Міністерство освіти і науки України

Відокремлений структурний підрозділ «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя»
(повне найменування вищого навчального закладу)

Відділення телекомунікацій та електронних систем
(назва відділення)

Циклова комісія комп'ютерної інженерії
(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

бакалавра
(освітній ступінь)

на тему: **Розробка проєкту модернізації комп'ютерної мережі ТОВ «Клео-П»**

Виконав: студент VII курсу, групи КІб-703

Спеціальності **123 Комп'ютерна інженерія**
(шифр і назва спеціальності)

Михайло ЛЮБУНЬ
(ім'я та прізвище)

Керівник Василь ПИЖ
(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 телекомунікацій та електронних систем
Циклова комісія комп'ютерної інженерії
Освітній ступінь бакалавр
Освітньо-професійна програма: Комп'ютерна інженерія
Спеціальність: 123 Комп'ютерна інженерія
Галузь знань: 12 Інформаційні технології

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"18" травня 2026 року

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

Любунь Михайлу Зиновійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи **Розробка проєкту модернізації комп'ютерної мережі ТОВ «Клео-П»**

керівник роботи Пиж Василь Степанович
(прізвище, ім'я, по батькові)

затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університетут імені Івана Пулюя» від 18.05.2026р №4/9-252.

2. Строк подання студентом роботи: 22 червня 2026 року.

3. Вихідні дані до роботи: плани приміщень, завдання на проектування, стандарти побудови СКС, документація на мережеве обладнання і сервери

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

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): План приміщень. Логічна топологія. Фізична топологія. Таблиця IP-адрес. Таблиця техніко-економічних показників. Модель мережі

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Ірина ЛЕЩИК методист, викладач		
Безпека життєдіяльності, основи охорони праці	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	18.05	
2	Збір і узагальнення інформації	21.05	
3	Написання першого розділу	25.05	
4	Розробка технічного та робочого проекту	1.06	
5	Написання спеціального розділу	8.06	
6	Розрахунок економічної частини	11.06	
7	Написання розділу охорони праці	12.06	
8	Виконання графічної частини	14.06	
9	Оформлення проекту	18.06	
10	Погодження нормоконтролю	19.06	
11	Попередній захист роботи	22.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 18 травня 2026 року

Студент _____ Михайло ЛЮБУНЬ
(підпис) (ім'я та прізвище)

Керівник роботи _____ Василь ПИЖ
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Любунь М З Розробка проєкту модернізації комп’ютерної мережі ТОВ «Клео-П»: кваліфікаційна робота на здобуття освітньо-професійного ступеня бакалавра, за спеціальністю 123 Комп’ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2026. -85с.

У даній кваліфікаційній роботі розглянуто та реалізовано проєкт модернізації корпоративної комп’ютерної мережі ТОВ «Клео-П» з урахуванням об’єднання віддалених структурних підрозділів.

Метою роботи є розробка та впровадження ефективної, відмовостійкої та захищеної мережевої інфраструктури підприємства. Для досягнення поставленої мети було вирішено такі завдання:

– У першому розділі сформовано та обґрунтовано технічне завдання на проєктування мережі, проаналізовано вихідні вимоги замовника та специфіку роботи ТОВ «Клео-П».

– У другому розділі проведено аналіз архітектури та плану приміщень підприємства, обґрунтовано вибір ієрархічної топології мережі. Розроблено логічну структуру з розподілом на віртуальні локальні мережі (VLAN), схему організації захищеного VPN-тунелю між корпусами, а також здійснено підбір сучасного комутаційного обладнання (на базі рішень MikroTik та L2-комутаторів доступу) і серверних платформ.

– У третьому розділі описано практичну реалізацію проєкту: наведено конфігураційні скрипти для налаштування маршрутизаторів під управлінням RouterOS, параметризацію VLAN, організацію VPN-з'єднання, а також комплекс засобів захисту мережі від шкідливого програмного забезпечення та несанкціонованого втручання.

– У четвертому розділі виконано техніко-економічне обґрунтування проєкту, розраховано капітальні та експлуатаційні витрати на розгортання мережі, визначено економічну ефективність модернізації.

– У п'ятому розділі висвітлено питання охорони праці, техніки безпеки та екологічних вимог під час проєктування, монтажу та експлуатації мережевого обладнання.

Пояснювальний матеріал роботи ілюстрований графічними схемами, аналітичними таблицями та рисунками.

Кваліфікаційна робота складається з двох основних частин:

1. Пояснювальна записка об'ємом ____ аркушів формату А4.

2. Графічний матеріал (демонстраційні плакати) об'ємом ____ аркушів формату А1.

ANNOTATION

Lyubun M Z Development of a project for the modernization of the computer network of LLC "Cleo-P": qualification work for obtaining an educational and professional bachelor's degree, specialty 123 Computer Engineering. Ternopil: VSP "TFK TNTU", 2026. -85p.

This qualification work considers and implements a project for the modernization of the corporate computer network of LLC "Cleo-P" taking into account the unification of remote structural divisions. The purpose of the work is to develop and implement an effective, fault-tolerant and secure network infrastructure of the enterprise.

To achieve the set goal, the following tasks were solved: • In the first section, the technical task for the network design was formed and substantiated, the initial requirements of the customer and the specifics of the work of LLC "Cleo-P" were analyzed.

- In the second section, an analysis of the architecture and layout of the enterprise's premises was carried out, the choice of a hierarchical network topology was justified. A logical structure with a division into virtual local area networks (VLANs), a scheme for organizing a secure VPN tunnel between buildings, and a selection of modern switching equipment (based on MikroTik solutions and L2 access switches) and server platforms were developed.
- The third section describes the practical implementation of the project: configuration scripts for configuring routers under RouterOS management, VLAN parameterization, organization of VPN connections, as well as a set of network protection tools against malicious software and unauthorized interference are provided.
- The fourth section provides a feasibility study of the project, calculates capital and operating costs for network deployment, and determines the economic efficiency of modernization.
- The fifth section highlights issues of labor protection, safety and environmental requirements during the design, installation and operation of network equipment.

The explanatory material of the work is illustrated with graphic diagrams, analytical tables and figures.

The qualification work consists of two main parts: 1. Explanatory note of ___ sheets of A4 format. 2. Graphic material (demonstration posters) of ___ sheets of A1 format.

ЗМІСТ

					2026.КРБ.123.703.09.00.00 ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Любцнь М З			Розробка проєкту модернізації комп'ютерної мережі ТОВ «Клео-П» Пояснювальна записка	Літ.	Арк.	Аркушів
Перевір.		Пиж В С						
Реценз.						ВСП ТФК ТНТУ КІ-703 м. Тернопіль		
Н. Контр.								
Затверд.								

ВСТУП

Актуальність теми. На сучасному етапі розвитку інформаційних технологій успішне функціонування будь-якого підприємства, незалежно від його масштабів та специфіки діяльності, критично залежить від ефективності його комунікаційної інфраструктури. Цифрова трансформація бізнесу, інтеграція хмарних сервісів, різке збільшення обсягів мультимедійного трафіку та необхідність забезпечення безперервного доступу до корпоративних ресурсів висувають жорсткі вимоги до корпоративних комп'ютерних мереж. Додатковим викликом для сучасного бізнесу є географічна розподіленість підрозділів (філіалів, окремих корпусів) та необхідність організації гнучких умов для віддаленої роботи співробітників.

Особливого значення набуває модернізація застарілих мережевих архітектур, які вже не здатні забезпечити належну пропускну здатність, масштабованість та належний рівень інформаційної безпеки. Традиційні однорангові мережі без чіткого логічного поділу є вразливими до внутрішніх загрозах, широкомовного шторму та несанкціонованого доступу до конфіденційних даних. У зв'язку з цим, впровадження ієрархічних моделей проектування, технологій віртуальних локальних мереж (VLAN), а також побудова захищених каналів зв’язку (VPN) за допомогою сучасного багатофункціонального обладнання є пріоритетним завданням для забезпечення стабільності бізнес-процесів.

Об'єктом модернізації у даній кваліфікаційній роботі є комп'ютерна мережа товариства з обмеженою відповідальністю «Клео-П». Поточний стан мережевої інфраструктури підприємства характеризується децентралізацією, відсутністю логічної сегментації трафіку та незахищеністю каналів зв’язку між територіально відокремленими корпусами, що створює значні ризики для безпеки та стабільності роботи.

Ефективним та економічно вигідним рішенням для розв'язання цих проблем є перехід на кероване мережеве обладнання під управлінням операційної

системи RouterOS від компанії MikroTik. Це дозволяє гнучко налаштовувати маршрутизацію, впроваджувати багаторівневі політики безпеки (Firewall, NAT, системи виявлення вторгнень) та організовувати криптографічно захищені VPN-тунелі промислового рівня без надмірних капітальних витрат на ліцензування.

Метою кваліфікаційної роботи є розробка, теоретичне обґрунтування та практична реалізація проєкту модернізації корпоративної комп'ютерної мережі ТОВ «Клео-П» на основі сучасних мережевих технологій та обладнання MikroTik для забезпечення високої продуктивності, масштабованості та захищеності корпоративних даних.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– Проаналізувати поточний стан мережевої інфраструктури ТОВ «Клео-П», виявити її вразливі місця та сформувати технічне завдання на проектування.

– Розробити оптимальну логічну та фізичну топологію мережі, враховуючи наявність віддаленого корпусу.

– Спроектувати схему логічної сегментації мережі за допомогою технології VLAN та розробити раціональний IP-план адресації.

– Обґрунтувати вибір активного та пасивного мережевого обладнання, а також серверних платформ.

– Розробити конфігураційні скрипти для налаштування маршрутизаторів MikroTik (керування VLAN, DHCP, маршрутизація, організація VPN-тунелю).

– Запропонувати комплекс заходів із кібербезпеки, включаючи налаштування міжмережевого екрана та антивірусного захисту.

– Виконати техніко-економічний розрахунок вартості впровадження проєкту та оцінити його ефективність.

– Проаналізувати вимоги з охорони праці та екологічної безпеки під час розгортання та експлуатації мережі.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Основним завданням кваліфікаційної роботи є комплексна модернізація та розробка архітектури корпоративної комп’ютерної мережі для ТОВ «Клео-П». Створення нової інфраструктури покликане вирішити низку критичних завдань для бізнесу та проєктується з урахуванням таких ключових вимог:

– Логічне та фізичне об’єднання розподілених структурних підрозділів. Проєкт передбачає створення єдиного інформаційного простору для всіх робочих станцій, що входять до складу різних відділів підприємства. Особлива увага приділяється інтеграції територіально віддаленого корпусу (філіалу) з головним офісом шляхом побудови захищеного криптографічного VPN-тунелю через публічні канали зв'язку. Це забезпечить прозору взаємодію співробітників так, ніби вони перебувають в одній локальній мережі.

– Організація спільного високошвидкісного та відмовостійкого доступу до мережі Інтернет. Оскільки точка входу інтернет-провайдера (WAN-інтерфейс) розташована в головному корпусі на прикордонному маршрутизаторі, архітектура мережі має забезпечувати раціональний розподіл пропускної здатності каналу між усіма користувачами обох корпусів. Для цього впроваджуються механізми трансляції мережевих адрес (NAT) та політики управління трафіком (QoS/QoS Shaper) на базі обладнання MikroTik.

– Забезпечення централізованого доступу до локальних та глобальних мережевих служб. Користувачі підприємства повинні мати безперешкодний, але чітко розмежований доступ до внутрішніх корпоративних сервісів (серверів баз даних, файлових сховищ, мережевих принтерів), а також до зовнішніх хмарних служб, корпоративної пошти та веб-ресурсів. Це

досягається шляхом розгортання служб DHCP, DNS та сегментації мережі на віртуальні підмережі (VLAN) з налаштуванням правил міжсегментного екранування (Firewall).

– Впровадження економічно ефективних засобів комунікації та обміну даними. Одним із пріоритетів проєкту є зниження капітальних (CAPEX) та експлуатаційних (OPEX) витрат підприємства на зв'язок. Використання технології VPN поверх звичайного інтернету замість оренди дорогих виділених ліній, а також вибір багатофункціонального та доступного обладнання MikroTik (RouterOS) дозволяє створити надійний і дешевий засіб швидкісного обміну інформацією без потреби купувати дорогі ліцензії.

1.1.2 Призначення розробки

Проєктована мережа призначена для забезпечення стабільної інформаційної інфраструктури ТОВ «Клео-П», яке функціонує як туристична агенція. Специфіка бізнесу пов’язана з постійною обробкою великих обсягів зовнішніх даних (онлайн-бронювання туров, авіаквитків, готелів), роботою з медіафайлами, веденням CRM-систем та збереженням персональних даних клієнтів.

Основні функції та завдання розробки:

– Внутрішній документообіг: створення швидкісного середовища для взаємодії відділів, зокрема обміну даними між Головним офісом та віддаленим корпусом через захищений VPN-канал.

– Централізоване сховище: розгортання корпоративного FTP-сервера для спільного доступу до документів і маркетингових матеріалів. Обладнання розміщується в телекомунікаційній шафі та підключається до ізольованого сегмента з підвищеним рівнем безпеки (VLAN 20 — Servers).

– Доступ до Інтернет та периферії: надання робочим станціям захищеного виходу в глобальну мережу та організація спільного доступу до друкувальної техніки через виділені сегменти (VLAN 40 та VLAN 70).

– Вимоги до продуктивності: Для усунення затримок під час передачі медіафайлів та забезпечення миттєвого відгуку сервісів, архітектура проєктується як повністю гігабітна. Швидкість передачі даних на всіх рівнях мережі становить 1000 Мбіт/с, що ліквідує проблему «вузьких місць» та закладає запас продуктивності для подальшого масштабування.

1.1.3 Вимоги до апаратного та програмного забезпечення

Проєктована мережа підлягає логічній сегментації на робочі групи (VLAN) із забезпеченням уніфікованої швидкості передачі даних 1000 Мбіт/с на всіх ділянках інфраструктури.

Вимоги до апаратного забезпечення:

– Маршрутизатори ядра та розподілу: Центральні пристрої (SW_7, SW_4, SW_9) мають базуватися на гігабітних платформах MikroTik з підтримкою апаратного шифрування IPsec (для VPN) та тегування трафіку (VLAN Trunking).

– Комутатори рівня доступу: Використовуються 16-портові L2-комутатори стандарту 1000Base-T для монтажу в 19-дюймову шафу. Вони мають бути ремонтопридатними та підтримувати базове адміністрування.

– Бездротова інфраструктура: Точка доступу (AP_1) повинна відповідати сучасному стандарту IEEE 802.11ax (Wi-Fi 6) для стабільної роботи в корпоративному середовищі.

Вимоги до програмного забезпечення та безпеки:

– Операційні системи: На робочих станціях (WS_1 – WS_33) передбачено використання Windows 10/11 Pro для забезпечення сумісності з мережевими протоколами. Обладнання маршрутизації має працювати під управлінням MikroTik RouterOS (v7).

– Бездротова безпека: Для захисту Wi-Fi сегмента (VLAN 50) обов'язкова підтримка сучасних стійких протоколів шифрування WPA2-PSK або WPA3-PSK.

1.1.4 Стадії та етапи розробки

Процес проєктування та модернізації корпоративної мережі ТОВ «Клео-П» розподіляється на такі послідовні стадії та етапи:

– Передпроєктне обстеження: детальне вивчення та аналіз наявної мережевої інфраструктури підприємства, виявлення її «вузьких місць», обмежень та технічних проблем.

– Аналіз програмного середовища: визначення складу та вимог прикладного і системного програмного забезпечення (мережевих служб, систем бронювання, баз даних), що буде функціонувати в мережі.

– Розробка архітектури (L1/L2 рівні): вибір типу мережі, обґрунтування оптимальної топології, підбір середовища передачі даних (кабельної інфраструктури) та іншого лінійного обладнання фізичного рівня.

– Розрахунок ємності рівня доступу: визначення точної кількості та конфігурації 16-портових комутаторів для забезпечення підключення всіх робочих груп користувачів та периферії.

– Проєктування комутаційних вузлів: визначення архітектури головного (ГКВ) та проміжних (ПКВ) телекомунікаційних вузлів, розрахунок стійко-місць у шафах для розміщення заліза.

– Обґрунтування засобів маршрутизації та безпеки: визначення потреби та вибір параметрів маршрутизаторів ядра й периметра (MikroTik) для організації міжмережевої взаємодії та захищених VPN-тунелів.

1.1.5 Вимоги до документації

У результаті виконання проєктних робіт та для забезпечення можливості подальшого обслуговування й масштабування мережі ТОВ «Клео-П», має бути розроблений та затверджений комплект такої технічної документації:

– Схема логічної топології мережі: детальний документ, що відображає логічну структуру мережі, розподіл пристроїв за віртуальними ло-

кальними мережами (VLAN 10 – VLAN 70), межі широкомовних доменів, схему IP-адресації, інтерфейси підключення маршрутизаторів MikroTik та логіку організації VPN-тунелю між корпусами.

– Схема фізичної топології мережі: план-схема реального розміщення активного та пасивного мережевого обладнання на об'єктах підприємства, що включає прив'язку до архітектурних планів приміщень, розташування телекомунікаційних шаф, серверів, робочих станцій, принтерів та бездротових точок доступу.

– Кабельний журнал та схеми трасування: документація, що містить маркування та траси прокладання кабельних ліній (структурованої кабельної системи — СКС), специфікацію крос-панелей, розеток, довжину кабельних трас та схеми розключення портів на 16-портових комутаторах доступу.

1.1.6 Техніко-економічні показники

Для оцінки ефективності розробки та впровадження модернізованої мережевої інфраструктури ТОВ «Клео-П» визначено такі ключові техніко-економічні показники, яким має відповідати готовий проєкт:

– Оптимальне співвідношення ціни та функціональності (Cost-Efficiency): використання багатофункціонального обладнання MikroTik під управлінням RouterOS дозволяє уникнути значних капітальних витрат на придбання додаткових ліцензій для маршрутизації, брандмауера чи VPN. Мережа проектується як сучасна, економічно вигідна, але з високим рівнем надійності корпоративного класу (Enterprise).

– Високий потенціал масштабованості (Scalability): архітектура мережі та вибір 16-портових комутаторів доступу закладають необхідний резерв вільних портів (не менше 30%). Це дозволяє підприємству розширювати штат працівників, підключати нові робочі станції чи периферійне обладнання без необхідності повної перебудови чи заміни ядра мережі.

– Пропускна здатність та інтеграція: лінійна структура проєктується з урахуванням швидкості передачі даних 1000 Мбіт/с (1 Гбіт/с). Проєкт забезпечує стабільний, збалансований та захищений доступ до мережі Інтернет для всіх користувачів Головного офісу та віддаленого корпусу.

– Гнучкість та мобільність (Бездротовий сегмент): інтеграція в структуру мережі окремого бездротового сегмента (VLAN 50) на базі точки доступу стандарту Wi-Fi 6 забезпечує мобільність працівників туристичної агенції всередині офісу та можливість безпечного підключення портативних пристроїв (ноутбуків, смартфонів).

1.1.7 Порядок контролю та прийому

Після успішного завершення всіх тестових процедур, підтвердження відсутності втрат пакетів та перевірки захищеності периметра мережі, оформляється технічний паспорт об'єкта та підписується двосторонній Акт приймання-передачі виконаних робіт, що засвідчує офіційне введення мережі підприємства в промислову експлуатацію.

Процедура приймання-здачі модернізованої комп'ютерної мережі ТОВ «Клео-П» в експлуатацію передбачає обов'язковий комплексний контроль відповідності виконаних робіт технічному завданню та включає такі етапи:

– Діагностика працездатності мережевих вузлів: проведення повного інструментального та програмного тестування всіх елементів інфраструктури. Перевірці підлягає коректність роботи маршрутизаторів MikroTik, 16-портових комутаторів доступу, серверної зони (VLAN 20), бездротової точки доступу та кінцевих робочих станцій.

– Контроль відповідності маркування кабельної системи: перевірка фізичного стану структурованої кабельної системи (СКС). Усі кабельні лінії, патч-панелі, комутаційні порти та абонентські розетки повинні мати чітке, стійке маркування відповідно до розробленого кабельного журналу. Це

необхідно для забезпечення швидкої діагностики та обслуговування мережі у майбутньому.

– Функціональне тестування за допомогою мережевого інструментарію: перевірка логічної структури мережі, доступності сервісів, правильності роздачі IP-адрес через DHCP та стабільності VPN-тунелю. Тестування виконується як за допомогою базових вбудованих утиліт операційних систем (ping, traceroute, nslookup), так і за допомогою спеціалізованого програмного забезпечення для моніторингу та аналізу трафіку (наприклад, MikroTik Torch, Wireshark, NetWatch).

1.2 Постановка задачі на розробку проекту. Характеристика підприємства, для якого створюється проект мережі

Об'єкт модернізації ТОВ «Клео-П» (туристична агенція) складається з двох територіально розподілених об'єктів: головного офісу та віддаленого корпусу. Згідно з технічним завданням та штатною структурою підприємства, робочі станції, сервери та периферія розподілені по відповідних кабінетах та функціональних зонах таким чином:

1. Головний офіс (Центральний вузол мережі):

– Серверна кімната (Головний комутаційний вузол — ГКВ): тут зосереджено центральне ядро мережі (маршрутизатор-комутатор SW_7), точка входу інтернет-провайдера (WAN), корпоративні сервери (S_1 та S_2), включаючи головний FTP-сервер для збереження даних, а також інше комутаційне та захисне обладнання, що розміщене в 19-дюймовій телекомунікаційній шафі.

– Економічний відділ: робоче місце бухгалтерії та економістів, де встановлено 3 персональні комп'ютери (WS_1 – WS_3), 1 мережевий принтер (PR_1) та локальний комутатор доступу.

– Кабінети керівництва: приміщення директора, помічника керівника та секретаря. Сумарно містять 3 персональні комп'ютери (WS_4 – WS_6) та 1 мережевий принтер (PR_2).

– Конференц-зал (Зона презентацій та бездротового доступу): приміщення для нарад та роботи з клієнтами. Обладнане 5 персональними комп'ютерами (WS_7 – WS_11), 1 мережевим принтером (PR_3), а також бездротовою точкою доступу (AP_1) стандарту Wi-Fi 6 для підключення мобільних пристроїв та ноутбуків.

– Кабінети менеджерів Головного офісу: робочі зони для обслуговування клієнтів. Розподілені на два приміщення, які сумарно містять 6 персональних комп'ютерів (WS_12 – WS_17) та 2 мережевих принтери (PR_4, PR_5).

2. Віддалений корпус (Філіал агенції):

– Кабінети менеджерів Віддаленого корпусу: великий робочий простір для персоналу з продажу турів. Містить 16 персональних комп'ютерів (WS_18 – WS_33) та 2 мережевих принтери (PR_7, PR_8). Для комутації цього корпусу та організації VPN-каналу зв'язку з Головним офісом використовуються маршрутизатори розподілу SW_4 та SW_9.

Сумарно мережа підприємства розрахована на підключення 33 робочих станцій, 2 серверів, 7 мережевих принтерів та 1 бездротової точки доступу, які логічно сегментуються на віртуальні підмережі (VLAN) для оптимізації трафіку та захисту даних.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Розробка та обґрунтування логічної та фізичної схем мережі

При організації комп’ютерної мережі виключно важливим є вибір топології, тобто компонування мережевих пристроїв і кабельної інфраструктури. Потрібно вибрати таку топологію, яка б забезпечила надійну та ефективну роботу мережі, зручне управління потоками мережевих даних. Бажано також, щоб мережа за вартістю створення та супроводом вийшла недорогою, але й залишалися можливості для її подальшого розширення та, бажано, для переходу до більш високошвидкісних технологій зв’язку.

Слід розрізняти поняття фізичної топології, тобто способу розміщення комп’ютерів, мережевого обладнання та їх з’єднаннях за допомогою кабельної інфраструктури, і логічної топології – структури взаємодії комп’ютерів та характеру поширення сигналів по мережі.

Базові мережеві топології. [21]

Існує три базові топології, на основі яких будується більшість мереж.

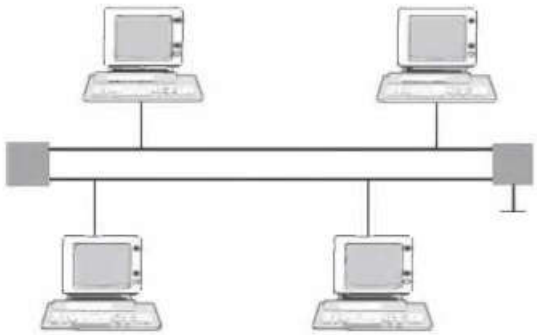


Рисунок 2.1.- Мережа з топологією «шина»

«Шина» (Bus). У цій топології всі комп’ютери з’єднуються між собою одним кабелем (див.рис. 2.1). Надіслані в таку мережу дані передаються всім

комп’ютерам, але обробляє їх тільки той комп’ютер, апаратна MAC-адреса мережного адаптера якого записана в кадрі як адреса одержувача.

Ця топологія виключно проста в реалізації та дешева (вимагає найменше кабелю), проте має ряд істотних недоліків.

Недоліки мереж типу «шина»:

– Такі мережі важко розширювати (збільшувати число комп’ютерів у мережі і кількість сегментів – окремих відрізків кабелю, які їх з’єднують).

– Оскільки шина використовується спільно, у кожен момент часу передачу може вести тільки один з комп’ютерів. Якщо передачу одночасно починають два або більше комп’ютерів, виникає спотворення сигналу (зіткнення, або колізія), що приводить до пошкодження всіх кадрів. Тоді комп’ютери змушені призупиняти передачу, а потім по черзі ретранслювати дані. Вплив зіткнень тим помітніший, чим вищий обсяг переданої по мережі інформації і чим більше комп’ютерів підключено до шини. Обидва ці фактори, природно, знижують як максимально можливу, так і загальну продуктивність мережі, сповільнюючи її роботу.

«Шина» є пасивною топологією – комп’ютери тільки «слухають» кабель і не можуть відновлювати затухаючі при передачі по мережі сигнали. Щоб подовжити мережу, потрібно використовувати повторювачі (репітери), які посилюють сигнал перед його передачею у наступний сегмент.

Надійність мережі з топологією «шина» невисока. Коли електричний сигнал досягає кінця кабелю, він (якщо не прийняті спеціальні заходи) відбивається, порушуючи роботу всього сегмента мережі. Щоб запобігти такому відображенню сигналів, на кінцях кабелю встановлюються спеціальні резистори (термінатори), поглинаючі сигнали. Якщо ж у будь-якому місці кабелю виникає обрив – наприклад, при порушенні цілісності кабелю або просто при від’єднанні конектора, – то виникають два незатермінованих сегменти, на кінцях яких сигнали починають відбиватися, і вся мережа перестає працювати.

Проблеми, характерні для топології «шина», призвели до того, що ці мережі, такі популярні ще десять років тому, зараз вже практично не викори-

стовуються.

«Кільце» (Ring). У даній топології кожен з комп’ютерів з’єднується з двома іншими так, щоб від одного він отримував інформацію, а іншому – передавав її (див.рис. 2.2). Останній комп’ютер підключається до першого, та кільце замикається.

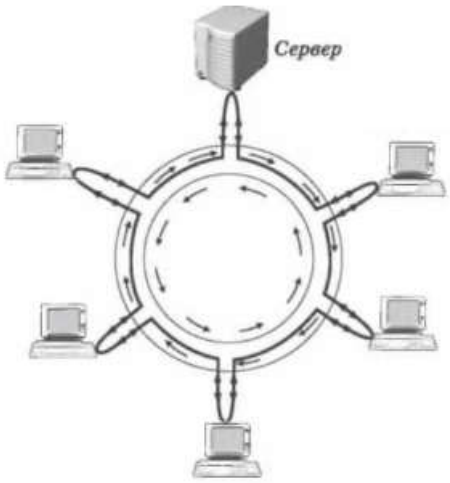


Рисунок 2.2 - Мережа з топологією «кільце»

Переваги та недоліки мереж з топологією «кільце»

Переваги: Оскільки у кабелів в цій мережі немає вільних кінців, термінатори тут не потрібні; кожен з комп’ютерів виступає у ролі повторювача, посилюючи сигнал, що дозволяє будувати мережі великої протяжності; через відсутність зіткнень топологія має високу стійкість до перевантажень, забезпечуючи ефективну роботу з великими потоками переданої по мережі інформації

Недоліки: Сигнал в «кільці» повинен пройти послідовно (і тільки в одному напрямку) через всі комп’ютери, кожен з яких перевіряє, чи не йому адресована інформація, тому час передачі може бути достатньо великим; підключення до мережі нового комп’ютера часто вимагає її зупинки, що порушує роботу всіх інших комп’ютерів; вихід з ладу хоча б одного з комп’ютерів або пристроїв порушує роботу всієї мережі; обрив або коротке замикання в будь-

якому з кабелів кільця робить роботу всієї мережі неможливою; щоб уникнути зупинки роботи мережі при відмові комп'ютерів або обриві кабелю, зазвичай прокладають два кільця, що істотно здорожує мережі.

Тут, так само як і для мереж з топологією «шина», недоліки в кілька разів переважують переваги, в результаті чого популярні раніше кільцеві мережі тепер використовуються набагато рідше.

Активна топологія «зірка» (Active Star). Ця топологія виникла на зорі обчислювальної техніки, коли до потужного центрального комп'ютера підключалися всі інші абоненти мережі. У такій конфігурації усі потоки даних йшли виключно через центральний комп'ютер, а він повністю відповідав за управління інформаційним обміном між усіма учасниками мережі. Конфлікти при такій організації взаємодії в мережі були неможливі, проте навантаження на центральний комп'ютер було настільки велике, що нічим іншим, крім обслуговування мережі, цей комп'ютер, як правило, не займався.

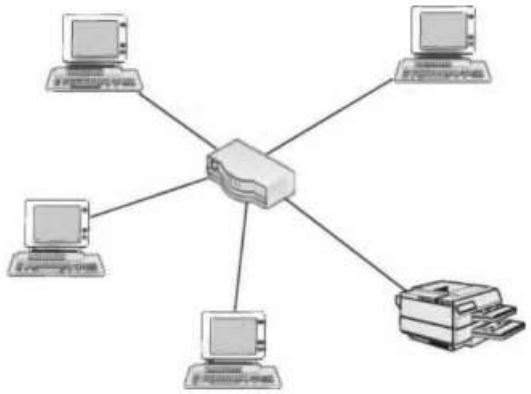


Рисунок 2.3 - Мережа з топологією «зірка»

Вихід його з ладу призводив до відмови всієї мережі, тоді як відмова периферійного комп'ютера або обрив зв'язку з ним на роботі решті мережі не позначався. Зараз такі мережі зустрічаються досить рідко. Набагато більш поширеною сьогодні топологією є схожий варіант – «зірка» (Star), або «пасивна зірка» (див.рис. 2.3). Тут периферійні комп'ютери підключаються не до

центрального комп’ютера, а до комутатора. В цьому випадку пристрій зв’язку не тільки ретранслює сигнали, що надходять, але і проводить управління їх обміном.

Незважаючи на більшу витрату кабелю, характерну для мереж типу «зірка», ця топологія має суттєві переваги перед іншими, що й зумовило її найширше застосування в сучасних мережах.

Переваги мереж типу «зірка»:

– Надійність – підключення до центрального комутатора та відключення комп’ютерів від нього ніяк не відбивається на роботі решти мережі; обриви кабелю впливають тільки на одиничні комп’ютери; термінатори не потрібні.

– Легкість при обслуговуванні та усуненні проблем – всі комп’ютери та мережеві пристрої підключаються до центрального з’єднувального пристрою, що істотно спрощує обслуговування та ремонт мережі.

– Захищеність – концентрація точок підключення в одному місці дозволяє легко обмежити доступ до життєво важливих об’єктів мережі.

Реальні комп’ютерні мережі постійно розширюються та модернізуються. Тому майже завжди така мережа є гібридною, тобто її топологія представляє собою комбінацію декількох базових топологій. Легко уявити собі гібридні топології, які є комбінацією «зірки» і «шини», або «кільця» і «зірки». Однак особливо слід виділити топологію «дерево» (tree), яку можна розглядати як об’єднання кількох «зірок». Саме ця топологія сьогодні є найбільш популярною при побудові локальних мереж.

Слід згадати про комірчату, або сіткову (mesh) топологію, в якій всі або багато комп’ютерів та інші пристрої з’єднані один з одним безпосередньо

Така топологія виключно надійна – при обриві будь-якого каналу передача даних не припиняється, оскільки можливі декілька маршрутів доставки інформації.

На фоні великого вибору старих і перспективно нових технологічних підходів у рамках групи Ethernet зупинимося на технології, що сьогодні тільки

здобуває повноцінну масовість використання у зв'язку зі зниженням вартості її компонентів.

Gigabit Ethernet може повноцінно забезпечити роботу таких додатків, як потокове відео, відеоконференції, передача складних зображень що пред'являють підвищені вимоги до пропускної здатності каналу. Переваги підвищення швидкостей передачі в корпоративних і домашніх мережах стають все більш необхідними, з падінням вартості на обладнання такого класу.

Gigabit Ethernet є прямим нащадком Ethernet і Fast Ethernet, що добре зарекомендували себе за майже двадцятилітню історію, зберігши їх надійність і перспективність використання.

Критерії на вибір кабелю теж стали більш жорсткими.

Для зменшення наведень, односпрямованої передачі, зворотних втрат, затримок і фазового зрушення, була прийнята до використання категорія 5е для неекранованої крученої пари. На рисунку 2.4 наведено стандарт обтискання кабеля вита пара.

RJ-45 разводка (TIA/EIA-568-B T568B)

Контакт	Пара	Провод	Цвет
1	2	1	бело-оранжевый
2	2	2	оранжевый
3	3	1	бело-зелёный
4	1	2	синий
5	1	1	бело-синий
6	3	2	зелёный
7	4	1	бело-коричневый
8	4	2	коричневый

Рисунок 2.4 — Позначення порядку обтискання кабелю типу “вита пара”

Таким чином, на основі проведеного аналізу архітектури підприємства та вимог до продуктивності, як базову модель побудови мережі ТОВ «Клео-П»

обрано ієрархічну зіркоподібну топологію. Після визначення фізичних параметрів інфраструктури та вибору гігабітних кабельних ліній зв'язку, ключовим етапом проектування є розробка та обґрунтування логічної структури мережі. Для забезпечення високої надійності, керованості та безпеки, мережева архітектура розділена на кілька рівнів:

– Рівень доступу (Access Layer): реалізований на базі шести 16-портових гігабітних комутаторів. На відміну від застарілих рішень, у модернізованому проєкті використовуються комутатори з підтримкою технології L2 (напівкеровані/Smart), що необхідно для коректної обробки тегованого трафіку.

– Рівень ядра та розподілу (Core/Distribution Layer): представлений високопродуктивними керованими маршрутизаторами MikroTik під управлінням RouterOS. Саме до них підводяться магістральні аплінки від комутаторів доступу.

Така архітектурна схема дозволяє реалізувати гнучку технологію віртуальних локальних мереж (VLAN), за допомогою якої корпоративна мережа сегментується на ізольовані робочі групи (департаменти). Сегментація на рівні L2 повністю ізолює внутрішній трафік кожного відділу, мінімізує широкомовний шторм (Broadcast storm) та захищає конфіденційні дані від несанкціонованого перехоплення всередині компанії.

Маршрутизація між створеними VLAN-сегментами здійснюється централізовано на пристроях MikroTik із застосуванням строгих правил міжмережевого екрана (Firewall).

Організація бездротового сегмента та гостьового доступу: Особливу логіку закладено для конференц-залу.

Бездротова точка доступу AP_1 інтегрована в один логічний сегмент (VLAN 50) разом із фіксованими робочими станціями цього приміщення. Оскільки у конференц-залі здебільшого працюють сторонні користувачі, партнери та клієнти агенції, проводяться презентації та навчання, цей сегмент повністю відокремлений від загальної корпоративної мережі. Користувачі

VLAN 50 мають доступ виключно до глобальної мережі Інтернет, що нівелює ризики кіберзагроз для внутрішніх серверів та баз даних ТОВ «Клео-П».

Обґрунтування та призначення захищеного тунелю: Оскільки підприємство має географічно розподілену структуру (Головний офіс та Віддалений корпус), критично важливим завданням проєкту є організація надійного зв'язку між ними.

Для цього поверх публічних каналів мережі Інтернет між маршрутизаторами MikroTik проектується захищений віртуальний тунель (VPN із шифруванням IPsec).

Впровадження VPN-тунелю вирішує три ключові завдання:

– Об'єднує віддалені робочі станції менеджерів філіалу з центральною IT-інфраструктурою головного офісу в єдиний безпечний периметр.

– Забезпечує криптографічний захист (шифрування) комерційної інформації та персональних даних клієнтів під час їх передачі через відкриту мережу Інтернет.

– Надає співробітникам віддаленого корпусу прозорий та швидкий доступ до корпоративного FTP-сервера та баз даних, розміщених у центральній серверній шафі.

Повна специфікація логічного поділу мережі, розподіл IP-адресації, шлюзів та призначення віртуальних мереж детально систематизовані та зведені у таблиці 2.1 та таблиці 2.2.

Таблиця 2.1 – Логічна адресація в мережі

Номер VLAN	Назва VLAN	Опис / Призначення	Діапазон IP-адрес	Маска мережі	Шлюз (Gateway)
1	2	3	4	5	6
—	WAN	Зовнішній інтерфейс (Інтернет від	Динамічна (DHCP) або статична від	—	—

Продовження таблиці 2.1

1	2	3	4	5	6
		провайдера на SW_7)	ISP		
—	VPN_Tunnel	Транзитна мережа для тунелю між SW_7 та SW_9	10.10.10.0/30	255.255.255.252	—
VLAN 10	Management	Управління мережевим залізом (MikroTik, L2-світчі)	192.168.10.0/27	255.255.255.224	192.168.10.1
VLAN 20	Servers	Серверна зона Головного корпусу (S_1, S_2)	192.168.10.32/27	255.255.255.224	192.168.10.33
VLAN 30	HQ_Users	Робочі станції Головного корпусу (WS_1 – WS_20)	192.168.10.64/26	255.255.255.192	192.168.10.65
VLAN 40	HQ_Printers	Мережеві принтери Головного корпусу (PR_1 –	192.168.10.128/27	255.255.255.224	192.168.10.129

Продовження таблиці 2.1

1	2	3	4	5	6
		PR_5)			
VLAN 50	HQ_Wi-Fi	Бездротова мережа Голо-вного корпу-су (AP_1)	192.168.11.0/24	255.255.255.0	192.168.11.1
VLAN 60	Branch_Users	Робочі станції Від-даленого корпусу (WS_21 – WS_33)	192.168.20.0/25	255.255.255.128	192.168.20.1
VLAN 70	Branch_Print	Мережеві принтери Віддаленого корпусу (PR_7, PR_8)	192.168.20.128/26	255.255.255.192	192.168.20.129

Таблиця 2.2 - Таблиця конфігурування VLAN на порту комутатора SW_4

Вихідний пристрій	Порт ви-ходу	Пристрій призначен-ня	Порт при-значення	Тип лі-нійного з'єднання	Тегування (Режим порту) / Прив'язка до VLAN
1	2	3	4	5	6
SW_7 (Edge)	ether1	INTERNET	Порт провайдера	Ethernet (Кручена пара /	WAN (DHCP/ Static IP)

Продовження таблиці 2.2

1	2	3	4	5	6
				Оптика)	
SW_7 (Edge)	ether2	SW_4 (HQ Dist)	ether1	Internal Trunk	Trunk (Дозволені: VLAN 10, 20, 30, 40, 50)
SW_4 (HQ Dist)	ether2	SW_1 (L2)	Port 16	Uplink	Trunk (Дозволені: VLAN 10, 30, 40)
SW_4 (HQ Dist)	ether3	SW_2 (L2)	Port 16	Uplink	Trunk (Дозволені: VLAN 10, 20, 30, 40)
SW_4 (HQ Dist)	ether4	SW_3 (L2)	Port 16	Uplink	Trunk (Дозволені: VLAN 10, 30, 40, 50)
SW_4 (HQ Dist)	ether5	SW_5 (L2)	Port 16	Uplink	Trunk (Дозволені: VLAN 10, 30, 40)
SW_4 (HQ Dist)	ether6	SW_6 (L2)	Port 16	Uplink	Trunk (Дозволені: VLAN 10, 30, 40)
SW_4 (HQ Dist)	ether7	S_1 (Сервер)	NIC 1	Access	Access (VLAN 20 — IP: 192.168.10.34)
SW_4 (HQ Dist)	ether8	WS_20 (ПК)	NIC	Access	Access (VLAN 30 192.168.10.66)
SW_1 (L2)	Port 1-6	WS_1 – WS_6	NIC	Access Line	Access (VLAN 30 — Динамічні IP)
SW_1	Port 7	PR_1	NIC	Access	Access VLAN 40

Продовження таблиці 2.2

1	2	3	4	5	6
(L2)		(Принтер)			— IP: 192.168.10.130)
SW_2 (L2)	Port 1-3	WS_7 – WS_9	NIC	Access Line	Access (VLAN 30 — Динамічні IP)
SW_2 (L2)	Port 4	S_2 (Сервер)	NIC	Access Line	Access (VLAN 20 — IP: 192.168.10.35)
SW_2 (L2)	Port 5	PR_2 (Принтер)	NIC	Access Line	Access (VLAN 40 — IP: 192.168.10.131)
SW_3 (L2)	Port 1-5	WS_10 – WS_14	NIC	Access Line	Access (VLAN 30 — Динамічні IP)
SW_3 (L2)	Port 6	AP_1 (Wi-Fi)	LAN	Access Line	Access (VLAN 50 — Магістраль для точок)
SW_3 (L2)	Port 7	PR_3 (Принтер)	NIC	Access Line	Access (VLAN 40 — IP: 192.168.10.132)
SW_5 (L2)	Port 1-3	WS_15 – WS_17	NIC	Access Line	Access (VLAN 30 — Динамічні IP)
SW_5 (L2)	Port 4	PR_4 (Принтер)	NIC	Access Line	Access (VLAN 40 — IP: 192.168.10.133)
SW_6 (L2)	Port 1-2	WS_18 – WS_19	NIC	Access Line	Access (VLAN 30 — Динамічні IP)

Продовження таблиці 2.2

1	2	3	4	5	6
SW_6 (L2)	Port 3	PR_5 (Принтер)	NIC	Access Line	Access (VLAN 40 — IP: 192.168.10.134)
SW_7 (Edge)	Логічний	SW_9 (Branch)	Логічний	VPN IPsec Tunnel	Маршрутизація між мережами корпорації
SW_9 (Branch)	ether2	SW_8 (L2)	Port 16	Uplink	Trunk (Дозволені: VLAN 10, 60, 70)
SW_9 (Branch)	ether3	SW_10 (L2)	Port 16	Uplink	Trunk (Дозволені: VLAN 10, 60, 70)
SW_9 (Branch)	ether4-6	WS_31 – WS_33	NIC	Access Line	Access (VLAN 60 — Динамічні IP)
SW_8 (L2)	Port 1-6	WS_21 – WS_26	NIC	Access Line	Access (VLAN 60 — Динамічні IP)
SW_8 (L2)	Port 7	PR_7 (Принтер)	NIC	Access Line	Access (VLAN 70 — IP: 192.168.20.130)
SW_10 (L2)	Port 1-4	WS_27 – WS_30	NIC	Access Line	Access (VLAN 60 — Динамічні IP)
SW_10 (L2)	Port 5	PR_8 (Принтер)	NIC	Access Line	Access (VLAN 70 — IP: 192.168.20.131)

2.2 Обґрунтування вибору комунікаційного обладнання

Специфіка діяльності ТОВ «Клео-П» як сучасної туристичної компанії висуває високі вимоги до надійності та швидкості передачі даних.

Для забезпечення повноцінного функціонування всіх робочих місць, підключення мережевої периферії та належної сегментації трафіку, на рівні доступу (Access Layer) необхідно розгорнути шість гігабітних 16-портових комутаторів.

Вибір обладнання рівня доступу має базуватися на критеріях економічної ефективності, високої продуктивності, підтримки стандарту 1000Base-T та обов'язкової підтримки тегування трафіку (стандарт IEEE 802.1Q) для коректної роботи віртуальних мереж (VLAN).

З метою підбору оптимального апаратного рішення проведемо техніко-економічний аналіз та порівняння трьох популярних на ринку моделей керованих/напівкерованих комутаторів аналогічного класу від провідних виробників (наприклад, MikroTik, TP-Link, D-Link).

Таблиця 2.3 — Порівняльна характеристика гігабітних 16-портових комутаторів рівня доступу

Критерій порівняння	TP-Link TL-SG1016	D-Link DGS-1016D	Mercusys MS116G
1	2	3	4
Кількість портів	16 портів RJ-45	16 портів RJ-45	16 портів RJ-45
Швидкість портів	10/100/1000 Мбіт/с	10/100/1000 Мбіт/с	10/100/1000 Мбіт/с
Комутаційна матриця	32 Гбіт/с	32 Гбіт/с	32 Гбіт/с

Продовження таблиці 2.3

1	2	3	4
Тип корпусу	Металевий, 19" (у стійку)	Металевий, 19" (у стійку)	Пластиковий, настільний
Охолодження	Пасивне (безшумне)	Пасивне (безшумне)	Пасивне (безшумне)
VLAN Pass-through	Підтримується	Підтримується	Не гарантується
Енергозбереження	Green Technology (до 84%)	D-Link Green	Green Technology
Орієнтовна ціна (грн)	~3 150 грн	~3 100 грн	~1 600 грн

На основі техніко-економічного аналізу, наведеного в таблиці 2.3, для реалізації рівня доступу мережі ТОВ «Клео-П» обрано модель TP-Link TL-SG1016 у кількості 7 одиниць, зовнішній вигляд якого зображено на рисунку 2.5. Вибір повністю некерованих пристроїв для робочих груп є інженерно та економічно виправданим з огляду на такі чинники:

– Логіка обробки трафіку та взаємодія з ядром мережі: На рівні кінцевих пристроїв (робочі станції працівників, мережеві принтери) трафік є повністю нетегованим. Користувачі підключаються до локальних некерованих комутаторів у своїх кабінетах за принципом Plug-and-Play. Далі кожен такий комутатор окремим лінком підключається до виділеного фізичного порту центрального керованого маршрутизатора MikroTik у серверній шафі. Сама логіка сегментації та маркування трафіку тегами (VLAN 10 – VLAN 70) реалізується безпосередньо на портах MikroTik, що дозволяє уникнути потреби купувати дорожчі керовані комутатори для кожного кабінету.

– Висока продуктивність: Усі 16 портів кожної з 7 моделей працюють на швидкості 1000 Мбіт/с (Gigabit Ethernet). Внутрішня комутаційна матриця ємністю 32 Гбіт/с гарантує передачу даних без затримок усередині робочої групи, що повністю задовольняє вимоги туристичної агенції під час роботи з базами даних та медіаконтентом.

– Надійність та ремонтопридатність: Некеровані комутатори не мають програмного забезпечення, яке потребує налаштування чи оновлення, що повністю виключає збої через людський фактор або програмні помилки. У разі фізичної поломки пристрою, будь-який працівник може виконати його швидку заміну за кілька хвилин без залучення висококваліфікованого сисадміна.

Рисунок 2.5 – Зовнішній вигляд комутатора TP-Link TL-SG1016

Оскільки для рівня доступу було обрано економічно вигідні некеровані комутатори, уся логічна структура мережі, керування віртуальними мережами (VLAN 10 – VLAN 70), забезпечення безпеки та організація захищеного зв'язку повністю покладається на маршрутизатори ядра та розподілу. Для реалізації цих завдань обрано професійне мережеве обладнання латвійської компанії MikroTik, яке працює під управлінням операційної системи RouterOS (v7).

Згідно з розробленою топологією мережі ТОВ «Клео-П», визначено та обґрунтовано вибір таких моделей для трьох ключових вузлів:

Центральне ядро мережі Головного офісу (SW_7): Для цього вузла обрано потужний маршрутизатор MikroTik RB5009UG+S+IN (або серію CCR). Цей

пристрій оснащений високопродуктивним 4-ядерним процесором та має 1-гігабітні порти, а також швидкісні порти 2.5G та 10G SFP+ для магістральних підключень. Його потужності з великим запасом вистачає для одночасної маршрутизації між усіма VLAN-сегментами Головного офісу, фільтрації трафіку через Firewall, балансування інтернет-каналу та обслуговування FTP-сервера.

Маршрутизатори розподілу та VPN (SW_4 та SW_9): Для організації захищеного каналу зв'язку між головним офісом та віддаленим корпусом обрано два маршрутизатори MikroTik hEX S (RB760iGS). Незважаючи на свої компактні розміри, ці пристрої мають вбудоване апаратне прискорення шифрування (IPsec crypto-offloading). Це дозволяє будувати високошвидкісні та захищені VPN-тунелі між двома корпусами через мережу Інтернет без завантаження центрального процесора, забезпечуючи передачу даних на повній гігабітній швидкості (1 Гбіт/с).

Переваги вибору обладнання MikroTik для проєкту:

– Повний контроль над VLAN: RouterOS дозволяє чітко закріпити кожен фізичний порт маршрутизатора за конкретним VLAN-тегом. Трафік від некерованих комутаторів робочих груп приходить на гігабітні порти MikroTik, де він маркується та ізолюється від інших відділів.

– Економічна доцільність: Операційна система RouterOS надає повний спектр функцій корпоративного класу (робота з VPN, динамічна маршрутизація, розширений Firewall, шейпінг швидкості QoS) без потреби купівлі будь-яких додаткових ліцензій чи підписок.

– Централізоване адміністрування: Використання утиліти WinBox або веб-інтерфейсу дозволяє системному адміністратору ТОВ «Клео-П» зручно керувати всією мережевою інфраструктурою підприємства, оперативно змінювати правила доступу та моніторити мережеву активність у реальному часі.

Для організації мобільного робочого простору в конференц-залі та забез-

печення гостьового доступу для клієнтів туристичної агенції ТОВ «Клео-П» в архітектуру мережі інтегровано бездротовий сегмент (VLAN 50). Сучасний ринок мережевого обладнання пропонує широкий спектр бізнес-рішень, що задовольняють вимогам щільного корпоративного середовища.

Для порівняння ми візьмемо сучасні корпоративні точки доступу стандарту Wi-Fi 6 (802.11ax) із підтримкою шифрування WPA3. Найкращим вибором для нашого проєкту буде модель від MikroTik, оскільки це дозволить управляти нею централізовано з головного маршрутизатора через вбудовану систему CAPsMAN. На основі техніко-економічного аналізу, наведеного в таблиці 2.4, для реалізації бездротового сегмента мережі обрано точку доступу MikroTik cAP ax (модель CAPGi-5HaxD2HaxD).

Таблиця 2.4 – Порівняльна характеристика точок доступу

Критерій порівняння	MikroTik cAP ax	Ubiquiti UniFi 6 Lite	TP-Link EAP610
1	2	3	4
Стандарт Wi-Fi	Wi-Fi 6 (802.11ax)	Wi-Fi 6 (802.11ax)	Wi-Fi 6 (802.11ax)
Макс. швидкість (5 ГГц)	1201 Мбіт/с	1201 Мбіт/с	1201 Мбіт/с
Макс. швидкість (2.4 ГГц)	574 Мбіт/с	300 Мбіт/с	574 Мбіт/с
Технологія живлення	PoE (802.3af/at) / DC	PoE (802.3af)	PoE (802.3at) / DC
Централізоване керування	Безкоштовне (CAPsMAN)	UniFi Controller	Omada Controller
Орієнтовна ціна	4 300 грн	4 700 грн	3 500 грн

В таблиці 2.5 наведено обране нами зведене обладнання.

Таблиця 2.5 — Перелік обладнання мережі

№ п.п	назва	Кількість	ціна
1	2	3	4
1	комутатор TP-Link TL-SG1016	7	3150,00 грн.
2	комутатор MikroTik RB5009UG+S+IN	1	8 900,00 грн.
3	Комутатор MikroTik hEX S (RB760iGS)	2	3200, 00 грн
4	точка доступу MikroTik cAP ax	2	4300,00 грн.

2.3 Особливості монтажу мережі

Комп'ютерні мережі можуть створюватися з використанням як мідних, так і оптичних кабелів. [22]

Виконуючи монтаж локальної мережі, враховують технічні вимоги виробника до прокладання кабелів.

Зокрема один з найважливіших показників - радіус вигину кабелю. Надмірний вигин може привести до зниження швидкості передачі даних для мідного кабелю і, як наслідок, невиконання вимог до категорії мережі, для оптичного кабелю - до зламу волокна, що потребують перекладки кабелю, установки муфти і т.п.

Прокладку кабелю виконують одним куском від вузла комутації СКС, до РМ. При прокладанні декількох кабелів в одному напрямку - прокладка виконується одним пучком.

При монтажі кабелю в гофрованої труби, спочатку кабель затягується в трубу за зонд. Після цього гофротруба з кабелем монтується на встановлених кліпсах, хомутах.

У разі прокладання кабелів формуються пучки і по порядку заводяться в комутаційні шафи.

Кабелі в обов'язковому порядку маркуються згідно з робочим проектом.

По закінченню прокладки кабелів, виконується монтаж (розшивання) на крос-панелях і РМ. Розшивання кабелю виконується відповідно до вимог до категорій СКС, виробників кабелів і компонентів СКС, в деяких випадках з використання фірмового інструменту. Монтаж СКС виконується навченим персоналом. У деяких випадках для сертифікації СКС, проектувальники, монтажники повинні вчитися в навчальних центрах виробників.

Підключення мережевого обладнання здійснюється від точок підключення електроживлення, призначених замовником. Для підключення монтуються електричні кабелі.

Якщо в складі СКС на РМ монтуються силові розетки на РМ, використовуються короби з перегородками. Мінімізуються перетину електричних кабелів і інформаційних. Підключення розеток на РМ здійснюється групами з установкою групового автомата відповідного номіналу.

Монтаж електричних мереж здійснюється навченим персоналом, з дотриманням правил електробезпеки і вимог ПУЕ.

В процесі пуско-налагоджувальних робіт виконуються:

– тестування новозбудованої СКС, магістральних кабелів за допомогою спеціалізованих вимірювальних приладів;

– перевірка, вимір електромережі відповідно до ПУЕ;

– включення, перевірка роботи джерела безперебійного живлення,

– включення, перевірка, настройка мережевого обладнання і тестування за програмами зазначеним в робочому проекті;

– організацією, що виконувала монтаж, передається замовнику виконавча документація, розроблена за діючими нормами і правилами.

До запобіжних заходів при монтажі та організації кабельних потоків відноситься запобігання різних механічних напружень в кабелі, що викликаються натягом, різкими вигинами і надмірним стягуванням пучків кабелів.

При монтажі кабелів в трасах і телекомунікаційних приміщеннях слід використовувати засоби маршрутизації кабельних потоків, їх кріплення і фікса-

ції.

Кабельні хомути (стяжки, бандаж і т. П.), Які використовуються для формування кабельних пучків, повинні розташовуватися на пучку так, щоб хомут міг вільно переміщатися в поздовжньому і поперечному напрямках. Не допускається затягування хомутів, що приводить до деформації оболонки кабелів. Не допускається кріплення телекомунікаційних кабелів за допомогою скоб.

Кабелі мережі будуть проведені попід стелею, понад підвісною стелею. Спуски виконані в порожнинах гіпсокартону.

2.4 Тестування мережі

Тестувати комп'ютерні мережі можна за допомогою різних методів та тестів, тестерів. [23]

Опис тестера RJ45 / RJ11. Зовнішній вигляд зображено на рисунку 2.6.

Універсальний тестер RJ45/Rj11 використовується для точного тестування локальної мережі під час прокладання мережних кабелів. Компактні габарити та невелика вага дозволять легко переносити кабельний lan тестер із собою, він не займає багато місця.

Мережевий тестер призначений для пошуку та вирішення проблем у мережах Ethernet, використовується для тестування кабелів:

UTP, FTP,

телефонних кабелів RJ11 та RJ12 (4/6 проводів).

Використовувати тестер можна для визначення цілісності витої пари.

Характеристики тестера

- Джерело живлення: 9В батарея 6F22 (купується окремо),
- Тестування кабелів UTP, FTP, RJ11, RJ12,
- 9 світлодіодних індикаторів,
- Функція автосканування з двома швидкостями:
- ВКЛ: нормальна швидкість,

– S: повільна швидкість
– Проведені тести:
– Схрещені пари,
– Невідповідність проводів,
– Інвертовані пари,
– Коротке замикання.

Тестер є одним із основних інструментів тестування локальної мережі, необхідних при проведенні монтажних та сервісних робіт у галузі телефонних та комп'ютерних мереж. Комплект складається з двох пристроїв, один із яких виконує функцію передавача, а інший – приймача.

Передавач генерує імпульси, які живлять дроти кабелю мережі. Завдяки функції автоматичного сканування легко визначити найпоширеніші помилки та несправності, включаючи обрив, замикання, перехрещення або перевернуті пари кабелів. Важливою перевагою Ethernet тестера є можливість роботи на двох швидкостях сканування: нормальній та повільній (режим S).

Мережний тестер кабелю Ethernet має 9 світлодіодів у передавальному модулі і таку ж кількість відповідних світлодіодів у приймачі. Завдяки подвійним роз'ємам можна тестувати як кабелі з роз'ємами RJ11 та RJ12 (телефонні), так і мережеві кабелі вита пара, що закінчуються роз'ємами RJ45 (LAN – Ethernet).

Функція автоматичного сканування дозволяє проводити випробування без залучення помічника – просто підключіть передавач до кабелю, що тестується, а потім перемістіться до місця, де знаходиться інший кінець мережного кабелю. Спостереження за послідовністю запалених діодів інтуїтивно повідомить вас про будь-які помилки або збої.

Тестування кабелів передачі даних (UTP)

Кабелі передачі даних Ethernet мають роз'єм rj-45. Мережеві кабелі, скінченні такими роз'ємами, є восьмижильними. Тому перевірка з'єднання виконується так само, як і кабелів з роз'ємами RJ11, але правильність з'єднання повинна бути підтверджена послідовним загорянням всіх світлодіодів, прону-

мерованих від 1 до 8.

Якщо виявлено перетин кабелю, послідовність світлодіодів на пристрої буде відрізнятися від послідовності, що відображається пристроєм, що передає.

Рисунок 2.6 – Кабельний тестер. Зовнішній вигляд.

2.5 Захист комп’ютерної мережі

Безпека мережі — заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу. Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів. Мережева безпека включає в себе дозвіл на доступ до даних в мережі, який надається адміністратором мережі. Користувачі вибирають або їм призначаються ID і пароль або інші перевірки автентичності інформації, що дозволяє їм здійснити доступ до інформації і програм у рамках своїх повноважень. Мережева безпека охоплює різні комп'ютерні мережі, як державні, так і приватні, які використовуються в повсякденних робочих

місцях для здійснення угод і зв'язків між підприємствами, державними установами та приватними особами. Мережі можуть бути приватними, такими як всередині туристичної агенції або відкритими, для публічного доступу. Мережева безпека бере участь в організаціях, підприємствах та інших типів закладів. Найбільш поширений і простий спосіб захисту мережевих ресурсів є присвоєння їм унікального імені та відповідного паролю.

Мережева безпека починається з аутентифікації, що зазвичай включає в себе ім'я користувача і пароль. Коли для цього потрібно тільки одна деталь аутентифікації (ім'я користувача), то це називають однофакторною аутентифікацією. При двофакторній аутентифікації, користувач ще повинен використати маркер безпеки або 'ключ', кредитну картку або мобільний телефон, при трьохфакторній аутентифікації, користувач повинен застосувати відбитки пальців або пройти сканування сітківки ока.

Після перевірки дійсності, брандмауер забезпечує доступ до послуг користувачам мережі. Для виявлення і пригнічування дії шкідливих програм використовується антивірусне програмне забезпечення або системи запобігання вторгнень (IPS).

Зв'язок між двома комп'ютерами з використанням мережі може бути зашифрований, щоб зберегти конфіденційніст

Система безпеки мережі не ґрунтується на одному методі, а використовує комплекс засобів захисту. Навіть якщо частина обладнання виходить з ладу, решта продовжує захищати дані Вашої туристичної агенції від можливих атак.

Встановлення рівнів безпеки мережі надає Вам можливість доступу до цінної ділової інформації з будь-якого місця, де є доступ до мережі Інтернет, а також захищає її від загроз.

Система безпеки мережі:

– Захищає від внутрішніх та зовнішніх мережних атак. Небезпека, що загрожує підприємству, може мати як внутрішнє, так і зовнішнє походження. Ефективна система безпеки стежить за активністю в мережі, сигналізує про аномалії та реагує відповідним чином.

– Забезпечує конфіденційність обміну інформацією з будь-якого місця та в будь-який час. Працівники можуть увійти до мережі, працюючи вдома або в дорозі, та бути впевненими у захисті передачі інформації.

– Контролює доступ до інформації, ідентифікуючи користувачів та їхні системи. Ви маєте можливість встановлювати власні правила доступу до даних. Доступ може надаватися залежно від ідентифікаційної інформації користувача, робочих функцій, а також за іншими важливими критеріями.

– Забезпечує надійність системи. Технології безпеки дозволяють системі запобігти як вже відомим атакам, так і новим небезпечним вторгненням. Працівники, замовники та ділові партнери можуть бути впевненими у надійному захисті їхньої інформації.

Засоби захисту комп’ютерних мереж:

Брандмауери. Централізовані брандмауери та брандмауери окремих комп’ютерів можуть запобігати проникненню зловмисного мережного трафіку до мережі, яка підтримує діяльність туристичної агенції.

Антивірусні засоби.

Більш захищена мережа може виявляти загрози, що створюють віруси, хробаки та інше зловмисне програмне забезпечення, і боротися з ним попереджувальними методами, перш ніж вони зможуть заподіяти шкоду.

Знаряддя, які відстежують стан мережі, грають важливу роль під час визначення мережних загроз.

Захищений віддалений доступ і обмін даними.

Безпечний доступ для всіх типів клієнтів із використанням різноманітних механізмів доступу грає важливу роль для забезпечення доступу користувачів до потрібних даних, незалежно від їх місцезнаходження та використовуваних пристроїв.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

Осікільки ми пишимо роботу про модернізацію мережі, тому питання налаштування серверів, встановлення на них програмного забезпечення NAS сервера, тощо, ми опустимо в цьому пункті. Тут ми опишимо налаштування лише зміненого обладнання, а саме налаштування головного комутатора головного офісу SW4, та маршрутизаторів SW& та SW9, з допомогою яких ми створюємо віддалений тунель між офісами.

3.1 Інструкція з інсталяції програмного забезпечення серверів та активного комутаційного обладнання

Конфігурування бездротової точки доступу за допомогою технології CAPsMAN

Для організації бездротового сегмента у конференц-залі (VLAN 50) використовується стельова точка доступу MikroTik cAP ax. У проєкті реалізовано централізоване керування за допомогою фірмової технології CAPsMAN (Controlled Access Point system Manager), інтегрованої в ОС RouterOS v7 (модуль Wifi).

При такій схемі сама точка доступу виступає в ролі "тонкого клієнта" (CAP), а всі параметри (SSID, частоти, паролі, прив'язка до VLAN) транслюються на неї в автоматичному режимі з головного маршрутизатора ядра SW_7 (CAPsMAN-контролера).

Етап 1. Конфігурування контролера CAPsMAN на маршрутизаторі ядра (SW_7)

Налаштування виконується через інтерфейс командного рядка (CLI) RouterOS v7. Спочатку створюються профілі безпеки, параметри каналу та конфігурація бездротової мережі для туристичної агенції:

1. Активація сервера CAPsMAN

/interface wifi capsman set enabled=yes interfaces=bridge

2. Створення профілю безпеки з підтримкою WPA2 та WPA3

/interface wifi security add name="Sec_Cleo_Guest" authentication-types=wpa2-psk,wpa3-psk

passphrase="Cleo_Travel_2026"

3. Налаштування параметрів (зв'язування з гостьовим VLAN 50)

/interface wifi datapath add name="DP_Cleo_Guest" vlan-id=50

4. Створення фінальної конфігурації бездротової мережі

/interface wifi configuration add name="Cfg_Cleo_Guest" ssid="Cleo_Travel_Guest"

security="Sec_Cleo_Guest" datapath="DP_Cleo_Guest"

country="Ukraine" installation=indoor

5. Створення правила автоматичного призначення конфігурації для точок доступу

/interface wifi capsman provisioning add action=create-dynamic-enabled master-configuration="Cfg_Cleo_Guest"

supported-bands=2ghz-ax,5ghz-ax

Етап 2. Налаштування точки доступу MikroTik cAP ax (AP_1)

Для того щоб точка доступу перейшла в режим керованого пристрою та знайшла контролер у мережі, на ній виконується мінімальна первинна команда переведення інтерфейсів у режим CAP:

Переведення вбудованих радіоінтерфейсів під керування CAPsMAN

/interface wifi cap set enabled=yes caps-man-addresses=192.168.40.1 interfaces=wifi1,wifi2

Альтернативно, переведення пристрою в режим CAP здійснюється апаратно: необхідно затиснути кнопку «Reset» на корпусі точки доступу cAP ax, подати живлення по кабелю PoE і відпустити кнопку через 5 секунд (коли почне блимати зелений світлодіод). Пристрій самостійно очистить локальну конфігурацію, надішле широкомовний запит у мережу, знайде контролер SW_7 та завантажить налаштування бездротової мережі Cleo_Travel_Guest із шифруванням WPA2/WPA3 та ізоляцією клієнтів у межах VLAN 50.

1. Створення загального комутаційного моста (bridge)

/interface bridge add name=bridge-remote vlan-filtering=no comment="головний міст віддаленого корпусу"

2. Додавання фізичних портів до моста та прив'язка access-портів

Для access-портів (ether2 та ether3) примусово вказуємо PVID=70.

Це означає, що будь-який нетегований трафік від ПК менеджерів, потрапляючи у цей порт, автоматично отримає мітку VLAN 70 всередині комутатора.

/interface bridge port add bridge=bridge-remote interface=ether1 comment="Trunk-порт до маршрутизатора SW_9" add bridge=bridge-remote interface=ether2 pvid=70 comment="Access-порт до некерованого комутатора 1" add bridge=bridge-remote interface=ether3 pvid=70 comment="Access-порт до некерованого комутатора 2"

3. Налаштування таблиці vlan (tagged та untagged інтерфейси)

/interface bridge vlan

Налаштування для VLAN 70: тегований на ether1, нетегований на ether2 та ether3

add bridge=bridge-remote tagged=ether1 untagged=ether2,ether3 vlan-ids=70

Налаштування для VLAN 40 (Керування): тегований на магістральному ether1 та тегований на самому програмному інтерфейсі bridge-remote, щоб пристрій мав власну IP-адресу

add bridge=bridge-remote tagged=bridge-remote,ether1 vlan-ids=40

4. Створення інтерфейсу керування та призначення ip-адреси

Створюємо віртуальний VLAN-інтерфейс поверх моста для віддаленого адміністрування

/interface vlan add interface=bridge-remote name=vlan40-management vlan-id=40

Призначаємо комутатору SW_4 статичну IP-адресу з підмережі керування

/ip address add address=192.168.40.4/24 interface=vlan40-management comment="IP-адреса SW_4 для утиліти WinBox"

Вказуємо основний шлюз для можливості підключення сисадміна з Головного офісу

/ip route add gateway=192.168.40.1 comment="Шлюз веде на центральний маршрутизатор"

5. Фінальна активація фільтрації vlan на мосту

Після введення цієї команди комутатор починає строго відсікати та маркувати трафік згідно з налаштованою таблицею bridge vlan

/interface bridge set [find name=bridge-remote] vlan-filtering=yes

Налаштування каналу VPN між корпусами.

Скрипт конфігурування для центрального маршрутизатора головного офісу SW_7 (MikroTik RB5009) та прикордонного маршрутизатора віддаленого корпусу SW_9 (MikroTik hEX S).

Обидва скрипти написані під актуальну версію MikroTik RouterOS v7 і повністю синхронізовані з нашою топологією, розподілом VLAN-ів, пулами DHCP та параметрами безпеки.

Програмна конфігурація центрального маршрутизатора ядра Головного офісу SW_7 (MikroTik RB5009UG+S+IN)

Цей пристрій є "серцем" мережі ТОВ «Клео-П». Він виконує роль головного комутаційного моста для некерованих комутаторів, здійснює між-VLAN маршрутизацію, роздає IP-адреси, захищає мережу брандмауером та виступає центральним сервером для VPN-тунелю.

Доречі, для симуляції wan приймаємо статичну ip головного офісу: 203.0.113.2

1. Створення головного моста з підтримкою фільтрації vlan

/interface bridge add name=bridge-core vlan-filtering=no comment="основний міст ядра"

2. Опис та додавання фізичних портів до моста (режим access для некерованих комутаторів), Кожен порт жорстко прив'язується до свого pvid (vlan)

/interface bridge port add bridge=bridge-core interface=ether2 pvid=10 comment="вхід від switch_economics" add bridge=bridge-core interface=ether3

pvid=20 comment="вхід від switch_servers" add bridge=bridge-core interface=ether4 pvid=30 comment="вхід від switch_managers_main_1" add bridge=bridge-core interface=ether5 pvid=30 comment="вхід від switch_managers_main_2" add bridge=bridge-core interface=ether6 pvid=40 comment="вхід від switch_management" add bridge=bridge-core interface=ether7 pvid=50 comment="вхід від switch_conference"

3. Створення віртуальних інтерфейсів vlan на мосту для маршрутизації

/interface vlan add interface=bridge-core name=vlan10-economics vlan-id=10 add interface=bridge-core name=vlan20-servers vlan-id=20 add interface=bridge-core name=vlan30-managers vlan-id=30 add interface=bridge-core name=vlan40-management vlan-id=40 add interface=bridge-core name=vlan50-conference vlan-id=50

4. Налаштування таблиці фільтрації bridge vlan

Програмний інтерфейс bridge-core має бути тегованим (tagged) для всіх vlan, щоб бачити трафік і маршрутизувати його

/interface bridge vlan add bridge=bridge-core tagged=bridge-core untagged=ether2 vlan-ids=10 add bridge=bridge-core tagged=bridge-core untagged=ether3 vlan-ids=20 add bridge=bridge-core tagged=bridge-core untagged=ether4,ether5 vlan-ids=30 add bridge=bridge-core tagged=bridge-core untagged=ether6 vlan-ids=40 add bridge=bridge-core tagged=bridge-core untagged=ether7 vlan-ids=50

Активація фільтрації на мосту

/interface bridge set [find name=bridge-core] vlan-filtering=yes

5. Призначення ip-адрес на інтерфейси (шлюзи для відділів)

/ip address add address=203.0.113.2/30 interface=ether1 comment="публічний ip головного офісу (wan)" add address=192.168.10.1/24 interface=vlan10-economics add address=192.168.20.1/24 interface=vlan20-servers add address=192.168.30.1/24 interface=vlan30-managers add address=192.168.40.1/24 interface=vlan40-management add address=192.168.50.1/24 interface=vlan50-conference

Шлюз за замовчуванням в інтернет

/ip route add gateway=203.0.113.1

6. Конфігурування пулів адрес та dhcp серверів

/ip dhcp-pool add name=pool-vlan10 ranges=192.168.10.10-192.168.10.100 add name=pool-vlan30 ranges=192.168.30.10-192.168.30.100 add name=pool-vlan40 ranges=192.168.40.10-192.168.40.100 add name=pool-vlan50 ranges=192.168.50.10-192.168.50.100

/ip dhcp-server add address-pool=pool-vlan10 interface=vlan10-economics name=dhcp-vlan10 disabled=no add address-pool=pool-vlan30 interface=vlan30-managers name=dhcp-vlan30 disabled=no add address-pool=pool-vlan40 interface=vlan40-management name=dhcp-vlan40 disabled=no add address-pool=pool-vlan50 interface=vlan50-conference name=dhcp-vlan50 disabled=no

/ip dhcp-server network add address=192.168.10.0/24 dns-server=8.8.8.8 gateway=192.168.10.1 add address=192.168.30.0/24 dns-server=8.8.8.8 gateway=192.168.30.1 add address=192.168.40.0/24 dns-server=192.168.20.10 gateway=192.168.40.1 add address=192.168.50.0/24 dns-server=1.1.1.1 gateway=192.168.50.1

7. Налаштування міжмережевого екрана (firewall) та ipsec bypass

Важливо: трафік, що йде через vpn у віддалений офіс (192.168.70.0/24), не повинен потрапляти під nat (masquerade)

/ip firewall nat add chain=srcnat action=accept src-address=192.168.0.0/16 dst-address=192.168.70.0/24 comment="ipsec vpn bypass" add chain=srcnat action=masquerade out-interface=ether1 comment="загальний nat в інтернет"

Блокування гостьового wi-fi (vlan 50) до корпоративних мереж

/ip firewall filter add chain=forward action=drop src-address=192.168.50.0/24 dst-address=192.168.10.0/24 comment="block guest to economics" add chain=forward action=drop src-address=192.168.50.0/24 dst-address=192.168.20.0/24 comment="block guest to servers"

8. Налаштування серверної частини site-to-site vpn (ipsec) до sw_9

/ip ipsec profile add name=vpn-profile dhier=sha256 enc-algorithm=aes-256

prf=sha256

/ip ipsec proposal add name=vpn-proposal auth-algorithms=sha256 enc-algorithms=aes-256-cbc

/ip ipsec peer add address=198.51.100.2/32 name=peer-remote-branch profile=vpn-profile exchange-mode=ike2

/ip ipsec identity add peer=peer-remote-branch secret="kleotravelkey2026"

/ip ipsec policy add src-address=192.168.0.0/16 dst-address=192.168.70.0/24 peer=peer-remote-branch proposal=vpn-proposal tunnel=yes action=encrypt

Програмна конфігурація маршрутизатора віддаленого корпусу sw_9 (mikrotik hex s)

Цей пристрій виступає шлюзом безпеки для філіалу. Він приймає інтернет-канал, піднімає клієнтську частину криптографічного тунелю ipsec до головного офісу, маркує локальний трафік менеджерів філіалу (vlan 70) та службове керування (vlan 40) і передає їх у trunk-порт комутатора розподілу sw_4.

Доречі, для симуляції wan приймаємо статичну ip відділеного корпусу: 198.51.100.2

1. Створення віртуальних vlan-інтерфейсів на порту ether2 (trunk до sw_4)

/interface vlan add interface=ether2 name=vlan40-remote-mgmt vlan-id=40 comment="службовий сегмент" add interface=ether2 name=vlan70-remote-managers vlan-id=70 comment="сегмент менеджерів філіалу"

2. Призначення ip-адрес на інтерфейси

/ip address add address=198.51.100.2/30 interface=ether1 comment="публічний ip філіалу (wan)" add address=192.168.70.1/24 interface=vlan70-remote-managers comment="шлюз для менеджерів філіалу" add address=192.168.40.9/24 interface=vlan40-remote-mgmt comment="ip маршрутизатора в мережі керування"

Шлюз за замовчуванням в інтернет для філіалу

/ip route add gateway=198.51.100.1

3. Конфігурування пулу адрес та dhcp сервера для відділеного корпусу (16 пк + периферія)

/ip dhcp-pool add name=pool-vlan70 ranges=192.168.70.10-192.168.70.150

/ip dhcp-server add address-pool=pool-vlan70 interface=vlan70-remote-managers name=dhcp-vlan70 disabled=no

/ip dhcp-server network add address=192.168.70.0/24 dns-server=8.8.8.8 gateway=192.168.70.1 comment="мережа менеджерів філіалу"

4. Налаштування firewall та ipsec bypass для філіалу

/ip firewall nat add chain=srcnat action=accept src-address=192.168.70.0/24 dst-address=192.168.0.0/16 comment="ipsec vpn bypass" add chain=srcnat action=masquerade out-interface=ether1 comment="загальний nat філіалу в інтернет"

5. Налаштування клієнтської частини site-to-site vpn (ipsec) до sw_7

/ip ipsec profile add name=vpn-profile dhier=sha256 enc-algorithm=aes-256 prf=sha256

/ip ipsec proposal add name=vpn-proposal auth-algorithms=sha256 enc-algorithms=aes-256-cbc

У ролі адреси вказуємо публічний ip головного офісу

/ip ipsec peer add address=203.0.113.2/32 name=peer-main-core profile=vpn-profile exchange-mode=ike2

/ip ipsec identity add peer=peer-main-core secret="kleotravelkey2026"

Політика шифрування: весь локальний трафік філіалу (70.0/24) автоматично загортається в тунель При зверненні до будь-якої підмережі головного офісу (192.168.0.0/16)

/ip ipsec policy add src-address=192.168.70.0/24 dst-address=192.168.0.0/16 peer=peer-main-core proposal=vpn-proposal tunnel=yes action=encrypt

Висновок: оскільки моделі rb5009 та hex s підтримують алгоритми апаратного криптоприскорення (aes-ni), шифрування трафіку тунелю за протоколом ipsec завантажує крипточип, залишаючи центральні процесори вільними для маршрутизації гігабітних потоків.

3.2 Моделювання мережі з Cisco Packet Tracer

Cisco Packet Tracer розроблений компанією Cisco і рекомендується використовувати при вивченні телекомунікаційних мереж та мережевого обладнання, а також для проведення уроків з лабораторних робіт у вищих закладах.

Основні можливості Packet Tracer: (за матеріалами [25])

– Дружній графічний інтерфейс (GUI), що сприяє кращому розумінню організації мережі, принципів роботи пристрою;

– Можливість змоделювати логічну топологію: робочий простір для створення мережі будь-якого розміру на CCNA-рівні складності;

– моделювання у режимі real-time (реального часу);

– режим симуляції;

– Багатомовність інтерфейсу програми: що дозволяє вивчати програму своєю рідною мовою.

– удосконалене зображення мережного обладнання зі здатністю додавати/видаляти різні компоненти;

– наявність Activity Wizard дозволяє мережевим інженерам, студентам та викладачам створювати шаблони мереж та використовувати їх надалі.

– проектування фізичної топології: доступна взаємодія з фізичними пристроями, використовуючи такі поняття як місто, будинок, стійка тощо;

Широке коло можливостей даного продукту дозволяє мережевим інженерам: конфігурувати, налагоджувати та будувати обчислювальну мережу.

Також даний продукт незамінний у процесі, оскільки дає наочне відображення роботи мережі, що підвищує освоєння матеріалу учнями.

Емулятор мережі дозволяє мережевим інженерам проектувати мережі будь-якої складності, створюючи та відправляючи різні пакети даних, зберігати та коментувати свою роботу.

Фахівці можуть вивчати та використовувати такі мережеві пристрої, як комутатори другого та третього рівнів, робочі станції, визначати типи зв'язків

між ними та з'єднувати їх.

На заключному етапі після того, як мережа спроектована, фахівець може приступати до конфігурування вибраних пристроїв за допомогою термінального доступу або командного рядка (див.рис 3.1).

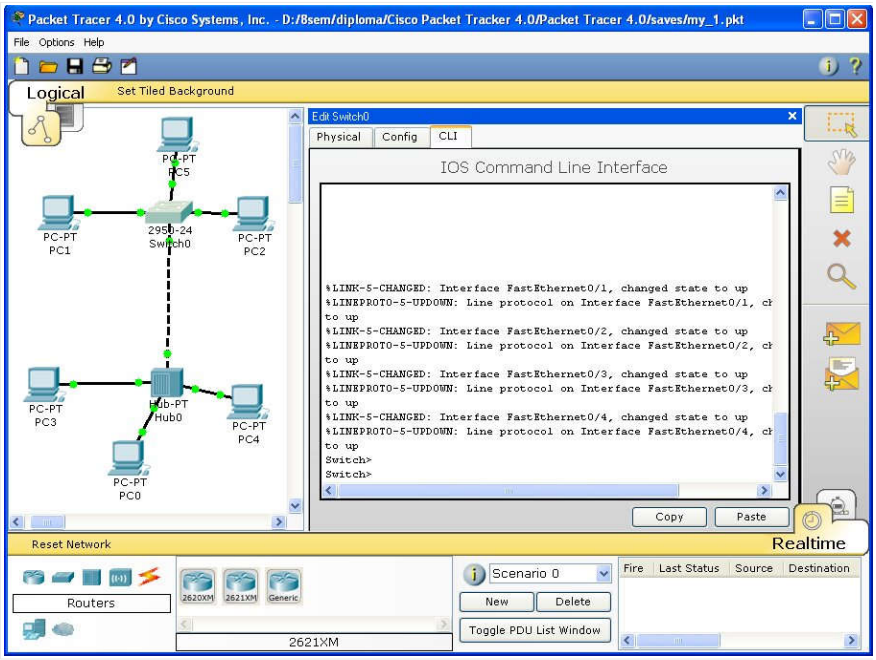


Рисунок 3.1 – Cisco Packet Tracer

Однією з найважливіших особливостей даного симулятора є у ньому «Режиму симуляції». У цьому режимі всі пакети, що пересилаються всередині мережі, відображаються у графічному вигляді.

Ця можливість дозволяє мережевим фахівцям наочно продемонструвати, за яким інтерфейсом зараз переміщається пакет, який протокол використовується і т.д.

Однак, це не всі переваги Packet Tracer: в «Режимі симуляції» мережеві інженери можуть не тільки відстежувати протоколи, що використовуються, але й бачити, на якому з семи рівнів моделі OSI даний протокол задіяний (див.рис 3.2).

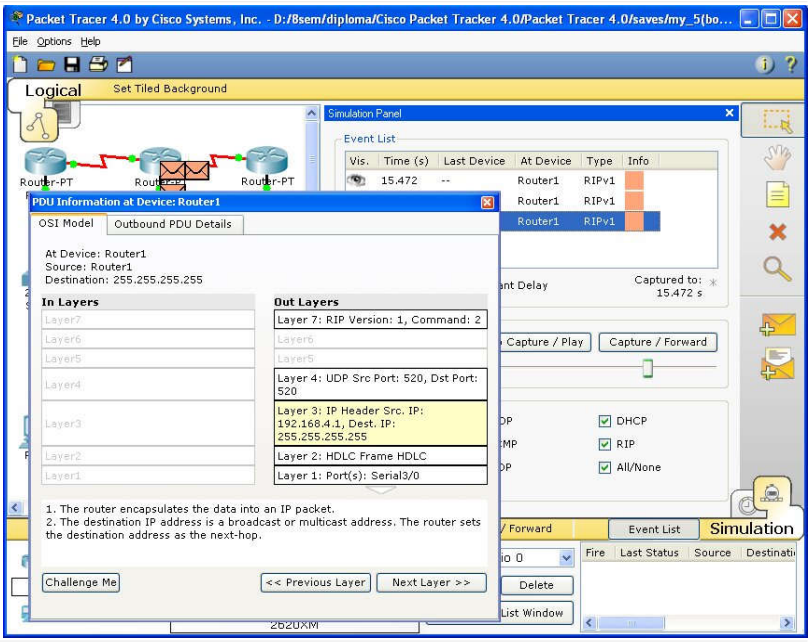


Рисунок 3.2- Аналіз семирівневої моделі OSI у Cisco Packet Tracer

Така простота і наочність, що здається на перший погляд, робить практичні заняття надзвичайно корисними, поєднуючи в них як отримання, так і закріплення отриманого матеріалу. Packet Tracer здатний моделювати велику кількість пристроїв різного призначення, а також багато різних типів зв'язків, що дозволяє проектувати мережі будь-якого розміру на високому рівні складності.

Інтерфейс Cisco Packet Tracer

Інтерфейс програми Cisco Packet Tracer представлений рисунку 3.3

На рисунку 3.3 зображено:

1. Головне меню програми;
2. Панель інструментів – дублює деякі пункти меню;
3. Перемикач між логічною та фізичною організацією;
4. Ще одна панель інструментів містить інструменти виділення, видалення, переміщення, масштабування об'єктів, а так само формування довільних пакетів;
5. Перемикач між реальним режимом (Real-Time) та режимом симуля-

ції;

6. Панель з групами кінцевих пристроїв та ліній зв'язку;

7. Самі кінцеві пристрої тут містяться всілякі комутатори, вузли, точки доступу, провідники.

8. Панель створення сценаріїв користувача;

9. Робочий простір;

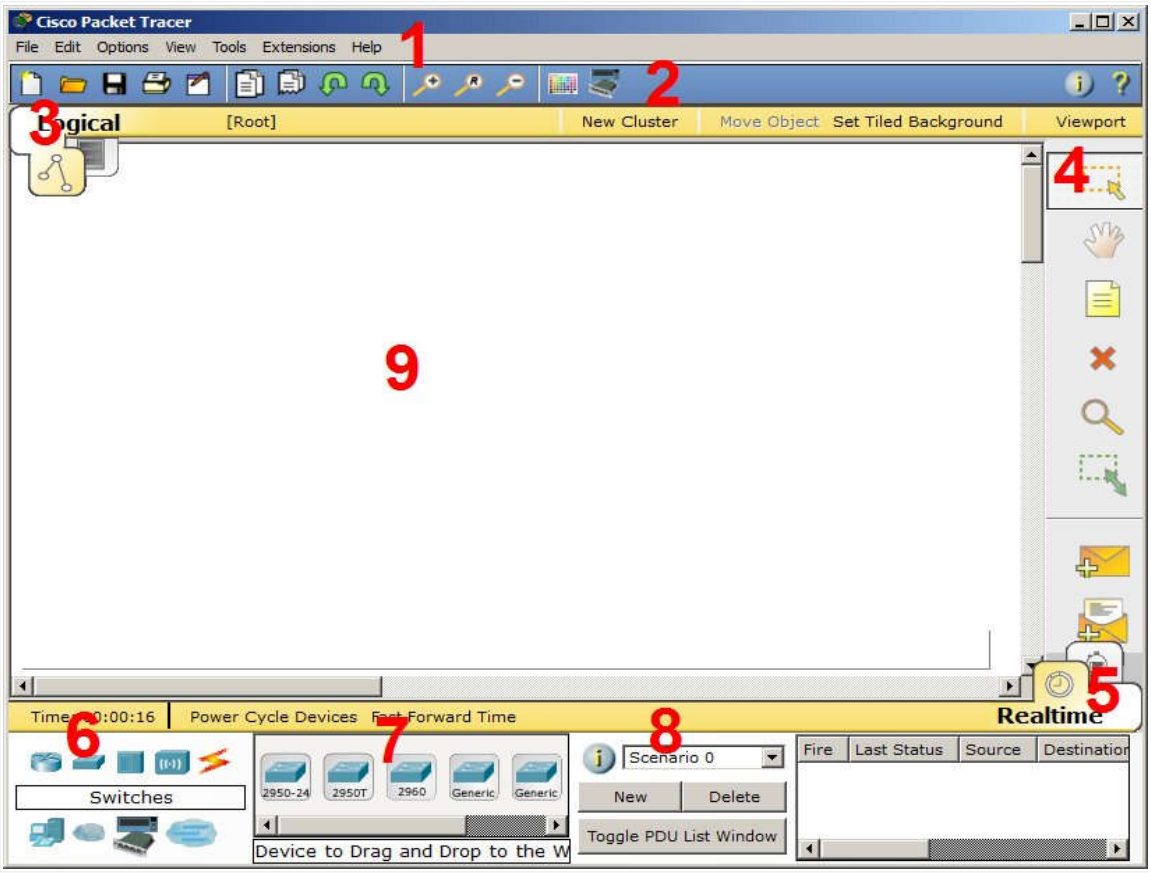


Рисунок 3.3 – Інтерфейс програми Cisco Packet Tracer

Більшу частину даного вікна займає робоча область, в якій можна розміщувати різні мережеві пристрої, з'єднувати їх різними способами і як наслідок отримувати різні мережеві топології.

Зверху, над робочою областю, розташована головна панель програми та її меню. Меню дозволяє виконувати збереження, завантаження мережевих топологій, налаштування симуляції та багато інших цікавих функцій. Головна

панель містить найчастіше використовувані функції меню.

Праворуч від робочої області, розташована бічна панель, що містить ряд кнопок, що відповідають за переміщення полотна робочої області, видалення об'єктів і т.д.

Знизу під робочою областю розташована панель обладнання

Дана панель містить у своїй лівій частині типи доступних пристроїв, а праворуч доступні моделі. При виконанні різних лабораторних робіт, цю панель доведеться використовувати набагато частіше, ніж усі інші. Тому розглянемо її докладніше.

При наведенні на кожний із пристроїв, у прямокутнику, що знаходиться в центрі між ними, буде відображатися його тип.

Розглядати конкретні моделі пристроїв кожного типу не має великого сенсу. На окремий розгляд заслуговують типи зєднань. Перерахуємо найчастіше використовувані їх (розгляд типів підключень йде зліва направо,).

Автоматичний тип – при цьому типі з'єднання PacketTracer автоматично вибирає найкращі тип з'єднання для вибраних пристроїв

Консоль – консольні з'єднання

Мідь Пряме – з'єднання мідним кабелем типу кручена пара , обидва кінці кабелю обтиснуті в однаковій розкладці. Підійде для таких з'єднань: комутатор - комутатор, комутатор - маршрутизатор, комутатор - комп'ютер та ін.

Мідь кросовер – з'єднання мідним кабелем типу кручена пара , кінці кабелю обтиснуті як кросовер. Підійде для з'єднання двох комп'ютерів.

Оптика – з'єднання за допомогою оптичного кабелю , необхідно для з'єднання пристроїв, що мають оптичні інтерфейси.

Телефонний кабель – звичайний телефонний кабель, який може знадобитися для підключення телефонних апаратів.

Коаксіальний кабель – підключення пристроїв за допомогою коаксіального кабелю .

Використовуючи даний продукт, ми створили модель мережі ТОВ «Клео-П», котра показана на рисунку 3.4, розроблена в Cisco Packet Tracer.

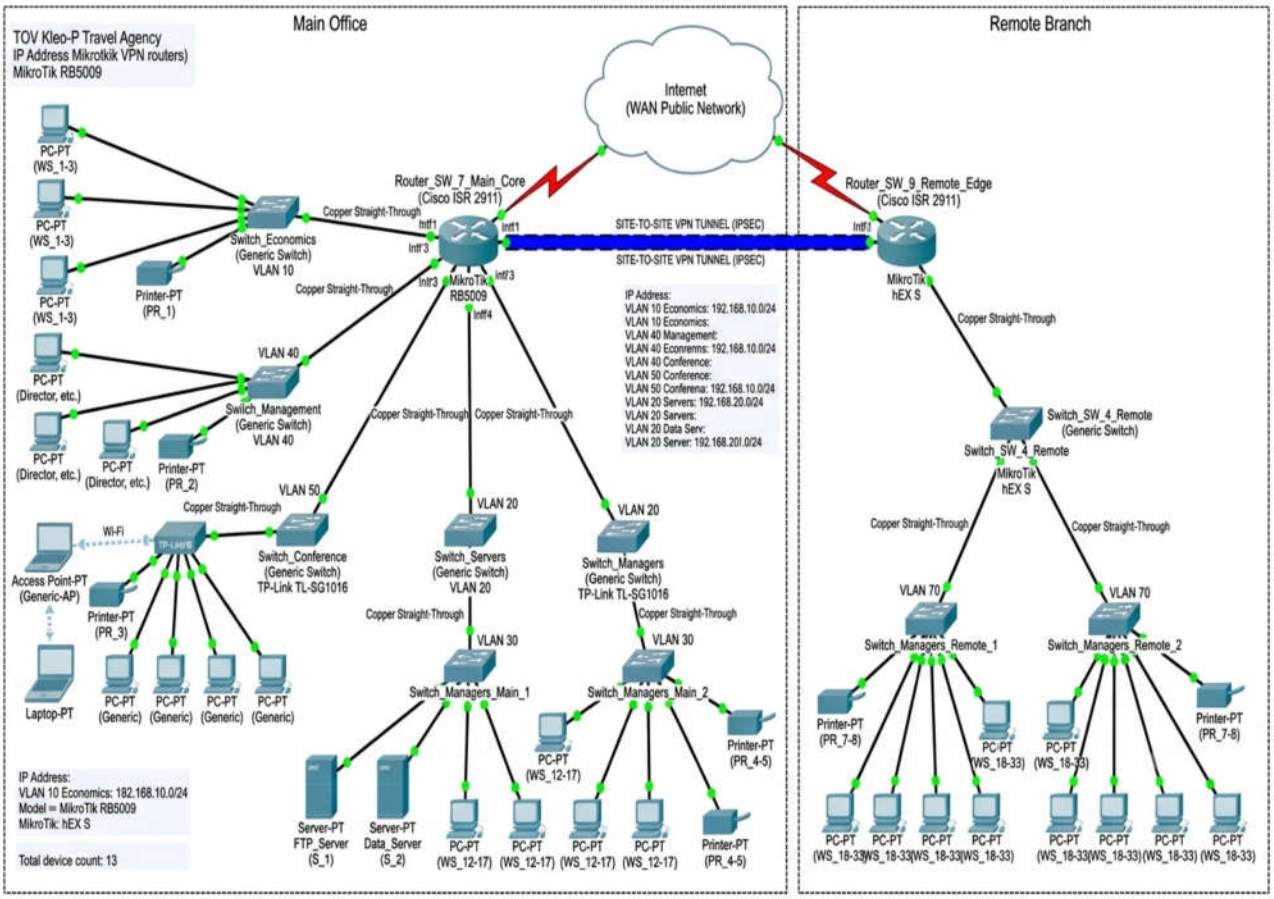


Рисунок 3.4 – Отримана модель мережі

Ця схема візуалізує все, що ми описували в попередніх пунктах:

– Логічний поділ: Мережа чітко розділена на два корпуси — головний офіс (Main Office) та віддалений корпус (Remote Branch).

– Інтернет та VPN: У верхній частині схеми розташована хмара «Internet (WAN)», яка з'єднує два корпуси. Синя пунктирна лінія показує захищений Site-to-Site VPN-тунель, налаштований між центральним маршрутизатором SW_7 та прикордонним SW_9.

– Головний офіс: Показує центральне ядро SW_7 (MikroTik RB5009). Від нього кабелі йдуть до 7 некерованих комутаторів робочих груп. Я згрупував їх за призначенням (Бухгалтерія, Менеджери, Сервери тощо). Та-

кож показано бездротовий сегмент у конференц-залі з точкою доступу та ноутбуком.

– Віддалений корпус: Показує маршрутизатор SW_9 (hEX S), який підключає через розподільчий комутатор SW_4 дві великі групи менеджерів філіалу.

– Інформаційні панелі: на схемі додані текстові блоки з деталізацією IP-адресації для кожного VLAN та специфікацією обраних нами моделей обладнання (MikroTik та TP-Link).

4 ЕКОНОМІЧНИЙ РОЗДІЛ

4.1 Визначення стадій техпроцесу та загальної тривалості проведення НДР

Визначення сукупних витрат часу, необхідних для успішного виконання науково-дослідної роботи (НДР), здійснюється шляхом детального структурування технологічного циклу на окремі стадії. Часові показники для кожного етапу розробки, а також їхня послідовність, представлені у таблиці 4.1.

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

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	2	3	4
1.	Постановка задачі, формування технічного завдання на проект локальної мережі. Узгодження майбутнього розміщення мережевих розеток.	Керівник проекту	20
2.	Проектування логічної та фізичної топології локальної мережі. Аналіз інформаційних потоків локальної мережі логістичного підприємства «Global-Express». Вибір оптимальної логічної та фізичної топології. Розробка логічної адресації та конфігурації для апаратного та програмного забезпечення. Врахування структури підприємства для сегментування локальної мережі на підмережі.	Інженер	15

Продовження таблиці 4.1

1	2	3	4
3.	Монтаж мережі (прокладання кабельних каналів, вертикальних та горизонтальних кабельних каналів). Здійснюється монтаж та підключення пасивного обладнання. Перевірка СКС локальної мережі на відповідність вибраній технології.	Техн ік	35
4.	Конфігурування мережевого обладнання (налаштування апаратного та програмного забезпечення). Налагодження мережі. Тестування конфігурацій апаратного та програмного забезпечення служб ЛОМ.	Інже нер	25
5.	Підготовка документації. Написання кабельного журналу, списку мережевого обладнання та його технічних характеристик.	Інже нер	5
		Разом	100

Сумарний час виконання операцій технологічного процесу проектування мережі становить 100 години, з них 20 годин – робота керівника проекту, 45 години – інженера, 35 години – техніка.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

У системі економічних відносин підприємства оплата праці розглядається як грошовий еквівалент вартості та ціни специфічного товару – робочої сили. Вона виступає у формі винагороди, яку роботодавець виплачує персоналу за фактично виконаний обсяг робіт або відпрацьований час. При цьому рівень

індивідуального заробітку працівника безпосередньо корелює з підсумковими показниками ефективності діяльності суб'єкта господарювання.

Для цілей даного проєкту загальний фонд оплати праці (ФОП) розраховується як сукупність основної та додаткової заробітної плати всіх залучених фахівців.

Основна заробітна плата розраховується за формулою:

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

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Виходячи з рекомендованих тарифних ставок встановимо таку ставку для керівник проекту – 250 грн, інженера – 200 грн./год. а для техніка – 160 грн./год.

Отже, основна заробітна плата для:

- керівника проекту – $З_{осн1} = 20 \cdot 250 = 5000$ грн.
- інженера – $З_{осн2} = 45 \cdot 200 = 9000$ грн.
- техніка – $З_{осн3} = 35 \cdot 160 = 5600$ грн.

Сумарна основна заробітна плата становить

Зосн=5000 +9000 + 5600 =19600 грн.

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

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

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

Отже, додаткова заробітна плата по категоріях працівників становить:

- керівника $З_{дод1}=5000 \cdot 0,12= 600$ грн.
- інженера $З_{дод1}=9000 \cdot 0,12= 1080$ грн.
- техніка $З_{дод3}=5600 \cdot 0,12= 672$ грн.

Сумарна додаткова заробітна плата становить:

$$З_{дод}=600 + 1080 + 672 = 2352 \text{ грн.}$$

Звідси загальні витрати на оплату праці (Во.п.) визначаються за форму-

лою:

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

Отже, загальні витрати на оплату праці становлять:

$$В_{о.п.} = 19600 + 2352 = 21952 \text{ грн.}$$

Крім того, слід визначити відрахування на соціальні заходи. Відрахування на соціальні заходи становлять 22%. Отже, сума відрахувань на соціальні заходи буде становити:

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

де ФОП – фонд оплати праці, грн.

$$В_{с.з} = 21952 \cdot 0,22 = 4829,44 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

№ п/п	Категорія праці-вни-ків	Основна заробітна плата, грн.			Додатк. заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на оплату праці, грн
		Тариф-на ставка, грн.	К-сть від-прац. год.	Фактично нарах. з/пл., грн.			
1	Керівник	250	20	5000	600	-	-
2	Інженер	200	45	9000	1080	-	-
3	Технік	160	35	5600	672	-	-
Разом				19600	2353	4829,44	26781,44

Отже, загальні витрати на оплату праці становлять 26781,44 грн.

4.3 Розрахунок матеріальних витрат

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

$$M_{BI} = q_i \cdot P_i \quad (4.5)$$

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу *i*-го виду.

Звідси, загальні матеріальні витрати можна визначити:

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

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. вимі-ру	Кі-лькість	Ціна, грн.	Сума, грн.
1	2	3	4	5	6
1	Комутаційна шафа	шт.	1	7900	7900
2	Розетка RJ-45 (категорія 6)	шт.	30	115	3450
3	Короб (середня ціна)	м.	90	112	10080
4	Кабель UTP (кат. 6) (бухта)	шт.	3	5445	16335
5	Патчкорди (кат. 6)	шт.	44	56	2464
6	комутатор TP-Link TL-SG1016	шт.	7	3150	22050
7	комутатор MikroTik RB5009UG+S+IN	шт.	1	8900	8900
8	Комутатор MikroTik hEX S (RB760iGS)	шт.	2	3200	6400
9	точка доступу MikroTik cAP ax	шт.	2	4300	8600
Р а з о м			-	-	86179

Отже, загальна сума матеріальних витрат на розробку мережі становить 86179 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання визначаються за формулою:

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

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 10 годин, споживана потужність – 0,5 кВт/год, вартість 1 кВт електроенергії – 9 грн. Тому витрати на електроенергію будуть становити:

$$З_е = 0,5 \cdot 10 \cdot 9 = 45 \text{ грн.}$$

4.5 Визначення транспортних затрат

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

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

де $Т_В$ – транспортні витрати.

Отже, $Т_В = 86179 \cdot 0,08 = 6894,32$ грн.

4.6 Розрахунок суми амортизаційних відрахувань

В процесі використання основних фондів виконуються заходи що до їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації. Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення. Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Мінімально

допустимі строки їх використання 2 роки.

Для визначення амортизаційних відрахувань застосовуємо формулу:

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

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

$Б_в$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$Н_А$ – норма амортизації, %;

Т – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 10 год., балансова вартість ПК - 29000 грн., тому, то амортизаційні відрахування становлять:

$$A = \frac{29000 \cdot 0{,}04}{150} \cdot 10 = 77{,}33 \ \ грн$$

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.

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

де $Н_В$ – накладні витрати.

$$Н_В = 21952{,}00 \cdot 0{,}4 = 8780{,}80 \ \text{грн.}$$

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 загального	
Витрати на оплату праці (основну і додаткову заробітну плату)	26781,44	21952	19,76	17,05
Відрахування на соціальні заходи	4829,44	4829,44	3,56	3,75
Матеріальні витрати	86179	86179	63,59	66,93
Витрати на електроенергію	45	45	0,03	0,03
Транспортні витрати	6894,32	6894,32	5,09	5,35
Амортизаційні відрахування	77,33	77,33	0,06	0,06
Накладні витрати	10712,57	8780,8	7,9	6,82
Собівартість	135519,1	128757,9	100	100

В таблиці 4.4 зазначено наступні види витрат: витрати на оплату праці, відрахування на соціальні заходи, матеріальні витрати, витрати на електроенергію, транспортні витрати, амортизаційні відрахування, накладні витрати, тобто собівартість ($С_в$) НДР розрахуємо за формулою:

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

Отже, собівартість дорівнює $С_В = 128757,9$ грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = C_в \cdot (1 + P_{рен}) \cdot (1 + ПДВ) \quad (4.12)$$

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

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

Отже, ціна НДР становить:

$$Ц = \sum (above) \quad = \sum (above) \; 135519{,}11 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 200862{,}3 \text{ грн}$$

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.

Прибуток розраховується за формулою:

$$П = Ц - C_в \quad (4.13)$$

де $П$ – прибуток;

$C_В$ – собівартість;

$$П = 201652{,}43 - 135519{,}11 = 72104{,}4 \text{ грн}$$

Економічна ефективність (Ер) полягає у відношенні результату виробництва до затрачених ресурсів і розраховується за формулою:

$$E_р = \frac{П}{C_в} = \frac{66133{,}22}{135519{,}11} = 0{,}56 \quad (4.14)$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень $Т_р$:

$$T_p = \frac{1}{E_p} \quad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку:

$$T_p = \frac{1}{0,49} = 1,8$$

Всі дані внесемо в зведену таблицю 4.5 економічних показників.

Таблиця 4.5 – Економічні показники НДР

№п/п	Показник	Значення
1.	Собівартість, грн.	128757,9 грн.
2.	Плановий прибуток, грн.	72104,4 грн.
3.	Ціна, грн.	200862,3 грн.
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,8

Загальна вартість розробленої комп'ютерної мережі логістичної компанії становить 128757,9 грн. Зважаючи на високі показники економічної ефективності – 0,56, кошти, вкладені в проведення проектних робіт окупляться за 1,8 року.

5. ОХОРОНА ПРАЦІ, ТЕХНІКИ БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1 Вжиті режимно-організаційні заходи, які забезпечують пожежну безпеку в ТОВ «Клео-П»

5.1.1 Нормативно-правова база та загальні принципи організації пожежної безпеки

Забезпечення пожежної безпеки на об'єктах ТОВ «Клео-П» (Головний офіс та Віддалений корпус) є невід'ємною частиною загальної системи охорони праці та цивільного захисту підприємства. Специфіка діяльності компанії як туристичної агенції пов'язана з постійним перебуванням у приміщеннях великої кількості людей (персонал компанії, клієнти, відвідувачі конференц-залу), а також із функціонуванням розвиненої телекомунікаційної інфраструктури, серверного обладнання, ПЕОМ та периферійних пристроїв. Це класифікує приміщення підприємства за категорією пожежної небезпеки переважно як такі, що мають підвищену концентрацію електрообладнання та горючих матеріалів (папір, пластик, меблі).

Правовою основою для розробки та впровадження режимно-організаційних заходів у ТОВ «Клео-П» є:

- Кодекс цивільного захисту України;
- Правила пожежної безпеки в Україні (НАПБ А.01.001-2014);
- Закон України «Про охорону праці»;
- чинні державні будівельні норми (зокрема, ДБН В.2.5-56:2014 «Системи протипожежного захисту»).

Згідно зі статтею 55 Кодексу цивільного захисту України, забезпечення пожежної безпеки покладається безпосередньо на власників та керівників суб'єктів господарювання. У ТОВ «Клео-П» керівництво загальною системою протипожежного захисту здійснює директор підприємства, а безпосереднє виконання режимних та організаційних функцій покладено на призначених посадових осіб.

5.1.2. Організаційні заходи забезпечення пожежної безпеки

Організаційні заходи є базовим елементом протипожежного захисту, оскільки вони визначають структуру управління, розподіл обов'язків, порядок документообігу та підготовку персоналу до дій у разі виникнення надзвичайної ситуації.

У ТОВ «Клео-П» реалізовано такі організаційні заходи:

1. Видання розпорядчої документації: Наказом директора затверджено «Положення про пожежну безпеку ТОВ „Клео-П“», призначено відповідальних осіб за протипожежний стан кожного окремого приміщення (кабінетів бухгалтерії, менеджерів, конференц-залу, серверної кімнати Головного офісу та приміщень Віддаленого корпусу). На видному місці біля телефонів розміщено таблички із зазначенням прізвища відповідального та номера телефону виклику оперативно-рятувальної служби цивільного захисту (101 або 112).

2. Навчання та інструктажі з питань пожежної безпеки: Відповідно до НАПБ Б.02.005-2003, усі працівники ТОВ «Клео-П» під час прийняття на роботу і в процесі трудової діяльності проходять інструктажі з питань пожежної безпеки. Система інструктажів включає:

– Вступний інструктаж — проводиться з усіма новоприйнятими працівниками незалежно від їхньої посади та освіти;

– Первинний інструктаж — проводиться безпосередньо на робочому місці перед початком виконання обов'язків;

– Повторний інструктаж — проводиться не рідше ніж один раз на рік для офісних приміщень з метою відновлення знань;

– Позаплановий інструктаж — проводиться у разі введення в експлуатацію нового мережевого чи серверного обладнання, зміни правил пожежної безпеки або після зафіксованих порушень;

– Цільовий інструктаж — проводиться перед виконанням разових робіт (наприклад, вогневих чи ремонтних робіт підрядними організаціями).

Усі результати інструктажів фіксуються в «Журналі реєстрації інструктажів з питань пожежної безпеки» під підпис інструктованого та особи, яка

проводила інструктаж.

3. Розробка та розміщення планів евакуації: Для Головного офісу та Віддаленого корпусу розроблено текстові та графічні плани евакуації людей на випадок пожежі згідно з вимогами ДСТУ ISO 23601:2019. Плани евакуації вивішені на видимих місцях на шляхах евакуації (у коридорах, біля виходів, у конференц-залі). Двічі на рік на підприємстві проводяться практичні тренування з евакуації персоналу та імітації ліквідації пожежі первинними засобами пожежогасіння.

5.1.3. Встановлення та підтримання протипожежного режиму (Режимні заходи)

Режимні заходи визначають правила поведінки людей, порядок утримання території, будівель, приміщень та експлуатації обладнання з метою мінімізації ризиків виникнення пожежі. Наказом директора в ТОВ «Клео-П» встановлено суворий протипожежний режим, який включає такі вимоги:

– Заборона куріння: Куріння тютюнових виробів, електронних сигарет та кальянів у всіх службових приміщеннях, коридорах, санітарних зонах та на балконах ТОВ «Клео-П» категорично заборонено. Організовано спеціальне місце для куріння на відкритому повітрі за межами будівель, яке позначене відповідним знаком, забезпечене урною з водою та первинними засобами пожежогасіння.

– Порядок утримання шляхів евакуації: Коридори,тамбури, проходи до основних та запасних виходів підтримуються вільними. Забороняється захаращувати евакуаційні шляхи меблями, коробками з паперами, сейфами чи побутовою технікою. Двері на шляхах евакуації відчиняються у напрямку виходу з приміщень і не мають засувів, які не можна відімкнути зсередини без ключа.

– Режим роботи після закінчення робочого дня: Після завершення робочої зміни кожен працівник зобов'язаний оглянути своє робоче місце, закрити вікна, вимкнути з електромережі персональний комп'ютер, принтер, локальне освітлення та кондиціонер. Забороняється залишати під

напругою пристрої, якщо це не обумовлено їхнім технологічним призначенням (наприклад, сервери та комутаційне обладнання). Відповідальна особа перевіряє приміщення, замикає його та робить відмітку в журналі контролю протипожежного стану.

5.1.4. Протипожежні вимоги до експлуатації електроустановок та телекомунікаційного обладнання

Оскільки в рамках даного проєкту розроблено та впроваджено сучасну мережеву інфраструктуру (включаючи маршрутизатори MikroTik RB5009 та hEX S, некеровані комутатори TP-Link TL-SG1016, сервери даних та бездротові точки доступу cAP ax), експлуатація електроустановок є головним джерелом потенційної пожежної небезпеки через ризики короткого замикання, перевантаження мережі або великого перехідного опору.

Для усунення цих ризиків у ТОВ «Клео-П» реалізовано комплекс техніко-режимних заходів:

1. Захист від перевантажень та коротких замикань: Усі силові та освітлювальні мережі підключені через автоматичні вимикачі та пристрої захисного вимкнення (ПЗВ / ПЗВ-Д), розраховані на відповідні струми навантаження. Забороняється використання несертифікованих або саморобних запобіжників («жучків»).

2. Вимоги до прокладання кабельних ліній: Усі локальні мережі (кабелі «вита пара» Cat5e/Cat6) та силові лінії прокладені в негорючих пластикових кабель-каналах (коробах) або всередині гофрованих труб, які не підтримують горіння. При проходженні кабелів крізь стіни отвори загерметизовані вогнестійким розчином для запобігання поширенню полум'я та диму між суміжними приміщеннями.

3. Особливості пожежної безпеки серверної кімнати: У серверній кімнаті Головного офісу, де зосереджено маршрутизатор ядра SW_7 та сервери S_1, S_2, встановлено жорсткі обмеження:

– Комутаційні шафи 19" надійно заземлені;

– Серверна кімната оснащена автономною системою кондиціонування для запобігання перегріву активного обладнання;

– Забороняється зберігання в серверній кімнаті сторонніх предметів, паперових архівів, канцтоварів та побутових приладів.

5.1.5. Заходи пожежної безпеки під час використання систем резервного та альтернативного живлення. З урахуванням сучасних реалій функціонування підприємств в Україні, критично важливим аспектом пожежної безпеки є правильна експлуатація джерел безперебійного живлення (ДБЖ) та акумуляторних батарей, що забезпечують безперервну роботу мережі MikroTik та TP-Link під час аварійних вимкнень електроенергії. У ТОВ «Клео-П» впроваджено такі режимні правила для систем живлення:

– Для резервування серверів та маршрутизаторів використовуються ДБЖ виключно промислового виробництва з герметичними свинцево-кислотними (AGM/GEL) або літій-залізо-фосфатними (LiFePO4) акумуляторами, які не виділяють вибухонебезпечного водню під час заряджання.

– Забороняється використання в офісних приміщеннях автомобільних стартерних акумуляторів із рідким електролітом.

– Корпуси ДБЖ встановлюються на негорючі підставки (керамічна плитка або металеві листи) у місцях, де забезпечено вільну циркуляцію повітря для охолодження радіаторів та вбудованих вентиляторів. Регулярно (не рідше ніж один раз на квартал) проводиться очищення обладнання від пилу, який може стати причиною займання при перегріві.

5.1.6. Забезпечення приміщень первинними засобами пожежогасіння

Відповідно до НАПБ А.01.001-2014 та Норм належності первинних засобів пожежогасіння, всі приміщення ТОВ «Клео-П» укомплектовані сертифікованими вогнегасниками. Вибір типу вогнегасників зумовлений класом можливої пожежі: для офісних приміщень з великою кількістю оргтехніки та серверів критично важливим є використання вуглекислотних вогнегасників (клас Е — гасіння електроустановок під напругою до 1000 В), оскільки вони, на відміну від порошкових, не пошкоджують мікросхеми та дорогі плати

маршрутизаторів і серверів.

Нормативний розрахунок потреби у вогнегасниках для об'єктів ТОВ «Клео-П» наведено в таблиці 5.1.

Таблиця 5.1 — Розрахунок потреби в первинних засобах пожежогасіння ТОВ «Клео-П»

Найменування приміщення	Площа, m2	Основне пожежне навантаження	Клас пожежі	Тип та марка вогнегасника	Необхідна кількість, шт.
Серверна кімната (Ядро мережі)	12	Сервери, комутатори, ДБЖ, кабелі	E	Вуглекислотний ВВ-3 (ОУ-5)	1
Конференц-зал (Зона Wi-Fi)	65	Ноутбуки, точка доступу, меблі	A, E	Порошковий ВП-5 Вуглекислотний ВВ-2	11
Кабінет менеджерів (Головний офіс)	120	ПЕОМ, принтери, паперові документи	A, E	Порошковий ВП-5 Вуглекислотний ВВ-3	21
Кабінет бухгалтерії та керівництва	45	ПЕОМ, паперові архіви, сейфи	A, E	Порошковий ВП-2 Вуглекислотний ВВ-2	11
Віддалений корпус (Кабінети менеджерів)	150	ПЕОМ, комутатор SW_4, принтери	A, E	Порошковий ВП-5 Вуглекислотний ВВ-3	22

Правила утримання та експлуатації вогнегасників:

– Вогнегасники розміщені на висоті не більше 1,5 метра від рівня підлоги в легкодоступних місцях (біля входів/виходів), вони не заважають евакуації та захищені від прямого сонячного проміння й теплового впливу опалювальних приладів.

– Усі вогнегасники мають облікові номери, забезпечені бирками та внесені до «Журналу обліку первинних засобів пожежогасіння».

– Особа, відповідальна за пожежну безпеку, щомісячно проводить зовнішній огляд пристроїв (перевірка цілісності пломб, наявності розтрубів, положення стрілки манометра для порошкових вогнегасників). Технічне обслуговування, перезарядка та зважування вуглекислотних вогнегасників здійснюються щорічно у спеціалізованих організаціях, що мають відповідну ліцензію ДСНС України.

5.1.7. Автоматичні системи протипожежного захисту та оповіщення

Для забезпечення максимального рівня безпеки та оперативного реагування приміщення Головного офісу та Віддаленого корпусу ТОВ «Клео-П» обладнані системами автоматичної пожежної сигналізації (АПС) та управління евакуацією людей (системи оповіщення про пожежу).

– Датчики виявлення: В офісних кабінетах, конференц-залі та серверній кімнаті на стелях встановлено оптико-електронні димові пожежні сповіщувачі (наприклад, типу СПД-3.2). Оскільки першою ознакою займання ізоляції кабелів чи елементів електроніки в комутаторах є виділення диму, дані датчики дозволяють зафіксувати пожежу на її початковій («тліючій») стадії.

– Ручні сповіщувачі: На шляхах евакуації (у коридорах та біля виходів із будівель) встановлено ручні пожежні сповіщувачі (кнопки червоного кольору типу SPR-1) для примусової активації сигналу тривоги будь-яким працівником підприємства, який першим виявив загрозу.

– Система оповіщення: При спрацюванні хоча б одного димового сповіщувача, сигнал надходить на приймально-контрольний прилад, який

автоматично запускає світлозвукові покажчики «ВИХІД» та сирени внутрішнього оповіщення, що генерують мовне повідомлення про необхідність негайної евакуації.

– Моніторинг: Сигнал тривоги від приймально-контрольного приладу через вбудований GSM/GPRS-комунікатор миттєво передається на пульт централізованого пожежного спостереження ДСНС для автоматичного виклику пожежно-рятувальних підрозділів.

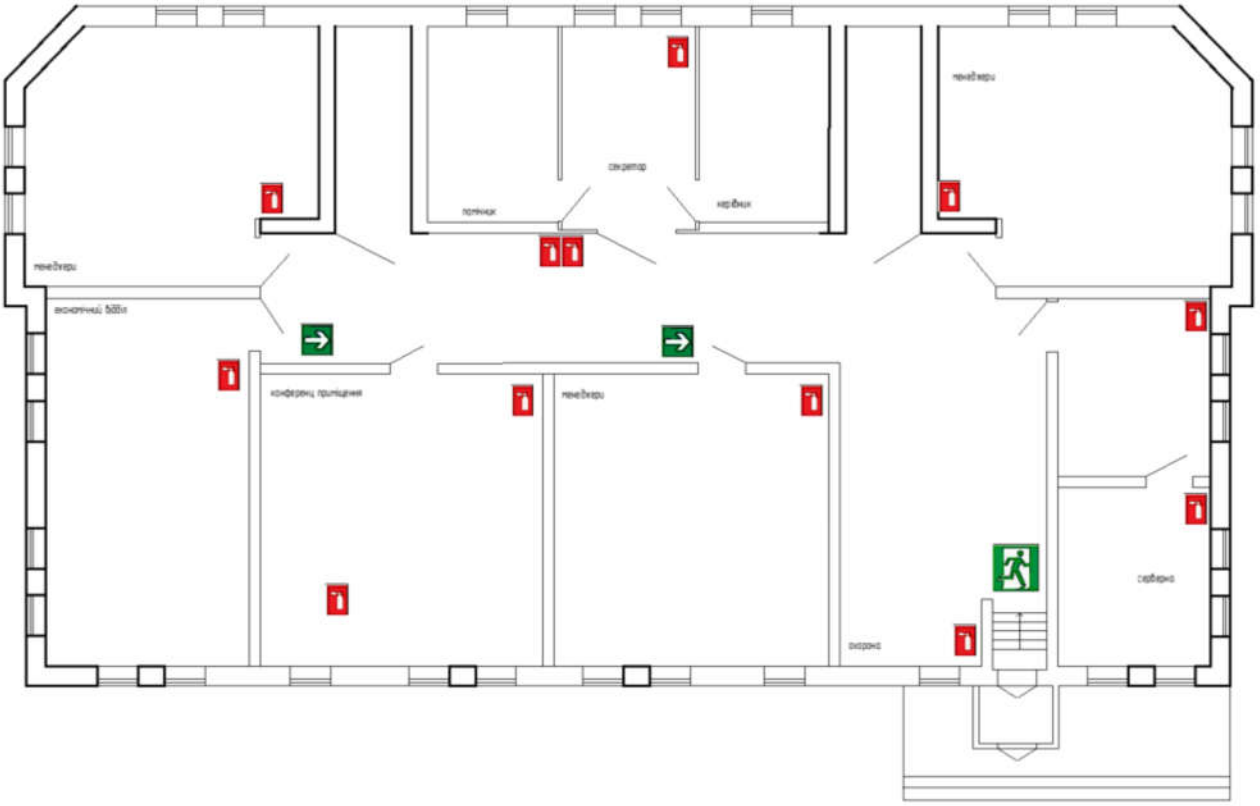


Рисунок 5.1 — Розміщення знаків евакуаційного виходу та вогнегасників у приміщенні

Впроваджений комплекс режимно-організаційних заходів у ТОВ «Клео-П» повністю відповідає чинному законодавству України в галузі пожежної безпеки та охорони праці. На рисунку 5.1 показані розміщення вогнегасників головного офісу та напрям руху до евакуаційного виходу та сам вихід. Чіткий розподіл посадових обов'язків, регулярне проведення інструктажів, дотримання суворого протипожежного режиму, правильний підбір вуглекислотних во-

гнегасників для захисту серверного та мережевого обладнання, а також функціонування автоматичної пожежної сигналізації дозволяють мінімізувати ризик виникнення пожежі, забезпечити надійний захист матеріальних цінностей компанії та, найголовніше, гарантувати безпеку життя і здоров'я персоналу та клієнтів туристичної агенції.

5.2 Порядок допуску працівників до робіт з обслуговування електрообладнання

Робота персоналу на підприємстві щодня пов'язана з використанням обладнання, що живиться від електромережі.

Навчання з електробезпеки необхідно проходити не тільки електрикам, а й роботодавцям, керівництву підприємства на якому працює сам робітник.

Необхідно пройти навчання працівників, посадових осіб та спеціалістів по електробезпеці по наступним правилам:

– НПАОП 40.1-1.28-98. Правила безпечної експлуатації електроустановок споживачів (ПБЕЕС);

– НПАОП 40.1-1.07-01. Правила експлуатації електрозахисних засобів (ПЕЕЗ);

– Правила улаштування електроустановок (ПУЕ);

– Правила технічної експлуатації електроустановок споживачів) (ПТЕЕС);

Хто зобов’язаний проходити навчання?

Щоб не допустити випадків електротравматизму і не спровокувати санкцій за несумлінне дотримання нормативних вимог, роботодавцям важливо занотувати категорії працівників, яким потрібно проводити навчання та перевірку знань з присвоєнням групи допуску.

Навчання зобов’язані проходити:

– Керівники компаній, фахівці, які відповідають за організацію роботи, тісно пов’язаної з електроенергією;

– Штатні співробітники, діяльність яких пов’язана з роботою на електроустановках різних типів та потужностей;

– Фахівці з охорони праці, які здійснюють інспектування електрообладнання та контролюють додержання нормативно-правових актів під час організації та виконання робіт.

Група з електробезпеки (“кваліфікаційна група“, “група допуску“) дає дозвіл персоналу компанії до виконання робіт в електроустановках, а також свідчить про рівень його підготовки. Некваліфікований працівник – це завжди ризик. Штрафи при перевірці, нещасні випадки, псування дорогого устаткування, збій роботи всього підприємства, неможливість впровадження нових технологій.

Які є групи допуску.

I групаз електробезпеки присвоюється всьому неелектричному персоналу, який в процесі своєї роботи на підприємстві стикається з електричними приладами та офісною технікою.

Група присвоюється співробітнику після проходження відповідного інструктажу, під розпис в журналі реєстрації інструктажів на I кваліфікаційну групу.

II група з електробезпеки присвоюється співробітникам, що працюють в електроустановках, але не мають права самостійно підключати їх в мережу.

III групаз електробезпеки дає можливість працівникам самостійно виконувати роботи в електроустановках. З цією групою співробітники можуть проводити огляд і обслуговування електроустаткування, а також бути спостерігачами або керівниками робіт в електроустановках до 1000 В.

IV група з електробезпеки присвоюється керівним посадовим особам, з великим професійним стажем, наприклад бригадиру, начальнику підрозділу, головному енергетику. Ця група буває до 1000 В та понад.

V група з електробезпеки присвоюється відповідальним співробітникам, які працюють з потужними електроустановками (до та понад 1000 В), а також випробовують обладнання підвищеною напругою.

Зверніть увагу! Особи, які несуть відповідальність за електрогосподарство і їх заступники повинні мати IV або V групу.

За недотримання встановлених вимог з електробезпеки передбачені штрафи.

Навчання з електробезпеки проводиться як для організацій, що використовують електроенергію в своїх потребах, так і для постачальників електроенергії

Працівнику, який пройшов перевірку знань Правил, видається витяг з проколу та посвідчення встановленої форми, , яке він зобов'язаний мати при собі під час роботи.

Посвідчення про перевірку знань працівника є документом, який засвідчує право на самостійну роботу в електроустановках на зазначеній посаді за фахом. Воно видається працівникові комісією з перевірки знань підприємства, організації після перевірки знань і є дійсним тільки після внесення відповідних записів. За відсутності посвідчення або за наявності посвідчення з простроченими термінами перевірки знань працівник до роботи не допускається. Посвідчення про перевірку знань підлягає заміні у випадку зміни посади або за відсутності місця для записів.

Періодичність навчання з електробезпеки

Періодичність проходження курсів з електробезпеки безпосередньо залежить від трудових обов'язків, покладених на співробітника. Раз на рік курси навчання проходять співробітники, які безпосередньо працюють, обслуговують або проводять випробування в електроустановках. Інженери з охорони праці та співробітники, непрацюючі з електричним обладнанням, курси навчання з електробезпеки проходять один раз в три роки.

Позапланове проходження навчання з електробезпеки проводиться в таких випадках:

- внутрішнє переведення працівника компанії на іншу посаду;
- зміна місця роботи;
- перерва в робочому стажі, терміном від трьох років;

– оновлення обладнання компанії;

– для виконання посадових обов'язків співробітнику необхідна більш висока група допуску;

– зміна нормативних актів і правил охорони праці.

ВИСНОВКИ

У межах виконання кваліфікаційної роботи було проведено комплексний аналіз стану інформаційно-телекомунікаційної системи (ІТКС) ТОВ «Клео-П» та здійснено її поетапну модернізацію з метою підвищення швидкодії, надійності та рівня інформаційної безпеки.

Технічна реалізація проєкту базувалася на впровадженні сучасного обладнання компанії MikroTik (моделі RB5009 та hEX S), що дозволило створити гнучку архітектуру мережі. Ключовим результатом модернізації стало впровадження технології VLAN (Virtual Local Area Network), яка забезпечила логічну ізоляцію трафіку між різними департаментами (бухгалтерія, менеджери, сервери, гостьовий сектор). Така сегментація не лише оптимізувала потік даних, усунувши «широкомовні шторми», але й суттєво підвищила рівень безпеки, унеможлививши несанкціонований доступ до конфіденційних сегментів мережі.

Особливу увагу в роботі було приділено захищеності каналів зв'язку між Головним офісом та Віддаленим корпусом. Завдяки розгортанню протоколу IPsec (Site-to-Site VPN) із використанням сучасних алгоритмів шифрування (AES-256), було забезпечено конфіденційність передачі даних у єдиному корпоративному просторі. Це дозволило відмовитися від ненадійних засобів доступу та створити надійний «криптографічний міст», який функціонує прозоро для кінцевих користувачів.

Проведена модернізація також охопила питання фізичної та організаційної безпеки. Були впроваджені чіткі режимно-організаційні заходи, що відповідають чинному законодавству України, зокрема у сфері пожежної безпеки. Обладнання серверної кімнати та робочих місць засобами пожежогасіння класу «Е» (вуглекислотні вогнегасники), а також інтеграція автоматичної системи пожежної сигналізації, забезпечують захист дороговартісного активного мережевого обладнання від потенційних техногенних ризиків.

Розроблена ієрархічна схема IP-адресації з використанням принципу

VLSM створила передумови для подальшого масштабування ІТКС ТОВ «Клео-П». Завдяки автоматизації розподілу адрес (DHCP-сервери) та виділенню сегмента керування (VLAN 40), адміністратори мережі отримали інструментарій для віддаленого моніторингу та діагностики обладнання, що мінімізує час простою сервісів у разі виникнення несправностей.

Поставлені завдання модернізації мережі виконані в повному обсязі. Розроблена система відповідає сучасним вимогам до корпоративних мереж, забезпечує високий рівень стійкості до відмов, ефективно підтримує бізнес-процеси туристичної агенції та має високий потенціал для подальшого розвитку без необхідності радикальних змін в архітектурі. Економічна доцільність проєкту підтверджується зниженням витрат на обслуговування мережі та підвищенням продуктивності праці персоналу за рахунок стабільного доступу до корпоративних інформаційних ресурсів.

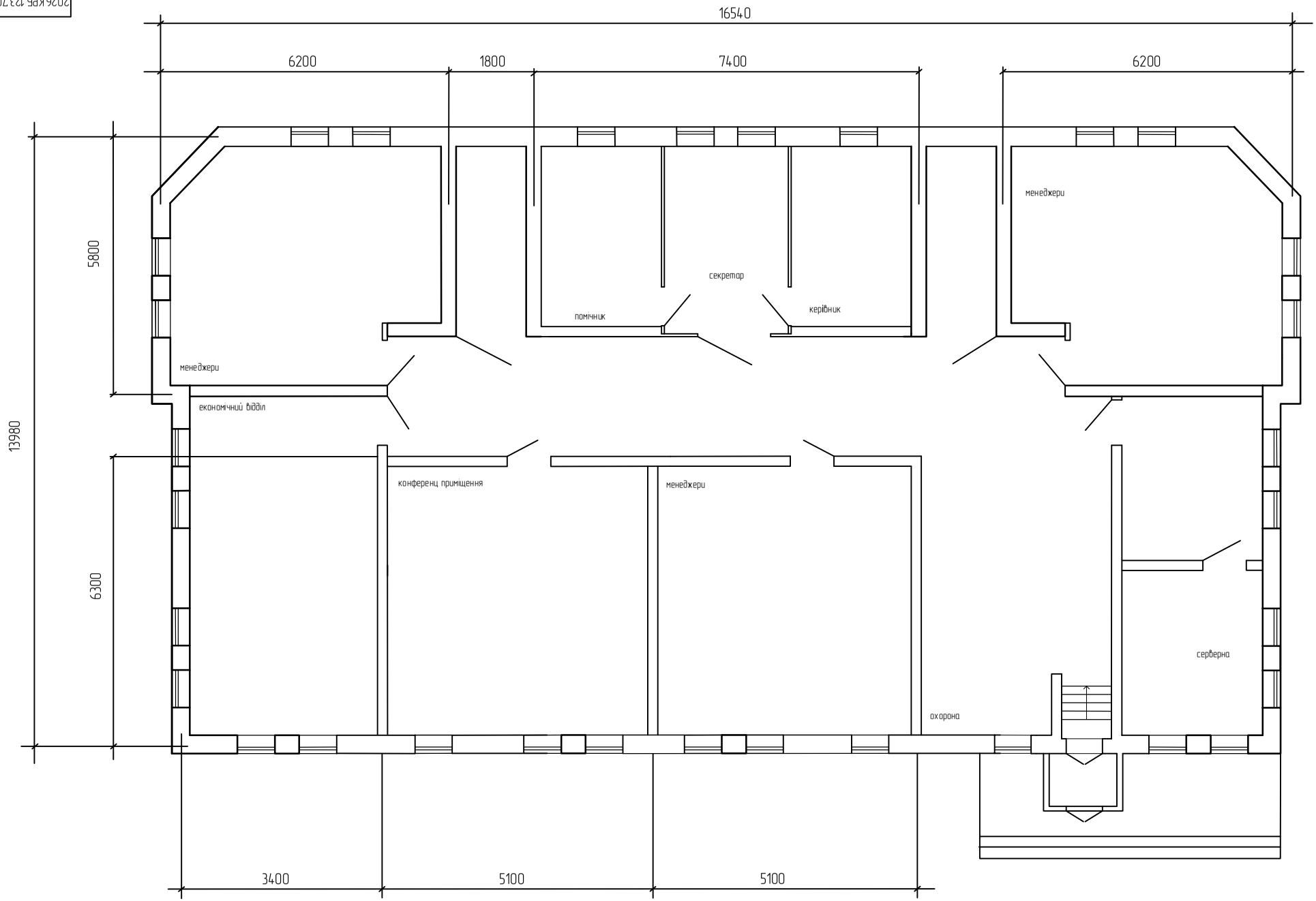
ПЕРЕЛІК ПОСИЛАНЬ

1. Таненбаум Е., Везерролл Д. Комп’ютерні мережі. 5-те вид. — Х. : Фабула, 2012. — 960 с.
2. Одом В. Офіційний посібник із сертифікації CCNA 200-301. Том 1. / Вендел Одом ; пер. з англ. — Нью-Йорк : Cisco Press, 2020. — 800 с.
3. Одом В. Офіційний посібник із сертифікації CCNA 200-301. Том 2. / Вендел Одом ; пер. з англ. — Нью-Йорк : Cisco Press, 2020. — 736 с.
4. Буров Є. В. Комп’ютерні мережі: технології, протоколи, сервіси : навч. посібник / Є. В. Буров. — Львів : Магнолія-2006, 2019. — 584 с.
5. Мельник В. А. Організація комп’ютерних мереж : підручник / В. А. Мельник, О. В. Корнейчук. — К. : Центр навчальної літератури, 2021. — 342 с.
6. Дішер М. Налаштування MikroTik RouterOS з нуля / Майкл Дішер. — Техас : LearnRouterOS, 2018. — 420 с.
7. Кулаков Ю. О. Сучасні технології локальних та корпоративних мереж : навч. посібник / Ю. О. Кулаков, О. В. Луцький. — К. : КНУ, 2016. — 280 с.
8. Каліновський Ю. В. Проектування та моделювання телекомунікаційних мереж у середовищі Cisco Packet Tracer : метод. вказівки / Ю. В. Каліновський. — Одеса : ОНАЗ ім. О. С. Попова, 2018. — 64 с.
9. MikroTik Help & Documentation [Електронний ресурс] : Офіційна база знань та документація RouterOS v7. — Режим доступу: https://help.mikrotik.com/docs/ (дата звернення: 14.05.2026).
10. Cisco Networking Academy [Електронний ресурс] : Навчальні матеріали та документація Cisco Packet Tracer. — Режим доступу: https://www.netacad.com/ (дата звернення: 14.05.2026).
11. RFC 4301 — Security Architecture for the Internet Protocol (IPsec) [Електронний ресурс] / Internet Engineering Task Force (IETF). — Режим доступу: https://datatracker.ietf.org/doc/html/rfc4301 (дата звернення:

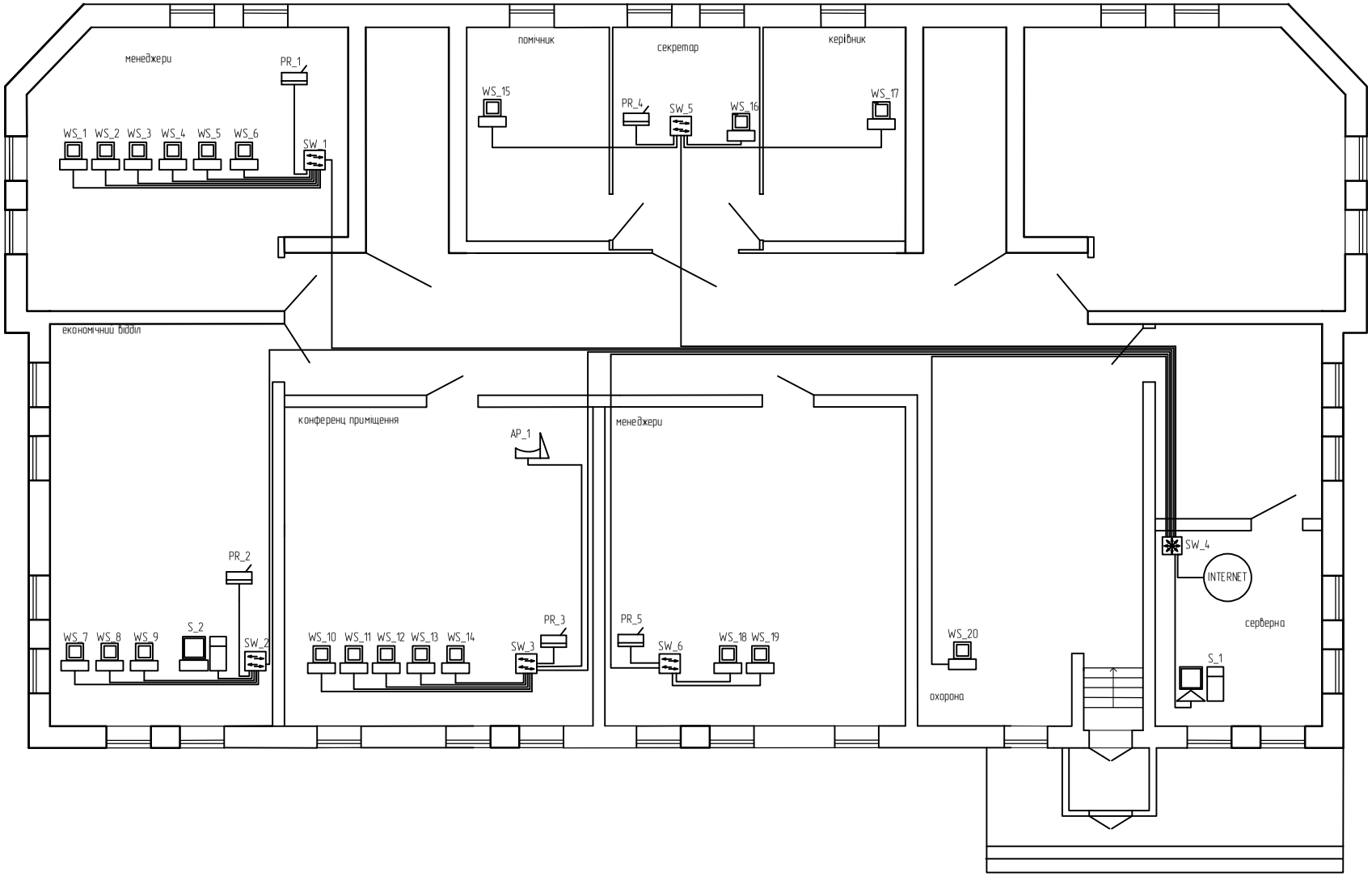
4.06.2026).

12. IEEE 802.1Q — Bridges and Bridged Networks (VLAN tagging) [Електронний ресурс] / IEEE Xplore Digital Library. — Режим доступу: https://ieeexplore.ieee.org/document/8403927 (дата звернення: 5.06.2026).
13. TP-Link Business Networking Support [Електронний ресурс] : Технічні специфікації та інструкції до комутаторів серії TL-SG1016. — Режим доступу: https://www.tp-link.com/uk/business-networking/ (дата звернення: 7.06.2026).
14. Офіційний веб-портал ДСНС України [Електронний ресурс] : Нормативні документи та рекомендації з цивільного захисту й пожежної безпеки під час воєнного стану. — Режим доступу: https://dsns.gov.ua/ (дата звернення: 8.06.2026).

2026.КРБ.123.703.09.00.01 ПП

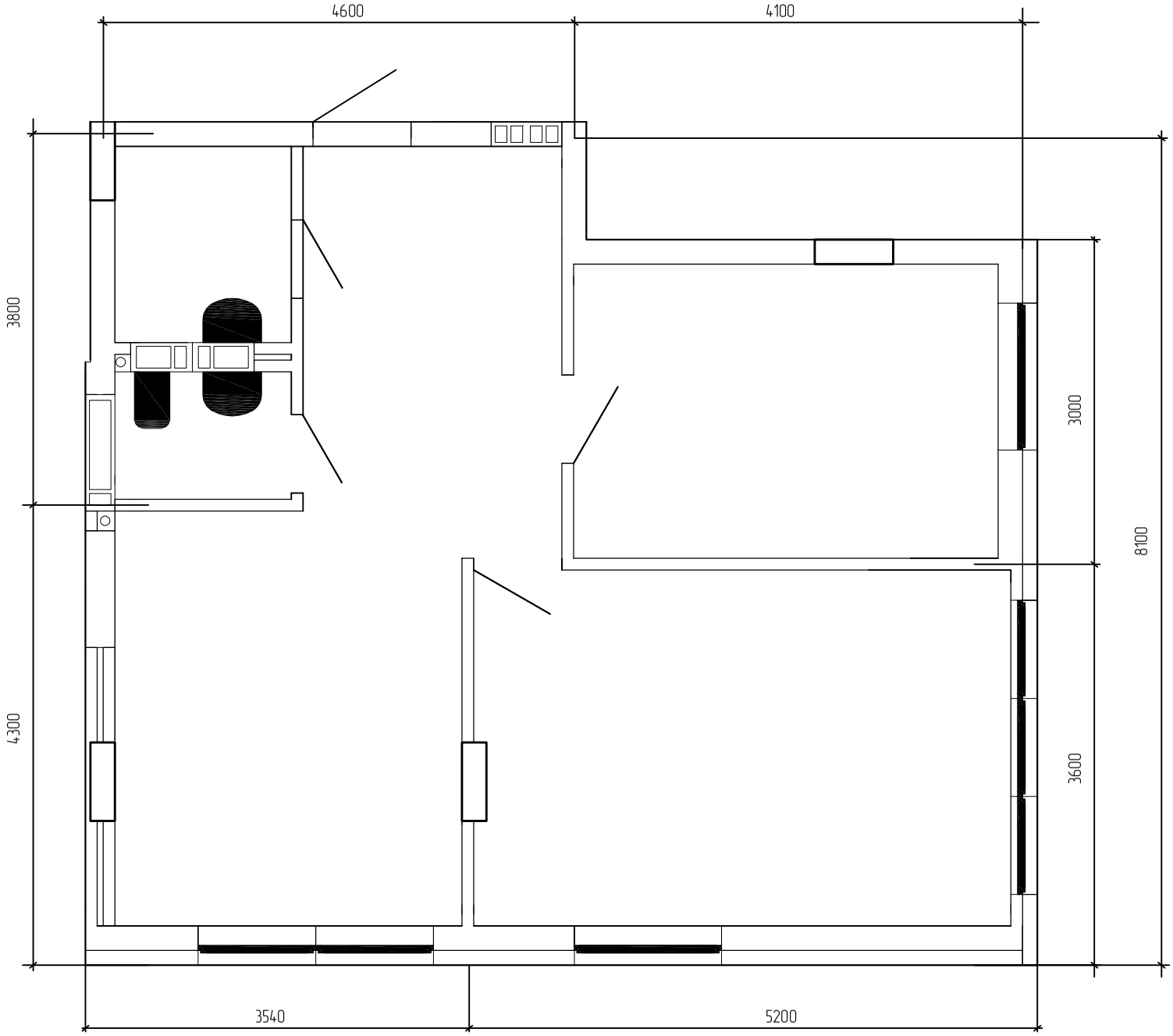


						2026.КРБ.123.703.09.00.01 ПП	
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту модернізації комп'ютерної мережі ТОВ «Клео-П» План Приміщень	Літ.	Маса	Масшт.
Розроб.		Лубінь М.З.						1:100
Керів.		Пик В.І.				Аркуш 1	Аркушів 1	
Н.контр.		Приймак В.А.				ВСП ТФК ТНТУ КІБ-703, м.Тернопіль		
Рецензія								
затв.								

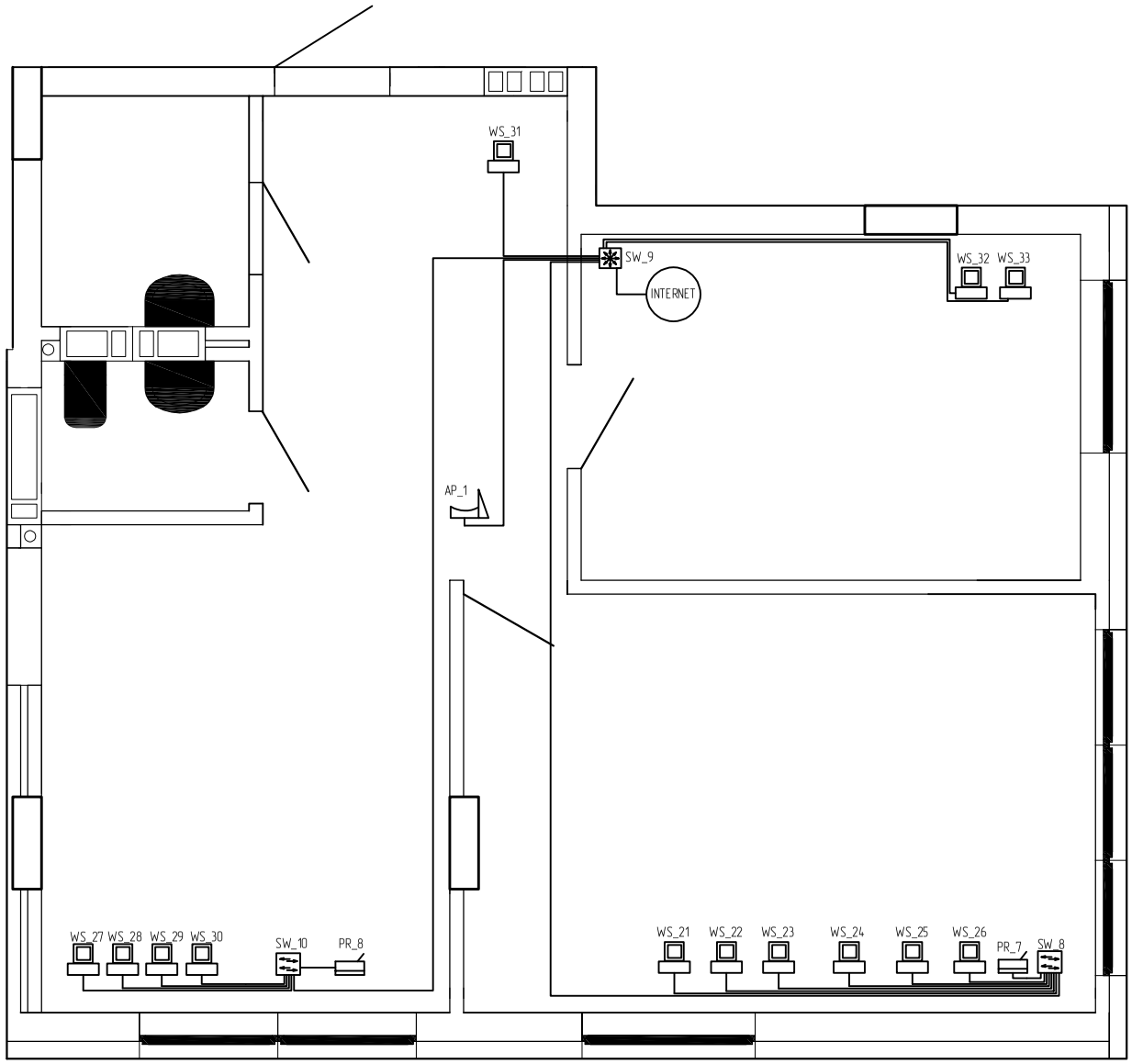


						2026.КРБ.123.703.09.00.01 ФТ	
Зм.	Арк.	№Докум.	Підпис	Дат.		Розробка проекту модернізації комп'ютерної мережі ТОВ «Клео-П» Фізична Топологія	Літ. / Маса / Масшт. 1:100
Розроб.		Людинь М.З.					
Керів.		Пик В.Є.					
Н.контр.		Прийомк В.А.					Аркуш 1 / Аркушів 1
Рецензія							ВСП ТФК ТНТУ КІБ-703, м.Тернопіль

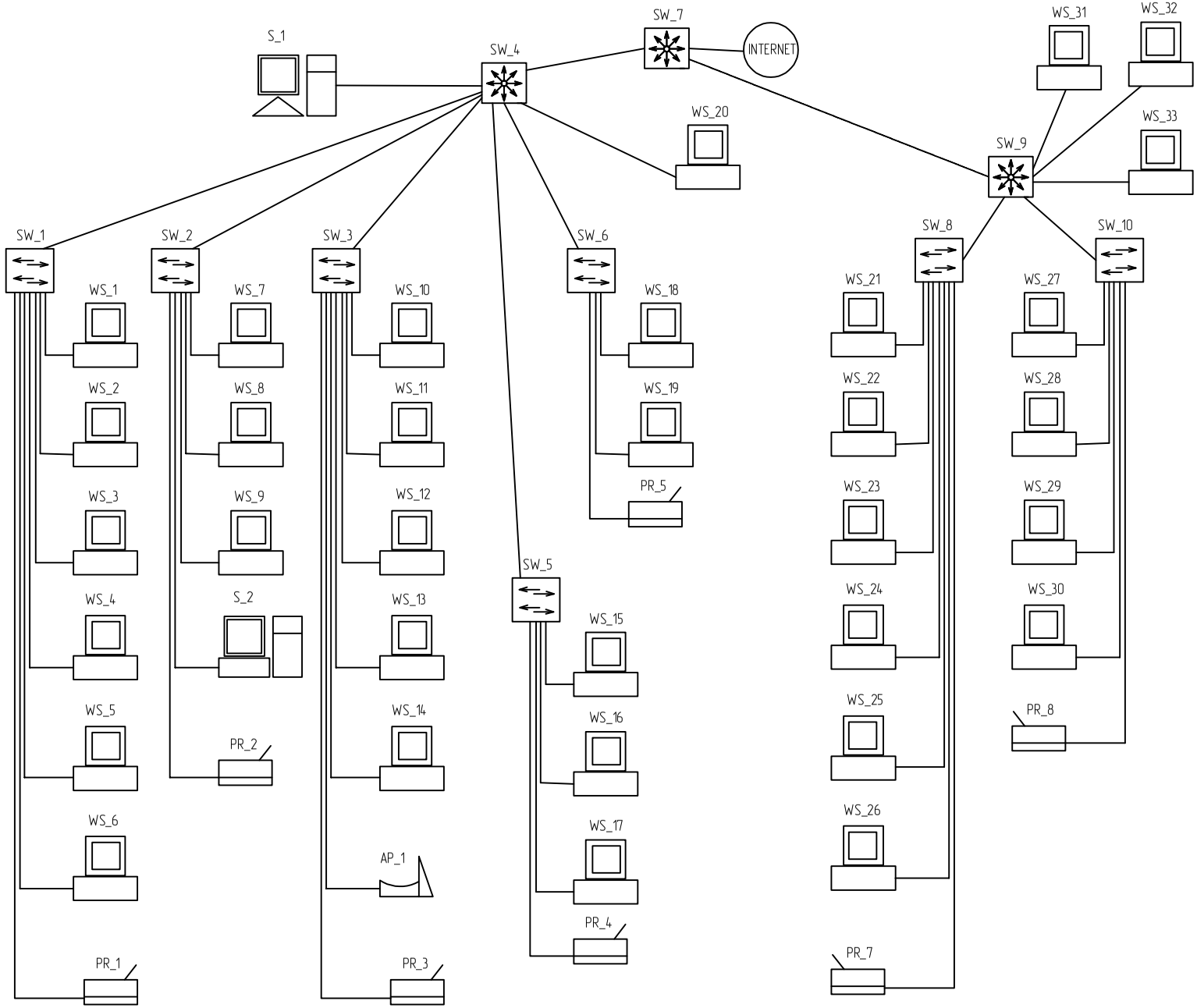
2026.КРБ.123.703.09.00.02 ПП



						2026.КРБ.123.703.09.00.02 ПП	
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту модернізації комп'ютерної мережі ТОВ «Клео-П» План Приміщень	Літ.	Маса	Масшт.
Розроб.		Лубінь М.З.						1:100
Керів.		Пшк В.С.						
Н.контр.		Приймак В.А.				Аркуш 1	Аркушів 1	
Рецензія						ВСП ТФК ТНТУ КІБ-703, м.Тернопіль		
Затв.								



						2026.КРБ.123.703.09.00.02 ФТ		
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту модернізації комп'ютерної мережі ТОВ «Клео-П» Фізична Топологія	Літ.	Маса	Масшт.
Розроб.		Людинь М.З.						1:100
Керів.		Пук В.Є.				Аркуш 1	Аркушів 1	
Нконтр.		Приймак В.А.				ВСП ТФК ТНТУ КІБ-703, м.Тернопіль		
Рецензія								
затв.								



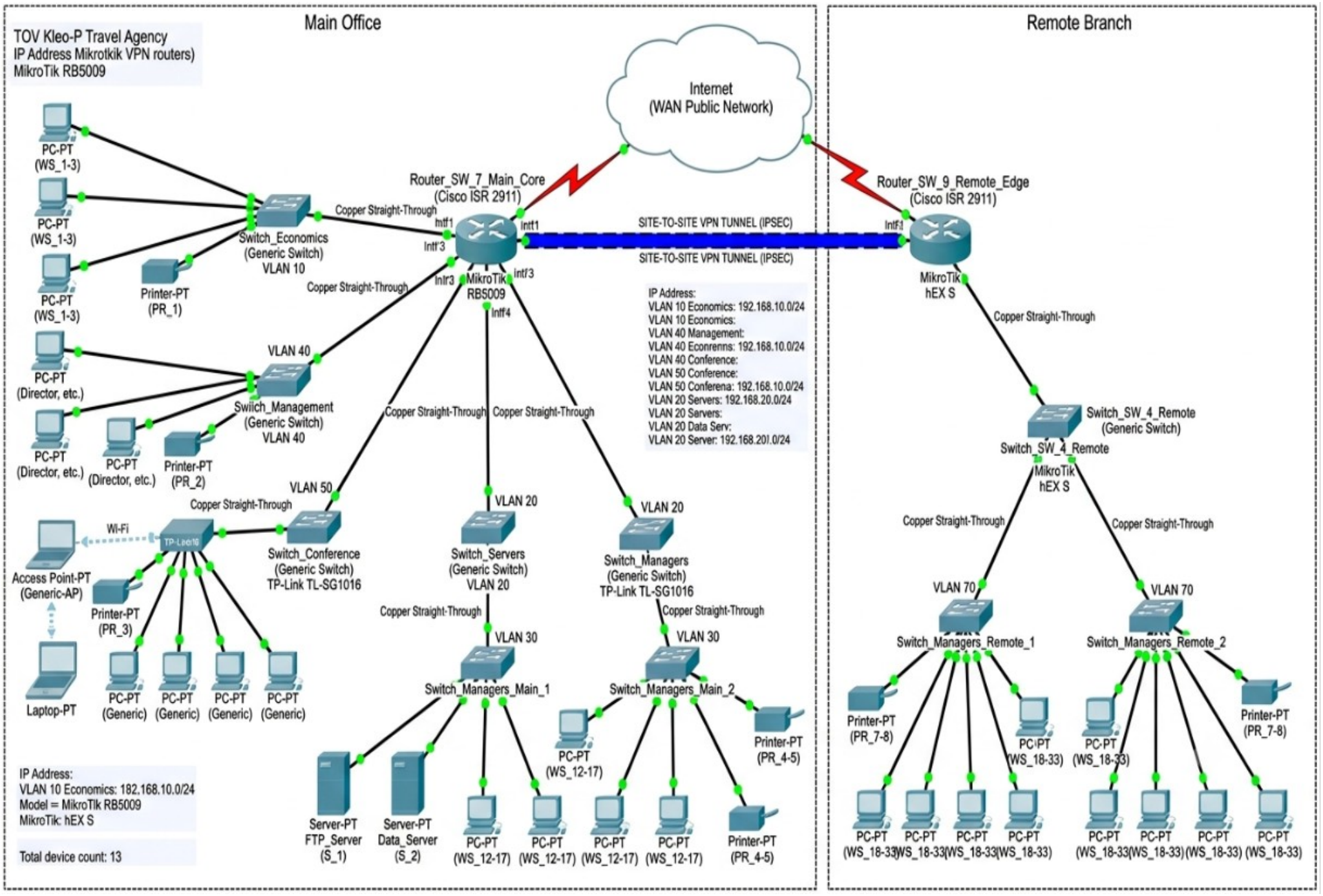
						2026.КРБ.123.703.09.00.00 ЛТ	
Зм.	Арк.	№Докум.	Підпис	Дат.		Розробка проекту модернізації комп'ютерної мережі ТОВ «Клео-П» Логічна Топологія	Літ. / Маса / Масшт.
Розроб.		Людинь М.З.					
Керів.		Пшк В.І.					Аркуш 1 / Аркушів 1
Нконтр.		Прийомк В.А.					ВСП ТФК ТНТУ КІБ-703, м.Тернопіль
Рецензія							
затв.							

Назва сегмента (VLAN)	Ідентифікатор (VLAN ID)	Адреса підмережі / CIDR	Маска підмережі	Основний шлюз (Gateway)	Діапазон адрес для DHCP / Статики	Тип призначення адрес
Економічний відділ (Бухгалтерія)	VLAN 10	192.168.10.0/24	255.255.255.0	192.168.10.1	192.168.10.10 — 192.168.10.100	Динамічний (DHCP)
Серверна зона (Data/FTP)	VLAN 20	192.168.20.0/24	255.255.255.0	192.168.20.1	192.168.20.2 — 192.168.20.254	Статичний
Менеджери (Головний офіс)	VLAN 30	192.168.30.0/24	255.255.255.0	192.168.30.1	192.168.30.10 — 192.168.30.100	Динамічний (DHCP)
Службовий сегмент (Керування)	VLAN 40	192.168.40.0/24	255.255.255.0	192.168.40.1	192.168.40.10 — 192.168.40.100	Змішаний (DHCP + Статика)
Конференц-зал (Гостьовий Wi-Fi)	VLAN 50	192.168.50.0/24	255.255.255.0	192.168.50.1	192.168.50.10 — 192.168.50.100	Динамічний (DHCP)
Менеджери (Віддалений корпус)	VLAN 70	192.168.70.0/24	255.255.255.0	192.168.70.1	192.168.70.10 — 192.168.70.150	Динамічний (DHCP)
WAN-канал (Головний офіс)	—	203.0.113.0/30	255.255.255.252	203.0.113.1	203.0.113.2	Статичний (Провайдер)
WAN-канал (Віддалений корпус)	—	198.51.100.0/30	255.255.255.252	198.51.100.1	198.51.100.2	Статичний (Провайдер)

Назва пристрою за топологією	Модель пристрою	Мережевий інтерфейс / Роль	Призначена IP-адреса	Опис призначення адреси в інфраструктурі
Router_SW_7_Main_Core	MikroTik RB5009	ether1 (WAN)	203.0.113.2	Зовнішній інтерфейс, точка підключення Інтернет та VPN-сервер
Router_SW_7_Main_Core	MikroTik RB5009	vlan40-management	192.168.40.1	Шлюз для мережі керування та Керівництва (Director, etc.)
Router_SW_9_Remote_Edge	MikroTik hEX S	ether1 (WAN)	198.51.100.2	Зовнішній інтерфейс філіалу, VPN-клієнт Site-to-Site
Router_SW_9_Remote_Edge	MikroTik hEX S	vlan40-remote-mgmt	198.168.40.9	Інтерфейс прикордонного маршрутизатора в мережі керування
Switch_SW_4_Remote	MikroTik hEX S	vlan40-management	192.168.40.4	Адреса комутатора розподілу філіалу для адміністрування
Access_Point-PT (AP_1)	MikroTik cAP ax	Інтерфейс CAP	192.168.40.5	Бездротова точка доступу (керується через CAPsMAN)
Server-PT (S_1)	Generic Server	FTP_Server	192.168.20.11	Корпоративний FTP-сервер для збереження файлів та бекапів
Server-PT (S_2)	Generic Server	Data_Server / DNS	192.168.20.10	Центральна база даних, локальний DNS та Active Directory
Printer-PT (PR_1)	МФУ	Бухгалтерія	192.168.10.200	Мережевий принтер економічного відділу (статична прив'язка)
Printer-PT (PR_2)	МФУ	Керівництво	192.168.40.200	Мережевий принтер дирекції (статична прив'язка)

ТАБЛИЦЯ ТЕХНІКО-ЕКОНОМІЧНИХ ПОКАЗНИКІВ

№ п\п	параметр	одиниці виміру	значення	№ п\п	параметр	одиниці виміру	значення
1	технологія мережі	–	ethernet 1000	7	марка точки доступу	–	MikroTik cAP ax
2	топологія мережі	–	гібридна	8	тип доступу до інтернет	–	вита пара
3	середовище передачі	–	Вита пара кат. 5E	9	термін окупності	рік	1,8
4	марка комутатора тунелю	–	MikroTik hEX S (RB760iGS)	10	плановий прибуток	грн	72104,4
5	марка головного комутатора	–	MikroTik RB5009UG+S+IN	11	собівартість	грн	128757,9
6	марка 16-ти портового комутатора	–	TP-Link TL-SG1016	12	ціна	грн	200862,3


Main Office
Remote Branch
TOV Kleo-P Travel Agency
IP Address Mikrotkik VPN routers)
MikroTik RB5009
Internet
(WAN Public Network)
Router_SW_7_Main_Core
(Cisco ISR 2911)
Router_SW_9_Remote_Edge
(Cisco ISR 2911)
SITE-TO-SITE VPN TUNNEL (IPSEC)
SITE-TO-SITE VPN TUNNEL (IPSEC)
Intf1
Intf3
Intf4
MikroTik
RB5009
MikroTik
hEX S
Copper Straight-Through
PC-PT
(WS_1-3)
Switch_Economics
(Generic Switch)
VLAN 10
Printer-PT
(PR_1)
VLAN 40
Swiich_Management
(Generic Switch)
VLAN 40
PC-PT
(Director, etc.)
Printer-PT
(PR_2)
VLAN 50
Switch_Conference
(Generic Switch)
TP-Link TL-SG1016
Wi-Fi
Access Point-PT
(Generic-AP)
Printer-PT
(PR_3)
Laptop-PT
PC-PT
(Generic)
VLAN 20
Switch_Servers
(Generic Switch)
VLAN 20
VLAN 30
Switch_Managers_Main_1
Server-PT
FTP_Server
(S_1)
Server-PT
Data_Server
(S_2)
PC-PT
(WS_12-17)
Printer-PT
(PR_4-5)
VLAN 20
Switch_Managers
(Generic Switch)
TP-Link TL-SG1016
VLAN 30
Switch_Managers_Main_2
IP Address:
VLAN 10 Economics: 192.168.10.0/24
VLAN 10 Economics:
VLAN 40 Management:
VLAN 40 Econrenns: 192.168.10.0/24
VLAN 40 Conference:
VLAN 50 Conference:
VLAN 50 Conferena: 192.168.10.0/24
VLAN 20 Servers: 192.168.20.0/24
VLAN 20 Servers:
VLAN 20 Data Serv:
VLAN 20 Server: 192.168.20l.0/24
IP Address:
VLAN 10 Economics: 182.168.10.0/24
Model = MikroTik RB5009
MikroTik: hEX S
Total device count: 13
Switch_SW_4_Remote
(Generic Switch)
Switch_SW_4_Remote
MikroTik
hEX S
VLAN 70
Switch_Managers_Remote_1
Switch_Managers_Remote_2
Printer-PT
(PR_7-8)
PC-PT
(WS_18-33)