Форма № Н-9.02

Міністерство освіти і науки України

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

(повне найменування вищого навчального закладу)

Відділення інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра

(освітньо-професійного ступеня)

на тему: **Розробка проєкту комп'ютерної мережі компанії "ІТ-М"**

Виконав: студент IV курсу, групи КІ-406

Спеціальності 123 Комп'ютерна інженерія

(шифр і назва спеціальності)

_____ Олександр ШКВАРОК

(ім'я та прізвище)

Керівник Олександра МАРЦЮК

(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
"30" березня 2026 року

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

Шкварок Олександру Володимировичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
   Розробка проєкту комп'ютерної мережі компанії "ІТ-М"

керівник роботи Марцюк Олександра Василівна
(прізвище, ім'я, по батькові)

затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя» від 27.03.2026р № 4/9-167.

2. Строк подання студентом роботи: 15 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 та безпека життєдіяльності.

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

6. Консультанти розділів роботи

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

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	31.03	
2	Збір і узагальнення інформації	08.05	
3	Написання першого розділу	15.05	
4	Розробка технічного та робочого проекту	22.05	
5	Написання спеціального розділу	28.05	
6	Розрахунок економічної частини	1.06	
7	Написання розділу охорони праці	3.06	
8	Виконання графічної частини	8.06	
9	Оформлення проєкту	10.06	
10	Погодження нормоконтролю	11.06	
11	Попередній захист роботи	12.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 31 березня 2026 року

Студент _____ Олександр ШКВАРОК
(підпис) (ім'я та прізвище)

Керівник роботи _____ Олександра МАРЦЮК
(підпис) ім'я та прізвище)

АНОТАЦІЯ

Шкварок О.В. Розробка проєкту комп’ютерної мережі компанії «IT-M»: кваліфікаційна робота на здобуття освітньо-професійного ступеня фахового молодшого бакалавра за спеціальністю 123 Комп’ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2026. -105с.

Кваліфікаційна робота присвячена проєктуванню сучасної локальної обчислювальної мережі для компанії «IT-M». У роботі реалізовано гібридну фізичну топологію, побудовану на основі стеку протоколів TCP/IP версії 4. Застосовано мережеві технології IEEE 802.3ab та IEEE 802.11ac, а також впроваджено засоби віртуалізації для підвищення ефективності серверних обчислень.

Особливу увагу приділено використанню безкоштовного програмного забезпечення для реалізації ключових мережевих сервісів, організації моніторингу стану мережі, а також аутентифікації користувачів при доступі до ресурсів. Робота має прикладне спрямування та передбачена для впровадження в компанії «IT-M».

Ключові слова: комп’ютерна мережа, гібридна топологія, TCP/IP, віртуалізація, моніторинг, аутентифікація.

ANNOTATION

Shkvarok O.V. Development of a Computer Network Project for the "IT-M" Company: qualification work for the attainment of the professional junior bachelor's degree in specialty 123 Computer Engineering. Ternopil: SEI "TCPC of TNTU", 2026. 105 pages.

This qualification work is dedicated to the design of a modern local area network for the company "IT-M". The project implements a hybrid physical topology based on the TCP/IP version 4 protocol stack. The network utilizes IEEE 802.3ab and IEEE 802.11ac technologies, along with virtualization tools to optimize server computing performance.

Special attention is given to the use of free software for the implementation of key network services, network monitoring procedures, and user authentication when accessing local network resources.

The work has a practical focus and is intended for implementation in the "IT-M" company.

Keywords: computer network, hybrid topology, TCP/IP, virtualization, monitoring, authentication.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

DNS-сервер (Domain Name Server) – сервер доменних імен, у задачу якого входить перетворення текстових доменних імен на IP-адреси.

HTTP (Hyper Text Transfer Protocol) – протокол, що забезпечує взаємодію користувача, який хоче отримати доступ до web-документів, із сервером, що надає можливість такого доступу.

IEEE – міжнародна організація інженерів в області електротехніки, радіоелектроніки і радіоелектронній промисловості. Світовий лідер в області розробки стандартів з електроніки та електротехніки. Штаб квартира організація знаходиться у Лондоні.

IP (Internet Protocol) – протокол, що забезпечує доставку даних у вигляді пакетів, що мають IP-адресу.

IP-адреса – числовий ідентифікатор, що надається кожному комп'ютеру (хосту), підключеному до Інтернет.

MAC (Media Access Control) - апаратна адреса ПК.

NAT (Network Address Translation) – мережева трансляція адес.

OSI (Open System Interface) – модель з'єднання відкритих систем.

TCP/IP (Transmission Control Protocol/Internet Protocol) – набір протоколів для керування обміном даними між комп'ютерами в глобальній мережі Інтернет.

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

VM – віртуальна машина.

XEN - багатоплатформенний гіпервізор розроблений в Кембриджському університеті.

ОС – операційна система.

ПК – персональний комп'ютер.

ВСТУП

Планування будь якої господарсько діяльності в сучасному світі неможливе без розвитку та інвестицій в мережеву інфраструктуру для зберігання та обробки даних [1]. Така інфраструктура покликана спростити ведення бізнесу, оскільки сучасний бізнес напряму пов’язаний з обміном інформацією, збереженням та аналізом даних, що являють собою результат виробничої діяльності. Проєктування локальної мережі компанії, мережевих сервісів дає можливість покращити продуктивність компанії, задіяти в виробничій діяльності нові технології для успішного конкурування на ринку з іншими компаніями.

У даному проєкті пропонується один з варіантів вирішення завдання організації інформаційної системи, яка включає об’єднання всіх ПК в мережу, впровадження локальних мережевих ресурсів, спільна робота з документами, використання мережі Інтернет в виробничій діяльності. Проєкт локальної мережі буде розроблятися для компанії «ІТ-М».

Розглянуто оптимальні варіанти оснащення компанії комплектом устаткування та програмного забезпечення, який є достатнім для вирішення поставленого завдання.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Аналіз технічного завдання

1.1.1 Найменування та сфера застосування проєкту

Проєкт валіфікаційної роботи присвячена реалізації комплексної технічної розробки за темою: «Розробка проєкту комп'ютерної мережі компанії «ІТ-М». Дослідження та проєктування виконані в межах відповідно до вимог і положень затвердженого замовником технічного завдання (ТЗ).

Створення мережевої архітектури базується на принципах інтеграції сучасних інфокомунікаційних технологій, врахуванні специфіки бізнес-процесів компанії-клієнта, а також на суворому дотриманні діючих міжнародних та галузевих стандартів (зокрема, сімейства IEEE 802.3, IEEE 802.11 та стандартів структурування СКС TIA/EIA-568). На етапі передпроєктного аналізу та формування концепції мережі було визначено та систематизовано ключові критерії, яким має відповідати створювана інфраструктура:

1. Об'єднання різнорідного клієнтського обладнання в єдину мережеву інфраструктуру: забезпечення спільної роботи стаціонарних робочих станцій, ноутбуків, інженерних терміналів та мобільних пристроїв у межах єдиної локальної мережі з використанням технології віртуальних локальних мереж (VLAN).

2. Організація надійного доступу до мережі Інтернет: забезпечення стабільного високошвидкісного підключення до зовнішніх мереж через прикордонний шлюз із підтримкою технології PPPoE та засобів контролю мережевого трафіку.

3. Централізоване використання інформаційних ресурсів: надання користувачам контрольованого доступу до файлових сховищ, серверних сервісів,

баз даних та інших ресурсів корпоративної мережі відповідно до встановлених прав доступу.

4. Забезпечення інформаційної безпеки мережі: реалізація механізмів розмежування доступу до мережевих ресурсів, фільтрації трафіку, контролю підключених пристроїв та захисту бездротових сегментів із використанням сучасних методів шифрування.

5. Автоматизація мережевих сервісів та адміністрування: впровадження служб автоматичного призначення мережевих параметрів, централізованого моніторингу та керування активним мережевим обладнанням.

6. Масштабованість і економічна ефективність мережі: побудова мережевої інфраструктури з можливістю подальшого збільшення кількості користувачів, розширення сервісів і модернізації обладнання без суттєвих змін існуючої топології.

Отримані в ході виконання проєкту технічні рішення, розроблена мережева архітектура, схеми побудови локальної мережі, результати розрахунків вартості обладнання та конфігураційні налаштування можуть бути використані під час створення або модернізації мережевої інфраструктури малих і середніх підприємств, проєктних організацій, офісних центрів та інших установ зі схожою структурою інформаційних ресурсів і користувачів.

Практичну цінність становлять також рішення щодо сегментації мережі за допомогою технології VLAN, організації міжмережевої взаємодії, централізованого адміністрування мережевих сервісів, розмежування прав доступу користувачів та забезпечення інформаційної безпеки. Запропоновані підходи можуть бути використані при проєктуванні нових мереж або вдосконаленні існуючих інформаційно-комунікаційних систем.

Окремі результати дослідження, зокрема принципи віртуалізації серверних ресурсів, організація мережевих сервісів на базі програмних платформ маршрутизації, а також методи захисту бездротових мереж, можуть бути

адаптовані для використання в організаціях різних форм власності залежно від їхніх технічних та економічних потреб.

1.1.2 Призначення розробки

На основі детального аналізу вихідних комунікаційних вимог підприємства, цей проєкт спрямований на комплексну реалізацію практичних програмно-апаратних рішень, що визначають його цільове інженерне призначення.

Базова задача проєкту - об'єднання всього парку персональних комп'ютерів, серверного обладнання та периферійних пристроїв у межах цілісної локальної обчислювальної мережі (ЛОМ) із впровадженням оптимальної топології «розширена зірка» з виділеним ядром комутації.

Реалізація цієї задачі неможлива без створення структурованого кабельного середовища, а саме проєктування та розгортання структурованої кабельної системи (СКС) на базі звитої пари категорії Cat.6, яка задовольняє високі вимоги щодо пропускної здатності, механічної надійності та гнучкості комутації.

Важливим завданням є забезпечення структурного масштабування, тобто формування резерву фізичної та логічної інфраструктури для забезпечення безперешкодного підключення нових абонентів або цілих підрозділів без заміни сервісів та без потреби реструктуризації мережевого ядра.

Програмно-апаратний захист периметра проектованої мережі передбачає розгортання засобів багаторівневого міжмережевого екранування (Stateful Firewall на базі Netfilter/iptables) для повноцінного захисту внутрішніх логічних сегментів від зовнішніх атак та сканування. При цьому важливо забезпечити внутрішню та зовнішню маршрутизацію та NAT, тобто спрямування транзитних пакетів у глобальну мережу Інтернет крізь єдиний шлюз безпеки із

впровадженням статичної/динамічної маршрутизації та механізмів трансляції мережевих адрес (NAT/MASQUERADE).

При побудові мережі важливо забезпечити захист бездротового ефіру, а саме : забезпечення конфіденційності, цілісності та автентичності даних у радіосегменті мережі шляхом реалізації протоколів WPA2-AES, ізоляції бездротових клієнтів у межах окремого VLAN 20 та впровадження апаратних фільтрів на базі списків доступу (Access List) за MAC-адресами.

Однією з задач проекту мережі є централізація інформаційних ресурсів, тобто конфігурування відмовостійкого мережевого сховища даних на базі сервера LENOVO ThinkSystem ST50 з організацією захищених протоколів передачі файлів (FTPS) для швидкого та розмежованого обміну даними всередині компанії.

Для стабільної роботи мережі потрібно передбачити системи телеметрії та/або моніторингу, задіявши сучасні кросплатформенні комплекси збору метрик і візуалізації (Prometheus, Node Exporter, Grafana) для безперервного контролю працездатності мережевого заліза та аналізу трафіку в режимі реального часу.

В результаті розробки повинно бути сформовано повний комплект технічної, експлуатаційної та кошторисної документації, яка містить детальну лофічну і фізичну топологію мережі, конфігураційні лістинги та специфікації застосованих апаратних і пасивних засобів.

1.1.3 Вимоги до апаратного і програмного забезпечення

Формування специфікації обладнання та програмних засобів для компанії «ІТ-М» базується на принципах високої відмовостійкості, цілодобового режиму експлуатації (24/7) та відповідності сучасним індустріальним стандартам.

1. Апаратні вимоги до активного обладнання

Серверні платформи (S_1, S_2): обов'язкова наявність багатоядерних процесорів архітектури x86-64 (Intel Xeon), не менше 32 ГБ оперативної пам'яті з

підтримкою ECC, інтеграція відмовостійких дискових масивів (RAID) та джерел безперебійного живлення (ДБЖ) з лінійно-інтерактивним або On-Line захистом.

Бездротові точки доступу (Wi-Fi AP): підтримка стандарту IEEE 802.11ac (Wi-Fi 5) у двох діапазонах (2.4/5 ГГц), антени з технологією MIMO, апаратна реалізація протоколів безпеки WPA2/WPA3-AES та підтримка списків контролю доступу (ACL) для фільтрації MAC-адрес.

Центральний комутатор ядра (L3 Core Switch): висока пропускна здатність внутрішньої матриці, підтримка апаратної маршрутизації, великий об'єм буферної пам'яті, супровід протоколів резервування (STP/RSTP, VRRP) та можливість централізованого керування через CLI та SNMP.

Комутатори рівня доступу (L2 Switches): наявність гігабітних портів (10/100/1000 Мбіт/с) для підключення клієнтів, підтримка тегування трафіку за стандартом IEEE 802.1Q (VLAN) та базових алгоритмів запобігання петлям (STP).

2. Вимоги до пасивних компонентів та СКС

Проєктування структурованої кабельної системи здійснюється за стандартом TIA/EIA-568. Усі пасивні елементи (неекранована вита пара, розетки, патч-панелі) повинні відповідати категорії Cat.6, що гарантує стабільну передачу даних на гігабітних швидкостях і задовольняє критерію економічної доцільності.

3. Вимоги до програмного забезпечення (ПО)

Системне та прикладне ПО серверів (Proxmox VE, Fedora Server) і робочих станцій має відповідати певним критеріям. Важливою є повноцінна підтримка сучасного стеку мережевих протоколів (TCP/IP, PPPoE, VLAN), наявність інтегрованих засобів захисту (Netfilter/iptables), регулярне оновлення компонентів безпеки ядра та антивірусних модулів, а також наявність вбудованих інструментів віддаленого адміністрування (SSH, WinBox) та агентів збору телеметрії (Node Exporter).

1.1.4 Вимоги до документації

Основна стадія реалізації проєкту комп'ютерної мережі для компанії «IT-M» передбачає проведення монтажно-налагоджувальних робіт, комплексне налаштування активного обладнання та проведення системного навантажувального тестування інфраструктури. Після підтвердження відповідності параметрів мережі критеріям вихідного технічного завдання здійснюється формування та верифікація повного комплекту проєктно-технічної та виконавчої документації, яка передається замовнику разом з актом приймання-передачі виконаних робіт.

Відповідно до діючих нормативних стандартів (зокрема, ДСТУ та ISO/IEC щодо оформлення системної документації), до підсумкового пакету документів ЛОМ висуваються такі базові вимоги:

1. Документація повинна містити вичерпний опис архітектури мережі, представлений у вигляді детальних схем фізичної топології (трасування кабельних трас, плани розміщення робочих станцій, комутаційних вузлів та серверних шаф) і логічної структури (схеми розподілу широкомовних доменів VLAN, маршрутизації транзитного трафіку та інше). Наявність таких схем забезпечує прозорість експлуатації та значно спрощує подальшу модернізацію або масштабування мережевого середовища.

2. Обов’язковою вимогою є наявність структурованого технічного розділу «Конфігурація комутаторів та серверів». У ньому фіксуються детальні карти IP-адресації для кожного логічного сегмента (VLAN 11–20), параметри масок підмереж, адреси основних шлюзів, DNS-серверів та конфігураційні лістинги операційних систем (Fedora Server, Proxmox VE, RouterOS). Формат збереження цих даних (текстові специфікації, інтерактивні електронні таблиці або бази даних IPAM) узгоджується із замовником для забезпечення зручності оперативного внесення змін у процесі адміністрування без руйнування загальної структури реєстру.

3. Самостійним критично важливим блоком виконавчої документації є «Корпоративна політика інформаційної безпеки». Цей розділ нормативно закріплює впроваджені інструменти захисту IT-інфраструктури: криптографічні протоколи бездротового ефіру, правила фільтрації пакетів міжмережевим екраном iptables, списки контролю доступу (ACL) на комутаторах ядра, налаштування аутентифікації адміністраторів, а також алгоритми антивірусного моніторингу та протидії зовнішнім векторам кібератак.

Наявність верифікованого комплекту документації такого рівня є запорукою мінімізації часу на локалізацію несправностей, підвищує керованість системи та гарантує безперервність бізнес-процесів підприємства.

1.1.5 Техніко-економічні показники

На основі проведених інженерних розрахунків, розробки логічної структури та фізичного рощташування обладнання і калькуляції вартості матеріальних ресурсів, сформовано перелік базових техніко-економічних критеріїв реалізації проєкту комп'ютерної мережі для компанії «IT-M».

Архітектурний базис інфраструктури виконується на основі гібридної фізичної топології («розширена зірка» з виділеним магістральним ядром комутації та комірчаста топологія для безпровідних сегментів).

Пропускна здатність кабельного сегмента у межах структурованої кабельної системи (СКС Cat.6) для всіх дротових робочих станцій та серверних інтерфейсів становить 1000 Мбіт/с (1 Gbps Full Duplex).

Продуктивність бездротового радіосегмента, а саме розрахункова швидкість передачі даних у Wi-Fi зоні (VLAN 20) за стандартом IEEE 802.11ac із застосуванням багатоканальних точок доступу MikroTik cAP ac досягає пікових значень до 1000 Мбіт/с (сумарно у двох частотних діапазонах).

Згідно вимог замовника виконано мінімізацію витрат на системне ПЗ, оскільки для розгортання серверних платформ (S_1, S_2) та системи віртуалізації

застосовується вільнопоширюване програмне забезпечення з відкритим вихідним кодом (Open Source): гіпервізор Proxmox VE та дистрибутив Linux Fedora Server x64, що повністю нівелює витрати на закупівлю серверних ОС.

Нормативи трудовитрат для проєкту мережі, а саме сумарна розрахункова трудомісткість повного циклу робіт, що включає передпроєктне дослідження, безпосередньо проєктування, монтаж СКС, конфігурування активного обладнання та фінальне пусконалагодження, регламентована в межах до 200 людино-годин.

Матеріальні інфраструктурні витрати апаратно-технічної реалізації проєкту (включаючи повний комплект активного та пасивного обладнання, СКС, системи ДБЖ та комутаційну шафу) повинна становити до 440 тис. грн.

Граничний бюджет проєкту, тобто загальний обсяг фінансування, що враховує закупівлю обладнання, оплату праці інженерної групи та інші витрати, встановлено з жорстким лімітом і не повинен перевищувати 600 000 гривень.

1.1.6 Стадії та етапи розробки

Процес створення та впровадження локальної обчислювальної мережі для компанії «IT-M» реалізується як системний інженерний цикл, що розподілений на кілька взаємопов'язаних етапів:

1. Передпроєктне дослідження та аналіз інформаційних потоків: На початковій стадії здійснюється детальний збір та систематизація вихідних даних щодо кількості кінцевих абонентів, специфіки прикладного програмного забезпечення, вимог до пропускної здатності магістральних каналів та інтенсивності мережевого трафіку. Результати аналізу дозволяють чітко сформувати технічне завдання та визначити архітектурний базис майбутньої мережі.

2. Проєктування фізичної топології та трасування СКС. Цей етап базується на детальному вивченні архітектурних планів офісних приміщень і робочих зон

компанії. На цьому етапі визначаються координати монтажу центральної комутаційної шафи, оптимальні маршрути прокладання пластикових коробів, схеми розміщення мережевих розеток RJ-45 та точок доступу з урахуванням діючих ергономічних, протипожежних та будівельних нормативів.

3. Аналіз ринку та специфікація апаратно-технічних засобів передбачає експертний відбір активного та пасивного обладнання за критеріями відмовостійкості, сумісності та економічної доцільності. Фінальна специфікація охоплює обчислювальні сервери Lenovo, керовані комутатори L2/L3-рівнів від D-Link, бездротові модулі MikroTik cAP ac, а також елементи комутаційного поля (патч-панелі, органайзери) та мідний провідник категорії Cat.6.

5. Розробка логічної архітектури та схем адресації. Цей етап присвячений віртуальному структуруванню мережевого простору. Він включає розбиття мережі на ізольовані широкомовні домени (VLAN 11–20), розробку схем статичної та динамічної IP-адресації, проєктування логіки міжмережевого екранування (iptables), конфігурування pull-моделі збору метрик (Prometheus) та розподілу прав доступу користувачів.

6. Монтажно-інтеграційні та пусконалагоджувальні роботи на об’єкті. При цьому виконується безпосередній фізичний монтаж кабельної інфраструктури, встановлення обладнання в шафу, кросування патч-панелей, розведення розеток та обтиск комутаційних шнурів відповідно до стандартів СКС (TIA/EIA-568). Паралельно здійснюється встановлення операційних систем (Fedora Server, Proxmox VE, RouterOS) та формування базових конфігураційних скриптів.

7. Комплексне інженерне тестування та аудит системи. Тут проводиться верифікація фізичної цілісності ліній зв'язку за допомогою кабельних аналізаторів, перевірка коректності маршрутизації пакетів, стрес-тестування пропускної здатності каналів під навантаженням, а також імітація позаштатних ситуацій (наприклад, знеструмлення мережі) для перевірки переходу на резервне живлення від ДБЖ TECNOWARE.

8. Фінальний етап - формування виконавчої та супровідної документації. Це заключний етап, що полягає в оформленні підсумкового пакету інженерних документів: фізична то логічна топології мережі, кабельних журналів, карт IP-адресації, лістингів налаштувань фаєрволу та інструкцій з експлуатації та превентивного моніторингу за допомогою графічних дашбордів Grafana.

1.1.7 Порядок контролю і прийому

Процедура завершення розробки, фіксації результатів та передачі готової комп'ютерної мережі компанії «ІТ-М» замовнику виконується у чітко регламентованій послідовності відповідно до вимог технічного завдання, умов договору та чинних стандартів (зокрема, ДСТУ 34.603-96 щодо стадій створення автоматизованих систем).

Процес здачі-приймання та інженерного контролю поділяється на кілька ключових етапів:

1. Попередній інспекційний контроль та аудит. Перед початком офіційного приймання інженерна група виконавця проводить внутрішній інструментальний аудит розгорнутої інфраструктури. На цьому етапі за допомогою спеціалізованих тестерів проводиться сертифікація ліній СКС Cat.6 на відповідність категорії, перевіряється стабільність комутації ядра мережі на базі зконфігурованого центрального комутатора, а також валідується коректність роботи політик міжмережевого екранування на шлюзі безпеки.

2. Комплексні та приймально-здавальні випробування. Ці випробування проводяться спільно уповноваженими представниками замовника та виконавця у заздалегідь узгоджені терміни. Під час тестів здійснюється імітація реальних експлуатаційних навантажень на мережу. Перевірці підлягає швидкість обміну даними у провідних (1000 Мбіт/с) та бездротових сегментах (окрема VLAN), відмовостійкість системи віртуалізації Proxmox VE на серверах та швидкість перемикання живлення на резервний контур від ДБЖ у разі аварійних ситуацій.

3. Технічне документування. За результатами успішного завершення випробувань здійснюється двостороннє підписання офіційних документів установленого зразка. Основним документом, що засвідчує успішну реалізацію проєкту, є Акт приймання-передачі виконаних робіт, який скріплюється підписами та печатками відповідальних осіб обох організацій.

4. Останній етап - передача супровідної документації та введення в експлуатацію. Разом із підписаним актом замовнику передається повний пакет виконавчої документації (схеми фізичної та логічної топологій, карти IP-адресації, лістинги конфігурацій). Окремо додається Формуляр (паспорт) системи та інструкція з експлуатаційного моніторингу, які чітко регламентують правила повсякденного обслуговування мережі, графік превентивного технічного догляду за обладнанням у комутаційній шафі та порядок дій системних адміністраторів у разі виникнення позаштатних ситуацій чи зафіксованих системою мережевих аномалій.

1.2 Постановка задачі на розробку проєкту. Характеристика компанії, для якої створюється проєкт мережі

Об'єктом проєктування у даній кваліфікаційній роботі є телекомунікаційна інфраструктура компанії «IT-M». Основним вектором комерційної діяльності підприємства є повний життєвий цикл програмного забезпечення: розробка, архітектурне проєктування, впровадження, розгортання та подальший комплексний технічний супровід складних програмних продуктів і сервісів.

Специфіка діяльності компанії вимагає побудови надійної, високошвидкісної та безпечної локальної обчислювальної мережі (ЛОМ), здатної ізолювати внутрішні інформаційні потоки та забезпечити безперебійний доступ до сервісів віртуалізації. Внутрішня організаційно-штатна структура та просторове розмежування підприємства складаються з таких функціональних підрозділів і технологічних зон:

Адміністративно-керівний сектор: робочі місця генерального директора, заступників з комерційної та технічної діяльності, а також офіс-менеджера. Потребує підвищеного рівня пріоритезації трафіку (QoS).

Фінансово-економічний відділ: централізована бухгалтерія та кадрова служба. Ключова вимога - суворе мережеве екранування (VLAN) для захисту персональних даних та фінансової звітності.

Управлінська ланка (Project Management): проєктні менеджери, керівники напрямків розробки та бізнес-аналітики, які здійснюють координацію виробничих циклів.

Технічне ядро інфраструктури: спеціалізована (серверна кімната) та робочі місця інженерів внутрішнього IT-відділу. Тут зосереджено центральний комутатор ядра L3 та обчислювальні сервери.

Департамент клієнтського сервісу (Helpdesk/Support): підрозділ оперативного технічного консалтингу, супроводу користувачів та обробки інцидентів у режимі реального часу.

Виробничий сектор (R&D Department): базове бізнес-ядро компанії, що включає відділи системного програмування, архітектурного тестування (QA) та безперервної інтеграції/розгортання (CI/CD) програмного забезпечення.

Соціально-побутова зона: приміщення для відпочинку персоналу та кухня. Мережевий доступ тут реалізується виключно через ізольований бездротовий сегмент (гостьовий Wi-Fi).

Логіко-структурна архітектура мережі, що проєктується, базується на гібридному технологічному принципі. Вона інтегрує високошвидкісні провідні канали зв'язку структурованої кабельної системи (СКС) та гнучкі бездротові радіосегменти (Wi-Fi) в межах єдиного керованого інформаційного простору з чітким розмежуванням прав доступу за допомогою технології IEEE 802.1Q.

На основі вимог замовника та технічного завдання сформовано такі граничні швидкісні характеристики системи:

Провідний локальний сегмент (LAN): будується на базі мідного провідника категорії Cat.6 та керованих гігабітних комутаторах, що гарантує пропускну здатність на рівні 1000 Мбіт/с (1 Gbps Full Duplex) для кожної робочої станції та до 10 Gbps на магістральних аплінках.

Бездротовий радіосегмент (WLAN): розгортається на базі дволінійних точок доступу. Для застарілих портативних пристроїв у діапазоні 2.4 ГГц забезпечується базовий поріг швидкості від 150 Мбіт/с. Для сучасного клієнтського обладнання, що функціонує у швидкісному діапазоні 5 ГГц за стандартом IEEE 802.11ac (Wi-Fi 5), архітектурно закладається пікова пропускна здатність до 1000 Мбіт/с.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЄКТУ

2.1 Аналіз та обґрунтування вибору логічного типу мережі

Логічна топологія (архітектура) комп'ютерної мережі визначає правила, протоколи та фізичні маршрути, за якими здійснюється безпосередній обмін інформаційними кадрами та пакетами між кінцевими хостами, незалежно від їхнього фізичного розташування. Якщо фізична топологія описує геометрію прокладання кабельних трас Cat.6, то логічна структура регламентує розподіл потоків даних на канальному (L2) та мережевому (L3) рівнях моделі OSI.

1. Мережева модель взаємодії та централізація ресурсів

Відповідно до вимог технічного завдання щодо забезпечення централізованого керування, автентифікації користувачів та операційного контролю, для компанії «IT-M» обрано клієнт-серверну модель (Client-Server Architecture) організації логічної структури. На противагу децентралізованим одноранговим мережам (Peer-to-Peer), клієнт-серверна архітектура дозволяє:

- концентрувати критично важливі корпоративні сервіси на виділених обчислювальних потужностях (сервери Lenovo ThinkSystem ST50);
- реалізувати єдину політику безпеки та ієрархічного доступу до даних;
- рганізувати централізоване резервне копіювання інформаційних масивів.

У межах розробленої логічної структури інфраструктурний сервер S_1 функціонує як мережеве сховище спільного доступу. Для первинної авторизації співробітників та розмежування прав доступу до каталогів файлової системи застосовується метод мандатного/рольового контролю на основі унікальних облікових даних (ідентифікатор користувача та криптостійкий пароль), що задовольняє базові корпоративні стандарти інформаційної безпеки.

2. Периметральний шлюз, NAT та PPPoE-інтеграція

Логічний зв'язок між ізольованою внутрішньою мережею підприємства та зовнішнім адресним простором глобальної мережі Інтернет забезпечується сервером-шлюзом S_2. Основними логічними функціями шлюзу є:

- трансляція мережевих адрес (NAT/Masquerading): перетворення внутрішніх приватних IP-адрес із діапазону RFC 1918 у легітимну публічну адресу, надану провайдером;

- маршрутизація та фільтрація (Stateful Firewall), тобто динамічний аналіз стану з'єднань за допомогою підсистеми Netfilter/iptables, що дозволяє блокувати несанкціоновані зовнішні запити та здійснювати контекстний контент-менеджмент вихідного трафіку персоналу відповідно до службових інструкцій;

- інкапсуляція тунельних з'єднань, а саме термінація сесії з провайдером здійснюється за допомогою протоколу PPPoE (Point-to-Point Protocol over Ethernet), який забезпечує захищений автентифікований обмін пакетами через логічний тунель «точка-точка».

3. Логічна сегментація інфраструктури за допомогою VLAN

Для локалізації широкомовного трафіку, оптимізації смуги пропускання комутаторів D- та запобігання внутрішнім загрозам (перехопленню даних між відділами) у проєкті реалізовано технологію логічного структурування VLAN (Virtual Local Area Network) згідно зі стандартом IEEE 802.1Q.

Завдяки впровадженню VLAN фізично єдина кабельна мережа офісу розділяється на декілька ізольованих логічних сегментів (широкомовних доменів), закріплених за конкретними підрозділами (відділ розробки, бухгалтерія, адміністрація, гостьова Wi-Fi зона тощо). Прямий обмін даними між цими віртуальними мережами на канальному рівні (L2) заблокований - будь-яка міжсегментна взаємодія можлива виключно через інтерфейси маршрутизації центрального комутатора L3, де діють суворі правила списків контролю доступу (ACL).

Детальні графічні схеми логічного розподілу корпоративної мережі на віртуальні підмережі VLAN, карти розподілу IP-адрес, масок та інструментальні

параметри для конфігурування керованого комутаційного обладнання наведено у Додатку Б.

2.2 Розробка схеми фізичного розташування кабелів та вузлів

Архітектурний базис локальної обчислювальної мережі компанії «ІТ-М» розроблено відповідно до специфікацій сімейства стандартів Gigabit Ethernet (IEEE 802.3ab), що гарантує високу пропускну здатність та мінімальні затримки при міжсегментному обміні даними.

На рівні окремих структурних підрозділів (кабінетів та робочих зон) фізична структура мережі реалізована за топологією типу «зірка» (Star Topology), де кожен інженерний термінал окремою лінією витої пари Cat.6 підключається до периферійного комутатора доступу (робочої групи). Магістральний каркас підприємства загалом об'єднаний за топологією «розширена зірка» (Extended Star Topology), де всі комутатори робочих груп другого рівня підключені до центрального комутатора ядра L3 (, розміщеного в головній комутаційній шафі.

Головними перевагами впровадження розширеної зіркоподібної архітектури є висока відмовостійкість (локальне пошкодження кабелю або вихід з ладу одного клієнтського порту не порушує працездатність інших сегментів системи), простота адміністрування, зручність пошуку несправностей та високий модернізаційний потенціал.

Для забезпечення мобільності персоналу та підключення портативних пристроїв у межах офісу розгорнуто бездротовий сегмент (WLAN). Фізичне розміщення точок доступу повинно бути організовано за стільниковим принципом (Cellular Topology), що дозволяє сформувати суцільну зону покриття без «сліпих плям» та гарантує стабільний рівень сигналу в усіх робочих зонах.

Інтеграція провідної кабельної інфраструктури СКС та бездротового радіосегмента реалізується на базі єдиної гібридної фізичної топології. Це

забезпечує апаратну узгодженість, спрощує масштабування мережі та дозволяє централізовано керувати всіма потоками даних за допомогою комутаційного поля головного вузла зв'язку.

2.2.1 Типи кабельних з’єднань та їх прокладка

Проєктування та монтаж кабельної інфраструктури ЛОМ виконується для об'єкта, архітектурно-планувальні особливості якого наведено на графічній схемі «План приміщення». Компанія «ІТ-М» здійснює операційну діяльність у межах третього поверху багатоповерхової адміністративної будівлі на правах довгострокової оренди.

Фізичне трасування та прокладання ліній зв'язку реалізується комбінованим методом із використанням пластикових кабельних коробів (кабель-каналів) різного перерізу, стінових штроб та захисних гофрованих труб за простором підвісної стелі (армстронг). Основним фізичним середовищем передачі інформаційних сигналів обрано чотирипарний мідний кабель типу U/UTP (неекранована вита пара) категорії Cat.6.

Вибір даного типу провідника вимагає суворого дотримання технологічних нормативів під час монтажно-налагоджувальних робіт (дотримання граничних радіусів вигину кабелю, зусилля натягу при протяжці, допустимої довжини ліній до 90 метрів та правил сусідства з силовими лініями електропередач). Порушення цих інженерних вимог призводить до деградації сигналів, збільшення рівня перехресних наводок (NEXT), втрати пакетів, затримок трафіку та передчасного виходу з ладу пасивних компонентів СКС.

Для забезпечення системної цілісності та гарантованого досягнення швидкості 1000 Мбіт/с, усі елементи комутаційного тракту — включаючи горизонтальні магістралі, мережеві розетки RJ-45, патч-панелі в комутаційній шафі та гнучкі патч-корди для підключення хостів — суворо відповідають єдиному стандарту категорії 6 (стандарт TIA/EIA-568).

2.2.2 Будова вузлів та необхідність їх застосування

Центральним елементом телекомунікаційної інфраструктури компанії «ІТ-М» є головний комутаційний вузол (ГКВ), який апаратно реалізується на базі закритої 19-дюймової шафи місткістю 15U. Усередині цього вузла консолідуються ключові компоненти ядра мережі: магістральний комутатор L3 D-Link, два обчислювальні сервери Lenovo ThinkSystem ST50 та онлайн-джерело безперебійного живлення (ДБЖ) TECNOWARE. Головний вузол виконує роль координаційного центру всієї ЛОМ, вирішуючи такі інженерні завдання:

- структурування кабельних потоків за допомогою крос-панелей та організаторів;

- надійна механічна фіксація та захист активного заліза від вібрацій;

- підтримка штатного температурного режиму за рахунок інтегрованих блоків вентиляторів;

- розмежування і суворе обмеження фізичного доступу сторонніх осіб до серверного та комутаційного обладнання.

З метою мінімізації капітальних інвестицій на розгортання пасивної інфраструктури, оптимізації загальної довжини кабельних трас та з огляду на порівняно невелику кількість кінцевих хостів, у проєкті не передбачено створення проміжних (поверхових) комутаційних вузлів.

Периферійні комутатори робочих груп (L2-керовані пристрої D-Link на 8 та 16 портів) інсталюються безпосередньо всередині відповідних функціональних підрозділів (відділів). Їх монтаж виконується настінним або настільним методом у спеціально відведених, безпечних та легкодоступних для проведення регламентного сервісного обслуговування місцях.

Аналогічним чином здійснюється настінно-стельовий монтаж бездротових точок доступу MikroTik cAP ac. Координати їх встановлення розраховані з урахуванням діаграми спрямованості інтегрованих всеспрямованих антен (Omni-directional), що дозволяє сформувати рівномірне радіопокриття робочого

простору, нівелювати ефект затухання сигналів від міжкімнатних перегородок та гарантувати стабільну швидкість передачі даних.

2.3 Обґрунтування вибору обладнання для проєкту мережі

При розгортанні бездротового сегмента інфраструктури точка доступу (Access Point) виконує функцію медіаконвертера та логічного мосту між провідним середовищем СКС і радіоефіром. З огляду на широкий асортимент телекомунікаційного обладнання на ринку, було проведено аналіз їхніх тактико-технічних характеристик. У додатку Б наведено порівняльну таблицю техніко-економічних параметрів сучасних моделей бездротових точок доступу.

За результатами аналізу, враховуючи обов'язкову підтримку стандарту IEEE 802.11ac, роботу в двох діапазонах (2.4/5 ГГц) та оптимальний баланс вартості й системної функціональності, для реалізації проєкту обрано точки доступу MikroTik cAP ac (RBcAPGi-5acD2nD) [14]. Зовнішній вигляд цього пристрою проілюстровано на рисунку 2.1.

Рисунок 2.1 –Точка wi-fi доступу Mikrotik RBcAPGi-5acD2nD

Дана точка доступу латвійського виробництва вирізняється високою відмовостійкістю операційної системи RouterOS, стабільністю радіопередачі та підтримкою апаратного шифрування, що робить її інтеграцію повністю доцільною. Конструкція корпусу передбачає два типи інсталяції - горизонтальну

(на стельові панелі) та вертикальну (на стіни), що гарантує адаптивність монтажу до архітектури офісу. Схеми фіксації пристрою наведено на рисунку 2.2.

Рисунок 2.2 – Варіанти монтажу точки доступу Mikrotik RBcAPGi

Центральним комутаційним вузлом локальної мережі стандарту Gigabit Ethernet виступає магістральний комутатор ядра (Core Switch). Цей керований пристрій здійснює високоефективну пакетну комутацію на канальному рівні (L2) та апаратну маршрутизацію на мережевому рівні (L3). Він відповідає за логічне ізолювання віртуальних підмереж VLAN, балансування трафіку між структурними відділами компанії та перенаправлення агрегованих потоків даних до прикордонного шлюзу безпеки для виходу в глобальну мережу Інтернет.

Детальний порівняльний аналіз технічних характеристик та функціональних можливостей різних моделей комутаторів наведено в додатку В.

У якості центрального пристрою ядра комутації в даному проєкту застосовано високопродуктивний керований комутатор L3-рівня D-Link DGS-3130-30TS.. З огляду на солідний запас продуктивності, наявність 24 гігабітних портів RJ-45 та 6 магістральних портів 10G SFP+, а також високу стабільність

роботи, повторна інтеграція цього комутатора в нову топологію є повністю виправданою. Загальний вигляд комутаційного пристрою ядра представлено на рисунку 2.3 [12].

Рисунок 2.3 – Загальний вигляд центрального комутатора ядра D-Link DGS-3130-30TS

Відповідно до розробленої топології «розширена зірка», для агрегації трафіку в межах великих структурних підрозділів (відділів) передбачено інтеграцію керованих комутаторів рівня доступу. Результати їх техніко-економічного аналізу також акумульовано в додатку В.

Для робочої групи з високою щільністю хостів обрано 16-портовий Smart-комутатор D-Link DGS-1100-16. Цей пристрій також є частиною наявного парку обладнання фірми. Завдяки підтримці тегування трафіку (IEEE 802.1Q VLAN), наявності базових функцій захисту та оптимізації смуги пропускання, його використання залишається раціональним [16].

Для кабінетів та відділів із меншою кількістю робочих станцій передбачено встановлення 8-портових моделей D-Link DGS-1100-08. Вони виступають конструктивними аналогами 16-портової версії, зберігають ідентичний інтерфейс керування та мережевий функціонал, але адаптовані під меншу кількість абонентських підключень. Зовнішній вигляд комутаторів доступу серії DGS-1100 проілюстровано на рисунку 2.4.

Рисунок 2.4 – Комутатори рівня доступу серії D-Link DGS-1100 (модифікації на 5 - 24 портів)

Для надійної фіксації активних і пасивних телекомунікаційних компонентів, структурування кабельних потоків СКС та організації єдиного координаційного центру мережі в межах цього проєкту передбачено встановлення настінної комутаційної шафи корисної місткістю 15U.

Відповідно до критеріїв механічної міцності, ефективності природної та примусової вентиляції, а також раціонального розподілу внутрішнього простору, обрано двосекційну розбірну модель UA-MGSWA155 вітчизняного виробництва (серія MGSWA від УХЛ-МАШ). Конструктивне виконання даної оболонки повністю задовольняє вимогам міжнародного стандарту IEC 297 (щодо розміщення 19-дюймового заліза) та діючого ДСТУ 3041-95.

Конструкція шафи оснащена перфорованими знімними бічними панелями на замках для оперативного сервісного доступу та передніми дверима із загартованого скла в металевій рамі, що дозволяє здійснювати візуальний моніторинг індикаторів комутаторів D-Link та серверів без порушення контуру безпеки. Зовнішній вигляд обраної комутаційної шафи проілюстровано на рисунку 2.5 [22].

Рисунок 2.5 – Комутаційна шафа

Для забезпечення ергономічного розміщення апаратних засобів, структурування ліній зв'язку та комплексного облаштування головного комутаційного вузла всередині захисної шафи передбачено інтеграцію пасивного мережевого обладнання: патч-панелей і горизонтальних кабельних організаторів. Впровадження цих елементів дозволяє систематизувати комутаційні шнури, мінімізувати механічні навантаження на інтерфейси пристроїв, суттєво спростити проведення регламентних робіт системними адміністраторами та гарантувати високу надійність кабельної інфраструктури компанії «IT-M».

Обчислювальне ядро локальної мережі архітектурно розподілено між двома автономними серверами:

Перший сервер (S_1) - виділений інфраструктурний вузол, що функціонує як корпоративне файлове сховище (NAS/File Server), а також забезпечує роботу локальних служб (DNS, DHCP, моніторинг) у межах віртуалізації Proxmox VE.

Другий сервер (S_2) - прикордонний шлюз безпеки (Edge Gateway under Fedora OS), призначений для міжмережевого екранування, маршрутизації

транзитного трафіку користувачів (VLAN 11–20) та організації PPPoE-сесії з провайдером для виходу в глобальну мережу Інтернет.

Детальний порівняльний аналіз альтернативних серверних платформ та обґрунтування обраної конфігурації представлено в додатку в.

Обидва апаратні вузли (S_1 та S_2) реалізовано на базі сучасних та надійних серверів у форм-факторі Tower - Lenovo ThinkSystem ST50, внутрішню компоновку та архітектуру материнської плати яких проілюстровано на рисунку 2.6 [21].

Дана серверна платформа була обрана завдяки оптимальному балансу обчислювальної потужності (підтримка процесорів Intel Xeon), високій стабільності під інтенсивними навантаженнями, наявності швидкісних інтерфейсів (SATA 6Gb, M.2 NVMe) та гнучким можливостям масштабування дискової підсистеми і оперативної пам'яті (до 4-х слотів DIMM). Крім того, з огляду на калькуляцію витрат, капіталовкладення в обладнання Lenovo є повністю економічно виправданими, оскільки за технічними характеристиками та показниками відмовостійкості воно суттєво випереджає конкурентні рішення аналогічного класу при збереженні прийнятної ринкової вартості.

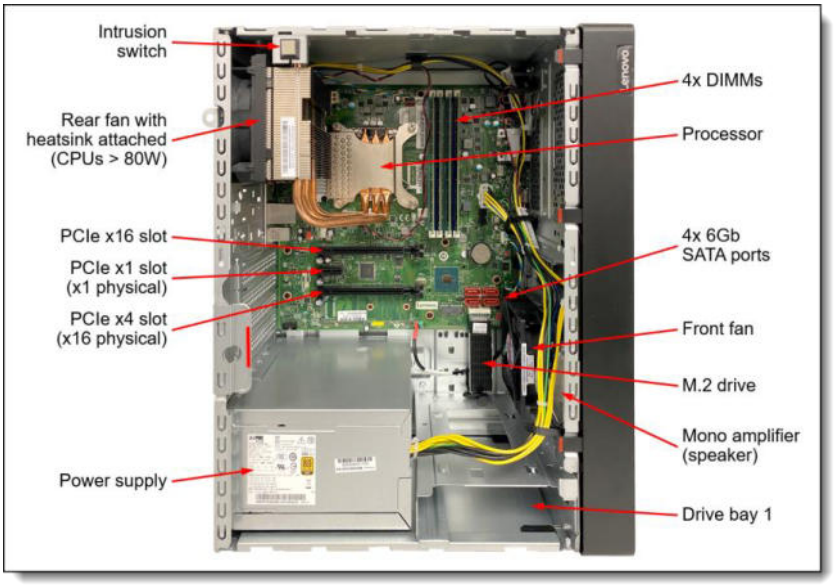


Рисунок 2.6 – Розміщення компонент в корпусі серверу LENOVO ST50

В таблиці 2.1 наведено перелік обладнання та інших мсатеріальних засобів для проєкту мережі

Таблиця 2.1 – Активне та пасивне обладнання

№ з/п	Перелік обладнання та інших матеріальних засобів	Один. виміру	Факт. використано	Ціна за шт., грн.	Загальна сума, грн.
1	Комутаційна шафа 15U (комплект з полками та блоком розеток UA-MGSWA155)	шт.	1	12500,00	12500,00
2	Патч-панель на 24 порти, Cat.6 (19", 1U)	шт.	1	2400,00	2400,00
3	Патч-корди UTP Cat. 6 (1.5 м / 3 м)	шт.	80	65,00	5200,00
4	ДБЖ (UPS) TECNOWARE EVO DSP-3 (або аналог On-Line 2000VA)	шт.	1	32000,00	32000,00
5	Короби пластикові для кабелю (різного січення)	м	120	85,00	10200,00
6	Ethernet-кабель UTP cat.6 (бухта 305 м, мідь)	бухта	2	6200,00	12400,00
7	Розетка мережева RJ-45 внутрішня/зовнішня під cat.6	шт.	50	175,00	8750,00
8	Комутатор центральний L3 D-Link DGS-3130-30TS	шт.	1	31500,00	31500,00
9	Комутатор керований D-Link DGS-1100-16	шт.	2	5800,00	11600,00
10	Комутатор керований D-Link DGS-1100-08	шт.	3	3100,00	9300,00
11	Точка доступу Wi-Fi MikroTik cAP ac (RBcAPGi-5acD2nD)	шт.	2	3400,00	6800,00
12	Сервер ЛОМ LENOVO ThinkSystem ST50 (Xeon/32GB RAM/RAID)	шт.	2	82000,00	164000,00
	РАЗОМ				306650,00

У результаті сумарного підрахунку вартості обладнання та матеріально-технічного забезпечення загальна сума становить 306650,00 грн, що входить в бюджет замовника.

2.4 Особливості монтажу мережі

Базовим технічним орієнтиром для побудови СКС виступає стандарт TIA/EIA-568-B, який прийшов на зміну TIA/EIA-568-A. Цей набір стандартів регламентує порядок встановлення телекомунікаційних систем усередині будівель, у тому числі правила підключення провідників до конекторів типу 8P8C, згідно зі схемами T568A і T568B, що широко застосовуються в мережах Ethernet [19].

Процес створення локальної мережі включає два основні етапи: розробку логічної структури комп'ютерної системи та побудову кабельної інфраструктури. У загальному вигляді LAN (локальна мережа) поєднує структуровану кабельну систему та мережеві компоненти — сервери, комп'ютери та периферійні пристрої, які функціонують як вузли мережі.

При організації кабельної частини слід передбачити можливість зміни кількості пристроїв протягом терміну експлуатації мережі. Важливо закласти резерви, що дозволять збільшити кількість підключень щонайменше на 50%, не вдаючись до повної перебудови інфраструктури. Для цього доцільно:

- забезпечити надлишкову пропускну здатність каналів передачі;
- залишити вільні порти на комутаторах;
- використовувати мережеві кабелі відповідного класу для високошвидкісного обміну даними.

Для досягнення стабільної та тривалої роботи системи важливо дотримуватись вимог до монтажу горизонтальної підсистеми. Серед основних заходів:

- практика використання якісних кабелів, здатних підтримувати сучасні швидкості передавання даних;
- використання сертифікованих елементів СКС;
- дотримання безпечної відстані від джерел електромагнітного впливу.

Крім того, актуальним є питання резервування - наявність дублюючих елементів мережі дозволяє значно знизити ризики відмов і зменшити витрати на обслуговування у перспективі. Хоча реалізація таких рішень на етапі впровадження може вимагати додаткових інвестицій, це забезпечує стабільність роботи всієї системи.

Передавання даних у мережі здійснюється через неекрановану виту пару шостої категорії (UTP Cat.6). Прокладаючи кабельні маршрути, необхідно дотримуватись нормативів монтажу, зокрема:

- витримувати мінімальні відстані від електромереж (не менше 50 см);
- уникати паралельного прокладання інформаційних і силових ліній без екранів або розділювальних елементів;
- користуватись кабельними трасами відповідно до чинних технічних стандартів.

Усі роботи з інсталяції мають відповідати вимогам EN 50174-2, який визначає правила сумісного прокладання мережевих та електричних кабелів, а також надає рекомендації щодо безпечної організації кабельного простору.

2.5 Обгрунтування вибору програмного забезпечення

У процесі підбору відповідного програмного забезпечення для побудови інформаційної інфраструктури компанії були визначені ключові вимоги, серед яких: відкритість, економічність, стабільність, функціональність і безпека.

Операційна система Linux задовольняє зазначені критерії та має низку переваг порівняно з іншими ОС, зокрема [20]:

- Відкритий вихідний код. Linux є системою з відкритим програмним кодом, що дає можливість вільно переглядати, модифікувати, адаптувати й розповсюджувати її відповідно до потреб користувача чи організації. Це дозволяє гнучко налаштовувати систему під конкретні задачі.

- Безоплатна ліцензія. Linux поширюється безкоштовно, що суттєво знижує загальну вартість впровадження інформаційних технологій та забезпечує економічно ефективне розгортання робочих місць і серверної інфраструктури.

Для клієнтських машин було обрано дистрибутив Linux Fedora 37 Workstation, що забезпечує стабільну та надійну роботу, водночас усі версії Fedora мають високий рівень сумісності.

На серверному рівні використовується Fedora 37 Server x64 OS для реалізації функціоналу файлового сервера та шлюзу до мережі Інтернет. Обраний дистрибутив дозволяє без труднощів розгортати необхідні мережеві сервіси, підтримує гнучку систему управління пакетами та має ефективний механізм оновлення.Ключові характеристики Fedora 37 Server [20]:

- функціональність міжмережевого екрану з фільтрацією за рівнями OSI: канальний, мережевий та транспортний;

- система автоматичного оновлення програмного забезпечення та, що дуже важливо, конфігурацій;

- інструменти для локального та віддаленого моніторингу апаратного стану (top, vmstat, uptime, ps, free, iostat, sar, mpstat);

- засоби аналізу та моніторингу мережевого трафіку, з можливістю перегляду пакетів на всіх мережевих інтерфейсах.

Таким чином обрані рішення відповідають вимогам стабільності, безпеки, масштабованості та зручності в адмініструванні.

2.6 Тестування та налагодження локальної мережі

Детальніше опишемо процедуру встановлення та тестування СКС. Монтаж структурованої кабельної системи (СКС) є відносно нескладною задачею за умови дотримання чинних стандартів і технічних рекомендацій. Якщо інсталяційні роботи виконані якісно, це гарантує надійність та довговічність побудованої мережі. Перевірка працездатності локальної мережі здійснюється у кілька етапів, що дозволяє комплексно оцінити її функціонування.

Основні етапи тестування мережі [2]:

- Фізичний рівень перевірки. Спершу оцінюється стан фізичної інфраструктури мережі: кабелі, роз'єми, комутатори та інше обладнання. Для цього застосовують спеціалізовані кабельні тестери, які дозволяють виявити обриви, замикання або порушення послідовності пар.

- Налаштування параметрів. Після перевірки фізичних з'єднань виконується конфігурація мережевих пристроїв: хостам призначаються IP-адреси, маски підмережі, шлюзи, DNS-сервери тощо.

- Тестування зв'язку. Далі перевіряється взаємодія між пристроями в мережі. Найпростішим методом є використання команди ping, яка дозволяє виявити втрату пакетів або затримки у передачі.

- Аналіз пропускної здатності. Для визначення продуктивності мережі використовують програмні утиліти або апаратні аналізатори трафіку, що генерують значний обсяг даних і вимірюють час їх передавання.

- Оцінка рівня безпеки. Один із найважливіших етапів — перевірка інформаційної безпеки мережі. Проводиться сканування на наявність незахищених портів, слабких паролів, несанкціонованих підключень, вразливостей. У цьому допомагають як спеціалізовані ПЗ, так і апаратні засоби.

Також розкриємо тпові проблеми в роботі локальної мережі. У процесі експлуатації ЛОМ можуть виникати різні порушення, що впливають на її стабільність та ефективність. Проблеми умовно поділяють на три категорії:

1. Фізичні збої. Сюди належать ушкодження кабельної інфраструктури, вихід з ладу мережевих карт, портів комутаторів або маршрутизаторів, а також порушення контактів у з’єднаннях.

2. Перевантаження мережі. Виникає, коли пристрої не справляються з потоком даних - через надмірну кількість підключень, неправильну конфігурацію або зовнішні атаки, наприклад, DDoS.

3. Програмні помилки. Можуть бути спричинені конфліктами в налаштуваннях мережевих протоколів, некоректним програмним забезпеченням або оновленням системи.

Для забезпечення стабільної роботи мережі необхідний постійний моніторинг, своєчасна діагностика та профілактичне обслуговування. Використання відповідних методик та інструментів дозволяє виявляти й усувати проблеми ще на етапі їх виникнення, мінімізуючи ризики простою або втрати даних.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Розробка інструкцій з налаштування ПЗ серверів

3.1.1 Інструкції з налаштування файлового сервера

Згідно з технічним завданням, для організації централізованого, швидкого та безпечного обміну файлами та зберігання інформаційних ресурсів компанії «IT-M» на базі локального сервера S_1 (IP-адреса 192.168.18.253 у межах VLAN 18) розгорнуто службу файлового обміну. Як програмну платформу обрано FTP-сервер ProFTPD, який відрізняється високою гнучкістю налаштування, модульною архітектурою та низькими вимогами до системних ресурсів.

Для захисту конфіденційних корпоративних даних від перехоплення в процесі автентифікації та передачі текстових чи бінарних потоків, стандартний незахищений протокол FTP модернізовано шляхом інтеграції криптографічного розширення FTPS (FTP over TLS) за допомогою бібліотек OpenSSL.

Процес розгортання та захисту файлового сховища на ОС Fedora Server реалізовано за такими етапами.

Етап 1. Встановлення програмного забезпечення

Оскільки пакет ProFTPD міститься в репозиторіях розширення EPEL, спочатку активуємо необхідне джерело пакетів, після чого виконуємо інсталяцію демона та інструментів генерації сертифікатів:

Bash

sudo dnf install -y epel-release

sudo dnf install -y proftpd openssl

Етап 2. Генерація криптографічних ключів та SSL/TLS сертифіката

Для шифрування сесій згенеруємо унікальний самопідписаний X.509 сертифікат безпеки строком дії на 365 днів та закритий ключ RSA розрядністю 2048 біт:

Bash

```
# Створення захищеної директорії для сертифікатів
sudo mkdir -p /etc/proftpd/ssl/
# Генерація пари ключів без парольної фрази (-nodes) для автоматичного старту служби
sudo openssl req -new -x509 -days 365 -nodes \
  -out /etc/proftpd/ssl/proftpd.cert.pem \
  -keyout /etc/proftpd/ssl/proftpd.key.pem
```

Для забезпечення безпеки обмежуємо права доступу до створеного приватного ключа: sudo chmod 600 /etc/proftpd/ssl/proftpd.key.pem.

Етап 3. Базова конфігурація та ізоляція користувачів

Головний конфігураційний файл у системі Fedora Server розташований за шляхом /etc/proftpd.conf. Відкриваємо його для редагування: sudo nano /etc/proftpd.conf та вносимо фундаментальні параметри безпеки:

Plaintext

```
ServerName                  "Corporate FTPS Server IT-M"
ServerType                  standalone
DefaultServer               on
# Ізоляція користувачів (Chroot) — обмеження доступу межами домашнього каталогу (~),
# що унеможливлює вихід користувача в корінь операційної системи
DefaultRoot                 ~
# Вимкнення зворотного пошуку DNS для прискорення процесу підключення клієнтів
IdentLookups                off
UseReverseDNS               off
# Робота з протоколом IPv6 вимикається за відсутності потреби
UseIPv6                     off
```

Етап 4. Активація криптографічного модуля TLS

Для чистоти архітектури винесемо налаштування шифрування в окремий файл, розкоментувавши або додавши в кінець /etc/proftpd.conf директиву: Include /etc/proftpd/tls.conf.

Далі створюємо файл конфігурації TLS (sudo nano /etc/proftpd/tls.conf) з такими параметрами, що відповідають сучасним стандартам безпеки:

Plaintext

<IfModule mod_tls.c>

TLSEngine on

TLSLog /var/log/proftpd/tls.log

Використовуємо лише стійкі версії протоколів (заборона застарілих SSLv2, SSLv3 та TLSv1.0)

TLSProtocol TLSv1.2 TLSv1.3

TLSOptions NoCertRequest EnableDiags

Шляхи до згенерованих сертифікатів та ключів

TLSRSACertificateFile /etc/proftpd/ssl/proftpd.cert.pem

TLSRSACertificateKeyFile /etc/proftpd/ssl/proftpd.key.pem

TLSVerifyClient off

Вимога обов'язкового використання TLS для автентифікації та передачі даних

TLSRequired on

</IfModule>

Етап 5. Конфігурування гостьового (анонімного) доступу

Для публічного скачування загальних документів чи дистрибутивів налаштовується ізольована директорія з обмеженням прав на запис:

Plaintext

<Anonymous /var/ftp/public>

User ftp

Group ftp

UserAlias anonymous ftp

```
    RequireValidShell         off
    MaxClients                10 "Вибачте, досягнуто ліміту підключень."
      # Заборона будь-яких операцій модифікації даних для анонімних користувачів
    <Limit WRITE>
      DenyAll
    </Limit>
</Anonymous>
```

Створюємо цільовий каталог: sudo mkdir -p /var/ftp/public та передаємо права системному користувачу: sudo chown -R ftp:ftp /var/ftp/public.

Етап 6. Інтеграція правил фільтрації у міжмережевий екран

Для проходження FTP-трафіку крізь локальний фаєрвол сервера S_1, відкриваємо керуючі порти 20, 21, а також виділений діапазон пасивних портів за допомогою утиліти iptables:

Bash

```
# Дозвіл вхідних запитів на стандартний порт ініціалізації FTP сесії
sudo iptables -A INPUT -p tcp --dport 21 -j ACCEPT
# Дозвіл для каналу передачі даних у пасивному режимі
sudo iptables -A INPUT -p tcp --dport 20 -j ACCEPT
```

Етап 7. Управління службою та автоматизація автозапуску

Замість застарілих скриптів ініціалізації, сучасне середовище Fedora використовує системний менеджер systemd. Реєструємо службу в автозавантаженні системи та здійснюємо її первинний пуск:

Bash

```
sudo systemctl enable proftpd
sudo systemctl start proftpd
```

Для моніторингу статусу працездатності демона та відслідковування активних підключень використовується команда: sudo systemctl status proftpd. У

випадку виникнення помилок авторизації аналізується спеціалізований лог-файл: tail -f /var/log/proftpd/tls.log.

3.1.2 Інструкції з налаштування шлюза під керуванням ОС Fedora Server

У проєктованій мережі компанії «IT-M» реалізовано дворівневу схему маршрутизації, що забезпечує максимальну продуктивність та безпеку інфраструктури. Розподіл функцій маршрутизації організовано за таким принципом:

Внутрішній трафік (Inter-VLAN): Комутацію та маршрутизацію пакетів між віртуальними мережами різних підрозділів (VLAN 11–17, 19, 20) здійснює високопродуктивний керований комутатор 3-го рівня (L3) D-Link DGS-3130-30TS (SW_4). Для кожної віртуальної мережі на комутаторі піднято відповідні інтерфейси (SVI), які виступають шлюзами за замовчуванням (наприклад, 192.168.11.254 для менеджерів, 192.168.19.254 для розробників тощо).

Зовнішній трафік (Internet): Весь трафік, який спрямований поза межі корпоративної мережі, комутатор SW_4 через статичний маршрут за замовчуванням (0.0.0.0/0) перенаправляє на внутрішній інтерфейс сервера-шлюзу S_2 (192.168.18.254).

Програмний шлюз на базі ОС Fedora Server виконує функції периферійного міжмережевого екрана (Firewall) та здійснює трансляцію адрес (NAT) для захисту внутрішнього адресного простору [13].

Структуру побудови та логіку взаємодії елементів мережевого периметра ілюструє рисунок 3.1, на якому представлено функціональну схему інкапсуляції PPPoE-з’єднання. Наведена схема наочно демонструє процес двонаправленого транзиту даних між ізольованими сегментами внутрішньої локальної мережі (LAN) та глобальною мережею Інтернет (WAN) крізь розгорнутий програмний шлюз безпеки.

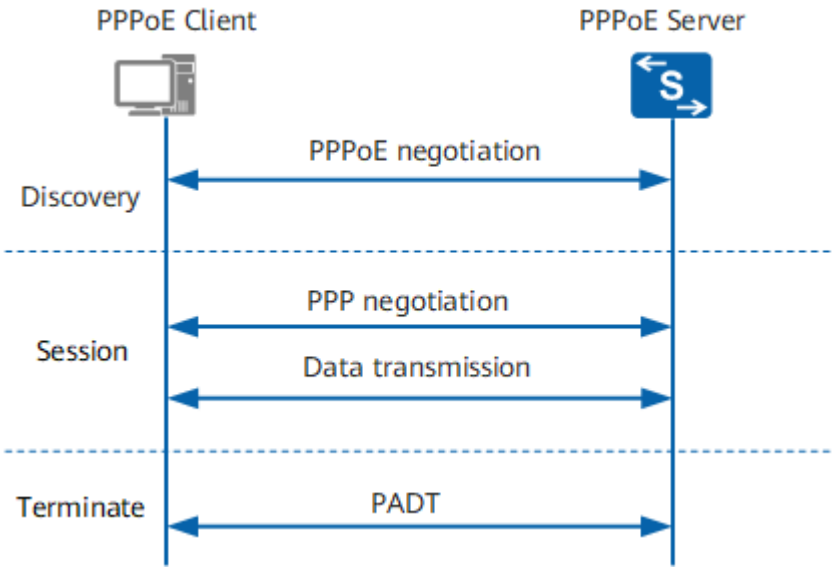


Рисунок 3.1 – Схема інкапсуляції та взаємодії PPPoE з’єднання

Мережеві інтерфейси шлюзу S_2 мають такі параметри конфігурації:

Внутрішній інтерфейс (LAN, пристрій eth0): підключений до порту комутатора SW_4 у межах VLAN 18 (Відділ комп'ютерного забезпечення). Йому призначено статичну IP-адресу 192.168.18.254/24.

Зовнішній інтерфейс (WAN, пристрій ppp0): віртуальний інтерфейс, який ініціалізує захищене PPPoE-з'єднання з обладнанням провайдера, проходячи автентифікацію за протоколом CHAP, та отримує динамічну зовнішню IP-адресу.

Нижче наведено лістинг автоматизованого скрипта myinet, який забезпечує базовий захист сервера, активує механізм маскарадингу для всієї корпоративної супермережі 192.168.0.0/16 та налаштовує Netfilter (iptables).

Bash

```
#!/bin/bash
# Скрипт ініціалізації міжмережевого екрана Edge Gateway на базі Fedora Server
# Функція динамічного визначення поточної WAN IP-адреси
get_wan_ip() {
    local iface=$1
```

```
    ip addr show "$iface" 2>/dev/null | grep 'inet ' | awk '{print $2}' | cut -d/ -f1
}
# Оголошення інтерфейсів
EXT_IF="ppp0"       # Інтернет-інтерфейс (PPPoE сесія)
INT_IF="eth0"       # Локальний інтерфейс (VLAN 18)
# Оголошення адресних просторів
LOCAL_SUPERNET="192.168.0.0/16"  # Охоплює всі підмережі компанії (VLAN 11-20)
LOOPBACK="127.0.0.1"
# Отримання поточної IP-адреси від провайдера
WAN_IP=$(get_wan_ip $EXT_IF)
# Динамічне завантаження модулів ядра для роботи підсистеми Netfilter
/sbin/depmod -a
for module in ip_tables iptable_filter iptable_nat iptable_mangle nf_conntrack nf_conntrack_ftp nf_nat_ftp xt_MASQUERADE xt_LOG xt_limit xt_REJECT; do
    /sbin/modprobe $module 2>/dev/null
done
# Оптимізація та захист параметрів ядра через sysctl
echo 1 > /proc/sys/net/ipv4/ip_forward                  # Дозвіл форвардингу транзитних пакетів
echo 1 > /proc/sys/net/ipv4/tcp_syncookies              # Захист від атаки SYN-Flood
# Захист від IP-спуфінгу та ігнорування редиректів
for file in /proc/sys/net/ipv4/conf/*/rp_filter; do echo 1 > "$file"; done
for file in /proc/sys/net/ipv4/conf/*/accept_redirects; do echo 0 > "$file"; done
for file in /proc/sys/net/ipv4/conf/*/accept_source_route; do echo 0 > "$file"; done
# Повне очищення існуючих таблиць та ланцюжків правил
/sbin/iptables -F
```

```
/sbin/iptables -X
/sbin/iptables -t nat -F
/sbin/iptables -t nat -X
# Встановлення загороджувальної політики за замовчуванням (DROP)
/sbin/iptables -P INPUT DROP
/sbin/iptables -P OUTPUT DROP
/sbin/iptables -P FORWARD DROP
# --- Вхідний трафік (INPUT) ---
# Блокування некоректних пакетів без прапора SYN
/sbin/iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
# Дозвіл локального інтерфейсу зворотного зв'язку
/sbin/iptables -A INPUT -i lo -j ACCEPT
# Дозвіл вхідного трафіку з локальної мережі компанії через INT_IF
/sbin/iptables -A INPUT -i $INT_IF -s $LOCAL_SUPERNET -j ACCEPT
# Дозвіл вхідних пакетів для вже встановлених з'єднань із зовнішнього світу
/sbin/iptables -A INPUT -i $EXT_IF -m state --state ESTABLISHED,RELATED -j ACCEPT
# Дозвіл діагностичних пакетів ICMP (ping)
/sbin/iptables -A INPUT -p icmp -j ACCEPT
# --- Вихідний трафік самого шлюзу (OUTPUT) ---
/sbin/iptables -A OUTPUT -o lo -j ACCEPT
/sbin/iptables -A OUTPUT -o $INT_IF -j ACCEPT
/sbin/iptables -A OUTPUT -o $EXT_IF -j ACCEPT
# --- Транзитний трафік (FORWARD) ---
# Дозвіл проходження пакетів з корпоративної мережі назовні в Інтернет
/sbin/iptables -A FORWARD -i $INT_IF -o $EXT_IF -s $LOCAL_SUPERNET -j ACCEPT
# Дозвіл зворотного інтернет-трафіку (відповіді на запити користувачів)
```

/sbin/iptables -A FORWARD -i $EXT_IF -o $INT_IF -m state --state ESTABLISHED,RELATED -j ACCEPT

Дозвіл транзитного проходження службових повідомлень ICMP

/sbin/iptables -A FORWARD -p icmp -j ACCEPT

--- Трансляція адрес (NAT / MASQUERADE) ---

Динамічне маскування адрес локальної мережі під поточну зовнішню IP-адресу тунелю ppp0

/sbin/iptables -t nat -A POSTROUTING -s $LOCAL_SUPERNET -o $EXT_IF -j MASQUERADE

Для інтеграції розробленого рішення у системне середовище Fedora Server створюється автоматизована служба systemd (/etc/systemd/system/myinet.service), яка виконує скрипт під час завантаження системи, що гарантує миттєве відновлення політик безпеки та працездатності NAT після перезапуску сервера шлюзу.

3.1.3 Інструкції з налаштування серверної віртуалізації засобами Proxmox

Для оптимізації використання обчислювальних потужностей, підвищення відмовостійкості та гнучкості управління корпоративними сервісами компанії «IT-M» впроваджено технологію апаратної віртуалізації. Як базову платформу обрано Proxmox Virtual Environment (Proxmox VE).

Proxmox VE — це відкрита система віртуалізації корпоративного рівня на базі дистрибутиву Debian GNU/Linux, яка поєднує в собі два типи віртуалізації:

KVM (Kernel-based Virtual Machine) — для повноцінної апаратної віртуалізації операційних систем (наприклад, Fedora Server);

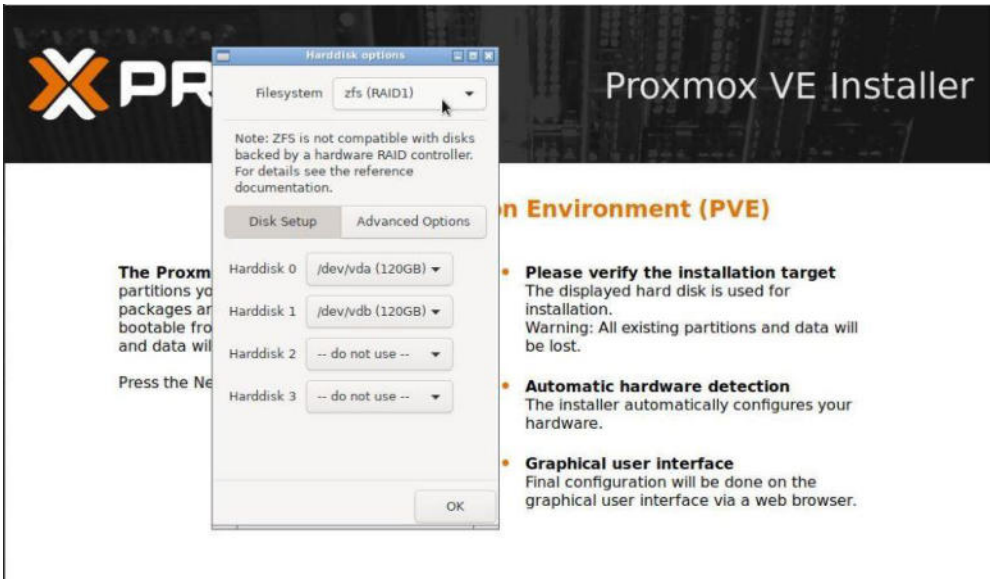
LXC (Linux Containers) — для легковагової контейнеризації ізольованих служб та додатків.

Використання Proxmox VE дозволяє відмовитися від дороговартісних ліцензій proprietary-рішень (VMware vSphere, Microsoft Hyper-V) без втрати функціональності. Гіпервізор розгортається безпосередньо на «голому залізі» (Bare Metal) сервера Lenovo ThinkSystem ST50 (S_1), дискова підсистема якого попередньо об'єднана в апаратний або надійний програмний RAID-масив для забезпечення цілісності даних.

Процесс інсталяції та первинного конфігурування складається з таких логічних етапів:

Етап 1. Первинна інсталяція ядра гіпервізора

Завантаження сервера здійснюється з підготовленого носія з ISO-образом Proxmox VE. На початковому екрані (див. рис. 3.2) обирається режим графічного встановлення Install Proxmox VE (Graphical).



Рисуноку 3.2 – Перший етап - встановлення гіпервізора Proxmox

На наступних кроках майстра інсталяції виконуються такі налаштування:

Вибір цільового накопичувача: Вказується масив (наприклад, /dev/sda), куди буде встановлено завантажувач та файлову систему (ext4 або ZFS).

Локалізація: Задається країна (Ukraine), часовий пояс (Europe/Kyiv) та розкладка клавіатури.

Обліковий запис: Встановлюється пароль суперкористувача (root) та вводиться контактна адреса електронної пошти адміністратора для отримання системних сповіщень.

Етап 2. Конфігурування мережевих параметрів та верифікація даних

На відміну від звичайних ОС, Proxmox VE потребує обов'язкового задання статичних мережевих параметрів під час інсталяції. Згідно з планом адресації для сервера S_1, вказуються такі дані:

Management Interface: Фізичний гігабітний адаптер сервера.

Hostname (FQDN): pve.it-m.local

IP Address: 192.168.18.253

Netmask: 255.255.255.0 (/24)

Gateway: 192.168.18.254 (IP-адреса нашого шлюзу S_2)

DNS Server: 192.168.18.254 або зовнішній DNS провайдера.

Перед фінальним запуску копіювання файлів відкривається підсумкове вікно Summary (див. рис. 3.3), де адміністратор зобов'язаний ретельно перевірити коректність конфігурації. Після підтвердження система форматує диски та розгортає пакети гіпервізора.

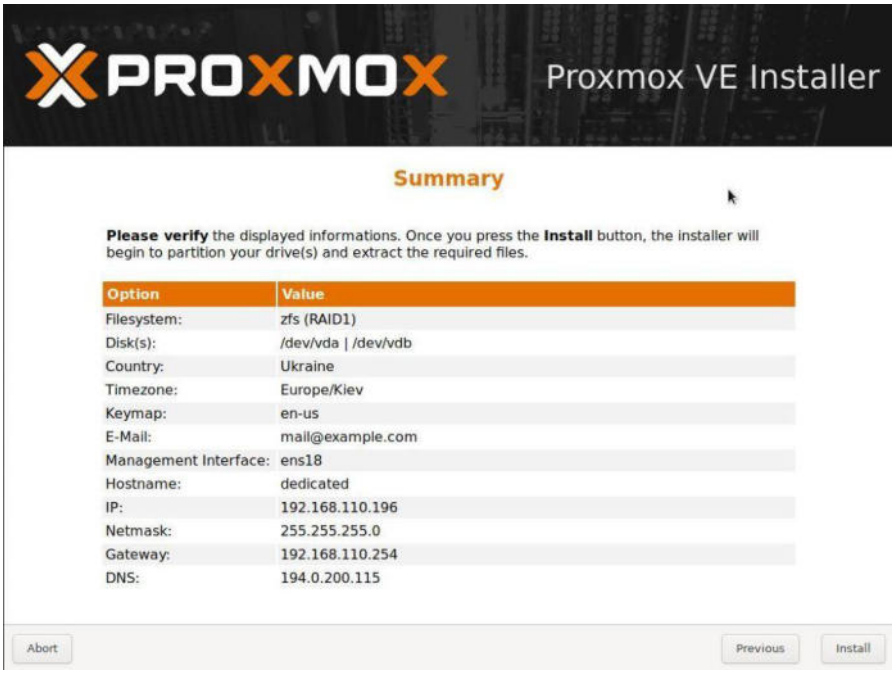


Рисунок 3.3 – Вікно загальних налаштувань (Summary)

Етап 3. Пост-інсталяційне налаштування сховища через веб-інтерфейс

Після автоматичного перезавантаження керування гіпервізором переходить у веб-панель за адресою https://192.168.18.253:8006. Авторизація виконується під обліковим записом root.

Першочергово проводиться налаштування та розподіл локального сховища даних (Storage), як показано на рисунку 3.4.

Директорія local (файлове сховище) використовується для зберігання ISO-образів операційних систем, шаблонів контейнерів (LXC) та резервних копій (vzdump).

Пул local-lvm (або ZFS простір) виділяється виключно під розміщення віртуальних дисків (raw, qcow2) майбутніх віртуальних машин для забезпечення максимальної швидкості операцій I/O (вводу-виводу).

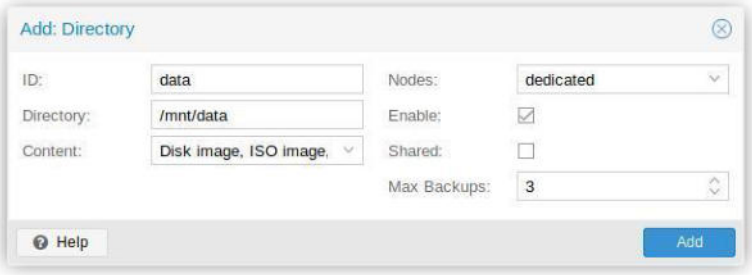


Рисунок 3.4 – Локація сховища даних та розподіл дисків

Етап 4. Налаштування мережевих інтерфейсів віртуального середовища

Для забезпечення комунікації майбутніх віртуальних машин із корпоративною мережею та між собою, у розділі System -> Network налаштовується віртуальний міст vmbr0 (Virtual Bridge), що діє як програмний комутатор (див. рис. 3.5).

Оскільки наша мережа побудована на базі 10 різних VLAN, інтерфейс vmbr0 конфігурується з підтримкою тегування (VLAN Aware). Це дозволяє центральному L3-комутатору SW_4 передавати трафік у Trunk-порт сервера, а

Proxmox буде самостійно розподіляти пакети між віртуальними машинами відповідно до призначеного їм номера VLAN.

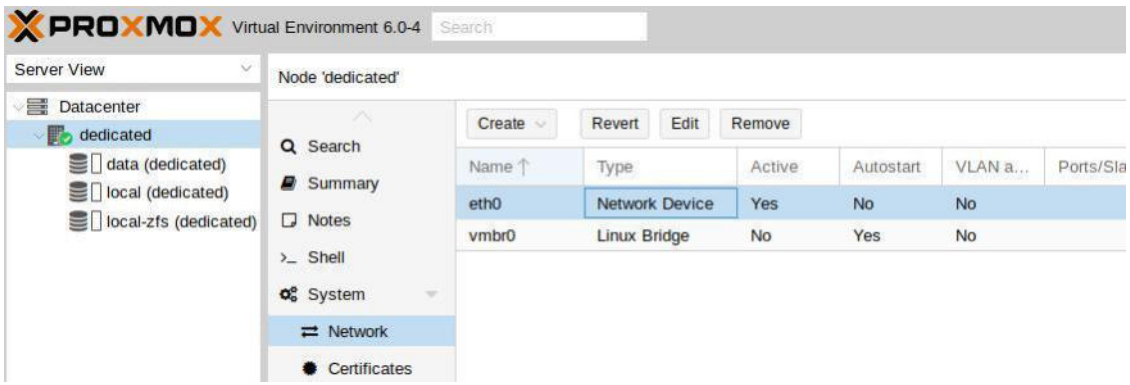


Рисунок 3.5 – Інтерфейси віртуального середовища та параметри мікропрограмної мережі

Після успішного виконання описаних кроків платформа Proxmox VE повністю готова до розгортання ізольованих віртуальних машин, першою з яких буде локальний сервер аутентифікації та мережевих служб.

3.2 Інструкції з налаштування активного комутаційного обладнання

3.2.1 Інструкції з налаштування Wi-Fi точок доступу

Для забезпечення мобільності персоналу, підключення портативних пристроїв та організації гостьового сегмента в офісі компанії «IT-M» розгорнуто корпоративну бездротову мережу. На апаратному рівні застосовано дволінійні точки доступу MikroTik cAP ac, які підтримують сучасний високошвидкісний стандарт IEEE 802.11ac (Wi-Fi 5) [14].

З метою дотримання суворих вимог інформаційної безпеки, бездротовий сегмент повністю ізольовано від провідної виробничої інфраструктури компанії. Увесь Wi-Fi трафік інкапсулюється у виділену віртуальну мережу VLAN 20 (адресний простір 192.168.20.0/24). Точки доступу функціонують у режимі

прозорого мережевого мосту (L2 Bridge). Централізовану динамічну видачу IP-адрес для бездротових клієнтів у межах усього сегмента реалізує виділений DHCP-сервер інфраструктурного вузла, що значно спрощує адміністрування та унеможливлює виникнення конфліктів IP-адрес у мережі.

Процедура конфігурування точок доступу через спеціалізоване графічне середовище управління (WinBox / WebFig) складається з кількох послідовних етапів.

Етап 1. Параметризація радіомодулів та частотного діапазону

На початковому кроці виконується активація бездротових інтерфейсів та вибір оптимальних частотних каналів для мінімізації взаємних завад в офісному приміщенні. Пристрій має два незалежних фізичних радіомодулі. Налаштування параметрів бездротового інтерфейсу для одночасної роботи у двох діапазонах (2.4 GHz — для стабільного покриття, 5 GHz — для забезпечення максимальної пропускної здатності) ініціюється у вікні конфігурації бездротової частини мережі, як ілюструє рисунок 3.6.

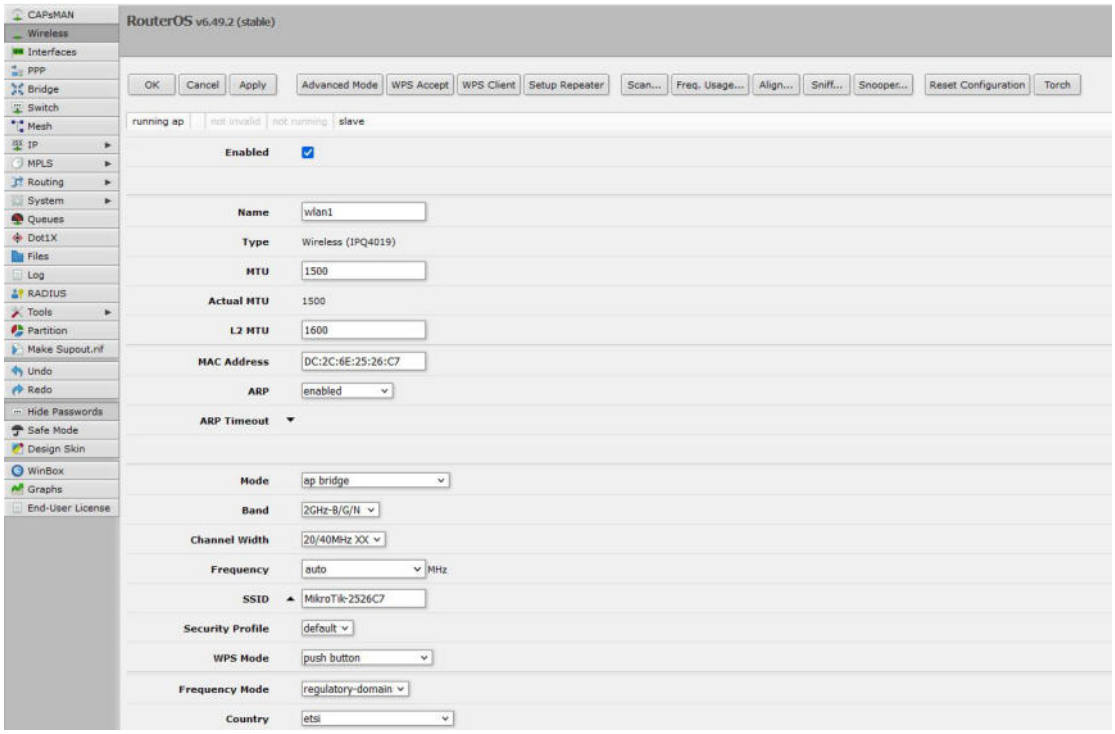


Рисунок 3.6 – Налаштування безпровідного інтерфейсу router

Етап 2. Конфігурування профілів безпеки та шифрування

Наступним критично важливим кроком є захист радіоефіру від несанкціонованого перехоплення даних та компрометації корпоративних паролів. Загальні параметри автентифікації наведено на рисунку 3.7.

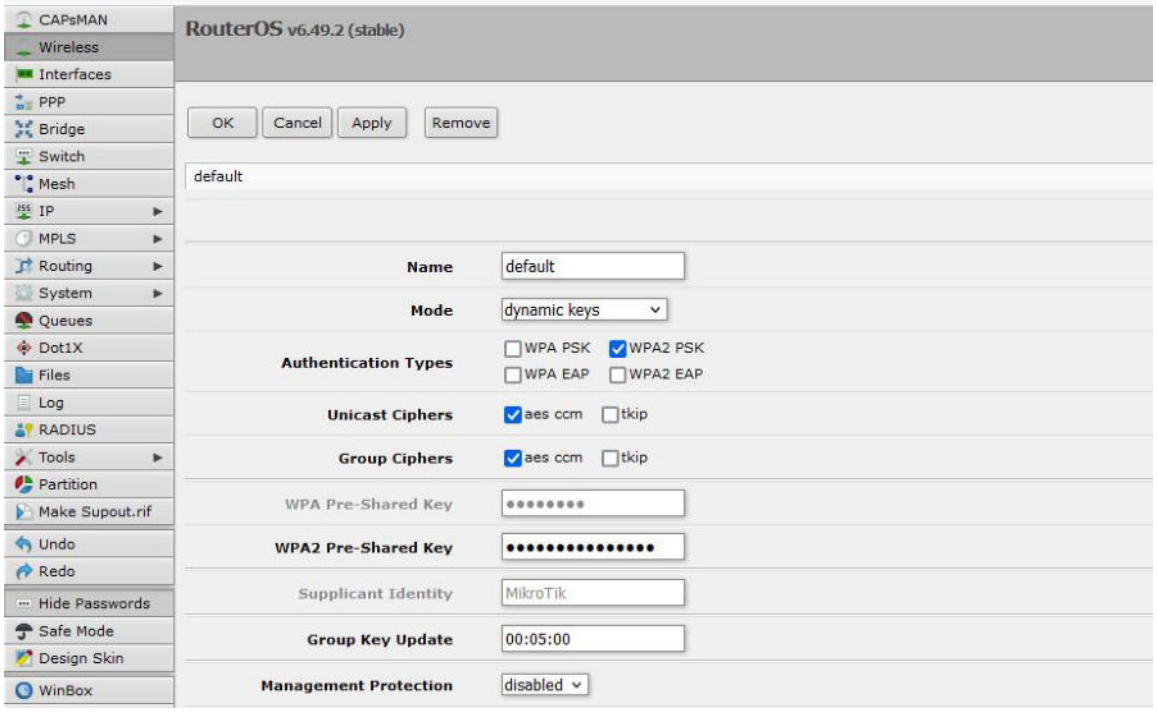


Рисунок 3.7 – Загальні параметри аутентифікації

У межах проєкту задіяно стандарт WPA2 PSK (Wi-Fi Protected Access 2 с Pre-Shared Key) з алгоритмом шифрування AES-CCMP. Історично протокол WPA першої версії базувався на механізмі TKIP, який створювався як тимчасова альтернатива застарілому та вразливому стандарту WEP. Проте використання застарілих методів шифрування (TKIP чи WEP) у сучасних мережах суворо заборонено, оскільки вони не лише критично знижують продуктивність стандарту 802.11ac, обмежуючи швидкість, а й створюють високі ризики несанкціонованого доступу. Застосування сучасного алгоритму AES гарантує стійкість до криптографічних атак без деградації пропускної здатності.

Етап 3. Налаштування інтерфейсів комутації (Local/Bridge)

Оскільки точка доступу підключається до абонентського комутатора робочої групи за допомогою магістрального кабелю, її внутрішній інтерфейс комутації має бути інтегрований у локальний міст та чітко відповідати параметрам, наведеним на рисунку 3.8.

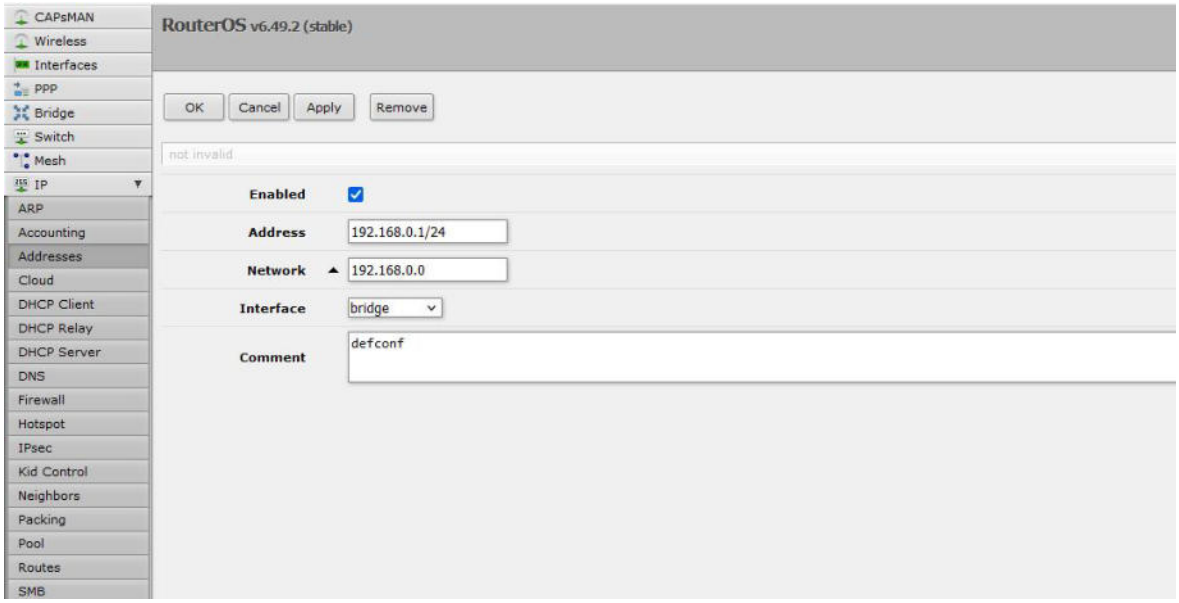
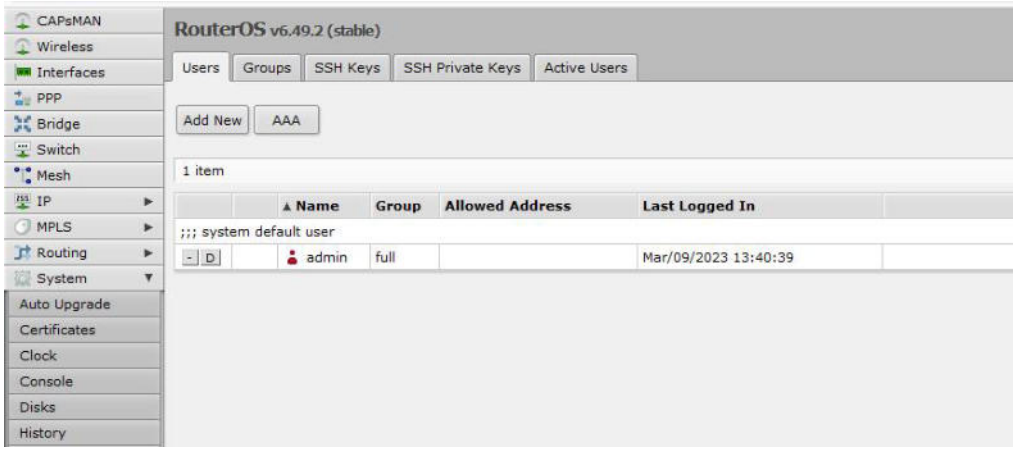


Рисунок 3.8 – Налаштування local інтерфейсу точки доступу

Для включення порту в роботу його стан переводиться в режим Enable. На цьому ж етапі фізичний порт Ethernet (зовнішній вихід до комутатора ядра) та віртуальні радіоінтерфейси (wlan) об'єднуються в єдиний програмний міст (Bridge) з підтримкою тегування IEEE 802.1Q, що дозволяє безперешкодно транслювати бездротовий трафік безпосередньо у VLAN 20.

Етап 4. Розмежування прав доступу адміністраторів (Управління користувачами)

Для забезпечення захисту самої операційної системи точки доступу від несанкціонованих змін конфігурації, на наступному кроці необхідно внести дані користувачів, які мають право керувати пристроєм, встановити складні паролі та задати відповідні рівні привілеїв, як показано на рисунку 3.9.



Рисуноку 3.9 – Задання користувачів

У системі створюються різні категорії облікових записів із чітко обмеженими рівнями доступу (Group):

Адміністратори (full) — повні права на зміну конфігурації мережі, оновлення мікропрограм та аудит безпеки;

Менеджери / Оператори (write) — право на поточний моніторинг та зміну базових параметрів (наприклад, зміна пароля Wi-Fi);

Працівники техпідтримки (read) — доступ виключно в режимі читання для перегляду логів та стану підключених клієнтів.

Додаткові інженерні налаштування безпеки

Після завершення базової конфігурації пристрою, для підвищення рівня захищеності бездротового периметра компанії «IT-M» реалізовано такі кроки:

Фільтрація за MAC-адресами (Access List): Обмеження доступу мобільних користувачів на рівні заліза. Пристрої, чиї унікальні MAC-адреси відсутні в дозволеному білому списку системи, автоматично відкидаються на етапі спроби асоціації з точкою доступу.

Оптимізація стеку протоколів: Вимкнення невикористовуваних сервісів (Discovery Protocol, Bandwidth Server) та чітке обмеження діапазону автоматичного розподілу IP-адрес на центральному DHCP-сервері, що обслуговує пул адрес для клієнтів цієї зони відпочинку.

3.2.2 Інструкції з налаштування центрального комутатора

Для забезпечення високошвидкісного обміну даними між структурними підрозділами компанії «IT-M» та розвантаження периферійного програмного шлюзу, у ядрі мережі застосовано комутатор 3-го рівня (L3) D-Link DGS-3130-30TS. Його використання дозволяє локалізувати широкомовний трафік у межах окремих віртуальних мереж (VLAN) та виконувати апаратну маршрутизацію між підмережами (Inter-VLAN Routing) на швидкості комутаційної матриці.

Технологія VLAN (Virtual Local Area Network) дає змогу гнучко групувати робочі станції в ізольовані логічні сегменти незалежно від їхнього фізичного розташування та підключення до проміжних комутаторів доступу [16]. Будь-які топологічні зміни чи переміщення персоналу між кабінетами реалізуються виключно програмним переконфігуруванням портів ядра мережі.

Нижче наведено лістинг покрокового налаштування центрального комутатора SW_4 з використанням фірмового інтерфейсу командного рядка D-Link CLI (D-OS).

1. Створення віртуальних локальних мереж (VLAN)

Переходимо в режим глобальної конфігурації та ініціалізуємо ідентифікатори (VLAN ID) і текстові мітки для кожного підрозділу відповідно до проєкту:

```
Switch# configure terminal
# Вхід у режим глобальної конфігурації пристрою
Switch(config)# vlan 11
Switch(config-vlan)# name vlan11
# Створення VLAN 11 та призначення імені (Адміністрація)
Switch(config)# vlan 12
Switch(config-vlan)# name vlan12
# Створення VLAN 12 (Бухгалтерія)
Switch(config)# vlan 13
```

```
Switch(config-vlan)# name vlan13
# Створення VLAN 13 (Менеджери)
Switch(config)# vlan 14
Switch(config-vlan)# name vlan14
# Створення VLAN 14 (Маркетинг)
Switch(config)# vlan 15
Switch(config-vlan)# name vlan15
# Створення VLAN 15 (HR та кадри)
Switch(config)# vlan 16
Switch(config-vlan)# name vlan16
# Створення VLAN 16 (Аналітики)
Switch(config)# vlan 17
Switch(config-vlan)# name vlan17
# Створення VLAN 17 (Технічна підтримка)
Switch(config)# vlan 18
Switch(config-vlan)# name vlan18
# Створення VLAN 18 (Комп'ютерне забезпечення та серверна)
Switch(config)# vlan 19
Switch(config-vlan)# name vlan19
# Створення VLAN 19 (Відділ розробки)
Switch(config)# vlan 20
Switch(config-vlan)# name vlan20
# Створення VLAN 20 (Зона відпочинку / Wi-Fi)
Switch(config-vlan)# exit
```

2. Конфігурування магістральних (Trunk) портів

Порти з 1 по 4 використовуються для підключення периферійних комутаторів доступу (SW_1–SW_3, SW_5, SW_6) та сервера віртуалізації Proxmox S_1. Ці порти налаштовуються у режим транку для передачі тегованого трафіку згідно зі стандартом IEEE 802.1Q:

Switch(config)# interface range ethernet 1/0/1 - 1/0/4

Одночасний вибір діапазону фізичних портів з 1 по 4

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

Переведення портів у магістральний режим (Trunk)

Switch(config-if-range)# switchport trunk allowed vlan all

Дозвіл проходження всіх створених VLAN через дані магістральні лінки

Switch(config-if-range)# exit

3. Конфігурування абонентських (Access) портів

Кінцеві пристрої (робочі станції, точки доступу, сервери) підключаються до нетегованих портів доступу. Кожному порту жорстко присвоюється його рідний VLAN ID:

--- Налаштування сегмента VLAN 20 (Wi-Fi та інфраструктура) ---

Switch(config)# interface range ethernet 1/0/5 , ethernet 1/0/15

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

Switch(config-if-range)# switchport access vlan 20

Switch(config-if-range)# exit

--- Налаштування сегмента VLAN 18 (Серверна та IT-відділ) ---

Switch(config)# interface range ethernet 1/0/6 - 1/0/9

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

Switch(config-if-range)# switchport access vlan 18

Switch(config-if-range)# exit

--- Налаштування сегмента VLAN 17 (Технічна підтримка) ---

Switch(config)# interface range ethernet 1/0/10 - 1/0/11

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

Switch(config-if-range)# switchport access vlan 17

Switch(config-if-range)# exit

--- Налаштування сегмента VLAN 16 (Аналітики) ---

Switch(config)# interface ethernet 1/0/12

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 16

Sitch(config-if)# exit

--- Налаштування сегмента VLAN 15 (HR та кадри) ---

Switch(config)# interface ethernet 1/0/13

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 15

Switch(config-if)# exit

--- Налаштування сегмента VLAN 13 (Проектні менеджери) ---

Switch(config)# interface ethernet 1/0/14

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 13

Switch(config-if)# exit

4. Створення віртуальних інтерфейсів L3 та активація маршрутизації

Для того, щоб комутатор міг пересилати пакети між різними підмережами, створюються інтерфейси розв'язки VLAN (SVI) і їм присвоюються відповідні IP-адреси, які будуть основними шлюзами (Default Gateway) для робочих станцій:

Switch(config)# interface vlan 11

Switch(config-if)# ip address 192.168.11.254 255.255.255.0

Активація L3-інтерфейсу для VLAN 11 та призначення IP шлюзу

Switch(config)# interface vlan 12

Switch(config-if)# ip address 192.168.12.254 255.255.255.0

Switch(config)# interface vlan 13

Switch(config-if)# ip address 192.168.13.254 255.255.255.0

Switch(config)# interface vlan 14

Switch(config-if)# ip address 192.168.14.254 255.255.255.0

Switch(config)# interface vlan 15

Switch(config-if)# ip address 192.168.15.254 255.255.255.0

Switch(config)# interface vlan 16

Switch(config-if)# ip address 192.168.16.254 255.255.255.0

Switch(config)# interface vlan 17

Switch(config-if)# ip address 192.168.17.254 255.255.255.0

Switch(config)# interface vlan 18

Switch(config-if)# ip address 192.168.18.254 255.255.255.0

Switch(config)# interface vlan 19

Switch(config-if)# ip address 192.168.19.254 255.255.255.0

Switch(config)# interface vlan 20

Switch(config-if)# ip address 192.168.20.254 255.255.255.0

Switch(config-if)# exit

5. Налаштування статичної маршрутизації (Шлюз за замовчуванням)

Для забезпечення доступу до глобальної мережі Інтернет створюється статичний маршрут за замовчуванням. Весь зовнішній трафік комутатор автоматично перенаправляє на внутрішню IP-адресу периферійного програмного шлюзу безпеки S_2 (Fedora Server), що знаходиться у VLAN 18:

Switch(config)# ip route 0.0.0.0 0.0.0.0 192.168.18.254

Створення дефолтного маршруту на Edge Gateway S_2

Switch(config)# exit

6. Збереження конфігурації

На завершення процедури конфігурування необхідно в обов'язковому порядку записати зміни з оперативної пам'яті (Running-Config) в енергонезалежну пам'ять комутатора (Startup-Config), щоб уникнути втрати налаштувань у разі знеструмлення пристрою:

Switch# copy running-config startup-config

Destination filename [startup-config]? My_Conf

Acknowledge laoding startup-config file... Success.OK!

3.2.3. Конфігурування комутаторів рівня доступу (робочих груп)

Комутатори периферійного рівня (рівня доступу) D-Link DGS-1100-08 та DGS-1100-16 призначені для безпосереднього підключення кінцевих абонентів (робочих станцій персоналу, принтерів, точок доступу Wi-Fi) у кабінетах компанії «IT-M». Основне завдання цих пристроїв — прийняти нетегований трафік від клієнтського пристрою, маркувати його відповідним тегом VLAN і передати через магістральний Uplink-канал на центральний L3-комутатор SW_4.

Налаштування кожного комутатора робочої групи здійснюється за уніфікованим інженерним алгоритмом через інтерфейс командного рядка (CLI).

Алгоритм конфігурування периферійного комутатора:

Ініціалізація та налаштування магістрального порту (Trunk): На кожному пристрої перший фізичний порт (ethernet 1/1 або eth1) виділяється под висхідний канал (Uplink) до центральної серверної. Він переводиться в режим trunk, що дозволяє йому транслювати кадри з тегами IEEE 802.1Q для віртуальних мереж підрозділів.

Реєстрація дозволених ідентифікаторів VLAN: У базі даних комутатора створюються лише ті номери VLAN, які безпосередньо присутні в конкретному кабінеті або проходять транзитом через цей вузол згідно зі специфікаціями таблиць Б1 та Б2.

Розподіл абонентських портів (Access): Порти, до яких підключаються ПК користувачів, конфігуруються як нетеговані (access). Прив'язка інтерфейсів до конкретних віртуальних мереж виконується строго відповідно до штатного розкладу підрозділів.

Практичний приклад конфігурації периферійного комутатора

Для демонстрації наведемо лістинг команд налаштування комутатора SW_1 (D-Link DGS-1100-08), який територіально розміщений у Кабінеті 5

(Відділ проєктних менеджерів — VLAN 13) згідно з проєктною матрицею комутації:

```
Switch# configure terminal
# Вхід у режим конфігурування параметрів периферійного комутатора
# --- Крок 1: Створення VLAN 13 (Проєктні менеджери) у базі пристрою -
Switch(config)# vlan 13
Switch(config-vlan)# name Project_Managers
Switch(config-vlan)# exit
# --- Крок 2: Конфігурування магістрального Uplink-порту до серверної ---
Switch(config)# interface ethernet 1/1
# Вибір першого порту для підключення до центрального комутатора SW_4
Switch(config-if)# switchport mode trunk
# Активація режиму Trunk для передачі маркованих пакетів
Switch(config-if)# switchport trunk allowed vlan 13
# Дозвіл проходження тегованого трафіку для VLAN 13
Switch(config-if)# exit
# --- Крок 3: Конфігурування абонентських портів доступу (Access) ---
Switch(config)# interface range ethernet 1/2 - 1/8
# Обрання портів з 2 по 8 під робочі станції менеджерів кабінету 5 (WS_6, WS_7, WS_8 та ін.)
Switch(config-if-range)# switchport mode access
# Переведення портів у режим кінцевого доступу (Access)
Switch(config-if-range)# switchport access vlan 13
# Прив'язка нетегованого трафіку з цих портів до VLAN 13
Switch(config-if-range)# exit
# --- Крок 4: Збереження поточної конфігурації в енергонезалежну пам'ять
Switch(config)# exit
Switch# write memory
```

Saving all configurations to NVRAM... Success.

За аналогічним алгоритмом, змінюючи номери інтерфейсів та ідентифікатори VLAN відповідно до таблиць додатка Б, здійснюється прошивка та введення в експлуатацію інших комутаторів робочих груп (SW_2 у кабінеті 6, SW_3 у кабінеті 7, SW_5 та SW_6 у кабінетах розробників).

Такий підхід повністю виключає змішування мережевих пакетів різних підрозділів на фізичному рівні, локалізує широкомовні шторми та значно спрощує подальше адміністрування та масштабування мережі компанії «IT-M».

3.3Інструкції з використання тестових наборів та тестових програм

Завершальним етапом розгортання та введення в експлуатаційну готовність комп'ютерної мережі компанії «IT-M» є комплексне тестування її компонентів. Верифікація працездатності здійснюється за висхідним принципом - від базового фізичного (кабельного) рівня до прикладного рівня мережевих сервісів та серверних платформ.

1. Діагностика фізичного та канального рівнів

Аналіз фізичного середовища передачі даних спрямований на виявлення дефектів комутації, пошкоджень структурованої кабельної системи (СКС), некоректного обтиску роз'ємів RJ-45 або незадовільної якості ліній зв'язку. Первинний контроль здійснюється за допомогою апаратних LAN-тестерів та світлодіодних індикаторів (LED) на інтерфейсах мережевих карт хостів і керованих комутаторів D-Link. Відсутність індикації (або аварійний червоний колір стабільного лінку) сигналізує про обрив провідників або апаратну несправність порту.

2. Програмний інструментарій міжплатформного тестування

Для локалізації логічних помилок адресації, перевірки доступності вузлів та оцінки пропускної здатності каналів у межах розроблених віртуальних

мереж (VLAN 11–20) використовується спеціалізоване кросплатформне програмне забезпечення:

- ICMP-діагностика (ping): Утиліта для експрес-оцінки доступності віддаленого хоста на мережевому рівні за допомогою ехо-запитів.

- Трасування шляху (tracert у Windows / traceroute у Linux): Інструмент визначення послідовності маршрутизаторів (хопів), через які проходять пакети до цільового вузла, що дозволяє локалізувати місце розриву зв'язку.

- Моніторинг сокетів (netstat): Відображає поточний стан активних мережевих TCP/UDP з'єднань, таблиці маршрутизації та статистику інтерфейсів.

- Аудит безпеки (nmap): Мережевий сканер, призначений для виявлення активних хостів у підмережі та інвентаризації відкритих портів на серверах.

- Аналіз трафіку (Wireshark): Інтерактивний аналізатор (сніфер) протоколів, який дозволяє перехоплювати та декодувати мережеві кадри з метою пошуку аномалій чи затримок передачі.

- Стрес-тестування (iperf3): Консольна утиліта для генерації синтетичного трафіку та точного вимірювання максимальної смуги пропускання мережевого тракту.

3. Практичні сценарії застосування тестових наборів

Нижче наведено практичні приклади виконання діагностичних команд з урахуванням архітектури та реального адресного простору мережі підприємства.

Сценарій А. Перевірка доступності шлюзу та серверних ресурсів

Для швидкої перевірки базового зв'язку між робочою станцією користувача та центральним шлюзом безпеки S_2 (Fedora Server) з командного рядка операційної системи Windows виконується запит:

DOS

ping 192.168.18.254

У разі стабільної роботи інтерфейсів утиліта відображає час затримки (RTT) у мілісекундах та відсоток втрачених пакетів. Для тривалого моніторингу стабільності лінку (наприклад, під час тестування бездротового покриття точок доступу у VLAN 20) застосовується прапорець безперервного надсилання пакетів:

DOS

ping 192.168.18.254 -t

Сценарій Б. Сканування та інвентаризація хостів підмережі

З метою аудиту робочих станцій, що отримали динамічні адреси, та виявлення несанкціонованих підключень у сегменті Відділу розробки (VLAN 19), адміністратор з консолі керування сервера S_1 запускає утиліту nmap у режимі швидкого ICMP-сканування (Ping Sweep) без аналізу портів:

Bash

nmap -sn 192.168.19.0/24

Ця операція дозволяє миттєво отримати актуальний список увімкнених комп'ютерів у даному кабінеті.

Сценарій В. Аудит захищеності та відкритих служб файлового сервера

Для перевірки коректності конфігурації міжмережевого екрана локального сервера S_1 та підтвердження того, що зовні відкриті виключно санкціоновані порти служб (наприклад, FTPS та вебінтерфейс Proxmox), виконується повне сканування всіх 65535 TCP-портів за допомогою такої команди:

Bash

nmap -p- 192.168.18.253

Результат сканування повинен підтвердити активність портів 21 (FTP), 8006 (Proxmox Web) та закритість або фільтрацію інших портів системи, що доводить ефективність налаштованих правил безпеки iptables.

3.4 Інструкції з моніторингу, технічної експлуатації та збору метрик в мережі

Безперервний автоматизований збір статистичних даних, аналіз телеметрії та превентивний моніторинг є фундаментальними передумовами забезпечення високої відмовостійкості, безпеки та стабільного функціонування корпоративної мережі компанії «IT-M». Оперативне виявлення латентних аномалій, деградації каналів зв'язку або критичного завантаження апаратних ресурсів (CPU, RAM, Storage I/O) на серверах та комутаторах дозволяє інженерному персоналу усувати інциденти до моменту виникнення критичних збоїв.

Для моніторингу сучасних гетерогенних мереж застосовується широкий спектр спеціалізованого програмного забезпечення:

Аналізатори пакетів (Wireshark): Використовуються для поглибленого аналізу мережевих протоколів та декодування трафіку безпосередньо у проблемних сегментах підмереж.

Системи на базі SNMP (PRTG Network Monitor, Nagios): Традиційні платформи для опитування активного мережевого обладнання та відстежування статусу портів.

Комплексні екосистеми (Zabbix): Потужні інструменти для моніторингу великих інфраструктур із вбудованими модулями триггерів та інтеграцією з корпоративними месенджерами (Slack, Telegram) для миттєвого сповіщення про аварії.

Найбільш прогресивним, гнучким та масштабованим індустріальним стандартом для збору метрик у віртуалізованих середовищах (таких як Proxmox VE на сервері S_1) є зв'язка збирача метрик Prometheus та аналітичної платформи візуалізації Grafana. У межах проєкту цю екосистему розгорнуто за наведеним нижче структурованим алгоритмом.

Крок 1. Розгортання та конфігурування Prometheus Server

Збір метрик побудований за Pull-моделлю, коли сервер Prometheus з певною періодичністю опитує цільові пристрої. Встановлення на Fedora Server виконується через штатні репозиторії або за допомогою створення ізольованого системного демона.

Файл конфігурації /etc/prometheus/prometheus.yml налаштовується на збір метрик із периферійного шлюзу S_2 та гіпервізора S_1:

YAML

```
global:
  scrape_interval: 15s  # Інтервал збору метрик за замовчуванням
  evaluation_interval: 15s
scrape_configs:
  - job_name: 'prometheus'
    static_configs:
      - targets: ['localhost:9090']
  - job_name: 'edge_gateway_s2'
    static_configs:
      - targets: ['192.168.18.254:9100'] # Опитування Node Exporter на шлюзі Fedora
  - job_name: 'proxmox_node_s1'
    static_configs:
      - targets: ['192.168.18.253:9100'] # Опитування Node Exporter на сервері віртуалізації
```

Для забезпечення безперебійної роботи у фоновому режимі та автоматичного старту у випадку перезавантаження апаратної частини створюється юніт-файл для системного менеджера systemd:

```
# Шлях до файлу: /etc/systemd/system/prometheus.service
[Unit]
Description=Prometheus Monitoring Time Series Database
After=network.target
```

[Service]

User=prometheus

Group=prometheus

Type=simple

ExecStart=/usr/local/bin/prometheus --config.file=/etc/prometheus/prometheus.yml --storage.tsdb.path=/var/lib/prometheus/

Restart=always

[Install]

WantedBy=multi-user.target

Активація та запуск служби: sudo systemctl enable --now prometheus.

Крок 2. Інсталяція демона збору метрик ОС (Node Exporter)

Щоб Prometheus міг отримувати дані про стан заліза серверів S_1 та S_2, на кожну операційну систему встановлюється утиліта node_exporter, яка транслює метрики ядра Linux у формат, зрозумілий для Prometheus. Вона також реєструється як служба systemd і відкриває для збору даних TCP-порт 9100.

Крок 3. Розгортання аналітичної платформи Grafana

Платформа Grafana відповідає за агрегацію отриманих від Prometheus часових рядів та їх перетворення на інтерактивні графічні дашборди. Інсталяція на сервері моніторингу реалізується за допомогою пакетного менеджера:

Bash

Додавання офіційного репозиторію Grafana та встановлення

sudo dnf install -y enterprise-grafana

Реєстрація служби в автозавантаженні та її запуск

sudo systemctl enable --now grafana-server

Після старту веб-інтерфейс платформи стає доступним за адресою http://192.168.18.253:3000 (або на виділеному IP-хості у VLAN 18).

Крок 4. Інтеграція компонентів та побудова дашбордів

Фінальний етап налаштування системи моніторингу виконується через графічну веб-панель Grafana:

Підключення джерела даних (Data Source): У розділі системних налаштувань обирається тип Prometheus, а у полі URL вказується адреса локального сервера збору метрик: http://localhost:9090. Виконується тест з'єднання Save & Test.

Імпорт графічних панелей: Для наочного відображення інформації імпортуються стандартизовані корпоративні шаблони (наприклад, Дашборд ID 1860).

Аналіз телеметрії: Створюються кастомізовані екрани, які в режимі реального часу відображають утилізацію мережевих інтерфейсів ppp0 та eth0 на шлюзі S_2, об'єм вільного місця у пулі сховища local-lvm на Proxmox та інтенсивність трафіку, що проходить крізь L3-комутатор ядра мережі.

Впровадження описаного комплексу моніторингу мінімізує час реакції IT-відділу компанії «IT-M» на позаштатні ситуації, спрощує локалізацію несправностей та забезпечує прозорість функціонування усіх рівнів інформаційної інфраструктури

3.5 Інструкції по налаштуванню засобів захисту мережі за допомогою міжмережевого екрану

Периферійний захист локальної мережі (LAN) компанії «IT-M» та безпосередньо самого операційного середовища шлюзу безпеки S_2 реалізовано на базі вбудованого в ядро Linux підсистемного комплексу Netfilter, управління яким здійснюється за допомогою утиліти iptables. Фільтрація пакетів, трансляція адрес (NAT) та розмежування прав доступу базуються на перевірці критеріїв заголовків IP-пакетів: адрес відправника (source) та отримувача (destination), транспортних протоколів (TCP, UDP, ICMP) та номерів системних портів.

Нижче наведено детальний аналіз архітектури побудови правил безпеки, які згруповані за трьома базовими вбудованими ланцюжками (INPUT, OUTPUT, FORWARD).

1. Фільтрація вхідного трафіку (Ланцюжок INPUT)

Ланцюжок INPUT відповідає за обробку пакетів, які адресовані безпосередньо самому серверу-шлюзу S_2 та його внутрішнім службам.

Сувора загороджувальна політика:

Bash

/sbin/iptables -P INPUT DROP

Ця команда встановлює безальтернативну політику заборони за замовчуванням. Будь-який вхідний пакет, який чітко не відповідає легітимним критеріям наступних дозволяючих правил, миттєво відкидається (DROP), що ізолює сервер від зовнішнього сканування.

Захист від сканування та несанкціонованих сесій:

Bash

/sbin/iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP

Контролює коректність встановлення TCP-з'єднань. Пакет, що намагається відкрити нову сесію (--state NEW), але не має встановленого прапора SYN, визначається як аномальний і блокується, що запобігає атакам типу Stealth FIN/Xmas сканування.

Дозвіл трафіку локальної петлі (Loopback):

Bash

/sbin/iptables -A INPUT -i lo -j ACCEPT

Забезпечує безперешкодну взаємодію внутрішніх системних процесів та служб сервера між собою через віртуальний інтерфейс 127.0.0.1.

Дозвіл доступу з корпоративної мережі:

Bash

/sbin/iptables -A INPUT -i eth0 -s 192.168.0.0/16 -j ACCEPT

Дозволяє повний вхідний доступ до служб шлюзу (наприклад, для адміністрування по SSH) через внутрішній інтерфейс eth0, але виключно для пристроїв, які належать до легітимної корпоративної супермережі компанії (VLAN 11–20).

Супровід встановлених сесій (Stateful Inspection):

Bash

/sbin/iptables -A INPUT -i ppp0 -m state --state ESTABLISHED,RELATED -j ACCEPT

Дозволяє проходження вхідних пакетів із зовнішнього інтерфейсу ppp0 (PPPoE тунель) лише у тому випадку, якщо вони є відповідями на запити, які раніше були легітимно ініційовані самим сервером (стани ESTABLISHED або RELATED).

Мережева діагностика:

Bash

/sbin/iptables -A INPUT -p icmp -j ACCEPT

Дозволяє обробку службових повідомлень протоколу ICMP, що необхідно для перевірки доступності шлюзу (ping) адміністраторами внутрішньої мережі.

2. Фільтрація вихідного трафіку (Ланцюжок OUTPUT)

Ланцюжок OUTPUT контролює пакети, що генеруються безпосередньо локальними процесами самого сервера-шлюзу S_2 та спрямовуються назовні.

Політика мінімальних привілеїв на вихід:

Bash

/sbin/iptables -P OUTPUT DROP

У межах підвищення безпеки вихідний трафік самого сервера також за замовчуванням блокується. Це локалізує активність зловмисника у випадку потенційного компрометування системи.

Санкціоновані вихідні канали:

Bash

/sbin/iptables -A OUTPUT -o lo -j ACCEPT

/sbin/iptables -A OUTPUT -o eth0 -d 192.168.0.0/16 -j ACCEPT

Дозволяється вихід системних пакетів у петлю зворотного зв'язку, а також у внутрішній інтерфейс eth0 для комунікації з інфраструктурними серверами (наприклад, для взаємодії з DNS/DHCP сервером S_1 на адресі 192.168.18.253).

Вихідні відповіді та запити в глобальну мережу:

Bash

/sbin/iptables -A OUTPUT -o ppp0 -j ACCEPT

Надає серверу право відправляти вихідні пакети через зовнішній інтерфейс ppp0 для оновлення системних компонентів ОС Fedora, синхронізації часу NTP та відправки відповідей зовнішнім клієнтам.

3. Контроль транзитного трафіку (Ланцюжок FORWARD)

Ланцюжок FORWARD є ключовим для архітектури шлюзу, оскільки він обробляє весь транзитний трафік користувачів з усіх кабінетів (VLAN 11–20), що прямує в Інтернет через S_2.

Загороджувальна транзитна політика (Критичний елемент безпеки):

Bash

/sbin/iptables -P FORWARD DROP

На відміну від небезпечної політики ACCEPT, встановлюється жорстке блокування. Пересилання будь-яких пакетів між інтерфейсами за замовчуванням заборонено. Шлюз пропустить лише авторизований трафік.

Маршрутизація користувацьких запитів в Інтернет:

Bash

/sbin/iptables -A FORWARD -i eth0 -o ppp0 -s 192.168.0.0/16 -j ACCEPT

Дозволяє транзитне пересилання пакетів, які надходять від внутрішньої мережі компанії через інтерфейс eth0 і спрямовуються у зовнішній світ через інтерфейс ppp0. Це забезпечує вихід в Інтернет усім підрозділам.

Зворотний транзитний трафік (Захист користувачів):

Bash

/sbin/iptables -A FORWARD -i ppp0 -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

Дозволяє проходження транзитних пакетів із глобальної мережі всередину компанії, але виключно як відповідь на запити, які раніше були надіслані самими

користувачами. Будь-які спроби зовнішнього ініціювання з'єднань з Інтернету в локальні кабінети автоматично відсікаються.

Транзит діагностичних утиліт:

Bash

/sbin/iptables -A FORWARD -p icmp -j ACCEPT

Забезпечує можливість кінцевим робочим станціям користувачів виконувати перевірку доступності зовнішніх інтернет-ресурсів за допомогою протоколу ICMP.

Впровадження описаного комплексу правил у поєднанні з активованим механізмом MASQUERADE у таблиці NAT забезпечує повну ізоляцію внутрішнього адресного простору компанії «IT-M», захищає інфраструктуру від зовнішніх вторгнень та гарантує суворий контроль над усіма інформаційними потоками perimeter-рівня.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Основним завданням економічного розділу кваліфікаційної роботи є проведення розрахунків, що дозволяють розрахувати собівартість та ціну проекту мережі, оцінити економічну доцільність створення комп'ютерної мережі для компанії «ІТ-М» та обґрунтувати рішення щодо її подальшого впровадження в діяльність підприємства.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

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

Таблиця 4.1 - Середній час виконання НДР та стадій технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Час виконання операції, год.
1	2	3	4
1	Постановка задачі, розробка технічного завдання.	Керівник проекту	8
2	Розробка проекту. На даному етапі проектується логічна та фізична топології локальної мережі.	Інженер	19
3	Монтаж мережі. На даному здійснюється монтаж на підключення пасивного мережевого обладнання.	Технік	42

Продовження таблиці 4.1

1	2	3	4
4	Налагодження мережі. На даному етапі інсталюються ОС серверів та робочих станцій. Конфігуруються мережеві служби та сервіси. Додатково буде проведено тестування роботи апаратної частини мережі на програмної частини (перевірка зв'язку між вузлами мережі, перевірка конфігурацій програмного забезпечення)	Інженер	30
5	Підготовка документації. На даному етапі готується технічна документація на локальну мережу. Інструкції з налаштування служб та сервісів.	Інженер	10
Разом		-	109

Сумарний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі для компанії «ІТ-М» складає 109 годин.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

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

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

Основна заробітна плата розраховується за формулою:

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

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Отже, основна заробітна плата для працівників становить:

1. Керівник проекту - $З_{осн1} = 8 \cdot 270 = 2160$ грн.
2. Інженер - $З_{осн2} = 59 \cdot 240 = 14160$ грн.
3. Технік - $З_{осн3} = 42 \cdot 190 = 7980$ грн.

Сумарна основна заробітна плата становить:

$$З_{осн} = 2160 + 14160 + 7980 = 24300 \text{ грн.}$$

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

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

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

Отже, додаткова заробітна плата по категоріях працівників становить:

- керівника проекту: $З_{дод1} = 2160 \cdot 0,12 = 259,2$ грн.
- інженера: $З_{дод2} = 14160 \cdot 0,12 = 1699,2$ грн.
- техніка: $З_{дод3} = 7980 \cdot 0,12 = 957,6$ грн.

Загальна додаткова заробітна плата становить:

$$З_{дод} = 259,20 + 1699,20 + 957,60 = 2916,00 \text{ грн.}$$

Звідси загальні витрати на оплату праці розраховуються за формулою 4.3:

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

$$В_{о.п} = 24300,00 + 2916,00 = 27216,00 \text{ грн.}$$

Відрахування на соціальні заходи становлять 22%. Отже, сума відрахувань на соціальні заходи буде становити:

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

де ФОП – фонд оплати праці, грн.

$$В_{с.з.} = 27216,00 \cdot 0,22 = 5987,52 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додатк. зароб. плата, грн.	Нарах. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тариф. ставка, грн.	К-сть від-працьов. год.	Фактично нарах. з/пл., грн.			
1	Керівник проекту	270	8	2160	259,2	-	-
2	Інженер	240	59	14160	1699.2	-	-
3	Технік	190	42	7980	957.6	-	-
Разом				24300	2916	5987,52	33203,52

Отже, загальні витрати на оплату праці становлять 33203,52 грн.

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни (формула 4.5):

$$M_{Bi} = q_i \cdot p_i \quad (4.5)$$

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 4.6:

$$З_{м.в.} = \sum M_{Bi} \quad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№ з/п	Перелік обладнання та інших матеріальних засобів	Один. виміру	Факт. використано	Ціна за шт., грн.	Загальна сума, грн.
1	2	3	4	5	6
1	Комутаційна шафа 15U (комплект з полками та блоком розеток UA-MGSWA155)	шт.	1	12500,00	12500,00
2	Патч-панель на 24 порти, Cat.6 (19", 1U)	шт.	1	2400,00	2400,00
3	Патч-корди UTP Cat. 6 (1.5 м / 3 м)	шт.	80	65,00	5200,00
4	ДБЖ (UPS) TECNOWARE EVO DSP-3 (або аналог On-Line 2000VA)	шт.	1	32000,00	32000,00
5	Короби пластикові для кабелю (різного січення)	м	120	85,00	10200,00
6	Ethernet-кабель UTP cat.6 (бухта 305 м, мідь)	бухта	2	6200,00	12400,00
7	Розетка мережева RJ-45 внутрішня/зовнішня під cat.6	шт.	50	175,00	8750,00
8	Комутатор центральний L3 D-Link DGS-3130-30TS	шт.	1	31500,00	31500,00
9	Комутатор керований D-Link DGS-1100-16	шт.	2	5800,00	11600,00

Продовження таблиці 4.3

1	2	3	4	5	6
10	Комутатор керований D-Link DGS-1100-08	шт.	3	3100,00	9300,00
11	Точка доступу Wi-Fi MikroTik cAP ac (RBcAPGi-5acD2nD)	шт.	2	3400,00	6800,00
12	Сервер ЛОМ LENOVO ThinkSystem ST50 (Xeon/32GB RAM/RAID)	шт.	2	82000,00	164000,00
	РАЗОМ				306650,00

Загальна сума матеріальних витрат на розробку мережі становить 306650,00 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання розраховуються за формулою 4.7:

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

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

Час роботи ПК над даним проектом становить 9 годин, споживана потужність - 0,5 кВт/год, вартість 1 кВт електроенергії – 15,94 грн. Тому витрати на електроенергію будуть становити:

$$З_е = 0,5 \cdot 9 \cdot 15,94 = 71,73 \text{ грн.}$$

4.5 Визначення транспортних затрат

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

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

де $Т_в$ – транспортні витрати.

Отже, транспортні витрати будуть становити:

$$Т_в = 306650,00 \cdot 0,09 = 27598,5 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

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

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

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

Враховуючи, що ПК працює над даним проектом 9 год., балансова вартість ПК – 29800 грн., тому:

$$A = \frac{29800 \cdot 0,04}{150} \cdot 9 = 71,52. \text{ грн}$$

4.7 Обчислення накладних витрат

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

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20 – 60 % від

суми основної та додаткової заробітної плати працівників, обчислюються за формулою 4.10.

$$Н_в = В_{о.п.} \cdot 0,2...0,6, \quad (4.10)$$

де $Н_в$ – накладні витрати.

$$Н_в = 27216 \cdot 0,3 = 8164,8 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

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

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

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці	27216	7,21
Відрахування на соціальні заходи	5987,52	1,59
Матеріальні витрати	306650,00	81,22
Витрати на електроенергію	71,73	0,02
Транспортні витрати	27598,5	7,31
Амортизаційні відрахування	71,52	0,02
Накладні витрати	8164,8	2,63
Собівартість	375760,01	100,00

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

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

Отже, собівартість дорівнює $С_в$ = 375760,01 грн

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою 4.12:

$$Ц = С_в \cdot (1+Р_{рен}) \cdot (1+ПДВ), \quad (4.12)$$

де $С_в$ – собівартість виконання НДР;

$Р_{рен.}$ – рівень рентабельності,

ПДВ – ставка податку на додану вартість.

$$Ц = 375760,01 \cdot (1+0,2) \cdot (1+0,2) = 541094,50 \text{ грн.}$$

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

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

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

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

де $К_В$ – затрати на проект;

$Г_п$ – грошовий потік за t – ий рік;

t – відповідний рік проекту;

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

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

$$ЧТВ = -375760,01 + \frac{306584,5}{(1+0,15)} + \frac{306584,5}{(1+0,15)^2} = 122657,12 \text{ грн}$$

Термін окупності визначається за формулою:

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

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

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

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

$$T_{ОК} = 1 + \frac{109164,78}{306584,5} = 1,4$$

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

Таблиця 4.5 - Техніко-економічні показники розробки мережі

№ п/п	Показник	Значення
1.	Собівартість, грн.	375760,01
2.	Плановий прибуток, грн.	165334,50
3.	Ціна, грн.	541094,50
4.	Чиста теперішня вартість, грн.	122657,12
5.	Термін окупності, рік	1,4

Розрахункова загальна вартість розробленої комп’ютерної мережі для компанії «IT-M» становить 541094,50 грн. Термін окупності становить 1,4 роки.

Аналіз отриманих параметрів підтверджує раціональне використання матеріально-технічних та трудових ресурсів під час проєктування. Розгортання гігабітної СКС забезпечує стабільну відмовостійкість внутрішніх сервісів, ліквідує обмеження пропускної здатності каналів зв'язку та оптимізує витрати робочого часу персоналу на міжсегментний обмін даними. Співвідношення витрат до швидкості повернення інвестицій свідчить про повну економічну доцільність практичного впровадження даного інженерного рішення в операційну діяльність підприємства.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

Охорона праці є важливою складовою діяльності будь-якого підприємства та спрямована на забезпечення безпечних і здорових умов праці працівників. Реалізація заходів з охорони праці дозволяє знизити ризик виробничого травматизму, професійних захворювань і виникнення аварійних ситуацій.

На відміну від промислових підприємств, у сфері інформаційних технологій працівники не зазнають впливу значної кількості небезпечних виробничих факторів. Проте під час експлуатації комп'ютерної техніки та мережевого обладнання виникають інші ризики, пов'язані з електробезпекою, пожежною безпекою, тривалою роботою за комп'ютером і впливом несприятливих факторів виробничого середовища. Тому дотримання вимог охорони праці є необхідною умовою безпечної та ефективної роботи персоналу підприємства.

5.1 Законодавчі вимоги щодо навчання та допуску працівників компанії “ІТ-М” до експлуатації електроустановок

У процесі експлуатації комп'ютерної мережі компанії «ІТ-М» використовуються персональні комп'ютери, серверне обладнання, комутатори, маршрутизатори, джерела безперебійного живлення та інші електротехнічні пристрої. Під час роботи з таким обладнанням працівники можуть контактувати з електроустановками, тому одним із важливих напрямів охорони праці є забезпечення належного рівня електробезпеки та виконання вимог чинного законодавства щодо навчання персоналу.

Відповідно до вимог нормативно-правових актів України працівники, діяльність яких пов'язана з експлуатацією, технічним обслуговуванням або ремонтом електрообладнання, повинні проходити спеціальне навчання та перевірку знань з питань охорони праці. Метою такого навчання є формування

навичок безпечної роботи з електроустановками, знання правил користування електрозахисними засобами та порядку дій у разі виникнення аварійних ситуацій [3, 6].

Перед початком виконання службових обов'язків працівники компанії проходять вступний інструктаж з охорони праці. Під час його проведення працівників ознайомлюють із загальними вимогами безпеки, правилами внутрішнього трудового розпорядку, особливостями експлуатації електрообладнання та порядком дій у разі виникнення небезпечних ситуацій. Після вступного інструктажу проводиться первинний інструктаж безпосередньо на робочому місці [5].

Працівники, які обслуговують електрообладнання або мають доступ до електрощитових та систем електроживлення, повинні проходити перевірку знань нормативних документів з електробезпеки. За результатами перевірки їм присвоюється відповідна група з електробезпеки. Для більшості працівників ІТ-підрозділу, які працюють із комп'ютерною технікою, достатньою є І група з електробезпеки. Працівники, які здійснюють обслуговування систем електроживлення або джерел безперебійного живлення, повинні мати вищу кваліфікаційну групу відповідно до характеру виконуваних робіт [4].

Однією з обов'язкових умов допуску до роботи є проходження періодичних інструктажів. Повторний інструктаж проводиться для підтримання належного рівня знань працівників щодо вимог охорони праці та безпечної експлуатації обладнання. Крім того, позапланові інструктажі проводяться у випадках зміни технологічного процесу, модернізації обладнання або після виникнення аварійних ситуацій [5].

Важливим елементом системи електробезпеки є навчання працівників наданню домедичної допомоги особам, які постраждали від дії електричного струму. Персонал повинен знати порядок звільнення потерпілого від дії струму, правила виклику екстрених служб та основні прийоми серцево-легеневої реанімації [3].

Таким чином, виконання законодавчих вимог щодо навчання та допуску працівників до експлуатації електроустановок є необхідною умовою безпечної роботи комп'ютерної мережі компанії «ІТ-М», сприяє зменшенню ризику нещасних випадків та забезпечує належний рівень електробезпеки на підприємстві.

Під час гасіння пожежі порошковими вогнегасниками потрібно брати до уваги те, що утворюється висока запиленість і, як наслідок, знижується видимість у приміщенні.

5.2 Призначення та завдання пожежної охорони в компанії “ІТ-М”

Під час експлуатації комп'ютерної мережі компанії «ІТ-М» використовується значна кількість електронного обладнання, яке споживає електричну енергію та працює в безперервному режимі. До складу мережевої інфраструктури входять сервери, комутатори, маршрутизатори, джерела безперебійного живлення, робочі станції користувачів та інші технічні засоби. Наявність великої кількості електрообладнання підвищує вимоги до забезпечення пожежної безпеки та організації ефективної системи протипожежного захисту [1].

Пожежна охорона на підприємстві призначена для попередження виникнення пожеж, захисту життя та здоров'я працівників, збереження матеріальних цінностей і забезпечення безперервної роботи інформаційної інфраструктури компанії. Основною метою пожежної охорони є своєчасне виявлення потенційних джерел займання та реалізація заходів, спрямованих на недопущення виникнення пожежонебезпечних ситуацій [6].

Одним із головних завдань пожежної охорони є контроль за дотриманням встановлених вимог пожежної безпеки. Для цього здійснюється регулярна перевірка стану електричних мереж, електрощитового обладнання, джерел безперебійного живлення та інших технічних засобів, які можуть стати

причиною виникнення займання. Особлива увага приділяється контролю за справністю електричних кабелів, станом контактних з'єднань та роботою систем захисту від коротких замикань і перевантажень [1].

Важливим напрямом діяльності є забезпечення приміщень первинними засобами пожежогасіння. У службових та технічних приміщеннях компанії повинні бути встановлені вогнегасники відповідного типу, придатні для ліквідації загорянь електрообладнання. Місця розташування вогнегасників необхідно позначати спеціальними знаками безпеки, що забезпечують швидкий доступ до них у разі виникнення надзвичайної ситуації [3].

До завдань пожежної охорони також належить організація навчання персоналу правилам пожежної безпеки. Працівники повинні знати порядок повідомлення пожежно-рятувальних служб, місця розташування евакуаційних виходів, правила використання вогнегасників та порядок евакуації з будівлі. Регулярне проведення інструктажів дозволяє підвищити рівень готовності персоналу до дій в аварійних ситуаціях [3].

Особливого значення набуває забезпечення безпечної експлуатації серверних приміщень. У таких приміщеннях концентрується значна кількість електронного обладнання, що працює цілодобово. Для зменшення ризику виникнення пожеж необхідно контролювати температурний режим, не допускати накопичення пилу, своєчасно проводити профілактичне обслуговування обладнання та забезпечувати справність систем електроживлення [5].

У разі виникнення пожежі одним із завдань пожежної охорони є організація безпечної евакуації працівників. Для цього на підприємстві розробляються плани евакуації, визначаються відповідальні особи та забезпечується вільний доступ до евакуаційних виходів. Наявність чітко визначеного алгоритму дій дозволяє мінімізувати наслідки надзвичайної ситуації та зменшити ризик травмування персоналу [5].

Отже, пожежна охорона в компанії «ІТ-М» виконує комплекс важливих функцій, спрямованих на попередження пожеж, захист працівників та забезпечення безпечної експлуатації комп'ютерної мережі. Виконання заходів пожежної безпеки сприяє підвищенню надійності роботи інформаційної інфраструктури та збереженню матеріальних ресурсів підприємства.

5.3 Створення оптимальних мікрокліматичних умов у приміщеннях з підвищеним виділенням тепла від техніки

Під час функціонування комп'ютерної мережі компанії «ІТ-М» значна кількість електронного обладнання працює в безперервному режимі та виділяє теплову енергію. Найбільшими джерелами тепловиділення є сервери, комутатори, маршрутизатори, джерела безперебійного живлення та системи зберігання даних. Підвищення температури в приміщеннях може негативно впливати як на працездатність персоналу, так і на надійність функціонування технічних засобів, тому створення оптимального мікроклімату є важливою складовою охорони праці [3].

Мікроклімат виробничого приміщення характеризується температурою повітря, відносною вологістю, швидкістю руху повітря та інтенсивністю теплового випромінювання. Підтримання цих параметрів у нормативних межах дозволяє забезпечити комфортні умови праці та зменшити негативний вплив виробничих факторів на організм людини [5.

Особливої уваги потребують приміщення, у яких розміщується серверне обладнання. У процесі роботи серверів відбувається постійне виділення тепла, що може призводити до перегріву електронних компонентів. Підвищення температури навіть на декілька градусів здатне негативно впливати на стабільність роботи обладнання, скорочувати термін його експлуатації та підвищувати ймовірність виникнення відмов [6].

Для підтримання необхідних параметрів мікроклімату в серверних приміщеннях доцільно використовувати системи кондиціонування повітря. Кондиціонери забезпечують відведення надлишкового тепла та підтримання стабільної температури незалежно від пори року. При проєктуванні комп'ютерної мережі компанії «ІТ-М» доцільно передбачити встановлення окремої системи кондиціонування для серверного приміщення, що забезпечить безперервну роботу обладнання навіть у разі значних теплових навантажень [3].

Крім кондиціонування, важливу роль відіграє вентиляція приміщень. Система вентиляції забезпечує видалення нагрітого повітря та надходження свіжого повітря із зовнішнього середовища. Ефективна вентиляція сприяє підтриманню необхідного рівня вологості та покращує загальний стан повітряного середовища в приміщенні [3].

Під час розміщення обладнання необхідно враховувати особливості циркуляції повітряних потоків. Серверні шафи та мережеві стійки повинні встановлюватися таким чином, щоб не створювати перешкод для проходження охолодженого повітря. Для покращення тепловідведення рекомендується залишати технологічні проходи між рядами обладнання та забезпечувати вільний доступ до вентиляційних отворів пристроїв [5].

Важливим заходом є регулярне технічне обслуговування обладнання. Пил, який накопичується в системах охолодження серверів та комутаторів, знижує ефективність теплообміну та може стати причиною перегріву електронних компонентів. Тому необхідно періодично очищувати вентиляційні отвори, радіатори та вентилятори від забруднень [3].

Для контролю параметрів мікроклімату доцільно використовувати датчики температури та вологості. Отримана інформація дозволяє своєчасно виявляти відхилення від нормативних значень та вживати заходів щодо усунення несприятливих факторів. У сучасних серверних приміщеннях такі датчики можуть інтегруватися в систему моніторингу мережевої інфраструктури та

автоматично повідомляти відповідальних осіб про виникнення небезпечних ситуацій.

Таким чином, створення оптимальних мікрокліматичних умов у приміщеннях з підвищеним виділенням тепла від техніки є важливою умовою забезпечення безпечної роботи персоналу та надійного функціонування комп'ютерної мережі компанії «ІТ-М». Використання систем вентиляції, кондиціонування та постійного контролю параметрів повітряного середовища дозволяє підтримувати належні умови експлуатації обладнання та сприяє підвищенню ефективності роботи підприємства.

ВИСНОВКИ

Результатом кваліфікаційної роботи є повністю спроектована комп'ютерна мережа компанії «ІТ-М». Вибрано стандарт та обладнання для провідного та безпровідного сегментів мережі. Описано процедуру конфігурування мережевого обладнання. При конфігуруванні мережевого обладнання та сервісів було враховано питання безпеки даних, що будуть зберігатися на серверах.

Особливу увагу приділено налаштуванню служб локальної мережі. Наведені інструкції можна практично використати для середніх за розміром локальних мереж.

В економічному розділі зроблено розрахунок собівартості робіт по розробці, встановленню та налаштуванню мережі компанії «ІТ-М».

В розділі охорона праці описано техніку безпеки при роботі з обчислювальною технікою та мережевим обладнанням.

ПЕРЕЛІК ПОСИЛАНЬ

1. Азаров О. Д., Захарченко С. М., Кадук О. В., Орлова М. М., Тарасенко В. П. Комп’ютерні мережі : навч. посіб. Вінниця : ВНТУ, 2020. 168 с.

2. Буров Є.В. Комп’ютерні мережі. Підручник. Том перший /Є.В. Буров, М.М. Митник - Львів: Видавництво ПП «Магнолія 2006» – 333 с.

3. Вахонєва Т.М. Основи охорони праці в Україні: навч. посіб. К.: Дакор, 2019. - 508 с.

4. Контроль та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології: навч. посіб. / А. М. Гуржій, С. Ф. Коряк, В. В. Самсонов, О. Я. Скляров. Харків: СМІТ, 2016. 544 с

5. Луценко Т. О., Калюжний В. С., Данілін О. М., Савченко О. В., Надьон О. В., Долгодуш М. М. Правові основи охорони праці : навч. посіб. Харків : НУЦЗУ, 2023. 223 с. URL: https://duikt.edu.ua/uploads/l_677_97327074.pdf (дата звернення: 02.06.2026).

6. Мелех Л. В. Безпека життєдіяльності та охорона праці : навч. посіб. Львів : Львівський державний університет внутрішніх справ, 2022. - 219 с.

7. Методичні вказівки до виконання кваліфікаційної роботи за спеціальністю 123 Комп’ютерна інженерія». Тернопіль. ВСП «ТФК ТНТУ», 2022.

8. Микитишин А.Г., Митник, П.Д. Стухляк. Телекомунікаційні системи та мережі. Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. 384 с.

9. Пашорін В. І., Костюк Ю. В. Видавець ФОП Марченко Т.В. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – 2-ге видання, виправлене і доповнене – Львів: Видавець ФОП Марченко Т.В. – 376 с.

10. Пистун І.П., Кіт Ю.В., Березовський А.П. Охорона праці: Практикум. Суми: Вид-во «Університетська книга», 2016.

11. Хомуляк М. О. Адміністрування комп’ютерних систем і мереж: навч. посібник / М. О. Хомуляк – Львів: “Магнолія – 2006” – 153 с.

12. D-Link . URL: https://www.dlink.com/ua/uk/for-business/switching. (дата звернення: 24.05.2026).

13. How to edit iptables rules. URL: https://docs.fedoraproject.org/en-US/quick-docs/how-to-edit-iptables-rules/. (дата звернення: 01.06.2026).

14. MikroTik-cAP-ac URL: https://www.technotrade.com.ua/Products/MikroTik-cAP-ac.php (дата звернення: 25.05.2026).

15. VLAN Trunk. URL: https://www.solarwindsmsp.com/blog/vlan-trunking/. (дата звернення: 01.06.2026).

16. VLAN. URL: https://fedoraproject.org/wiki/Networking/VLAN/. (дата звернення: 01.06.2026).

17. Кабель категорії 6. URL: https://uk.wikipedia.org/wiki/%D0%92%D0%B8%D1%82%D0%B0_%D0%BF%D0%B0%D1%80%D0%B0/. (дата звернення: 20.05.2026).

18. Комутатор DGS-1100. URL: https://lanmarket.ua/ua/upravlyaemyy-urovnya-2-/dgs-1100. (дата звернення: 20.05.2026).

19. Огляд технологій, застосованих для побудови локальних мереж. URL: http://easy-code.com.ua/2016/08/oglyad-texnologij-zastosovuvanix-dlya-pobudovi-lokalnix-merezh-lokalni-merezhi-statti/. (дата звернення: 20.05.2026).

20. Реалізація Linux Fedora Server. URL: https://books.google.com.ua/books?id=MfH9B0oF1pEC&pg=PA363&lpg=PA363&dq=vlan+linux+fedora&source=bl&ots=Rs_L-bU8-w&sig=ACfU3U2Tgq4KKPoH_WCMItJDMZ5zNwxhNg&hl=uk&sa=X&ved=2ahUKEwjrwunP3tvpAhU1wcQBHT1IAgUQ6AEwB3oECAoQAQ#v=onepage&q=vlan%20linux%20fedora&f=false/. (дата звернення: 03.06.2026).

21. Сервер LENOVO ThinkSystem ST50 URL: https://www.moyo.ua/server-lenovo-thinksystem-st50-7y48a007ea/446190.html (дата звернення: 27.05.2026).

22. Шафа комутаційна. URL: https://net-server.com.ua/shkaf-nastennyy-19-15u-600kh500mm-shg-razbornoy-chernyy-ua-mgswa155b/ (дата звернення: 27.05.2026).

ДОДАТКИ

Додаток А. IP –адресація

Таблиця А1 – Таблиця IP-адрес

№ п/п	Назва вузла	IP-адреса	Маска	Шлюз	VLAN	DNS	Назва відділу
1	2	3	4	5	6	7	8
1	WS_1	192.168.11.1	/24	192.168.11.254	11	192.168.18.253	Менеджери проєктів
2	WS_2	192.168.11.2	/24	192.168.11.254	11	192.168.18.253	
3	WS_3	192.168.11.3	/24	192.168.11.254	11	192.168.18.253	
4	WS_4	192.168.11.4	/24	192.168.11.254	11	192.168.18.253	
5	WS_5	192.168.12.1	/24	192.168.12.254	12	192.168.18.253	Бухгалтерія і відділ розрахунків
6	WS_6	192.168.12.2	/24	192.168.12.254	12	192.168.18.253	
7	WS_7	192.168.12.3	/24	192.168.12.254	12	192.168.18.253	
8	WS_8	192.168.12.4	/24	192.168.12.254	12	192.168.18.253	
9	WS_9	192.168.12.5	/24	192.168.12.254	12	192.168.18.253	
10	WS_10	192.168.13.1	/24	192.168.13.254	13	192.168.18.253	Переговорна і зал засідань
11	WS_11	192.168.14.1	/24	192.168.14.254	14	192.168.18.253	Відділ технічної підтримки
12	WS_12	192.168.14.2	/24	192.168.14.254	14	192.168.18.253	
13	WS_13	192.168.14.3	/24	192.168.14.254	14	192.168.18.253	
14	WS_14	192.168.14.4	/24	192.168.14.254	14	192.168.18.253	
15	WS_15	192.168.15.1	/24	192.168.15.254	15	192.168.18.253	Кабінет директора
16	WS_16	192.168.16.1	/24	192.168.16.254	16	192.168.18.253	Офіс-менеджер
17	WS_17	192.168.17.1	/24	192.168.17.254	17	192.168.18.253	Заступник директора
18	WS_18	192.168.17.2	/24	192.168.17.254	17	192.168.18.253	
19	WS_19	192.168.18.1	/24	192.168.18.254	18	192.168.18.253	Відділ комп’ютерного забезпечення
20	WS_20	192.168.18.2	/24	192.168.18.254	18	192.168.18.253	
21	WS_21	192.168.19.1	/24	192.168.19.254	19	192.168.18.253	Відділ розробки
22	WS_22	192.168.19.2	/24	192.168.19.254	19	192.168.18.253	
23	WS_23	192.168.19.3	/24	192.168.19.254	19	192.168.18.253	
24	WS_24	192.168.19.4	/24	192.168.19.254	19	192.168.18.253	
25	WS_25	192.168.19.5	/24	192.168.19.254	19	192.168.18.253	
26	WS_26	192.168.19.6	/24	192.168.19.254	19	192.168.18.253	
27	WS_27	192.168.19.7	/24	192.168.19.254	19	192.168.18.253	
28	WS_28	192.168.19.8	/24	192.168.19.254	19	192.168.18.253	
29	WS_29	192.168.19.9	/24	192.168.19.254	19	192.168.18.253	
30	WS_30	192.168.19.10	/24	192.168.19.254	19	192.168.18.253	
31	WS_31	192.168.19.11	/24	192.168.19.254	19	192.168.18.253	
32	WS_32	192.168.19.12	/24	192.168.19.254	19	192.168.18.253	
33	WS_33	192.168.19.13	/24	192.168.19.254	19	192.168.18.253	
34	WS_34	192.168.19.14	/24	192.168.19.254	19	192.168.18.253	
35	AP_1	192.168.20.100 (діапазон 192.168.20.1-192.168.20.99)		192.168.11.254	20	192.168.18.253	(спільна)

Продовження таблиці А1

1	2	3	4	5	6	7	8
36	AP_2	192.168.20.200 (діапазон 192.168.20.101-192.168.20.199)	/24	192.168.20.254	20	192.168.18.253	(спільна)
37	SW_1	192.168.10.201	/24	192.168.10.254	1	192.168.18.253	
38	SW_2	192.168.10.202	/24	192.168.10.254	1	192.168.18.253	
39	SW_3	192.168.10.203	/24	192.168.10.254	1	192.168.18.253	
40	SW_4	192.168.10.204	/24	192.168.10.254	1	192.168.18.253	
41	S_1	192.168.18.253	/24	192.168.18.254	18	192.168.18.253	Відділ комп'ютерного забезпечення
42	S_2	192.168.18.254	/24	Динамічна	18	Динамічно	Відділ комп'ютерного забезпечення
		Динамічна			-		

Додаток Б. Налаштування VLAN

Таблиця Б1 - Таблиця логічної адресації локальної мережі

Позначення вузлів	Робоча група/ Кількість вузлів		Назва кабінету та його номер		Номер VLAN	Адреса підмережі/Маска
WS_1-WS4, SW_1	-	5	Менеджери проєктів	5	11	192.168.11.0 / 24
WS_5-WS_9, SW_2	-	4	Бухгалтерія і відділ розрахунків	4	12	192.168.12.0 / 24
WS_10	-	1	Переговорна і зал засідань	12	13	192.168.13.0 / 24
WS_11-WS_14, SW_3	-	5	Відділ технічної підтримки	7	14	192.168.14.0 / 24
WS_15	-	1	Кабінет директора	1	15	192.168.15.0 / 24
WS_16	-	1	Офіс-менеджер	2	16	192.168.16.0 / 24
WS_17-WS_18	-	2	Заступник директора	3	17	192.168.17.0 / 24
WS_19-WS_20, S_1, S_2, SW_4	-	5	Відділ комп’ютерного забезпечення	6	18	192.168.18.0 / 24
WS_21-WS_34, SW_5,SW_6	-	15	Відділ розробки	13	19	192.168.19.0 / 24
AP_1, AP_2	-	2			20	192.168.20.0 / 24

Таблиця Б2 - Таблиця конфігурування VLAN

№ п/п	Позначення вузла	Номер порту	Тип порту	Назва мережевого пристрою	Номер порту	Тип порту	Номер VLAN
1	2	3	4	5	6	7	8
1	WS_1-WS4	-	-	SW_1	2-5	Access	11
2	WS_5-WS_9	-	-	SW_2	2-6	Access	12
3	WS_10	-	-	SW_4	14	Access	13
4	WS_11-WS_14	-	-	SW_3	2-5	Access	14
5	WS_15	-	-	SW_4	13	Access	15
6	WS_16	-	-	SW_4	12	Access	16
7	WS_17-WS_18	-	-	SW_4	10-11	Access	17
8	WS_19-WS_20, S_1, S_2	-	-	SW_4	6-7, 8-9	Access	18
9	WS_21-WS_34	-	-	SW_5	2-14	Access	19
10	AP_1, AP_2	-	-	SW_4	5,15	Access	20
11	SW_1	1	Trunk	SW_4	1	Trunk	-
12	SW_2	1	Trunk	SW_4	2	Trunk	-
13	SW_3	1	Trunk	SW_4	3	Trunk	-
14	SW_5	1	Trunk	SW_4	4	Trunk	-
14	SW_6	1	Trunk	SW_4	5	Trunk	-

Додаток В. Порівняння обладнання

Таблиця В1 - Порівняння технічних показників безпровідних точок доступу

Характеристика	Wi-Fi Cisco CBW240AC-E	Mikrotik RBcAPGi-5acD2nD	Linksys LAPAC 2600C-EU
Відповідність стандартам	IEEE 802.11 a, IEEE 802.11 ac, IEEE 802.11 b, IEEE 802.11 g, IEEE 802.11 n, IEEE 802.3af PoE, IEEE 802.x		
WAN-інтерфейс	1Гбіт/с		
Частота	2,4 Ггц, 5Ггц		
Безпека даних	WEP, WPA, WPA-PSK, WPA2-ENT, WPA2-PSK		
Керування	Веб		
Наявність DHCP-сервера	Так		

Таблиця В2 - Порівняння технічних характеристик центральних комутаторів

Характеристика	D-Link DGS-3130-30TS	Cisco Catalyst 3750G-24	Ubiquiti UniFi Switch PRO 24
Підтримка функцій 2-го рівня моделі OSI	Так	Так	Так
Підтримка базових функцій 3-го рівня моделі OSI	Так	Так	Так
Комутація кадрів/пакетів	96 Гбіт/с	32 Гбіт/с	88 Гбіт/с
Кадрів/пакетів в секунду	71,4	38,7	64,47
К-сть портів 100/1000	24+4	24+2	24+2
Засоби віддаленого керування	WEB, Telnet, SSH	WEB, Telnet, SSH	WEB, Telnet, SSH

Таблиця В3 - Порівняння параметрів комутаторів робочої групи

Технічний параметр	TP-LINK TL-SG2210P	D-Link DGS-1100-8	Cisco SG200
Управління	керований	керований	керований
Кількість портів	8	8	8
Підтримувана швидкість	10/100/1000 Мбіт/с	10/100/1000 Мбіт/с	10/100/1000 Мбіт/с
Підтримувані основні мережеві протоколи	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab		

Таблиця В4 - Порівняльний аналіз 16-ти портових комутаторів

Технічні характеристики/ модель комутатора	D-Link DGS-1100-16	TP-LINK TL-SG2216	Cisco C1000-16T-2G
Швидкість шини, Гбіт/с	32	32	32
Швидкість пересилки пакетів 64 байт, млн./с	23,81	23,8	23,8
К-сть портів 10/100/1000	16 + 2 SFP	16 + 2 SFP	16+2 SFP
Підтримка базових протоколів канального рівня (VLAN, Port Mirroring, Spanning Tree, IGMP, QoS)	Так	Так	Так

Таблиця В5 - Порівняльна характеристика апаратних платформ серверів

	Dell EMC T40	LENOVO ThinkSystem ST50
Процесор	Intel Xeon E-2224G (3,5 - 4,7 ГГц)	Intel Xeon E-2224G (3.5 - 4.7 ГГц)
Пам’ять	32ГБ (DDR4-2400)	32ГБ (DDR4-2400)
ЖМД	HDD: 2 x 2 ТБ; SSD: 2 x 512 ГБ	HDD: 2 x 2 ТБ; SSD: 2 x 512 ГБ
RAID-контролер	Intel Rapid Storage	Intel Rapid Storage
Мережевий адаптер	2 x 1000Мбіт/с (інтегрований)	2 x 1000Мбіт/с (інтегрований)
БЖ	650Вт	650Вт
Відеоадаптер	інтегрований	інтегрований

Додаток Г. Технічні характеристики D-Link DGS-1100-08/16.

Кількість портів:

1. 8 чи 16 портів 10/100/1000BaseT.

Функції на портах:

1. IEEE 802.3.
2. IEEE 802.3u.
3. Підтримка режиму повного/напівдуплекса (для напівдуплекса 10/100Мбіт/с, для повного дуплексу 1000 Мбіт/с).
4. Автопогодженням.
5. Автовизначення MDI/MDIX.
6. Управління потоком IEEE 802.3x в режимі повного дуплексу.
7. IEEE 802.3az.

Продуктивність:

1. Пропускна здатність комутатора: 16 Гбіт/с.
2. Максимальна швидкість перенаправлення пакетів: 11.9 Mpps.
3. Таблиця MAC-адрес: 8K записів на пристрій.
4. Буфер пакетів: 2 Мб.
5. Flash-пам'ять: 2 МБ.

Індикатори:

1. Power (на пристрій).
2. Link/Activity/Speed (на порт).

VLAN:

1. На основі порту.
2. 802.1Q tagged VLAN.
3. Surveillance VLAN.
4. Management VLAN.
5. Групи VLAN: Макс. 32 статичних VLAN, Макс. 4094 VIDs.

Функції рівня 2:

1. Таблиця MAC-адрес: 8K.

2. Управління потоком: Управління потоком 802.3x, Запобігання блокування HOL.

3. Jumbo-фрейми розміром до 9216 байт.

4. IGMP Snooping: IGMP v1/v2 Snooping, Підтримка до 32 IGMP-груп.

5. Link Aggregation: 2 групи, 2-4 порту на групу.

6. Функція Loopback Detection.

7. Діагностика кабелю.

8. Port Mirroring: One-to-One.

9. Статистика: Tx Ok, Tx Error, Rx Ok, Rx Error.

Якість обслуговування (QoS):

1. 802.1p.

2. 4 черги на порт.

3. Механізми обробки черг: Strict, Weighted Round Robin (WRR).

4. Управління смугою пропускання: На основі порту (вхідні/вихідні, вибирається зі списку з мінімальним значенням 8 Кбіт/с).

Додаток Д. Технічні характеристики точки доступу MikroTik CAP AC (RBCAPGI-5ACD2ND.

Операційна система: RouterOS L4

CPU: 716 MHz

ROM/RAM: 128Мб

Локальна пам'ять: 16МБ, Flash

Ethernet порти (Uplink): 2x RJ45 (1000M)

PoE: 1 порт, passive PoE

Wi-Fi: 2.4 GHz і 5GHz (5 генерація)

Антена: вбудована, 2.5 dBi

Живлення: DC 17-57В / PoE (802.3 af/at)

Потужність споживання: 13Вт

Операційна система: RouterOS L4

CPU: 716 MHz

ROM/RAM: 128Мб

Локальна пам'ять: 16МБ, Flash

Ethernet порти (Uplink): 2x RJ45 (1000M)

PoE: 1 порт, passive PoE

Wi-Fi: 2.4 GHz і 5GHz (5 генерація)

Антена: вбудована, 2.5 dBi

Живлення: DC 17-57В/PoE (802.3 af/at)

Потужність споживання: 13Вт