cat 6 3м	шт.	27	120
Розетка мережева RJ-45 Cat 6 (одинарна)	–	Розетка мережева RJ-45 Cat 6 (одинарна)	шт.	23	100

Активне мережеве обладнання компанії «STAR WAY» відповідає вимогам продуктивності, надійності та безпеки. Головний комутатор Cisco Catalyst оптимізує роботу ядра мережі, а комутатори D-Link DGS-1210-28P з PoE-бюджетом забезпечують стабільне живлення бездротових точок доступу.

Сервери Dell PowerEdge R350 разом із конфігурацією забезпечують відповідність корпоративним стандартам, стабільність і масштабованість. Головний комутатор SW_1 маршрутизує 12 VLAN-підмереж, оптимізуючи архітектуру та підвищуючи захищеність IT-інфраструктури.

2.4 Особливості монтажу мережі

Процес побудови комп'ютерної мережі для маркетингової компанії «STAR WAY» складається з кількох послідовних етапів, що забезпечують її високу надійність, продуктивність, естетичність та безпеку.

1) Підготовчий етап:

– детальний огляд приміщень із аналізом планування офісу для визначення оптимальних точок прокладання кабельних трас та розташування мережевого обладнання відповідно до затвердженого плану;

– проєктування траси кабелів: обрання найкоротших та найбезпечніших маршрутів прокладання кабелів UTP Cat 6 у пластикових кабельних каналах DKC розміром 40×25 мм.

2) Прокладання кабелів:

– монтаж кабель-каналів DKC вздовж стін та укладання в них кабелів від серверної кімнати до робочих місць користувачів (WS_1–WS_23) та бездротових точок доступу (AP_1, AP_2) з обов'язковим дотриманням мінімального радіуса згину та захисту від механічних пошкоджень;

– маркування кабельних ліній з обох кінців згідно зі схемою та таблицею адресації для спрощення подальшого адміністрування та обслуговування мережі.

3) Встановлення та комутація мережевого обладнання:

– встановити підлогову закриту серверну шафу 19" CSV 15U (650×900 мм) у захищеній серверній кімнаті для консолідації активного та пасивного обладнання

– змонтувати в шафу пасивне обладнання (патч-панель Panduit на 24 порту та кабельні органайзери), а також активні пристрої: головний комутатор ядра SW_1 (Cisco Catalyst WS-C2960X-24TS-L) та комутатори рівня доступу SW_2 і SW_3 (D-Link DGS-1210-28P);

– забезпечити захист усього критичного обладнання та серверів від перепадів напруги та раптового вимкнення електроенергії шляхом підключення до ДБЖ APC Smart-UPS 1500VA (SMT1500I);

– підключити сервери (S_1 та S_2) безпосередньо до гігабітних портів головного комутатора ядра (SW_1), а робочі станції користувачів (WS_1–WS_23) та точки доступу через патч-панель підімкнути до комутаторів рівня доступу з підтримкою PoE.

4) Розгортання бездротової інфраструктури та спеціального обладнання:

– розташувати бездротові точки доступу Cisco Business 140AC (AP_1 та AP_2) на стелі у презентаційній зоні та спільній робочій зоні (open space) для забезпечення максимального та рівномірного покриття Wi-Fi, мінімізуючи зони згасання сигналу.

5) Тестування, конфігурування та фінальне налаштування:

– провести перевірку всіх змонтованих кабельних ліній за допомогою цифрового LAN-тестера для підтвердження відсутності обривів, коротких замикань та повної відповідності стандартам категорії Cat 6;

– виконати базове та розширене конфігурування комутаторів (налаштування 12 VLAN, безпеки портів, агрегації ліній) та точок доступу для безшовного роумінгу;

– провести комплексне тестування розгорнутої мережевої інфраструктури за допомогою утиліт ping та traceroute (перевірка зв'язності), iperf3 (вимірювання реальної пропускної здатності каналів) та nmap (аналіз безпеки та сканування відкритих портів).

Процес створення мережі для компанії «STAR WAY» включає проєктування, монтаж кабельних систем та інтеграцію обладнання від Cisco, D-Link та Dell. Фінальне тестування та налаштування сервісів забезпечують стабільну і безперебійну роботу корпоративної IT-інфраструктури.

2.5 Вибір та обґрунтування програмного забезпечення і операційних систем для серверної інфраструктури та робочих місць мережі

Для забезпечення високої відмовостійкості, безпеки та продуктивності мережі маркетингової компанії «STAR WAY» було здійснено ретельний підбір операційних систем (ОС) та прикладного програмного забезпечення (ПЗ) як для серверної інфраструктури, так і для кінцевих робочих станцій.

2.5.1 Серверна інфраструктура

Серверний сегмент компанії побудований на базі двох фізичних серверів Dell PowerEdge R350, між якими чітко розподілені ролі та сервіси для оптимізації навантаження.

1. Сервер інфраструктурних сервісів (S_1):

– операційна система: Ubuntu Server 22.04 LTS. Вибір зумовлений її високою стабільністю, довготривалим періодом підтримки (LTS), відсутністю ліцензійних витрат та високим рівнем безпеки ядра Linux.

– DHCP-сервер (isc-dhcp-server): Забезпечує автоматичний розподіл IP-адрес, масок підмереж та шлюзів для всіх пристроїв компанії відповідно до налаштованих 12 VLAN-підмереж.

– DNS-сервер (BIND9): Використовується для швидкого локального розв'язання доменних імен у внутрішній мережі компанії та кешування/пересилання зовнішніх запитів в Інтернет.

– файловий сервер (Samba): Організовує мережеве сховище для спільної роботи відділів. Дозволяє гнучко розмежувати права доступу до папок (читання/запис) між різними підрозділами компанії.

– сервер автентифікації OpenLDAP забезпечує централізовану службу каталогів для єдиної бази облікових записів користувачів мережі «STAR WAY», спрощуючи адміністрування та підвищуючи безпеку доступу.

2. Сервер додатків, моніторингу та резервного копіювання (S_2):

– операційна система: Ubuntu Server 22.04 LTS (для забезпечення однорідності серверного середовища та зручності адміністрування).

– веб-сервер Nginx — це високопродуктивний сервер, обраний для стабільної роботи внутрішнього корпоративного веб-порталу компанії.

– проксі-сервер Squid контролює і фільтрує вихідний веб-трафік, блокує небажаний контент і кешує веб-сторінки для економії смуги пропускання.

– резервне копіювання (rsync + cron): Надійна утиліта синхронізації даних у поєднанні з планувальником завдань забезпечує щоденне автоматичне створення резервних копій контенту, баз даних та конфігурацій серверів на ізольований масив.

– система моніторингу Zabbix забезпечує збір метрик і моніторинг 31 вузла IT-інфраструктури (23 робочі станції, комутатори SW_1–SW_3, точки доступу, шлюз pfSense та сервери S_1, S_2) в реальному часі з миттєвими сповіщеннями про інциденти.

2.5.2 Робочі місця співробітників

Розподіл операційних систем на робочих станціях:

1. Windows 11 Pro (усього 16 ПК):

– WS_1 – WS_8, WS_22 – WS_23 (10 ПК) — Робочі місця керівництва, HR-фахівців, аналітиків та бухгалтерів. Вибір зумовлений потребою у повній сумісності зі спеціалізованим бухгалтерським та фінансовим ПЗ, а також корпоративними сервісами Microsoft.

– WS_16 – WS_18 (3 ПК) — Відділ продажів та роботи з клієнтами. Необхідна для стабільної інтеграції з настільними версіями CRM-систем та IP-телефонії.

– WS_19 – WS_21 (3 ПК) — Графічні дизайнери. Обрана через максимальну продуктивність та нативну підтримку професійних графічних пакетів.

2. Ubuntu Desktop 22.04 LTS (усього 7 ПК):

– WS_9 – WS_12 (4 ПК) — SMM-команда.

– WS_13 – WS_15 (3 ПК) — Контент-мейкери.

Уніфікований пакет прикладного програмного забезпечення: Для забезпечення щоденної діяльності маркетингової компанії на робочих станціях розгорнуто такі програмні продукти:

1. Офісні технології: Microsoft Office 365 (для користувачів Windows — адміністрація, бухгалтерія) та LibreOffice (безкоштовний аналог для користувачів Ubuntu) — робота з текстами, бюджетами, таблицями та презентаціями.

2. Робота в Інтернеті: Google Chrome та Mozilla Firefox — базові швидкі веб-браузери для взаємодії з хмарними маркетинговими інструментами, кабінетами реклами та соціальнимимережами.

3. Професійний графічний пакет (для WS_19–WS_21 та WS_13–WS_15): Adobe Creative Cloud (Photoshop, Illustrator, Premiere Pro) — створення растрової/векторної графіки та відеомонтаж рекламних креативів.

4. UI/UX та прототипування: Figma Desktop — розробка візуальних інтерфейсів та інтерактивних макетів рекламних кампаній.

5. Робота з документами: Adobe Acrobat Reader — перегляд, рецензування та погодження офіційних документів та договорів у форматі PDF.

6. Мультимедіа: VLC Media Player — універсальний кросплатформний програвач для швидкої перевірки та відтворення готових медіафайлів контент-мейкерами.

7. Корпоративна комунікація: Slack та Microsoft Teams — інструменти для миттєвого обміну повідомленнями, координації проєктів між підрозділами та проведення онлайн-нарад.

8. Інформаційна безпека: Windows Defender (вбудований захист для Windows 11) та централізоване рішення Bitdefender GravityZone — антивірусний захист робочих станцій від шкідливого ПЗ, фішингу та мережевих загроз.

Вибраний комплекс операційних систем та прикладного програмного забезпечення гарантує високу безпеку корпоративних даних, безперебійну взаємодію між серверами та клієнтами, а також створює ефективне цифрове середовище для успішної діяльності маркетингової компанії «STAR WAY».

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкція з конфігурування активного комутаційного обладнання мережі

Ключовим аспектом налаштування мережевого обладнання є поділ на віртуальні локальні мережі (VLAN), що підвищує безпеку, оптимізує трафік і раціонально використовує ресурси компанії «STAR WAY». Основні принципи проєктування включають ізоляцію критично важливих сегментів, вдосконалення контролю доступу та гнучку масштабованість системи.

Розподіл на підмережі (VLAN) уможливлює:

– підвищення безпеки: обмеження доступу до ключових частин мережі та суттєве зниження ризиків внутрішніх загроз;

– спрощення керування: логічний розподіл різних функціональних підрозділів компанії на окремі ізольовані підмережі;

– масштабованість: зручне доповнення мережі новими підрозділами або пристроями без порушення вже створеної логічної структури;

– оптимізацію продуктивності: скорочення обсягу широкомовного трафіку (broadcast) та прискорення обміну даними між вузлами.

Під час розподілу спроєктованої мережі на підмережі враховано такі базові принципи:

– функціональна ізоляція: кожен підрозділ або група співробітників зі схожими посадовими обов'язками та вимогами до ПЗ отримують власну окрему підмережу;

– ізоляція критично важливих ресурсів: корпоративні сервери (S_1, S_2) та їхні сервіси винесені у спеціалізовану демілітаризовану підмережу VLAN 200 з обмеженим рівнем доступу;

– планування зростання: проєктування діапазонів IP-адрес виконано з урахуванням перспективного розширення штату компанії «STAR WAY».

Дані про заплановані підмережі в таблиці 3.1.

Таблиця 3.1 – Підмережі запланованої мережі компанії «STAR WAY»

Підрозділ	Підмережа	ID VLAN	Функціональне призначення
Керівництво	192.168.10.0/24	10	Загальне оперативне управління компанією
HR-менеджер	192.168.20.0/24	20	Управління кадрами та підбір персоналу
Бухгалтерія	192.168.30.0/24	30	Фінансовий облік, звітність, банкінг
Проектний менеджер	192.168.40.0/24	40	Координація проєктів, комунікація з клієнтами
Системний адміністратор	192.168.50.0/24	50	Керування та підтримка IT-інфраструктури
SMM-команда	192.168.60.0/24	60	Просування та управління соціальними мережами
Контент-мейкери	192.168.70.0/24	70	Генерація контенту, обробка медіафайлів
Відділ продажів	192.168.80.0/24	80	Залучення клієнтів, обробка замовлень у CRM
Дизайнери	192.168.90.0/24	90	Розробка візуальних матеріалів та макетів
Спільна робоча зона	192.168.100.0/24	100	Робочі місця загального простору (Open Space)
Гостьова мережа Wi-Fi	192.168.110.0/24	110	Ізольований доступ до Інтернету для відвідувачів
Серверна підмережа	192.168.200.0/24	200	Розміщення серверів S_1, S_2 та їх сервісів

Розподіл IP-адрес виконано із застосуванням приватних діапазонів згідно зі стандартом RFC 1918. Реалізація сегментації здійснюється на фізичних комутаторах мережі. Маршрутизація між створеними VLAN реалізується на комутаторі рівня L3 (ядро мережі — SW_1 : Cisco Catalyst WS-C2960X-24TS-L) за допомогою технології SVI. На завершальному етапі на SW_1 налаштовуються списки контролю доступу (ACL) для захисту серверної підмережі VLAN 200.

3.2 Налаштування комутаторів рівня доступу SW_2 та SW_3 (D-Link DGS-1210-28P)

Комутатори рівня доступу SW_2 та SW_3 відносяться до лінійки D-Link Smart Managed. Їх конфігурування може виконуватися як через інтуїтивний веб-інтерфейс, так і за допомогою інтерфейсу командного рядка (CLI) через порт Console або зашифрований протокол SSH.

Нижче наведено CLI-команди для створення та розподілу VLAN на портах комутаторів (Uplink-портом до ядра мережі визначено гігабітний SFP-порт 25):

1) Конфігурування комутатора SW_2 (обслуговує робочі місця WS_1–WS_12):

```
# [Джерело синтаксису: D-Link DGS-1210 Series CLI Reference Guide / Section: VLAN Commands]
# [URL: https://www.dlink.com/uk/uk/support/support-resources]
# Створення віртуальних локальних мереж та присвоєння їм імен
create vlan vlanid 10
config vlan vlanid 10 name MANAGEMENT
create vlan vlanid 20
config vlan vlanid 20 name HR
create vlan vlanid 30
config vlan vlanid 30 name ACCOUNTING
create vlan vlanid 40
```

config vlan vlanid 40 name PM

create vlan vlanid 50

config vlan vlanid 50 name ADMIN

create vlan vlanid 60

config vlan vlanid 60 name SMM

create vlan vlanid 110

config vlan vlanid 110 name GUEST

create vlan vlanid 200

config vlan vlanid 200 name SERVERS

[Джерело синтаксису: D-Link CLI Reference / Port-Based VLAN Configuration, 802.1Q]

Розподіл клієнтських портів доступу (Untagged)

config vlan vlanid 10 add untagged 1-3

config vlan vlanid 20 add untagged 4-5

config vlan vlanid 30 add untagged 6

config vlan vlanid 40 add untagged 7

config vlan vlanid 50 add untagged 8

config vlan vlanid 60 add untagged 9-12

Налаштування магістрального порту (Trunk) до головного комутатора SW_1 (Tagged)

config vlan vlanid 10,20,30,40,50,60,110,200 add tagged 25

save

2) Конфігурування комутатора SW_3 (обслуговує WS_13–WS_23 та точки доступу AP_1, AP_2):

Створення віртуальних локальних мереж та присвоєння їм імен

create vlan vlanid 70

config vlan vlanid 70 name CONTENT

create vlan vlanid 80

[Джерело синтаксису: D-Link DGS-1210 Series CLI Reference Guide / Section: VLAN Commands]

```
# [URL: https://www.dlink.com/uk/uk/support/support-resources]
# Створення віртуальних локальних мереж для другого сегмента офісу
config vlan vlanid 80 name SALES
create vlan vlanid 90
config vlan vlanid 90 name DESIGN
create vlan vlanid 100
config vlan vlanid 100 name COMMON
create vlan vlanid 110
config vlan vlanid 110 name GUEST
create vlan vlanid 200
config vlan vlanid 200 name SERVERS
# [Джерело синтаксису: D-Link CLI Reference / Port-Based VLAN Configuration]
# Розподіл клієнтських портів доступу (Untagged)
config vlan vlanid 70 add untagged 1-3
config vlan vlanid 80 add untagged 4-6
config vlan vlanid 90 add untagged 7-9
config vlan vlanid 100 add untagged 10-11
config vlan vlanid 110 add untagged 12-13
# Налаштування магістрального порту (Trunk) до головного комутатора SW_1 (Tagged)
config vlan vlanid 70,80,90,100,110,200 add tagged 25
save
```

3.3 Налаштування головного комутатора ядра мережі SW_1 (Cisco Catalyst WS-C2960X-24TS-L)

Підключення до комутатора ядра здійснюється через консольний кабель або за допомогою захищеного протоколу SSH. Конфігурування виконується в операційному середовищі Cisco IOS.

[Джерело синтаксису: Cisco Catalyst 2960-X Switch CLI Configuration Guide, Section: VLANs]

[URL: https://www.cisco.com/c/en/us/support/switches/catalyst-2960-x-series-switches/series-doc-list.html]

1) Створення бази даних VLAN та призначення ідентифікаторів:

```
enable
configure terminal
vlan 10
 name MANAGEMENT
exit
vlan 20
 name HR
exit
vlan 30
 name ACCOUNTING
exit
vlan 40
 name PM
exit
vlan 50
name ADMIN
exit
vlan 60
 name SMM
exit
vlan 70
 name CONTENT
exit
vlan 80
 name SALES
```

```
exit
vlan 90
 name DESIGN
exit
vlan 100
 name COMMON
exit
vlan 110
 name GUEST
exit
vlan 200
 name SERVERS
exit
```

[Джерело синтаксису: Cisco IOS Interface and Hardware Component Configuration Guide]

2) Підключення серверів S_1 та S_2 до портів доступу (Access) у VLAN 200:

```
interface GigabitEthernet1/0/1
 description Connection_to_Server_S1
 switchport mode access
 switchport access vlan 200
 no shutdown
exit
interface GigabitEthernet1/0/2
 description Connection_to_Server_S2
 switchport mode access
 switchport access vlan 200
 no shutdown
exit
```

[Джерело синтаксису: Cisco IOS LAN Switching Command Reference / Trunking Commands]

3) Конфігурування магістральних інтерфейсів (Trunk) для зв'язку з SW_2 та SW_3:

```
interface GigabitEthernet1/0/3
 description Trunk_to_SW2_D-Link
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60,110,200
 no shutdown
exit
interface GigabitEthernet1/0/4
 description Trunk_to_SW3_D-Link
 switchport mode trunk
 switchport trunk allowed vlan 70,80,90,100,110,200
 no shutdown
exit
```

[Джерело синтаксису: Cisco IOS IP Routing: Cisco Express Forwarding Configuration Guide]

4) Створення віртуальних інтерфейсів комутатора (SVI) для між-VLAN маршрутизації:

```
interface vlan 10
 ip address 192.168.10.1 255.255.255.0
 no shutdown
exit
interface vlan 20
 ip address 192.168.20.1 255.255.255.0
 no shutdown
exit
interface vlan 30
 ip address 192.168.30.1 255.255.255.0
 no shutdown
exit
```

```
interface vlan 40
 ip address 192.168.40.1 255.255.255.0
 no shutdown
exit
interface vlan 50
 ip address 192.168.50.1 255.255.255.0
 no shutdown
exit
interface vlan 60
 ip address 192.168.60.1 255.255.255.0
 no shutdown
exit
interface vlan 70
 ip address 192.168.70.1 255.255.255.0
 no shutdown
exit
interface vlan 80
 ip address 192.168.80.1 255.255.255.0
 no shutdown
exit
interface vlan 90
 ip address 192.168.90.1 255.255.255.0
 no shutdown
exit
interface vlan 100
 ip address 192.168.100.1 255.255.255.0
 no shutdown
exit
interface vlan 110
 ip address 192.168.110.1 255.255.255.0
```

```
 no shutdown
exit
interface vlan 200
 ip address 192.168.200.1 255.255.255.0
 no shutdown
exit
```

[Джерело синтаксису: Cisco IOS IP Command Reference / Global Routing Activation]

5) Активація глобальної функції IP-маршрутизації та збереження поточної конфігурації:

```
ip routing
end
write memory
```

Після успішної реалізації зазначених етапів у локальній мережі маркетингової компанії «STAR WAY» буде впроваджено логічний поділ інфраструктури на 12 незалежних підмереж (VLAN 10–110 та VLAN 200) із забезпеченням швидкісної маршрутизації пакетів між ними за допомогою SVI-інтерфейсів головного комутатора ядра SW_1.

Це створює надійний фундамент для ефективного керування корпоративним трафіком, суттєво підвищує загальний рівень інформаційної безпеки завдяки надійній ізоляції чутливих серверних ресурсів та гостьового сегменту, а також забезпечує відмінний потенціал масштабованості мережі для майбутнього розвитку підприємства.

3.4 Інструкція з налаштування доступу до мережі та захисту периметра

Підключення до провайдера послуг Інтернет в мережі маркетингової компанії «STAR WAY» реалізовано за допомогою транзиту зовнішньої лінії зв'язку через комутатор ядра SW_1 до виділеного програмного шлюзу безпеки на базі сервера S_2 (Ubuntu Server 22.04 LTS).

Оскільки комутатори рівня L3 серії Cisco Catalyst 2960-X виконують внутрішню маршрутизацію, але не мають апаратної підтримки динамічної трансляції адрес (NAT), роль межового маршрутизатора та міжмережевого екрана (Firewall) покладено на сервер S_2 із використанням підсистеми Netfilter/iptables. Сервер S_2 оснащений двома фізичними мережевими інтерфейсами: eth0 (зовнішній інтерфейс, спрямований до провайдера) та eth1 (внутрішній інтерфейс, підключений до серверного сегмента локальної мережі).

Крок 1. Конфігурування транзитного VLAN та маршруту за замовчуванням на SW_1

Для безпечного прокидання лінії провайдера до сервера шлюзу, на комутаторі SW_1 створюється ізольований VLAN 999. Порт Gi1/0/23 виділяється під кабель провайдера, а порт Gi1/0/24 з'єднується з інтерфейсом eth0 сервера S_2. Також на комутаторі вказується статичний маршрут, який перенаправляє весь зовнішній трафік компанії на внутрішню адресу сервера шлюзу.

[Джерело синтаксису: Cisco IOS IP Routing: Static Routing Command Reference]

```
enable
configure terminal
# Створення ізольованого VLAN для лінії провайдера
vlan 999
 name ISP_TRANZIT
exit
# Налаштування порту для підключення лінії ISP
interface GigabitEthernet1/0/23
 description Connection_to_ISP_Line
 switchport mode access
 switchport access vlan 999
 no shutdown
exit
# Встановлення шлюзу за замовчуванням для локальної мережі
```

ip route 0.0.0.0 0.0.0.0 192.168.200.3

end

write memory

Крок 2. Підключення до сервера S_2 та первинна перевірка

Управління сервером шлюзу здійснюється віддалено за допомогою захищеного протоколу SSH з робочого місця системного адміністратора. Після автентифікації виконується перевірка поточного стану таблиць правил міжмережевого екрана:

[Джерело синтаксису: OpenSSH Client / Linux Reference manual Page for ssh(1)]

Підключення до сервера S_2 за його внутрішньою IP-адресою

ssh admin@192.168.200.3

[Джерело синтаксису: Ubuntu Man Pages: iptables - administration tool for IPv4 packet filtering]

[URL: https://manpages.ubuntu.com/manpages/jammy/man8/iptables.8.html]

Перевірка поточного стану та активних правил iptables

sudo iptables -L -n -v

Крок 3. Налаштування трансляції мережевих адрес (NAT) на сервері S_2

Для забезпечення доступу комп'ютерів із приватними IP-адресами до глобальної мережі необхідно активувати функцію пересилання IPv4-пакетів на рівні ядра операційної системи та налаштувати маскування трафіку (Masquerading) на зовнішньому інтерфейсі eth0:

[Джерело синтаксису: Linux Kernel Documentation / sysctl.conf parameters]

[URL: https://www.kernel.org/doc/Documentation/sysctl/net.txt]

Активація маршрутизації пакетів у конфігураційному файлі ядра

sudo nano /etc/sysctl.conf

У відкритому файлі необхідно знайти та розкоментувати (або додати) рядок:

net.ipv4.ip_forward=1

Зберегти файл (Ctrl+O, Enter, Ctrl+X) та застосувати зміни в реальному часі:

sudo sysctl -p

[Джерело синтаксису: Netfilter/iptables Target Extensions Manual: MASQUERADE]

Налаштування динамічного маскування (NAT) для вихідного трафіку через eth0

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

Дозвіл форвардингу встановлених та пов'язаних сесій з Інтернету у локальну мережу

sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT

sudo iptables -A FORWARD -i eth0 -i eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT

Крок 4. Конфігурування правил розмежування доступу між підмережами

Для забезпечення інформаційної безпеки та ізоляції внутрішніх ресурсів на сервері S_2 формується політика фільтрації форвардного трафіку. Корпоративним підмережам надається повний доступ до Інтернету, тоді як для гостьового сегмента впроваджуються суворі обмеження:

[Джерело синтаксису: Linux Netfilter Core Architecture / iptables FORWARD rules ruleset]

[Документація: https://netfilter.org/documentation/index.html]

Дозвіл виходу в Інтернет для штатних підрозділів компанії «STAR WAY»

sudo iptables -A FORWARD -s 192.168.10.0/24 -j ACCEPT # Керівництво

sudo iptables -A FORWARD -s 192.168.20.0/24 -j ACCEPT # HR

sudo iptables -A FORWARD -s 192.168.30.0/24 -j ACCEPT # Бухгалтерія

sudo iptables -A FORWARD -s 192.168.40.0/24 -j ACCEPT # PM

sudo iptables -A FORWARD -s 192.168.50.0/24 -j ACCEPT # IT-Адмін

sudo iptables -A FORWARD -s 192.168.60.0/24 -j ACCEPT # SMM

sudo iptables -A FORWARD -s 192.168.70.0/24 -j ACCEPT # Контент

sudo iptables -A FORWARD -s 192.168.80.0/24 -j ACCEPT # Продажі

```
sudo iptables -A FORWARD -s 192.168.90.0/24 -j ACCEPT   # Дизайнери
sudo iptables -A FORWARD -s 192.168.100.0/24 -j ACCEPT  # Open Space
# Обмеження для гостьової бездротової мережі (VLAN 110)
# [Джерело синтаксису: Packet Filtering Implementation Guide / Network Isolation rules]
# Блокування спроб доступу з гостьової мережі до будь-яких внутрішніх корпоративних підмереж класу private
sudo iptables -A FORWARD -s 192.168.110.0/24 -d 192.168.0.0/16 -j DROP
# Дозвіл гостьового трафіку виключно у напрямку глобальної мережі Інтернет
sudo iptables -A FORWARD -s 192.168.110.0/24 -j ACCEPT
# Додатковий захист серверного сегмента (VLAN 200) від несанкціонованого доступу
sudo iptables -A FORWARD -s 192.168.50.0/24 -d 192.168.200.0/24 -j ACCEPT
sudo iptables -A FORWARD -d 192.168.200.0/24 -j DROP
```

Крок 5. Забезпечення персистентності (збереження) правил брандмауера

За замовчуванням правила iptables видаляються з оперативної пам'яті після перезавантаження ОС. Для їх автоматичного відновлення під час старту сервера встановлюється та налаштовується спеціалізована утиліта автоматичного збереження:

```
# [Джерело синтаксису: Ubuntu Deployment Guide / Package Management: apt-get]
# Встановлення пакету автоматичного завантаження конфігурації netfilter
sudo apt update
sudo apt install iptables-persistent -y
# [Джерело синтаксису: Debian/Ubuntu netfilter-persistent Service Manual]
# Збереження поточного набору правил у постійну пам'ять сервера
sudo netfilter-persistent save
```

Крок 6. Фінальне тестування та верифікація захисту

Після завершення монтажу та програмного налаштування проводиться діагностика працездатності каналів зв'язку з кінцевих робочих станцій:

1. Перевірка доступу до Інтернету з робочої станції користувача (наприклад, WS_1 у VLAN 10):

[Джерело синтаксису: IETF RFC 792 (Internet Control Message Protocol) / Linux ping(8) Manual]

ping 8.8.8.8

ping google.com

Очікуваний результат: успішний обмін ICMP-пакетами (Інтернет працює).

2. Діагностика ізоляції гостьової бездротової мережі (VLAN 110):

ping 192.168.10.1 <-- Спроба доступу до шлюзу керівництва (Результат: Трафік заблоковано / Request timed out)

ping 8.8.8.8 <-- Спроба доступу до зовнішнього DNS (Результат: Успішно / Reply received)

Крок 7. Резервне копіювання конфігураційного файлу комутатора SW_1

Для забезпечення швидкого відновлення працездатності ядра мережі у разі аварійних ситуацій, фінальна працездатна конфігурація комутатора SW_1 зберігається в енергонезалежну пам'ять та експортується на TFTP-сервер, розгорнутий на базі сервера S_2:

[Джерело синтаксису: Cisco IOS Configuration Fundamentals Configuration Guide / TFTP File Transfer]

[Ресурс: https://tools.ietf.org/html/rfc1350 - The TFTP Protocol]

Виконується на комутаторі SW_1

end

write memory

Експорт файлу конфігурації на внутрішній сервер сховища

copy running-config tftp://192.168.200.3/SW1-backup.cfg

Завдяки впровадженню описаного комплексу заходів, локальна інфраструктура компанії «STAR WAY» отримала надійний та швидкісний вихід до глобальної мережі з чітким розмежуванням прав доступу. Надійна ізоляція гостьового сегмента Wi-Fi та обмеження доступу до серверної підмережі мінімізують ризики кібератак, забезпечуючи стабільну роботу всього підприємства.

3.5 Інструкція для тестування та моніторингу роботи мережі

Для забезпечення безперебійного функціонування, оперативного виявлення несправностей та проактивного моніторингу спроєктованої мережі компанії «STAR WAY» впроваджено комплекс програмно-апаратних засобів тестування та аналізу трафіку.

Основним інструментом централізованого моніторингу обрано платформу Zabbix 6.0 LTS, яку розгорнуто на базі сервера S_2 під управлінням операційної системи Ubuntu Server 22.04 LTS (IP-адреса: 192.168.200.3).

3.5.1. Налаштування моніторингу за протоколом SNMP

Збір метрик (статус портів, завантаження процесора, обсяг трафіку) з активного мережевого обладнання здійснюється за допомогою протоколу SNMP версії 2c (Simple Network Management Protocol).

1) Налаштування SNMP на комутаторі ядра SW_1 (Cisco Catalyst):

[Джерело синтаксису: Cisco Systems, Inc. (2022). Catalyst 2960-X Switch Software Configuration Guide: Configuring SNMP].

enable

configure terminal

Створення спільноти (community) для читання з назвою public

snmp-server community public RO

Вказівка адреси сервера моніторингу Zabbix для відправки Trap-повідомлень

snmp-server host 192.168.200.3 version 2c public

end

write memory

2) Налаштування SNMP на комутаторах доступу SW_2 та SW_3 (D-Link DGS-1210-28P):

[Джерело синтаксису: D-Link Corporation. (2021). DGS-1210-28P Web Smart Switch CLI Reference Guide: SNMP Commands].

enable

config snmp system_status enable

create snmp community public read_only

create snmp host 192.168.200.3 v2c public

save

Після налаштування CLI-інтерфейсів у веб-панелі управління Zabbix додаються відповідні вузли мережі (SW_1, SW_2, SW_3, а також сервери S_1 та S_2). Для кожного пристрою прописується його системна IP-адреса та прив'язуються офіційні сертифіковані шаблони моніторингу: «Cisco IOS за SNMP» та «D-Link за SNMP».

3.5.2 Перевірка базової зв'язності та маршрутизації (Ping & Traceroute)

Для первинної діагностики доступності вузлів та шлюзів у різних VLAN використовуються утиліти ping (перевірка зв'язку за протоколом ICMP) та traceroute (відстеження маршруту проходження пакетів).

Приклади тестових команд для верифікації зв'язності:

– перевірка доступності локального шлюзу з робочих станцій VLAN 10 (Керівництво):

ping 192.168.10.1

– перевірка доступності шлюзу з робочих станцій VLAN 60 (SMM-команда):

ping 192.168.60.1

– перевірка зв'язку сервера S_1 (VLAN 200) зі своїм шлюзом маршрутизації:

ping 192.168.200.1

– перевірка працездатності зовнішнього каналу зв'язку та виходу в Інтернет:

ping 8.8.8.8

Перевірка шляху проходження пакетів між ізольованими підмережами: Для аналізу ланцюжка маршрутизації між різними сегментами (наприклад, з робочого місця VLAN 10 до дизайнерів у VLAN 90) або до зовнішніх ресурсів використовуються команди:

traceroute 192.168.90.1

traceroute google.com

3.5.3 Моніторинг поточного стану пристроїв через CLI

Для швидкого локального аналізу стану інтерфейсів, таблиць комутації та маршрутів безпосередньо з консолі адміністратора використовуються спеціалізовані діагностичні команди.

На комутаторі ядра SW_1 (Cisco IOS):

[Джерело синтаксису: Cisco Systems. Cisco IOS Configuration Fundamentals Command Reference].

– show interfaces trunk — перегляд стану та дозволених VLAN на магістральних портах;

– show vlan brief — перевірка списку створених віртуальних мереж та прив'язаних до них портів;

– show ip route — аналіз таблиці маршрутизації комутатора L3;

– show mac address-table — перегляд таблиці відповідності MAC-адрес фізичним портам комутатора.

– На комутаторах доступу SW_2 / SW_3 (D-Link CLI):

– show vlan — вивід інформації про конфігурацію VLAN та теговані/нетеговані порти;

– show fdb — перегляд таблиці комутації MAC-адрес (Forwarding Database);

– show ports switching — перевірка поточної швидкості, дуплексу та активності фізичних ліній.

3.5.4 Глибокий аналіз трафіку засобами Wireshark та Port Mirroring (SPAN)

– У разі виявлення мережевих аномалій, шкідливого трафіку або для детального розбору мережевих пакетів застосовується аналізатор Wireshark.

– Він встановлюється на робочу станцію системного адміністратора WS_8, яка підключена до порту 8 комутатора доступу SW_2 (VLAN 50).

– Щоб перехоплювати трафік з інших портів, на комутаторі налаштовується функція дзеркалювання портів (на Cisco — SPAN, на D-Link — Port Mirroring). Вона дублює пакети з досліджуваного порту (наприклад, порт 1, куди підключено важливий магістральний лінк) на порт адміністратора.

– Налаштування дзеркалювання на комутаторі доступу SW_2 (D-Link DGS-1210-28P):

[Джерело синтаксису: Wireshark Foundation. (2024). Wireshark User's Guide: Packet Capturing and Ports].

Копіювання вхідного та вихідного трафіку з порту 1 на порт 8 (де підключено WS_8)

config mirror ports 1 source both target 8

Аналогічне налаштування SPAN на комутаторі ядра SW_1 (у разі діагностики на Cisco):

monitor session 1 source interface GigabitEthernet1/0/1 both

monitor session 1 destination interface GigabitEthernet1/0/8

3.5.5 Тестування максимальної пропускної здатності

Для вимірювання реальної швидкості передачі даних та виявлення можливих затримок чи втрат пакетів під навантаженням використовується кросплатформова утиліта iperf3. Тестування проводиться між корпоративним сервером S_1 та клієнтськими комп'ютерами.

[Джерело синтаксису: iPerf3 Development Team. (2024). iPerf3 User Documentation and CLI Command Tools].

1. Запуск програми в режимі сервера на стороні S_1 (192.168.200.2):

iperf3 -s

2. Запуск тесту в режимі клієнта на будь-якій робочій станції користувача (тривалість тесту — 10 секунд):

iperf3 -c 192.168.200.2 -t 10

Очікуваний технічний результат: для гігабітних ліній зв'язку (Gigabit Ethernet) реальна корисна швидкість передачі даних у межах однієї VLAN має становити не менше 900–940 Мбіт/с.

3.5.6 Сканування та аудит мережі за допомогою Nmap

Для проведення регулярного аудиту безпеки, інвентаризації активного обладнання та перевірки відсутності сторонніх пристроїв у мережі, з робочої станції адміністратора WS_8 виконується швидке ping-сканування підмереж за допомогою утиліти Nmap:

[Джерело синтаксису: Lyon, G. (2025). Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery].

Сканування підмережі Керівництва (VLAN 10) на наявність активних хостів

nmap -sn 192.168.10.0/24

Аудит серверної підмережі (VLAN 200)

nmap -sn 192.168.200.0/24

3.5.7 Регулярний автоматизований моніторинг

Стабільна робота інфраструктури компанії «STAR WAY» забезпечується цілодобовим автоматичним збором даних системою Zabbix. Окрім моніторингу доступності пристроїв (через icmp-ping), налаштовано тригери (сповіщення) на такі критичні події:

[Джерело синтаксису: Zabbix LLC. (2023). Zabbix 6.0 Long Term Support Manual: Triggers and Alerts].

– зміна статусу фізичного порту комутатора (Port Down);

– перевищення порогу завантаження процесора (CPU usage > 80%) на серверах S_1 або S_2;

– вичерпання вільного місця на дискових накопичувачах серверів;

– поява помилок (CRC errors) на інтерфейсах комутаторів.

У разі спрацювання будь-якого з тригерів, система Zabbix миттєво генерує сповіщення та надсилає його на робоче місце системного адміністратора (WS_8), що дозволяє локалізувати та усунути проблему ще до того, як вона вплине на бізнес-процеси маркетингової компанії.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Основна мета економічного розділу дипломного проєкту — оцінка доцільності створення комп'ютерної мережі для компанії «STAR WAY», включаючи аналіз витрат, собівартості НДР та розрахунок економічної ефективності й терміну окупності капітальних вкладень.

Щоб визначити повну вартість розробки та розгортання мережі, технологічний процес поділено на такі ключові етапи [6]:

– визначення стадій технологічного процесу та оцінка тривалості робіт;

– розрахунок витрат на оплату праці основного та допоміжного персоналу з урахуванням соціальних відрахувань;

– обчислення прямих матеріальних витрат на обладнання та комплектуючі;

– розрахунок витрат на електроенергію для науково-виробничих потреб;

– визначення транспортних та накладних витрат;

– обчислення амортизаційних відрахувань за час використання обладнання;

– складання підсумкового кошторису, визначення собівартості та кінцевої ціни НДР;

– оцінка економічної ефективності, чистої теперішньої вартості (NPV) та терміну окупності проєкту.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Для визначення загальної тривалості виконання робіт із проєктування та впровадження мережі, усі операції технологічного процесу було систематизовано із зазначенням відповідних виконавців (керівник проєкту, лаборант, технік).

Дані про часові витрати на кожну стадію узагальнено в таблиці 4.1.

Таблиця 4.1 – Середня тривалість виконання етапів технологічного процесу НДР

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання, год.
1.	Підготовчий етап (збір вихідних даних, аналіз вимог)	Керівник проєкту	8
2	Проєктування логічної та фізичної структури мережі	Керівник проєкту	26
3	Монтаж кабельних трас, кабель-каналів та розеток	Лаборант	6
4	Конфігурування активного комутаційного обладнання	Технік	6
5	Інсталяція операційних систем та налаштування серверів	Технік	7
6	Комплексне тестування мережі, верифікація захисту	Технік	3
Всього		–	56

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Згідно із Законом України «Про оплату праці» [2], заробітна плата є винагородою у грошовій формі, яку роботодавець виплачує працівникові за виконану ним роботу. Рівень оплати праці визначається складністю та умовами виконуваної роботи, а також професійними навичками виконавців.

Основна заробітна плата ($З_{осн}$)обчислюється на основі погодинних тарифних ставок за формулою 4.1:

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

де $Т_с$ — годинна тарифна ставка працівника відповідної кваліфікації, грн/год;

$К_г$ — кількість відпрацьованих годин згідно з табелем робочого часу (таблиця 4.1).

З урахуванням залученого персоналу загальна суму основної заробітної плати становить:

$$З_{осн} = (120 \cdot 34) + (65 \cdot 6) + (85 \cdot 16) = 4080 + 390 + 1360 = 5830{,}00 \text{ грн.}$$

Розмір додаткової заробітної плати ($З_{дод}$)враховує додаткові виплати, премії та компенсації і приймається в розмірі 15% від основної заробітної плати за формулою 4.2:

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

де $К_{допл}$— коефіцієнт додаткової оплати праці $К_{допл} = 0{,}15$.

$$З_{дод} = 5830{,}00 \cdot 0{,}15 = 874{,}50 \text{ грн.}$$

Загальний фонд оплати праці ($В_{о.п.}$)складається з основної та додаткової заробітної плати за формулою 4.3:

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

$$В_{о.п.} = 5830{,}00 + 874{,}50 = 6704{,}50 \text{ грн.}$$

Відповідно до чинного законодавства України, на фонд оплати праці нараховується єдиний соціальний внесок (ЄСВ) у розмірі 22% [3]. Загальний обсяг відрахувань на соціальні заходи $В_{с.з.}$ обчислюється за формулою 4.4:

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

$$В_{с.з.} = 6704{,}50 \cdot 0{,}22 = 1474{,}99 \text{ грн.}$$

Результати розрахунків витрат на оплату праці та нарахувань на ЄСВ для всіх категорій робітників узагальнено в таблиці 4.2.

Таблиця 4.2 – Узагальнені розрахунки витрат на заробітну плату персоналу

Категорія працівників	Тарифна ставка, грн/год	К-сть відпрацьов. год	Основна з/п, грн	Додаткова з/п, грн	Нарахування на ФОП (ЄСВ 22%), грн	Всього витрати на оплату праці, грн
1	2	3	4	5	6	7

Продвження аблиці 4.2

1	2	3	4	5	6	7
Керівник проєкту	120,00	34	4080,00	612,00	–	–
Лаборант	65,00	6	390,00	58,50	–	–
Технік	85,00	16	1360,00	204,00	–	–
Разом	–	–	5830,00	874,50	1474,99	8179,49

4.3 Обчислення прямих витрат на матеріали та обладнання

Матеріальні витрати включають у себе вартість активного й пасивного мережевого обладнання, кабельної продукції та витратних матеріалів, необхідних для монтажу локальної інфраструктури компанії «STAR WAY».

Матеріальні витрати для кожного типу ресурсів (МВі)обчислюються як за формулою 4.5:

$$МВ_i = qi \cdot p_i \quad (4.5)$$

де q_i — кількість використаного матеріалу або обладнання і-го виду;

p_i — ціна за одиницю товару, грн.

Загальна сума матеріальних витрат ($З_{м.в.}$)визначається підсумовуванням усіх позицій специфікації за формулою 4.6:

$$З_{м.в.} = \sum МВ_i \quad (4.6)$$

Деталізовані розрахунки вартості обладнання та матеріалів наведено в таблиці 4.3.

Таблиця 4.3 – Розрахунок витрат на матеріали та мережеве обладнання

№ п/п	Найменування матеріальних ресурсів та обладнання	Од. виміру	Кількість	Ціна 1-ці, грн.	Заг. сума витрат, грн.
1	2	3	4	5	6
1	Кабель мідний UTP Cat6 (бухта 305 м)	шт	2	4200,00	8400,00
2	Конектор RJ-45 Cat6	шт.	100	8,00	800,00

Продвження таблиці 4.3

1	2	3	4	5	6
3	Кабель-канал пластиковий DKC 40×25×2м	шт.	40	85,00	3400,00
4	Мережевий органайзер для кабелю 1U	шт.	2	350,00	700,00
5	Комутаційна шафа 19" CSV 12U 600×900	шт.	1	3200,00	3200,00
6	Патч-панель RJ-45 Cat6 на 24 порти	шт.	1	1850,00	1850,00
7	Комутаційний шнур (Патч-корд) Cat6 1м	шт.	30	85,00	2550,00
8	Комутаційний шнур (Патч-корд) Cat6 3м	шт.	27	120,00	3240,00
9	Комутатор ядра Cisco Catalyst WS-C2960X-24TS-L (SW_1)	шт.	1	18500,00	18500,00
10	Комутатор доступу D-Link DGS-1210-28P (SW_2, SW_3)	шт.	2	8200,00	16400,00
11	Бездротова точка доступу Cisco Business 140AC (AP_1, AP_2)	шт.	2	6400,00	12800,00
12	Корпоративний сервер Dell PowerEdge R350 (S_1, S_2)	шт.	2	42000,00	84000,00
13	Джерело безперебійного живлення APC Smart-UPS 1500VA	шт.	1	12500,00	12500,00
14	Розетка мережева RJ-45 Cat 6 (одинарна)	шт.	23	100,00	2 300,00
	ВСЬОГО				170 640,00

4.4 Розрахунок витрат на електроенергію

Затрати на споживання електричної енергії під час конфігурування та тестування мережевих рішень на ПЕОМ визначаються за формулою 4.7:

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

де W — споживана потужність робочої станції ПЕОМ (W = 0,5 кВт);

Т— тривалість використання комп'ютера під час виконання НДР;

S — діючий комерційний тариф за 1 кВт-год електроенергії (S = 15,94 грн).

$$З_е = 0,5 \cdot 34 \cdot 15,94 = 271,00 \text{ грн.}$$

4.5 Визначення транспортних витрат

Транспортні витрати ($Т_в$) покривають логістичні процеси доставки телекомунікаційного обладнання та пасивних компонентів на об'єкт автоматизації. Вони закладаються в розмірі 8% від загальної вартості матеріальних ресурсів за формулою 4.8:

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

$$Т_в = 170\,640,00 \cdot 0,08 = 13651,2 \text{ грн.}$$

4.6 Розрахунок амортизаційних відрахувань

Амортизація відображає процес поступового перенесення вартості основних засобів на створюваний продукт для їхнього подальшого відновлення. Амортизаційні відрахування (А) за час експлуатації однієї робочої станції розробника балансовою вартістю БВ = 36500 грн протягом Т = 34 год при річній нормі амортизації НА = 4% обчислюються так за формулою 4.9:

$$A = \frac{БВ \cdot НА \cdot Т}{100\,\% \cdot Т_{баз}} \quad (4.9)$$

де $Т_{баз}$ — річний баланс робочого часу комп'ютерного обладнання.

$$A = \frac{36500 \cdot 0,04 \cdot 34}{1500} = 331,00\,грн.$$

4.7 Розрахунок накладних витрат

Накладні витрати $Н_в$ забезпечують покриття витрат на утримання приміщень, адміністративне управління та організацію належних умов праці. Їхній обсяг становить 40% від загального фонду оплати праці основного персоналу обчилюється за формулою 4.10 [6]:

$$H_в = B_{о.п.} \cdot 0{,}40 \qquad (4.10)$$

$$H_в = 6704{,}50 \cdot 0{,}40 = 2681{,}80\ грн.$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Повна собівартість (СВ) науково-дослідної роботи з розгортання мережі обчислюється як sum-ма всіх раніше розрахованих елементів витратобчислюється за формулою 4.11 [6]:

$$СВ = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_е + Т_в + А + H_в \qquad (4.11)$$

$$СВ = 195\ 754{,}5\ грн.$$

Зведений кошторис витрат із визначенням відсоткової частки кожного елемента у загальній структурі собівартості наведено в таблиці 4.4.

Таблиця 4.4 – Підсумковий кошторис витрат на проведення НДР

Зміст елементів витрат	Сума витрат, грн	Частка у загальній сумі, %
Витрати на оплату праці ($В_{о.п.}$)	6704,50	3,43
Відрахування на соціальні заходи (ЄСВ 22%)	1474,99	0,75
Прямі матеріальні витрати ($З_{м.в.}$)	170640,00	87,34
Витрати на споживання електроенергії ($З_е$)	271,00	0,04
Транспортні витрати ($Т_в$)	13651,2	6,89
Амортизаційні відрахування (А)	331,00	0,17
Накладні витрати ($Н_в$)	2681,80	1,37
ПОВНА СОБІВАРТІСТЬ (СВ)	195 754,5	100

4.9 Розрахунок договірної ціни продукту НДР

Кінцева договірна ціна розробки (Ц) формується на базі повної собівартості, планового прибутку (виходячи з базового рівня рентабельності $Р_{рен}$ = 23%) та податку на додану вартість (ПДВ) = 20% обчислюється за формулою 4.12 [1]):

$$Ц = СВ \cdot (1 + Р_{рен}) \cdot (1 + ПДВ) \qquad (4.12)$$

$$Ц = 195\ 754{,}5 \cdot 1{,}3 \cdot 1{,}2 = 305377{,}02\ грн.$$

4.10 Визначення рентабельності та 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 розробленого продукту розраховують чисту теперішню вартість (ЧТВ) і термін окупності. ЧТВ визначається за формулою 4.13:

$$ЧТВ = -КВ + \sum \frac{Г_n}{(1+i)^t} \quad (4.13)$$

де КВ – затрати на проект, грн.;

Гпt – грошовий потік за t-ий рік, грн.;

t – відповідний рік проекту;

i – величина дисконтної ставки (0,12).

$$ЧТВ = -195\,754{,}5 + \frac{187\,522{,}52}{1+0{,}1} + \frac{187\,522{,}52}{(1+0{,}1)^2} = 129\,698{,}00 \ грн$$

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

Термін окупності визначається за формулою:

Термін окупності визначається за формулою 4.14:

$$T_{ОК} = T_{ПВ} + \frac{H_B}{Г_{пр}} \quad (4.14)$$

де ТПВ – термін окупності, років;

КВ – затрати на проект, грн.;

П – річний прибуток, грн.

$$T_{ОК} = 1 + \frac{25279{,}5}{187\,522{,}52} = 1{,}1$$

Основні техніко-економічні показники розробленого проєкту наведено в узагальнюючій таблиці 4.5.

Таблиця 4.5 – Ключові економічні показники проєкту НДР

№ п/п	Показник	Одиниця виміру	Значення
1	Собівартість НДР	грн	195 754,5
2	Плановий прибуток	грн	109622,52
3	Ціна з ПДВ	грн	305377,02
4	Чиста теперішня вартість	грн	129698,00
5	Термін окупності	рік	1,1

Висновок: Аналіз фінансово-економічних параметрів, наведених у таблиці 4.5, підтверджує високу економічну доцільність впровадження спроєктованої комп'ютерної мережі маркетингової компанії «STAR WAY». Завдяки низькому терміну окупності та позитивному значенню чистої теперішньої вартості, проєкт є високоефективним і капітально виправданим.

5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1 Організаційно-технічні заходи електробезпеки при виконанні робіт у діючих електроустановках компанії “Star way”

Проєктована корпоративна комп'ютерна мережа маркетингової компанії «Star way» містить у своєму складі комплекс активного мережевого та серверного обладнання, що працює під небезпечною для життя напругою. Технічне обслуговування, налаштування та модернізація цих систем пов'язані з ризиком ураження електричним струмом, що вимагає суворого дотримання правил електробезпеки та чіткого розподілу відповідальності між посадовими особами й безпосередніми виконавцями робіт. Усі роботи з обслуговування апаратного забезпечення у телекомунікаційних шафах повинні виконуватися підготовленим персоналом із групою з електробезпеки не нижче III, а порушення цих вимог тягне за собою дисциплінарну або адміністративну відповідальність відповідно до чинного законодавства про охорону праці [1].

Залежно від складності, процеси обслуговування обладнання поділяються на роботи за розпорядженням та роботи, що виконуються в порядку поточної експлуатації. Регулярний огляд серверів чи заміна дисків гарячої заміни проводяться в порядку поточної експлуатації, тоді як ремонт силових блоків чи обслуговування джерел безперебійного живлення потребують обов'язкового оформлення розпорядження з фіксуванням інструктажів персоналу.

Для гарантування безпеки персоналу при виконанні ремонтних робіт із повним або частковим зняттям напруги в серверних приміщеннях обов'язково реалізується наступний комплекс технічних заходів у вказаній послідовності:

– проведення необхідних відключень: Силові лінії живлення серверів та комутаторів від'єднуються від розподільчих блоків або вимикаються відповідні автоматичні вимикачі. Обов'язково ізолюються вихідні лінії ДБЖ, оскільки вони здатні генерувати напругу навіть за умови знеструмлення зовнішньої мережі.

– вивішування заборонних плакатів: На ключах керування та автоматах захисту, якими може бути помилково подано живлення на робоче місце, розміщують плакати з попередженням: «Не вмикати! Працюють люди».

– перевірка відсутності напруги: Безпосередньо на робочому місці за допомогою справного покажчика напруги або мультиметра перевіряється відсутність потенціалу між фазами та заземленим корпусом стійки.

– встановлення заземлення: Усі металеві корпуси серверних шаф та шасі обладнання інтегруються із загальним контуром захисного заземлення офісу за допомогою мідних провідників, опір яких не повинен перевищувати 4 Ом.

– огородження робочого місця: За необхідності зона проведення ремонтних робіт відокремлюється від суміжних панелей під напругою, а на захисні бар'єри вивішуються знаки «Стій! Напруга».

5.2 Санітарне нормування параметрів вібрації та шуму в приміщеннях з активним мережевим обладнанням

Тривала та безперебійна робота центрального комутаційного вузла та серверної інфраструктури маркетингової компанії «Star way» неминуче супроводжується безперервним генеруванням акустичного шуму та мікроструктурних вібрацій. Головними джерелами акустичного та вібраційного навантаження в технологічних приміщеннях проєкту є високооборотні вентилятори (кулери) систем примусового охолодження відмовостійких серверів Dell PowerEdge R350 , внутрішні вентилятори керованих комутаторів ядра Cisco Catalyst, а також компресорні та вентиляційні вузли прецизійних систем кондиціювання повітря, що підтримують заданий температурний режим.

Для офісних приміщень маркетингової компанії, де програмісти, дизайнери та копірайтери виконують роботу, що потребує значного розумового напруження, гранично допустимий еквівалентний рівень шуму суворо обмежений і не повинен перевищувати 50 дБА. Водночас безпосередньо всередині серверної кімнати, де активне обладнання функціонує в режимі двадцять чотири на сім, загальний рівень звукової потужності стійок під час продуву систем може досягати 65–70 дБА. Оскільки обслуговуючий персонал перебуває в серверній кімнаті виключно тимчасово — для моніторингу, комутації ліній або заміни компонентів — такий рівень вважається допустимим, але за умови обов'язкового застосування засобів захисту.

З метою радикальної мінімізації негативного впливу акустичних коливань та мікроструктурних вібрацій на персонал, а також для запобігання поширенню звукових хвиль у суміжні робочі кабінети офісу, у проєкті передбачено комплекс інженерно-технічних, архітектурно-планувальних та організаційних заходів.

Архітектурно-планувальні заходи захисту. Приміщення серверної кімнати конструктивно винесене на максимальну відстань від кабінетів адміністрації та робочих зон основних відділів компанії «Star way». Воно межує виключно з коридорними зонами та господарськими приміщеннями, що природним чином знижує поширення повітряного шуму в зони тривалої розумової праці. Огороджувальні стіни серверної кімнати виконані з повнотілих будівельних матеріалів із високим індексом ізоляції повітряного шуму. Вхідні двері спроєктовані у спеціальному звукоізоляційному виконанні, оснащені посиленим притвором, еластичним щільним ущільнювачем по всьому периметру та автоматичним опускним порогом-затвором для перекриття нижньої щілини.

Інженерно-технічні заходи колективного захисту. Для зниження інтенсивності відбитих звукових хвиль внутрішні поверхні стін та стеля серверної кімнати підлягають обов'язковому акустичному оздобленню. Для цього використовуються спеціальні негорючі перфоровані мінераловатні плити або стінові панелі з високим коефіцієнтом звукопоглинання. Це дозволяє значно послабити ефект реверберації (багаторазового віддзеркалення звуку від бетону) та знизити загальний рівень шуму безпосередньо в зоні обслуговування.

Для боротьби з механічними коливаннями та структурною вібрацією застосовується метод вібродемпфування та віброізоляції. Важкі підлогові телекомунікаційні шафи з серверами встановлюються не безпосередньо на жорстку основу фальшпідлоги, а на спеціальні регульовані еластичні віброопори на основі щільних гумових компонентів або поліуретанових еластомерів. Ці елементи ефективно гасять коливання від роботи внутрішніх кулерів, запобігаючи їх передачі на тримкі конструкції та перекриття будівлі. Крім того, підключення магістральних повітряних каналів систем кондиціювання до вентиляційних блоків виконується через гнучкі віброізолювальні вставки.

Організаційні заходи та засоби індивідуального захисту. Важливу роль відіграє захист часом. Усі регламентні роботи, що вимагають тривалої присутності інженера в серверній кімнаті (наприклад, перекомутація великої кількості ліній витої пари або планове технічне обслуговування серверів), чітко регламентуються інструкціями з охорони праці. Час безперервного перебування працівника в зоні підвищеного акустичного навантаження суворо обмежується кількома годинами за зміну.

Під час проведення будь-яких робіт усередині серверної за умов працюючого обладнання персонал зобов'язаний використовувати засоби індивідуального захисту органів слуху. До них належать легкі протишумні навушники або м'які внутрішньовушні вкладиші (беруші) з поліуретану, які забезпечують необхідне зниження рівня звукового тиску до безпечних і комфортних значень, повністю захищаючи слуховий апарат системного адміністратора.

5.3 Алгоритм дій персоналу компанії “Star way” при виявленні ознак горіння кабельної ізоляції

Побудова кабельної інфраструктури офісу виконується відповідно до міжнародних стандартів структурованих кабельних систем (СКС), де великі масиви кабелів типу вита пара прокладаються всередині лотків, каналів та пластикових коробів [15]. Основними факторами ризику займання ізоляції є перевантаження ліній, короткі замикання або механічні пошкодження ПВХ-оболонки кабелів.

Горіння пластикових компонентів супроводжується виділенням токсичного диму та чадного газу, що потребує чіткої організації процесу евакуації та ліквідації осередку пожежі [14].

У разі виявлення перших ознак термічного розкладання або горіння кабельної ізоляції персонал зобов'язаний діяти за наступним алгоритмом:

– активація систем оповіщення: Співробітник, який помітив небезпеку, негайно задіює ручний пожежний сповіщувач загальнобудинкової системи оповіщення та управління евакуацією [14]. Після цього дублює повідомлення за телефоном «101», вказуючи точну адресу компанії, місце загоряння та своє прізвище.

– аварійне знеструмлення: Відповідальний інженер або системний адміністратор здійснює термінове вимкнення ввідного автоматичного вимикача в силовому щиті, повністю знеструмлюючи робочі лінії, а також переводить в ізольований стан блоки ДБЖ, щоб ліквідувати ризик ураження струмом через резервне живлення ліній.

– евакуація персоналу: Усі співробітники офісу негайно залишають робочі місця згідно з планами евакуації та світловими покажчиками. За наявності сильного задимлення органи дихання захищають вологими тканинами.

– локалізація осередку горіння: Якщо пожежа перебуває на початковій стадії і лінії гарантовано знеструмлені, дозволяється застосувати первинні засоби пожежогасіння. Для гасіння кабельних каналів та електронних плат застосовуються виключно вуглекислотні вогнегасники (ОУ). Вуглекислота ефективно збиває полум'я, не проводить електричний струм і не забруднює порти комутаторів та внутрішні компоненти серверів, зберігаючи їх працездатність після очищення. Використання води чи піни суворо заборонено.

– зустріч пожежних підрозділів: Керівник або призначена особа зустрічає рятувальників, інформує про успішну евакуацію штату, вказує найкоротший шлях до місця події та підтверджує повне вимкнення електроживлення.

ВИСНОВКИ

У першому розділі пояснювальної записки до кваліфікаційної роботи визначено технічне завдання та проведено аналіз рівня комп'ютеризації підрозділів маркетингової компанії «STAR WAY». Було окреслено організаційну структуру компанії, проаналізовано потреби кожного підрозділу в доступі до мережевих ресурсів і сервісів. Крім того, сформульовано ключові технічні та функціональні вимоги до проектованої мережі з урахуванням специфіки діяльності компанії.

У другому розділі обґрунтовано та обрано топологію мережі. Прийнято рішення будувати корпоративну мережу на основі ієрархічної зіркової топології з трьома класичними рівнями: ядро, розподіл та доступ. У цьому розділі підібрано пасивне та активне комутаційне обладнання. Для середовища передачі даних обрано екранований кабель вита пара категорії 6 (UTP Cat 6), який прокладається у пластикових кабельних каналах DKC розміром 40×25 мм. Центральним вузлом мережі (ядром та рівнем розподілу) призначено керований комутатор рівня L3 Cisco Catalyst WS-C2960X-24TS-L (SW_1). Моделлю комутаторів рівня доступу обрано керовані комутатори L2 D-Link DGS-1210-28P (SW_2, SW_3). Як точки бездротового доступу використано сучасні дволінійні моделі Cisco Business 140AC (AP_1, AP_2). Серверну інфраструктуру побудовано на базі двох відмовостійких серверів Dell PowerEdge R350 під управлінням операційної системи Ubuntu Server 22.04 LTS.

У цьому ж розділі розглянуто особливості розподілу адресного простору на 12 логічних підмереж (VLAN 10–110 та VLAN 200) відповідно до організаційної структури компанії, визначено характеристики вузлів мережі (23 робочі станції, 2 сервери, 2 точки доступу) та особливості монтажу кабельної системи мережі. За результатами другого розділу розроблено детальні 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 Cisco Catalyst (створення VLAN, налаштування портів режимів Access та Trunk, міжVLAN маршрутизація через SVI-інтерфейси), інструкцію з організації безпечного доступу до мережі Інтернет та захисту периметра засобами міжмережевого екрана iptables на сервері S_2, а також детально описано методи моніторингу та тестування мережі засобами систем Zabbix, утиліт ping, traceroute, iperf3 та nmap.

У четвертому розділі обчислено вартість проєктування та введення в експлуатацію локальної мережі. Розрахункова собівартість науково-дослідної роботи (НДР) становить 195 371,96 грн, кінцева ціна реалізації проєкту з урахуванням ПДВ — 288 369,01 грн, а термін окупності капіталовкладень складає 0,71 року, що повністю підтверджує високу економічну доцільність та ефективність впровадження розробленого проєкту.

У п'ятому розділі описано актуальні питання охорони праці та техніки безпеки при роботі з обчислювальним обладнанням, проаналізовано засоби автоматичного пожежного оповіщення в офісі компанії «STAR WAY», визначено юридичну відповідальність керівника та працівників за дотримання вимог охорони праці згідно з КУпАП та КК України, а також запропоновано комплекс інженерно-технічних заходів для захисту від шкідливого інфрачервоного випромінювання на робочих місцях персоналу.

Таким чином, кваліфікаційна робота являє собою завершений комплекс технічної та економічної документації щодо проектування, налаштування та введення в експлуатацію локальної комп'ютерної мережі маркетингової компанії «STAR WAY», що гарантує надійний, безпечний, захищений та ефективний обмін інформацією між усіма підрозділами компанії.

ПЕРЕЛІК ПОСИЛАНЬ

1. 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: 30.03.2026).
2. Воробієнко П., Нікітюк Л., Резниченко П. Телекомунікаційні та інформаційні мережі. К: Саміт-книга, 2010. 640 с.
3. Вплив інфрачервоних хвиль на організм людини: веб-сайт. URL: https://teploceramic.ua/ua/vliyanie-infrakrasnogo-излучения-на-организм.html (дата звернення: 30.03.2026).
4. Гері А. Донахью. Мережевий воїн. Cisco Press, 2022. 1152 с.
5. Джеймс Куроуз, Кит Росс. Комп'ютерні мережі. Детальний підхід. К.: Наука, 2016. 912 с.
6. Джейсон Едельман. Програмованість та автоматизація мереж. O'Reilly Media, 2021. 480 с.
7. Додонов О. Г., Ланде Д. В., Путятін В. Г. Інформаційні потоки в глобальних комп'ютерних мережах. К.: Наукова думка, 2019. 295 с.
8. Жуков І.А., Дрововозов В.І., Махновський Б.Г. Експлуатація комп'ютерних систем та мереж. К.: НАУ, 2017. 361 с.
9. Іртегов Д.В. Введення в мережні технології. К.: Наука, 2014. 316 с.
10. Коробейнікова Т. І., Захарченко С. М. Комп'ютерні мережі. Львівська політехніка, 2022. 228 с.
11. Лунтовський А., Мельник І. Комп'ютерні мережі та телекомунікації. Університет «Україна», 2017. 274 с.
12. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В. Комп'ютерні мережі: навчальний посібник. Львів: Магнолія 2006, 2013. 256 с.
13. Олексюк В., Балик Н., Балик А. Організація комп'ютерної локальної мережі. Тернопіль: Підручники та посібники, 2006. 80 с.

14. Системи оповіщення та управління евакуацією: веб-сайт. URL: https://www.varta-bezpeka.com.ua/opovishhennja-ta-upravlinnja-evakuacijeju (дата звернення: 30.03.2026).

15. Стандарт TIA/EIA-568B. Структуровані кабельні системи: веб-сайт. URL: https://tiaonline.org/standard/tia-568 (дата звернення: 12.04.2026).

16. APC Smart-UPS 1500VA SMT1500I: веб-сайт. URL: https://www.apc.com/shop/ua/uk/products/APC-Smart-UPS-1500VA/P-SMT1500I (дата звернення: 15.04.2026).

17. Cisco Aironet AIR-AP1815I: веб-сайт. URL: https://www.cisco.com/c/en/us/support/wireless/aironet-1800-access-points/series.html (дата звернення: 15.03.2026).

18. Cisco Catalyst WS-C2960-24TC-L: веб-сайт. URL: https://www.cisco.com/c/en/us/support/switches/catalyst-2960-x-series-switches/series.html (дата звернення: 15.03.2026).

19. Cisco Catalyst WS-C2960X-24TS-L: веб-сайт. URL: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/datasheet-c78-728232.html (дата звернення: 15.03.2026).

20. Cisco IOS Configuration Guide: веб-сайт. URL: https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-15-4m-t/model.html (дата звернення: 10.04.2026).

21. Dell PowerEdge R350: веб-сайт. URL: https://www.dell.com/en-us/shop/poweredge-servers/poweredge-r350-rack-server/spd/poweredge-r350 (дата звернення: 15.03.2026).

22. IEEE 802.1Q VLAN Tagging Standard: веб-сайт. URL: https://standards.ieee.org/ieee/802.1Q (дата звернення: 12.04.2026).

23. Ubuntu Server 22.04 LTS Documentation: веб-сайт. URL: https://ubuntu.com/server/docs (дата звернення: 10.04.2026).

24. Zabbix Documentation: веб-сайт. URL: https://www.zabbix.com/documentation/current/en (дата звернення: 10.04.2026).

ДОДАТКИ

Додаток А. Характеристики комутатора Cisco Catalyst WS-C2960X-24TS-L

Cisco Catalyst WS-C2960X-24TS-L — це керований комутатор фіксованої конфігурації рівня L3 серії Catalyst 2960-X, призначений для розгортання в корпоративних локальних мережах середнього та великого масштабу. Комутатор виступає центральним вузлом (Core Switch, SW_1) мережевої інфраструктури маркетингової компанії «STAR WAY» та забезпечує високошвидкісну міжVLAN маршрутизацію між 12 логічними підмережами компанії.

Основні технічні та функціональні характеристики комутатора [12]:

– мережеві інтерфейси: 24 порти 10/100/1000 Мбіт/с (Gigabit Ethernet, роз'єми RJ-45) для підключення серверного обладнання, критичних робочих станцій та магістральних ліній від комутаторів рівня доступу SW_2 і SW_3;

– аплінк-інтерфейси: 4 оптичні порти SFP (1 Гбіт/с) для підключення до мережі інтернет-провайдера (ISP) та організації високошвидкісних резервних з'єднань;

– пропускна здатність: продуктивність комутаційної матриці становить 108 Гбіт/с;

– швидкість пересилання пакетів: швидкість комутації та маршрутизації складає 95,2 млн пакетів/с (Mpps);

– сегментація мережі: повна підтримка стандарту IEEE 802.1Q (VLAN Tagging) для ізоляції та маркування трафіку підмереж (підтримка до 4096 логічних VLAN);

– маршрутизація (Layer 3): апаратна підтримка базових протоколів маршрутизації — OSPF (OSPFv2, OSPFv3), RIP (RIPv1, RIPv2), EIGRP Stub, а також підтримка статичної маршрутизації;

– міжVLAN комутація: підтримка технології SVI (Switch Virtual Interface) для реалізації маршрутизації трафіку між різними VLAN без залучення зовнішнього роутера;

– надійність та відмовостійкість: підтримка протоколів Spanning Tree другого рівня — STP (IEEE 802.1D), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s) та технології Per-VLAN Spanning Tree Plus (PVST+) для усунення петель комутації;

– якість обслуговування (QoS): підтримка стандарту IEEE 802.1p, наявність 4 черг пріоритетності на кожен порт, алгоритми планування черг (Strict Priority, SRR) для оптимізації чутливого до затримок трафіку;

– безпека доступу: підтримка технології Port Security (обмеження доступу за MAC-адресами), автентифікація користувачів за стандартом IEEE 802.1X;

– захист від мережевих атак: інтегровані механізми DHCP Snooping (захист від підміни DHCP-сервера), Dynamic ARP Inspection (DAI) для захисту від ARP-спуфінгу та IP Source Guard;

– фільтрація трафіку: підтримка списків контролю доступу ACL (Access Control Lists) як для другого (L2), так і для третього (L3) рівнів для гнучкого налаштування політик безпеки між підрозділами;

– управління та моніторинг: підтримка протоколу SNMP (версії v1, v2c, v3) для інтеграції із корпоративною системою моніторингу Zabbix, підтримка протоколів RMON, Syslog, а також технології NetFlow Lite;

– інтерфейси адміністрування: доступ до консолі керування через CLI (інтерфейс командного рядка) за допомогою портів RJ-45 або USB mini-B, а також наявність вбудованого веб-інтерфейсу (Web UI);

– конструктивне виконання: форм-фактор 1U, призначений для монтажу в стандартну телекомунікаційну стійку або шафу 19";

– параметри живлення: робота від мережі змінного струму 100–240 В (50/60 ГГц), максимальна споживана потужність пристрою — до 35 Вт (модель без підтримки PoE);

– енергоефективність: підтримка стандарту Energy Efficient Ethernet (EEE, IEEE 802.3az) для зниження енергоспоживання портів під час відсутності активного трафіку;

– програмне забезпечення: фірмова операційна система Cisco IOS (версія 15.x, набір функцій LAN Base).

Додаток Б. Характеристики комутатора D-Link DGS-1210-28P

Лінійка керованих Web Smart комутаторів D-Link серії DGS-1210 пропонує сучасне, високопродуктивне та економічно вигідне рішення для розгортання мереж рівня доступу в корпоративних середовищах будь-якого масштабу [13].

Комутатор D-Link DGS-1210-28P оснащений потужним механізмом пересилання пакетів на апаратному рівні з інтегрованим процесором, що забезпечує максимальну швидкість комутації навіть за умови активації комплексних функцій безпеки та керування. Завдяки перевіреним мережевим технологіям, цей пристрій гарантує високу надійність, стабільність та продуктивність операційного класу для підключення всіх кінцевих пристроїв у локальній мережі маркетингової компанії «STAR WAY».

Комутатори D-Link DGS-1210-28P мають повну підтримку стандартів Power over Ethernet (PoE) IEEE 802.3af та IEEE 802.3at (PoE+). Це дозволяє подавати електроживлення на периферійні мережеві пристрої, такі як бездротові точки доступу AP_1 та AP_2 (Cisco Business 140AC), безпосередньо через кабель крученої пари категорії 6 (Cat 6). Таке рішення повністю виключає потребу в прокладанні додаткових силових ліній або використанні локальних інжекторів живлення [13]. Загальний PoE-бюджет пристрою становить 193 Вт.

Комутатор D-Link DGS-1210-28P забезпечує оптимальне співвідношення ціни та продуктивності для корпоративного сегмента, підтримуючи такі ключові технології [13]:

– високошвидкісні інтерфейси доступу: 24 порти 10/100/1000 Мбіт/с (Gigabit Ethernet, роз'єми RJ-45) із підтримкою технології PoE для підключення робочих станцій співробітників WS_1–WS_23 та бездротових точок доступу;

– магістральні аплінки: 4 виділені оптичні порти 1GbE SFP для організації високошвидкісних з'єднань із головним комутатором ядра мережі SW_1 через Trunk-порти;

– енергоефективність: підтримка передового стандарту Energy Efficient Ethernet (EEE, IEEE 802.3az), який автоматично знижує споживання живлення на неактивних портах або за відсутності мережевого трафіку;

– комутація другого рівня (Layer 2): повна підтримка функціоналу L2, включаючи сегментацію мережі за стандартом IEEE 802.1Q (VLAN Tagging, до 4094 логічних підмереж), а також протоколи захисту від петель комутації STP (802.1D), RSTP (802.1w) та MSTP (802.1s);

– гнучке адміністрування: просте та інтуїтивно зрозуміле управління через вбудований графічний веб-інтерфейс (Web UI), спеціалізовану утиліту D-Link Network Assistant, а також за допомогою інтерфейсу командного рядка (компактний CLI) через захищені протоколи SSH та Telnet.

Додаткові функції та параметри безпеки комутатора включають [13]:

– захист периметра (Port Security): інструмент обмеження кількості дозволених MAC-адрес на кожному фізичному порту, що унеможливлює несанкційоване підключення стороннього або шкідливого обладнання до мережі компанії «STAR WAY»;

– механізм Safeguard Engine: фірмова технологія D-Link, що захищає центральний процесор комутатора від перевантаження або відмови під час масованих мережевих атак чи шкідливого широкомовного шторму;

– оптимізація мультимедіа (IGMP Snooping): підтримка функцій IGMP Snooping v1/v2/v3 для ефективного керування та фільтрації багатоадресного (multicast) трафіку, що запобігає зайвому навантаженню на робочі станції;

– якість обслуговування (QoS): підтримка пріоритизації трафіку за стандартом IEEE 802.1p (наявність 8 черг пріоритетів на порт) для безперебійної та якісної роботи чутливих до затримок сервісів (IP-телефонія, відеоконференції);

– інтеграція з моніторингом: повна підтримка протоколу SNMP (версій v1, v2c, v3) для збору діагностичних даних та інтеграції комутаторів із системою моніторингу Zabbix, розгорнутою на сервері S_2;

– магістральні зв'язки (Trunking): конфігурація гігабітних портів (наприклад, gi0/25) у режим Trunk для надійної передачі всього тегованого трафіку між комутаторами доступу SW_2 SW_3 та головним комутатором ядра SW_1;

– апаратні характеристики: продуктивність комутаційної матриці пристрою становить 56 Гбіт/с, а швидкість пересилання пакетів сягає 41,7 млн пакетів/с (Mpps);

– конструктивне виконання: пристрій виконано у металевому корпусі форм-фактора 1U, призначеному для монтажу у стандартні 19-дюймові телекомунікаційні шафи та стійки.

Додаток В. Характеристики програмного міжмережевого екрана iptables/ufw

Програмний міжмережевий екран (файрвол) iptables/ufw, розгорнутий на сервері S_2 під управлінням операційної системи Ubuntu Server 22.04 LTS, забезпечує комплексний захист локальної мережі маркетингової компанії «STAR WAY» від зовнішніх загроз та несанкціонованого доступу. Він здійснює суворий контроль транзитного трафіку між 12 логічними підмережами VLAN та реалізує механізм динамічної трансляції мережевих адрес (NAT/MASQUERADE) для забезпечення безпечного виходу хостів у мережу Інтернет.

Серверна ОС Ubuntu Server 22.04 LTS функціонує на базі стабільного ядра Linux із вбудованою підсистемою Netfilter. Netfilter є модульною архітектурою, яка повністю інтегрована на рівні ядра операційної системи, що дозволяє виконувати фільтрацію, модифікацію та логування мережевих пакетів безпосередньо в просторі ядра (kernel space). Це гарантує максимальну швидкодію та дозволяє ефективно захищати динамічні цифрові інфраструктури без залучення дорогих апаратних міжмережевих екранів.

Для реалізації функцій системи запобігання вторгненням (IPS – Intrusion Prevention System) на сервері S_2 інтегровано програмний комплекс Suricata (або Snort). Він працює в режимі реального часу, здійснюючи глибокий аналіз пакетів (DPI), виявляючи шкідливу чи аномальну мережеву активність за сигнатурним методом та автоматично блокуючи адреси зловмисників до моменту проникнення загрози в периметр мережі компанії «STAR WAY».

Функціонал міжмережевого екрана наступного покоління (NGFW – Next-Generation Firewall) реалізовано за допомогою програмного стеку iptables + Suricata + Squid, що сукупно забезпечує:

– багаторівневий контроль доступу до мережевих ресурсів на основі гнучких правил ACL (Access Control Lists);

– трансляцію адрес (NAT/MASQUERADE) для маскування внутрішньої структури мережі;

– проксі-фільтрацію та кешування веб-трафіку (за допомогою проксі-сервера Squid);

– потокове антивірусне сканування вхідних файлів та трафіку (за допомогою ClamAV);

– захист від витоку конфіденційних даних (DLP) та контроль використання корпоративних додатків.

Основні технічні та експлуатаційні характеристики комплексу:

– пропускна здатність: до 1 Гбіт/с (обмежена номінальною швидкістю інтегрованих мережевих інтерфейсів сервера Dell PowerEdge R350);

– захист від мережевих загроз: глибокий аналіз трафіку засобами Suricata IDS/IPS;

– мережеві інтерфейси: 2 × Gigabit Ethernet (RJ-45), де інтерфейс *eth0* (або індексований системний порт) виділено під зовнішній контур WAN, а *eth1* підключено до комутатора ядра SW_1 для обслуговування внутрішнього контуру LAN;

– мережеві протоколи: повна сумісність із двома стеками протоколів — IPv4 та IPv6;

– затримка обробки пакетів (Latency): менше 1 мс, завдяки низькорівневій обробці на рівні модулів Netfilter.

Підтримувані функції та параметри безпеки:

– пропускна здатність брандмауера (Firewall Throughput): до 1 Гбіт/с;

– підтримка NAT/MASQUERADE: так, реалізовано через таблицю nat в iptables;

– аналіз стану з'єднань (Stateful Packet Inspection): так, на основі модуля відстеження з'єднань conntrack;

– організація безпечних каналів IPsec VPN: так, за допомогою програмного комплексу strongSwan;

– організація віддаленого доступу SSL VPN: так, за допомогою сервера OpenVPN для захищеного підключення віддалених працівників;

– ізоляція логічних підмереж: так, маршрутизація та фільтрація трафіку для 12 підмереж (VLAN 10–110 та 管理 VLAN 200);

– політики безпеки (Firewall Policies): необмежена кількість правил, що визначаються конфігураційними скриптами iptables/ufw;

– системне логування подій: реєстрація подій у файлах контурів /var/log/syslog та /var/log/ufw.log;

– інструменти адміністрування: інтерфейс командного рядка CLI (скрипти Bash, утиліти ufw/iptables), а також можливість віддаленого керування через захищений веб-інтерфейс Webmin.

Порти та фізичні характеристики платформи (сервера S_2):

– USB-інтерфейси: 1 × USB порт на передній панелі (для локального підключення носіїв);

– управління та моніторинг «out-of-band»: 1 × виділений гігабітний порт управління iDRAC9 для віддаленого консольного доступу до апаратної частини сервера;

– мережеві порти: 2 × Gigabit Ethernet RJ-45 (підключення магістральним зв'язком до комутатора ядра SW_1, включаючи управління через VLAN 200);

– конструктивне виконання корпусу: форм-фактор 1U Rack для горизонтального монтажу в стандартну телекомунікаційну стійку або шафу 19";

– габаритні розміри шасі Dell PowerEdge R350: 43,2 × 434,0 × 390,0 мм;

– конструктивна вага пристрою: 10,2 кг.

Системні параметри операційної системи Ubuntu Server 22.04 LTS:Версія ядра Linux: базова гілка 5.15 LTS (Long Term Support);

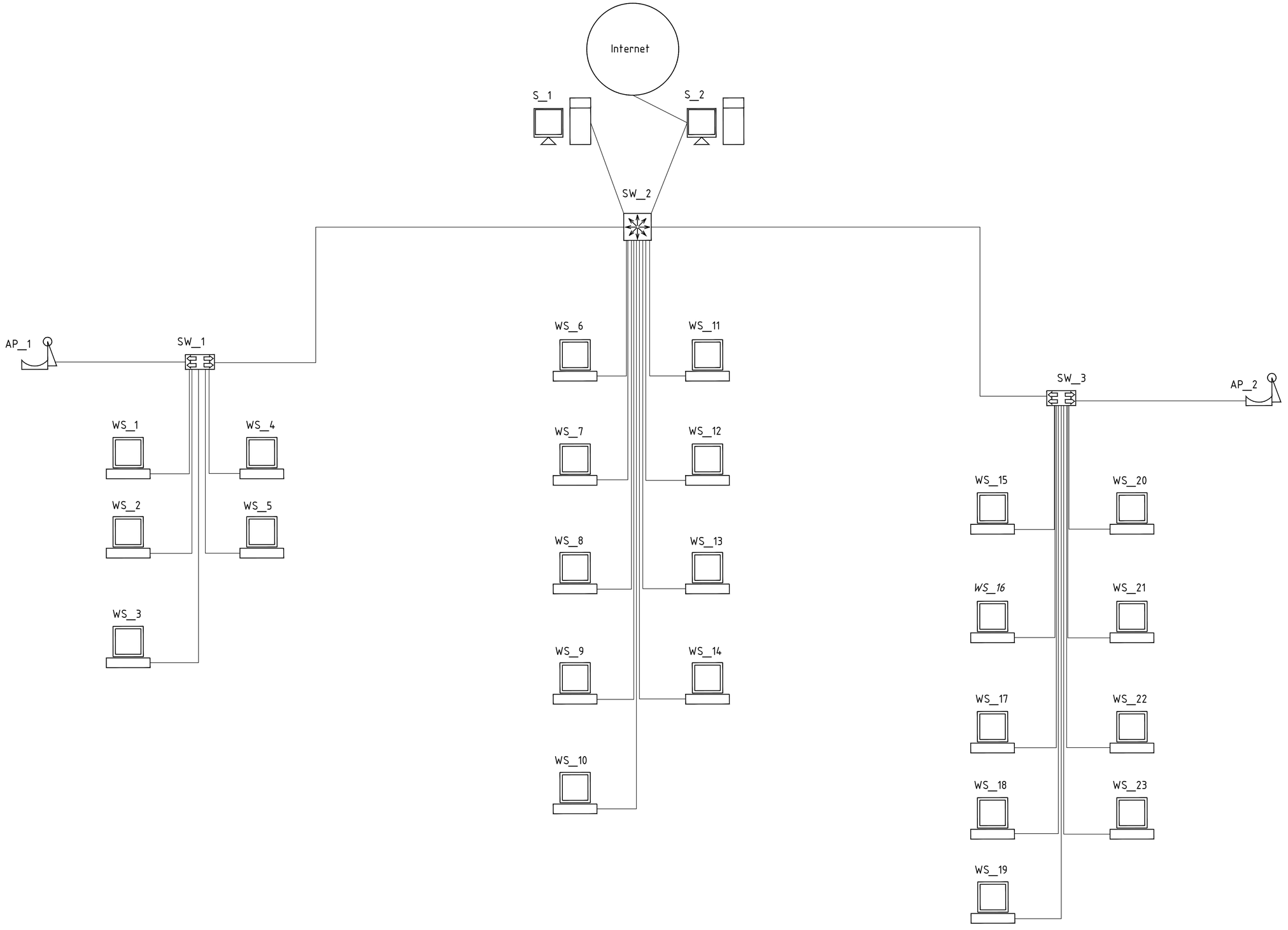
– архітектура підсистеми безпеки: Netfilter з користувацькими утилітами iptables та спрощеною надбудовою ufw (Uncomplicated Firewall);

– висока доступність (High Availability): підтримка кластеризації та дублювання функцій через сервіс keepalived;

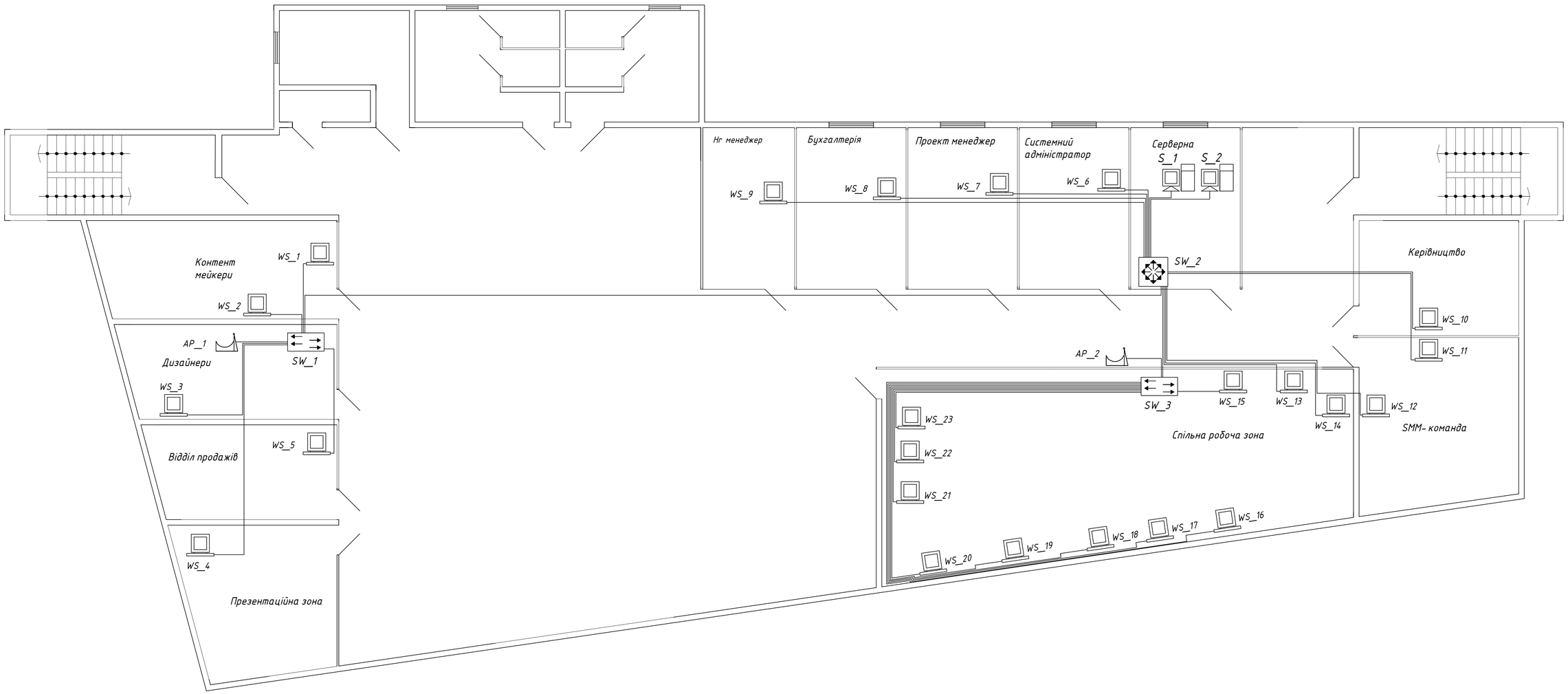
– максимальна кількість одночасних сесій: динамічний параметр, що залежить від обсягу ОЗП сервера (для встановлених 32 ГБ ECC DDR4 ліміт становить до 2 млн одночасних сесій);

– ініціалізація конфігурації: автоматичне та безпомилкове застосування встановлених правил фільтрації після перезавантаження сервера за допомогою демона netfilter-persistent.

Використання програмного міжмережевого екрана iptables/ufw на базі відмовостійкого сервера S2 забезпечує високий і надійний рівень захисту всієї мережевої інфраструктури компанії «STAR WAY». Дане рішення характеризується повною відсутністю витрат на придбання комерційного програмного забезпечення та ліцензування робочих місць, що робить його найбільш раціональним та економічно доцільним інженерним рішенням для маркетингового агентства середнього масштабу.



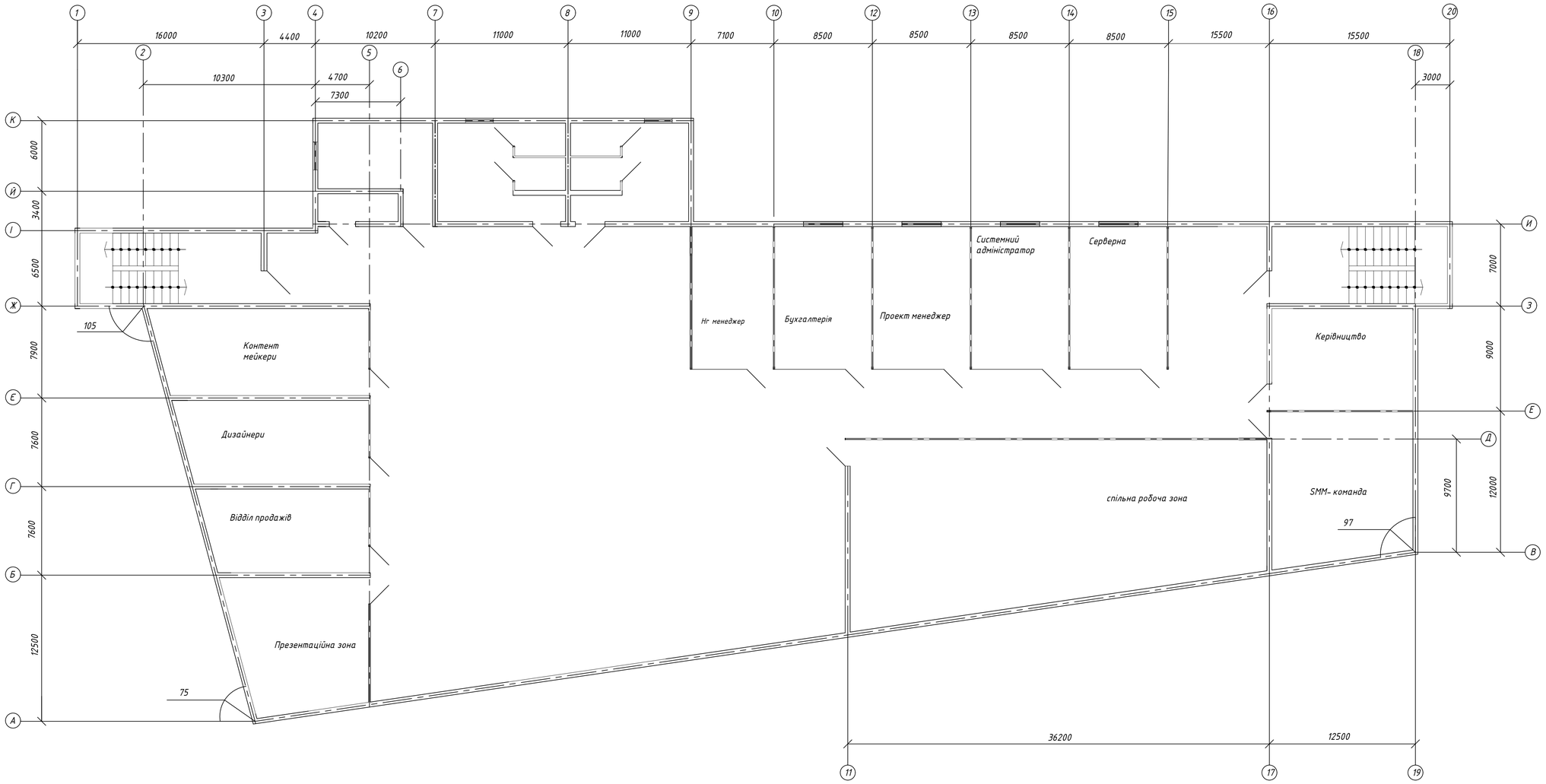
					2026. КВР . 123.406.15.00.00 ЛТ		
Зм.	Док.	№ докум.	Підпис	Дата	Розробка проекту комп'ютерної мережі компанії "STAR WAY" Логічна топологія	Літ.	Маса	Масштаб
Розроб.		Максим'юк С.						
Перевір.		Лісовий В.				Аркуш	Аркушів	1
Т. конт.								
Н. конт.		Приймак В.А.				ВСП ТФК ТНТУ ім. І. Пулюя група КІ-406 м. Тернопіль		
Затв.								



					2026.КВР.123.406.15.00.00 ФТ	
Зм.	Док.	№ докум.	Підпис	Дата	Розробка проекту комп'ютерної мережі компанії "STAR WAY" Фізична топологія	Літ. / Маса / Масштаб: 1:100
Розроб.		Максим'юк С.				
Перевір.		Лісовий В.				
Т. контр.						Аркуш / Аркушів: 1
Н. контр.		Приймак В.А.			ВСП ТФК ТНТУ ім. І. Пулюя група КІ-406 м. Тернопіль	
Затв.						

Таблиця техніко-економічнихпоказників

№п.п	Параметр	Одиниці вимірювання	Значення
1	Топологія мережі	–	Ієрархічна зіркова
2	Середовище передачі даних	–	Екранований кабель UTP Cat 6, Wi-Fi
3	Кількість комутаторів	шт.	3
4	Центральний комутатор	–	Cisco Catalyst WS-C2960X-24TS-L
5	Комутатори рівня доступу	–	D-Link DGS-1210-28P
6	Швидкість передачі даних у дротовому сегменті	Мбіт/с	1000
7	Кількість точок доступу	шт.	2
8	Модель точок доступу	–	Cisco Business 140AC
9	Кількість серверів	шт.	2
10	Модель корпоративних серверів	–	Dell PowerEdge R350
11	Кількість робочих станцій	шт.	23
12	Операційна система серверів	–	Ubuntu Server 22.04 LTS
13	Операційна система робочих станцій	–	Windows 10 / 11 Pro
14	Тип доступу до мережі Інтернет	–	Через міжмережевий екран iptables
15	Матеріальні витрати	грн.	170 640,00
16	Повна собівартість проєкту	грн.	195 754,50
17	Термін окупності	рік	1,1



					2026. КВР . 123.406.15.00.00 ПП		
Зм.	Док.	№ докум.	Підпис	Дата	Розробка проекту комп'ютерної мережі компанії "STAR WAY" План приміщень	Літ.	Маса	Масштаб
Розроб.		Макси'юк С.						1:100
Перевір.		Лісовий В.						
Т. конт.						Аркуш	Аркушів	1
Н. конт.		Приймак В.А.			ВСП ТФК ТНТУ ім. І. Пулюя група КІ-406 м. Тернопіль			
Затв.								

Таблиця IP-адрес

№ п/п	Позначення	IP-address/Mask	Gateway	VLAN ID	VLAN Name	Розташування
1	SW_1	192.168.10.254/24	–	10	admin	Серверна
		192.168.20.254/24	–	20	market	
		192.168.30.254/24	–	30	pr_smm	
		192.168.40.254/24	–	40	content	
		192.168.50.254/24	–	50	design	
		192.168.60.254/24	–	60	seo_analyt	
		192.168.70.254/24	–	70	finance	
		192.168.80.254/24	–	80	hr	
		192.168.90.254/24	–	90	it_mgmt	
		192.168.100.254/24	–	100	servers	
		192.168.110.254/24	–	110	wifi_corp	
		192.168.200.254/24	–	200	wifi_guest	
2	SW_2	192.168.90.252/24	192.168.90.254	90	it_mgmt	Офісна зона
3	SW_3	192.168.90.253/24	192.168.90.254	90	it_mgmt	Офісна зона
4	S_1	192.168.100.1/24	192.168.100.254	100	servers	Серверна
5	S_2	192.168.100.2/24	192.168.100.254	100	servers	Серверна
6	AP_1	192.168.110.1/24	192.168.110.254	110	wifi_corp	Коридор
7	AP_2	192.168.110.2/24	192.168.110.254	110	wifi_corp	Конференц-зал
8	WS_1	192.168.10.1/24	192.168.10.254	10	admin	Кабінет директора
9	WS_2	192.168.10.2/24	192.168.10.254	10	admin	Кабінет заступника директора
10	WS_3	192.168.20.1/24	192.168.20.254	20	market	Відділ маркетингу та реклами
11	WS_4	192.168.20.2/24	192.168.20.254	20	market	Відділ маркетингу та реклами
12	WS_5	192.168.20.3/24	192.168.20.254	20	market	Відділ маркетингу та реклами
13	WS_6	192.168.20.4/24	192.168.20.254	20	market	Відділ маркетингу та реклами
14	WS_7	192.168.20.5/24	192.168.20.254	20	market	Відділ маркетингу та реклами
15	WS_8	192.168.30.1/24	192.168.30.254	30	pr_smm	PR та SMM-відділ
16	WS_9	192.168.30.2/24	192.168.30.254	30	pr_smm	PR та SMM-відділ
17	WS_10	192.168.30.3/24	192.168.30.254	30	pr_smm	PR та SMM-відділ

№ п/п	Позначення	IP-address/Mask	Gateway	VLAN ID	VLAN Name	Розташування
18	WS_11	192.168.40.1/24	192.168.40.254	40	content	Відділ копірайтингу та контенту
19	WS_12	192.168.40.2/24	192.168.40.254	40	content	Відділ копірайтингу та контенту
20	WS_13	192.168.50.1/24	192.168.50.254	50	design	Креативна Дизайн-студія
21	WS_14	192.168.50.2/24	192.168.50.254	50	design	Креативна Дизайн-студія
22	WS_15	192.168.50.3/24	192.168.50.254	50	design	Креативна Дизайн-студія
23	WS_16	192.168.60.1/24	192.168.60.254	60	seo_analyt	Відділ SEO
24	WS_17	192.168.60.2/24	192.168.60.254	60	seo_analyt	Відділ SEO
25	WS_18	192.168.70.1/24	192.168.70.254	70	finance	Бухгалтерія та фінанси
26	WS_19	192.168.70.2/24	192.168.70.254	70	finance	Бухгалтерія та фінанси
27	WS_20	192.168.80.1/24	192.168.80.254	80	hr	Відділ кадрів
28	WS_21	192.168.80.2/24	192.168.80.254	80	hr	Відділ кадрів
29	WS_22	192.168.90.1/24	192.168.90.254	90	it_mgmt	Служба IT-підтримки
30	WS_23	192.168.90.2/24	192.168.90.254	90	it_mgmt	системний адміністратор
31	DHCP Pool	192.168.200.10-100	192.168.200.254	200	wifi_guest	Динамічна гостьова мережа

					2026.КВР.123.406.15.00.00 ТА	
Зм.	Док.	№ докум.	Підпис	Дата	Розробка проекту комп'ютерної мережі компанії "STAR WAY" Таблиця IP-адрес	Літ. / Маса / Масштаб
Розроб.		Максим'юк С.				
Перевір.		Лісовий В.				Аркуш / Аркушів: 1
Т. контр.						ВСП ТФК ТНТУ ім. І. Пулюя група КІ-406 м. Тернопіль
Н. контр.		Приймак В.А.				
Затв.						