Міністерство освіти і науки України

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

Відділення інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян
(назва відділення)

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра
(освітньо-професійного ступеня)

на тему: **Розробка проекту модернізації комп'ютерної мережі корпусу №6 ТНТУ ім. І. Пулюя**

Виконала: студентка IV курсу, групи КІ-406
Спеціальності 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

_____ Софія ВОРОЩУК
(ім'я та прізвище)

Керівник _____ Ігор КАПАЦІЛА
(ім'я та прізвище)

Рецензент _____ Олександра КОЗАК
(ім'я та прізвище)

Тернопіль – 2026

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

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

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"30" березня 2026 року

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

Ворощук Софії Вікторівні
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проекту модернізації комп'ютерної мережі корпусу №6 ТНТУ ім. І. Пулюя**

керівник роботи Капаціла Ігор Богданович
(прізвище, ім'я, по батькові)

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

2. Строк подання студентом роботи: 15 червня 2026 року.

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

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

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

6. Консультанти розділів роботи

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

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	01.04	
2	Збір і узагальнення інформації	08.05	
3	Написання першого розділу	15.05	
4	Розробка технічного та робочого проекту	22.05	
5	Написання спеціального розділу	28.05	
6	Розрахунок економічної частини	1.06	
7	Написання розділу охорони праці	3.06	
8	Виконання графічної частини	8.06	
9	Оформлення проєкту	10.06	
10	Погодження нормоконтролю	11.06	
11	Попередній захист роботи	12.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 31 березня 2026 року

Студент _____ Софія ВОРОЩУК
(підпис) (ім'я та прізвище)

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

АНОТАЦІЯ

Розробка проекту модернізації комп'ютерної мережі корпусу №6 ТНТУ ім. І. Пулюя // Кваліфікаційна робота // Ворощук Софія// Відокремлений структурний підрозділ «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя», група КІ-406// Тернопіль, 2026 // с. – 84 , рис. – 10 , табл. – 13 , кресл. – 5, додат. – 7.

Ключові слова: МЕРЕЖА, VLAN, КОМУТАЦІЯ, WI-FI, МАРШРУТИЗАЦІЯ.

Мета роботи - комплексна модернізація існуючої локальної обчислювальної мережі навчального корпусу університету відповідно до сучасних вимог освітнього процесу та адміністративного управління.

Пояснювальна записка складається з п'яти розділів.

В першому розділі виконано аналітичний огляд існуючої мережевої інфраструктури та сучасних рішень для побудови корпоративних мереж. Сформульовано технічне завдання, визначено вимоги до апаратного та програмного забезпечення, обґрунтовано призначення розробки.

В другому розділі розроблено логічну та фізичну схеми мережі, обґрунтовано вибір комунікаційного обладнання. Описано особливості монтажу кабельної інфраструктури та методики тестування комп'ютерної мережі корпусу.

В третьому розділі описано налаштування шлюза MikroTik, комутаторів та точок доступу з підтримкою CAPsMAN і сегментацією мережі засобами VLAN. Наведено інструкції з тестування, захисту та моніторингу мережевої інфраструктури.

В четвертому розділі розраховано економічну ефективність проекту модернізації мережі та визначено його собівартість. У п'ятому розділі описано вимоги з охорони праці, техніки безпеки та екологічні норми під час виконання мережевих робіт.

ABSTRACT

Development of a Project for the Modernization of the Computer Network in Building No. 6 of the Ivan Pul'uj Ternopil National Technical University // Qualification Thesis // Voroshchuk Sofiia // Separate Structural Unit "Ternopil Vocational College of the Ivan Pul'uj Ternopil National Technical University," Group KI-406/ / Ternopil, 2026 // pp. – 84, figs. – 10 , tables – 13 , drawings – 5, appendices – 7.

Keywords: NETWORK, VLAN, SWITCHING, WI-FI, ROUTING.

The purpose of this work is the comprehensive modernization of the existing local computer network of the university's academic building in accordance with modern requirements for the educational process and administrative management.

The explanatory note consists of five sections.

The first section provides an analytical review of the existing network infrastructure and modern solutions for building corporate networks. The technical specifications are formulated, hardware and software requirements are defined, and the rationale for the development is justified.

The second section presents the logical and physical network diagrams and justifies the selection of communication equipment. The specifics of installing the cabling infrastructure and methods for testing the building's computer network are described.

The third chapter describes the configuration of the MikroTik gateway, switches, and access points with CAPsMAN support and network segmentation using VLANs. Instructions for testing, securing, and monitoring the network infrastructure are provided.

The fourth chapter calculates the economic efficiency of the network modernization project and determines its cost. The fifth chapter describes occupational health and safety requirements and environmental standards during the performance of network work.

ЗМІСТ

ДОДАТКИ

ВСТУП

Стрімкий та безперервний розвиток галузі інформаційних технологій сформував низку принципово нових можливостей і парадигм у сфері проектування та експлуатації комп’ютерних мереж. Основними рушійними факторами цього процесу стали:

– Масове впровадження персональних обчислювальних систем: Поява на ринку відносно доступних за вартістю, але водночас високопродуктивних персональних комп'ютерів і робочих станцій, які здатні локально вирішувати широкий спектр складних інженерних, наукових та повсякденних завдань.

– Інтенсифікація інформаційного обміну: Постійне зростання потреби кінцевих користувачів та організацій у спільному використанні розподілених інформаційних, апаратних (накопичувачі, друкувальні пристрої) та програмних ресурсів, а також у забезпеченні високошвидкісного обміну великими масивами даних.

– Еволюція мережевої інфраструктури: Поява й активне впровадження різноманітних високотехнологічних апаратних і програмних засобів комунікації, які дозволяють ефективно та надійно інтегрувати окремі обчислювальні пристрої у масштабовані локальні та корпоративні мережі.

У сучасній технічній літературі комп’ютерна (обчислювальна) мережа розглядається як складна інженерна сукупність комп’ютерів та допоміжних периферійних пристроїв, що інтегровані за допомогою фізичних чи бездротових каналів зв’язку в єдину інформаційну систему. Головною метою такого об'єднання є забезпечення трансляції потоків даних, гарантування спільного доступу до мережевих ресурсів та централізоване керування ними.

При цьому всі об’єкти (комп’ютери, сервери, контролери), які виступають джерелами або безпосередніми споживачами інформації в межах цієї системи, класифікуються як її абоненти. Фізичний процес передачі даних у мережевому середовищі реалізується за допомогою кодування інформації в електричні сигнали або електромагнітні хвилі. Роль середовища поширення цих сигналів виконують кабельні лінії зв’язку (кручена пара, волоконно-оптичні лінії) або

безпровідний простір, функціонування яких підтримується відповідним приймально-передавальним обладнанням.

Будь-який технічний пристрій, що безпосередньо інтегрований у фізичну інфраструктуру передачі даних і має власну мережеву адресу, дефініюється як вузол мережі. Взаємопов'язана сукупність таких елементів формує комунікаційну підсистему, яка є базовим базисом для організації стійкої взаємодії між абонентами.

Таким чином, сучасні комп’ютерні системи та мережі виступають стратегічним інструментом, що суттєво розширює потенціал людства у сфері автоматизованої обробки, довготривалого зберігання та оперативного передавання інформації на будь-які відстані.

У зв'язку з цим, кваліфікований фахівець із комп’ютерних систем та мереж повинен володіти комплексними компетенціями для роботи на високому професійному рівні з різнорідними типами даних. Його завдання полягає у забезпеченні стабільного функціонування як локальних сегментів, так і глобальних мережевих інтерфейсів, а також у впровадженні передових інформаційних ресурсів для оптимізації професійної діяльності підприємств та установ.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Темою даної кваліфікаційної роботи є «Розробка проекту модернізації комп’ютерної мережі корпусу №6 ТНТУ ім. І. Пулюя». Інфраструктурні та технологічні потреби навчального корпусу університету мають свою специфіку, проте загалом інтегрують у собі базові вимоги, що висуваються до сучасних корпоративних та академічних мережевих систем. До основних із них належать:

− Централізований розподіл даних: Санкціонований доступ викладачів, студентів та адміністрації до баз даних, електронних журналів, репозиторіїв і навчально-методичних матеріалів з робочих місць або лабораторій.

− Раціональний розподіл технічних ресурсів: Колективне використання периферійного обладнання (мережевих принтерів, обчислювальних стендів) у межах корпусу.

− Спільне використання програмних ресурсів: Централізоване розгортання, ліцензування та експлуатація мережевих версій інженерного і прикладного ПЗ на базі комп'ютерних класів кафедри.

− Розподіл обчислювальних ресурсів: Об'єднання потужностей серверів і робочих станцій для складних розрахунків, обробки даних і моделювання.

− Колективна науково-освітня діяльність: Колаборація між науковими групами, кафедрами та підрозділами університету над спільними проектами.

− Стабільний доступ до Інтернету: Надійний зв'язок для дистанційного навчання, наукових баз даних, хмарних сервісів та відеотрансляцій.

1.1.2 Призначеннння розробки

Модернізована комп'ютерна мережа корпусу №6 ТНТУ створюється для забезпечення продуктивного, комфортного та захищеного інформаційно-

комунікаційного середовища на підтримку освітнього процесу, наукової діяльності та адміністрування.

Впровадження проекту надає користувачам розширений спектр функціональних можливостей і характеризується такими ключовими параметрами:

− Продуктивність: Мінімальний час реакції мережі на запити користувачів при взаємодії з внутрішніми та зовнішніми ресурсами.

− Пропускна здатність: Обсяг даних, що передається за одиницю часу; швидкість магістральних каналів і абонентських ліній — 1000 Мбіт/с (Gigabit Ethernet).

− Надійність та відмовостійкість: Безперебійне функціонування компонентів мережі та механізми захисту цілісності й конфіденційності інформації.

− Керованість: Засоби моніторингу, збору статистики трафіку та централізованого адміністрування.

− Масштабованість: Підключення нових робочих станцій і аудиторій без перебудови базової інфраструктури.

− Гнучкість архітектури: Збереження працездатності та перемаршрутизація даних у разі виходу з ладу окремих вузлів чи ліній зв'язку.

− Кросплатформена інтегрованість: Сумісність різнорідного обладнання та програмного забезпечення від різних виробників.

− Функціональна прозорість: Приховування складності мережевих процесів від кінцевого користувача при простому доступі до дозволених ресурсів.

− Локальне сховище даних: Централізоване зберігання навчально-методичних матеріалів на базі виділеного FTP/file-сервера.

− Інтеграція з WAN: Підключення мережі корпусу до загальноуніверситетської опорної мережі та Інтернету з дотриманням політик безпеки.

1.1.3 Вимоги до апаратного та програмного забезпечення

Проектована локальна обчислювальна мережа навчального корпусу №6 ТНТУ має бути розроблена, побудована та сконфігурована таким чином, щоб повною мірою задовольняти комплекс технічних, експлуатаційних та економічних вимог.

− Логічна сегментація мережі: Поділ на VLAN для розмежування доступу між категоріями користувачів (адміністрація, викладачі, комп'ютерні класи, студентська мережа) та зниження широкомовного трафіку.

− Доступність апаратного забезпечення: Обладнання має бути загальнодоступним, економічно доцільним, підтримувати задану швидкість передачі даних, мати високий показник надійності (MTBF) та забезпечувати можливість оперативної заміни й модернізації.

− Централізоване адміністрування: Інструменти ефективного моніторингу й адміністрування всієї мережевої інфраструктури з робочого місця системного адміністратора.

− Бездротовий доступ: Точки доступу Wi-Fi на базі стандартів IEEE 802.11ax/ac із зворотною сумісністю та обов'язковим шифруванням WPA3 або WPA2-Enterprise.

− Керованість комутаційного обладнання: Керований комутатор ядра (Layer 2/3) з підтримкою QoS, моніторингу портів і дзеркалювання трафіку.

− Мережеві сховища: Виділений файловий сервер або NAS для централізованого зберігання навчально-методичних матеріалів, дистрибутивів ПЗ та архівних даних.

− Колективні периферійні пристрої: Інтеграція мережевих принтерів і БФП із спільним доступом для авторизованих користувачів відповідних робочих груп.

1.1.4 Вимоги до документації

У результаті виконання проектно-конструкторських етапів модернізації комп’ютерної мережі корпусу №6 ТНТУ має бути сформований повний пакет супровідної технічної та експлуатаційної документації. До обов'язкового складу графічних та текстових матеріалів проекту належать:

− Інженерний журнал: Документ із хронологією проектних рішень, специфікаціями обладнання, таблицею IP-адресації, конфігураціями активних пристроїв та результатами тестування.

− Схема логічної топології: Графічний документ із архітектурою інформаційних потоків, організацією VLAN, схемами маршрутизації та логічним взаємозв'язком між серверами, комутаторами і робочими станціями.

− Схема фізичної топології: План корпусу №6 із трасуванням кабелів, розташуванням комутаційних шаф, крос-панелей, розеток RJ-45, точок доступу Wi-Fi та серверного обладнання на поверхах.

− Матриця типових проблем: Таблиця потенційних збоїв мережі з методами діагностики, регламентом профілактичних робіт та інструкціями для адміністратора щодо відновлення працездатності системи.

Документування телекомунікаційної інфраструктури є критично важливим етапом, що забезпечує стабільну експлуатацію та обслуговування мережі. Технічна документація відображає поточний стан архітектури системи, мінімізує час усунення аварій і слугує основою для подальшого масштабування та модернізації. Після завершення проектування та погодження документації здійснюється перехід до практичної реалізації — монтажу, комутації та пусконалагодження телекомунікаційної системи.

1.1.5 Техніко-економічні показники проекту

Успішна реалізація проекту модернізації мережі корпусу №6 ТНТУ визначається балансом технічної ефективності та економічної доцільності. На

передпроектні дослідження, проектування, монтаж, тестування та налаштування інфраструктури відводиться від 250 до 300 людино-годин.

Проект розробляється з урахуванням таких техніко-економічних вимог і обмежень:

− Сучасність та цінова оптимізація: Використання актуальних рішень з оптимальним співвідношенням вартості й функціональних можливостей, що є критичним для бюджету державного ЗВО.

− Бюджетні рамки на обладнання: Вибір керованих комутаторів рівня доступу та розподілу в межах 20 000–30 000 грн за одиницю для дотримання загального кошторису.

− Швидкісні характеристики: Дуплексна передача даних на рівні 100/1000 Мбіт/с (Fast Ethernet для периферії, Gigabit Ethernet для серверів і магістральних ліній).

− Масштабованість: Резервні порти, вільне місце в шафах і кабель-каналах для підключення нових робочих місць без додаткових капіталовкладень у ядро мережі.

− Централізований шлюз WAN: Захищена точка виходу зі збалансованим доступом до Інтернету для всіх авторизованих сегментів корпусу.

− Бездротові технології: Високопродуктивні точки доступу Wi-Fi для покриття лінійних зон і лекційних аудиторій корпусу.

− Мережеве сховище: Локальний файловий сервер або NAS для зберігання інформаційних баз, резервних копій та внутрішнього обміну ресурсами ТНТУ.

1.1.6 Стадії та етапи розробки

У процесі проектування модернізації локальної обчислювальної мережі (ЛОМ) корпусу №6 ТНТУ необхідно дослідити та врахувати комплекс взаємопов'язаних технічних, структурних та експлуатаційних аспектів, зокрема:

− Місткість та масштабованість: Визначення оптимальної кількості точок підключення з урахуванням поточних потреб і резервного потенціалу для нового обладнання.

− Просторова структура об'єкта: Врахування архітектурних особливостей корпусу №6, розподілу користувачів по поверхах і розташування серверних, аудиторій та адміністративних приміщень.

− Інформаційні потоки: Аналіз щільності внутрішнього та зовнішнього трафіку, оцінка пікових навантажень з урахуванням мультимедійних і хмарних освітніх технологій.

− Мультисервісність середовища: Передача різнорідних типів даних (документи, бази даних, потокове відео, телеметрія) із забезпеченням параметрів QoS.

− Вибір апаратних засобів: Обґрунтування вибору активного та пасивного обладнання за критеріями продуктивності, сумісності, надійності та вартості.

− Структурована кабельна система: Оцінка методів прокладання кабельних трас і захист ліній від механічних пошкоджень та електромагнітних завад.

− Моніторинг та безпека: Інструменти адміністрування, виявлення збоїв, кібербезпеки та захисту від несанкціонованого доступу.

− Програмне забезпечення: Вибір мережевих ОС, серверного ПЗ і СУБД за критеріями швидкодії, вартості ліцензування та розмежування прав доступу.

− Інтеграція із суміжними мережами: Захищена взаємодія мережі корпусу з опорною мережею ТНТУ та ресурсами Інтернету.

Системний аналіз зазначених факторів на початкових етапах дозволяє виявити інфраструктурні проблеми та сформулювати додаткові технічні завдання. Передпроектний етап є фундаментальним для формування обґрунтованих технічних вимог до мережі корпусу №6 ТНТУ, що мінімізує ризики архітектурних помилок і забезпечує раціональні рішення на наступних стадіях проекту.

1.1.7 Порядок контролю та прийому

Контроль якості та приймання модернізованої ЛОМ корпусу №6 ТНТУ є фінальним етапом проекту, що підтверджує відповідність розгорнутої інфраструктури вимогам технічного завдання.

Введення системи в експлуатацію регламентується такими обов'язковими положеннями:

− Перевірка мережевих вузлів: Інструментальне та програмне тестування всіх активних і пасивних вузлів, комутаційного обладнання, серверів, точок доступу та робочих станцій.

− Маркування кабельної інфраструктури: Уніфіковане маркування кабелів, патч-панелей, шаф і розеток згідно зі стандартами СКС (TIA/EIA-606) для зручності обслуговування та локалізації несправностей.

− Методологія тестування: Перевірка ліній зв'язку кабельними аналізаторами (Fluke Networks); тестування логічного рівня, маршрутизації та пропускної здатності утилітами ping, traceroute, iperf або комплексними пакетами моніторингу.

− Здача в експлуатацію: Виконавець після завершення робіт направляє замовнику офіційне повідомлення з повним пакетом виконавчої документації (схеми, паспорти заземлення, результати сертифікації).

− Приймальна комісія: Університет протягом п'яти робочих днів видає наказ про створення комісії з представників ІТ-відділу, кафедри та профільних фахівців.

− Фіксація результатів: За відсутності зауважень комісія та підрядник підписують двосторонній «Акт приймання-передачі виконаних робіт з модернізації мережі в експлуатацію».

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

Метою кваліфікаційної роботи є розробка проекту модернізації локальної обчислювальної мережі корпусу №6 ТНТУ ім. І. Пулюя — навчально-

адміністративного корпусу, що забезпечує виконання навчальних планів, лабораторні заняття, наукову діяльність та керування підрозділами.

Модернізована система має об'єднати робочі станції, сервер та периферію в єдиний захищений інформаційний простір, забезпечивши обмін даними, централізоване зберігання, доступ до академічних ресурсів і вихід до Інтернету. Відповідно до функціонального зонування корпусу №6, обладнання розміщуватиметься у таких приміщеннях:

− Технічна зона із сервером: Центральний вузол із головною телекомунікаційною шафою, керованими комутаторами, файловим сервером (FTP/NAS), ДБЖ та магістральними кабельними лініями.

− Адміністративний блок: Робочі станції для керівництва кафедри та викладачів із доступом до електронних ресурсів.

− Навчальні класи та лабораторії: Аудиторії зі стаціонарними ПК та мережевими принтерами (БФП) для виконання лабораторних робіт, моделювання та інженерних розрахунків.

− Коридорні зони: Бездротові точки доступу Wi-Fi для рівномірного покриття корпусу і підключення мобільних пристроїв згідно з політиками університету.

Попереднє розташування обладнання буде змінюватися відповідно до нової розробленої фізичної топології. План приміщень корпусу №6 ТНТУ ім. І. Пулюя — навчально-адміністративного корпусу наведено на листі 2026.КВР.123.406.04.00.00 ПП.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Розробка та обґрунтування логічної та фізичної схем мережі

Для побудови локальної комп'ютерної мережі на сьогоднішній день є два варіанти провідна та безпровідна мережі. Для навчального закладу можуть розглядатися обидва варіанти. Тому оберемо і оцінимо обидві технології.

Ethernet як технологія локальних мереж.

Еволюція Ethernet пройшла кілька принципових етапів, кожен з яких супроводжувався кратним збільшенням пропускної здатності та зміною фізичного середовища передачі. Від початкових 10 Мбіт/с на коаксіальному кабелі технологія послідовно перейшла до Fast Ethernet (100 Мбіт/с), Gigabit Ethernet (1000 Мбіт/с) на кручений парі категорії Cat5e/Cat6, а згодом — до 10 Gigabit Ethernet і вище. Паралельно змінювалася топологія мереж: від шинної до зіркоподібної з використанням комутаторів (switch), що фактично усунуло проблему колізій, оскільки кожен порт комутатора утворює окремий колізійний домен. Перехід до повнодуплексного режиму роботи дозволив вузлам одночасно передавати й отримувати дані, що вдвічі збільшило ефективну пропускну здатність з'єднання. Застосування волоконно-оптичних кабелів розширило можливості Ethernet за межі будівель, забезпечивши передачу даних на відстані до десятків кілометрів.

Сьогодні Ethernet залишається фундаментальною технологією не лише для корпоративних і університетських мереж, але й для центрів обробки даних, промислової автоматизації та телекомунікаційних магістралей. Стандарти 40G, 100G і 400G Ethernet активно впроваджуються у магістральних вузлах і серверних кластерах. Технологія Power over Ethernet (PoE) розширила функціональність мережевої інфраструктури, дозволивши передавати електроживлення разом з даними одним кабелем до точок доступу Wi-Fi, IP-камер та VoIP-телефонів. Уніфікованість, широка підтримка виробниками обладнання, низька вартість компонентів та постійний розвиток стандартів IEEE

802.3 гарантують Ethernet статус незамінної базової технології локальних мереж на найближчі десятиліття.

Застосування технології Wi-Fi для доступу до локальних мереж.

Wi-Fi — це сукупність стандартів бездротового зв'язку сімейства IEEE 802.11, що забезпечують передачу даних у радіодіапазонах 2,4 ГГц та 5 ГГц (а в новітніх специфікаціях — також 6 ГГц). Технологія набула масового поширення завдяки можливості організації бездротового доступу до локальної мережі та Інтернету без прокладання кабельної інфраструктури до кожного кінцевого пристрою. В університетських і корпоративних середовищах Wi-Fi розгортається на основі точок доступу (Access Point), підключених до провідної інфраструктури комутаторів, і забезпечує підключення мобільних пристроїв, ноутбуків та планшетів у межах зони покриття. Еволюція стандартів — від 802.11b/g/n до 802.11ac (Wi-Fi 5) і 802.11ax (Wi-Fi 6/6E) аж до WiFi 8 (802.11bn) — супроводжувалася суттєвим зростанням теоретичної пропускної здатності: від кількох мегабіт до кількох гігабіт за секунду.

Безпека бездротового з'єднання є одним із ключових аспектів проектування Wi-Fi інфраструктури в локальних мережах, тому сучасні мережі обов'язково використовують WPA2-Enterprise або WPA3, які забезпечують надійне шифрування трафіку та централізовану автентифікацію користувачів через сервер RADIUS і протокол 802.1X. Такий підхід дозволяє розмежовувати доступ між категоріями користувачів — наприклад, між студентами, викладачами та адміністрацією — шляхом прив'язки бездротових сегментів до відповідних VLAN. Для забезпечення безшовного покриття великих приміщень застосовуються системи керованих точок доступу з централізованим контролером (WLC), що координує роумінг між точками, балансування навантаження та єдину політику безпеки. У контексті університетської мережі Wi-Fi виступає не доповненням, а повноцінним рівноправним рівнем доступу, інтегрованим із провідною інфраструктурою Ethernet у єдине конвергентне середовище.

Вибір технології і топології для проєкту мережі.

В якості базової технології обрано Ethernet (IEEE 802.3). Вибір обумовлений простотою монтажу, широкою доступністю сумісних компонентів, зручністю обслуговування та підтримкою швидкостей 100/1000 Мбіт/с, що забезпечує достатній запас пропускної здатності для поточних і перспективних потреб корпусу.

Мережа побудована за топологією «розширена зірка», де робочі станції підключаються до комутаторів рівня доступу, які з'єднуються з центральним комутатором ядра у головній телекомунікаційній шафі. Така ієрархічна структура забезпечує централізоване керування трафіком, спрощує діагностику та дозволяє підключати нові вузли без впливу на працездатність системи.

Інтеграція бездротових точок доступу Wi-Fi (IEEE 802.11ax/ac) у коридорах та аудиторіях надає топології гібридного характеру. Точки доступу підключаються до комутаторів через інтерфейси PoE, що усуває потребу в окремому живленні. Така конвергентна архітектура забезпечує єдиний захищений інформаційний простір для всіх користувачів корпусу.

В мережі буде застосована гібридна топологія.

Гібридна топологія поєднує елементи кількох базових архітектур в єдину мережеву структуру, адаптовану до конкретних потреб об'єкта. Найпоширенішим прикладом є інтеграція провідної деревоподібної Ethernet-інфраструктури з бездротовими сегментами Wi-Fi, що утворює конвергентне середовище для одночасного обслуговування стаціонарних робочих станцій і мобільних пристроїв. Гібридна архітектура забезпечує максимальну гнучкість, дозволяє оптимально розподілити навантаження між провідним і бездротовим сегментами та поєднати переваги кожної з базових топологій. Водночас складність проектування, налаштування та подальшого адміністрування такої мережі є суттєво вищою, а забезпечення єдиної політики безпеки для різнорідних сегментів вимагає застосування додаткових програмно-апаратних засобів захисту.

Кабельна підсистема і вибір середовища передавання

Мережева інфраструктура корпусу №6 ТНТУ будується на основі технології Ethernet 1000Base-T із використанням неекранованої витої пари

категорії Cat5e. Даний тип кабелю є оптимальним вибором для горизонтальної підсистеми університетської мережі, оскільки забезпечує стабільну передачу даних на швидкості до 1 Гбіт/с при максимальній довжині сегменту 100 метрів — достатній для охоплення будь-якого приміщення корпусу від розподільної телекомунікаційної шафи. Усі електричні та механічні характеристики кабелю — імпеданс, загасання, перехресні наведення (NEXT/FEXT) — визначаються в процесі виробництва і підтверджуються відповідним маркуванням та сертифікатом відповідності стандарту TIA/EIA-568-B.

Для забезпечення цілісності та стабільності характеристик усього тракту передавання кабелі горизонтальної підсистеми будуть використовуватись у комплексі з патч-кордами, комутаційними панелями та активним мережевим обладнанням тієї ж категорії Cat5e або вищої. Змішування компонентів різних категорій у межах одного каналу неприпустиме, оскільки зводить сукупні характеристики лінії до найнижчого елемента ланцюга і може призвести до нестабільної роботи або зниження швидкості з'єднання

Схема обтискання кабелів RJ45 приведено на рисунку 2.1.

В таблиці 2.1 представлено логічну адресацію в мережі, в таблиці 2.2 наведено параметри конфігурування VLAN.

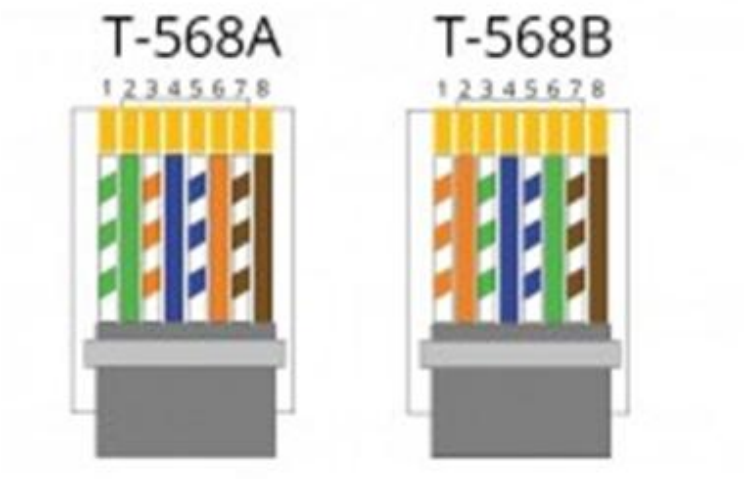

Рисунок 2.1 — Обтискання конектора некранованої витої пари категорії 5е.

Таблиця 2.1 – Логічна адресація в мережі

Позначення вузлів	Робоча група/ Кількість вузлів		Назва кабінету	Номер VLAN	Адреса підмережі/ Маска
1	2	3	4	5	6
WS_1 – WS_10, S_1	stud1	11	Лабораторія конструювання і проектування	11	192.168.11.0/24
WS_11 – WS_13	stud2	3	Кафедра обладнання харчових технологій	12	192.168.12.0/24
PR_1, PR_2	stud2	2	Кафедра обладнання харчових технологій	12	192.168.12.0/24
WS_14	stud2	1	Лекційна аудиторія (ліва)	12	192.168.12.0/24
WS_15	stud2	1	Секція фрезерування	12	192.168.12.0/24
WS_16	stud2	1	Завідувач кафедри	12	192.168.12.0/24
WS_17 – WS_20	fablab	4	Секція лазерного різання / Лабораторія "ФабЛаб"	20	192.168.20.0/24
WS_21	work	1	Лабораторія процесів та апаратів харчових виробництв	30	192.168.30.0/24

Продовження таблиці 2.1

1	2	3	4	5	6
WS_22, PR_3	work	2	Лабораторія міні виробництв	30	192.168.30.0/24
WS_23	work	1	Лабораторія експлуатації обладнання	30	192.168.30.0/24
AP_1	wifi	1	Лабораторія новітніх технологій	40	192.168.40.0/24
AP_2	wifi	1	Дослідницька лабораторія	40	192.168.40.0/24
SW_1 – SW_5	mngt	5	Мережева інфраструктура (Управління)	10	192.168.10.0/24

Таблиця 2.2 - Таблиця конфігурування VLAN

№ п/п	Познач. вузла	Номер порту	Тип порту	Назва мереж. пр-ю	Номер порту	Тип порту	Номер VLAN
1	2	3	4	5	6	7	8
1	SW_3	1	Trunk	SW_2	2	Trunk	10, 11, 12, 20, 30, 40
2		2	Trunk	SW_1	24	Trunk	10, 11
3		3	Trunk	SW_4	24	Trunk	10, 12, 20
4		4	Access	AP_1	wan	Access	40
5		5	Access	WS_11	eth0	Access	12
6		6	Access	WS_12	eth0	Access	12
7		7	Access	WS_13	eth0	Access	12
8		8	Access	PR_1	eth0	Access	12
9		9	Access	PR_2	eth0	Access	12

Продовження таблиці 2.2

1	2	3	4	5	6	7	8
10	SW_1	1–10	Access	WS_1 – WS_10	eth0	Access	11
11		11	Access	S_1	eth0	Access	11
12	SW_4	1–4	Access	WS_17 – WS_20	eth0	Access	20
13		5	Access	WS_14	eth0	Access	12
14		6	Access	WS_15	eth0	Access	12
15		7	Access	WS_16	eth0	Access	12
16		8	Trunk	SW_5	24	Trunk	10, 30, 40
17	SW_5	1	Access	WS_21	eth0	Access	30
18		2	Access	WS_22	eth0	Access	30
19		3	Access	WS_23	eth0	Access	30
20		4	Access	PR_3	eth0	Access	30
21		5	Access	AP_2	wan	Access	40

2.2 Обґрунтування вибору комунікаційного обладнання

Для реалізації запроектованої комп’ютерної мережі необхідно використати наступне обладнання:

- 2 комутатори робочих груп з 16 портами (для вузлів SW_1 та SW_4);
- 1 комутатор робочої групи з 8 портами (для вузла SW_5);
- 1 центральний керований комутатор із кількістю портів від 12 до 16 (для вузла SW_3);
- 1 маршрутизатор для забезпечення маршрутизації VLAN та доступу до мережі Інтернет (для вузла SW_2);
- 2 точки доступу Wi-Fi для забезпечення бездротового покриття корпусу (для вузлів AP_1 та AP_2);

– 1 серверний персональний комп’ютер для забезпечення роботи локальних сервісів (для вузла S_1).

Вибір обладнання здійснюється на підставі актуальних пропозицій, представлених на відкритому торговому майданчику (маркетплейсі) https://rozetka.com.ua/ .

Вибір комутаторів робочих груп з 16 портами (для вузлів SW_1 та SW_4)

Основні критерії:

кількість портів — до 16;

швидкість портів — 1000 Мбіт/с;

За результатами попереднього аналізу ринку до розгляду відібрано три моделі комутаторів, порівняльні технічні характеристики яких наведено у таблиці 2.3. Всі пристрої є Smart/Web-керованими комутаторами рівня доступу.

Таблиця 2.3 – Порівняльна характеристика комутаторів робочих груп з 16 портами

Критерії порівняння	Модель 1: MikroTik CSS318-16G-2S+IN	Модель 2: D-Link DGS-1100-16V2	Модель 3: TP-Link TL-SG116E
1	2	3	4
Виробник	MikroTik (Латвія)	D-Link (Тайвань)	TP-Link (Китай)
Кількість портів RJ45	16 портів (10/100/1000 Mbps)	16 портів (10/100/1000 Mbps)	16 портів (10/100/1000 Mbps)
Додаткові SFP порти	2 порти 10G SFP+ (оптика)	Відсутні	Відсутні
Комутаційна матриця	36 Gbps	32 Gbps	32 Gbps

Продовження таблиці 2.3.

1	2	3	4
Функціонал L2 (VLAN)	Портові та теговані (802.1Q)	Портові та теговані (802.1Q)	Портові та теговані (802.1Q)
Охолодження	Пасивне (безвентиляторне, тихе)	Пасивне (безвентиляторне, тихе)	Пасивне (безвентиляторне, тихе)
Форм-фактор / Корпус	Настільний / Металевий	Настільний / Монтаж у 19" стійку	Настільний / Металевий
Вартість, грн	5100	6100	3300

На основі порівняння параметрів та враховуючи співвідношення вартості до функціональних можливостей, для використання в мережі обрано модель комутатора MikroTik CSS318-16G-2S+IN. Зовнішній вигляд пристрою представлено на рисунку 2.2.

Рисунок 2.2 – Комутатор MikroTik CSS318-16G-2S+IN

Для реалізації вузла SW_5 (який згідно з топологією обслуговує лабораторію міні-виробництв) вибираємо бюджетний керований комутатор на 8 гігабітних портів. За результатами попереднього аналізу ринку до розгляду відібрано три моделі комутаторів. Для вибору конкретної моделі комутатора складемо таблицю 2.4. Усі три пристрої підтримують стандарт IEEE 802.1Q

(VLAN), працюють безшумно завдяки пасивному охолодженню і є максимально доступними за ціною.

Таблиця 2.4 – Порівняльна характеристика комутаторів робочих груп з 8 портами

Критерії порівняння	Модель 1: MikroTik CSS610-8G-2S+IN	Модель 2: D-Link DGS-1100-08V2	Модель 3: TP-Link TL-SG108E
1	2	3	4
Виробник	MikroTik (Латвія)	D-Link (Тайвань)	TP-Link (Китай)
Кількість портів RJ45	8 портів (10/100/1000 Mbps)	8 портів (10/100/1000 Mbps)	8 портів (10/100/1000 Mbps)
Додаткові оптичні порти	1 роз'єм SFP	Відсутні	Відсутні
Тип керування	Web-інтерфейс / SwOS	Web-інтерфейс / Утиліта DNA	Web-інтерфейс / Утиліта Easy Smart
Комутаційна матриця	16 Gbps	16 Gbps	16 Gbps
Робота з VLAN (802.1Q)	Повна підтримка (Tagged / Untagged)	Повна підтримка (Tagged / Untagged)	Повна підтримка (Tagged / Untagged)
Додаткові функції	Порт-дзеркалювання, Storm Control	Loopback Detection, IGMP Snooping	Loop Prevention, Rate Limiting
Матеріал корпусу	Металевий	Металевий	Металевий
Вартість, грн	1800	2100	1600

Рисунок 2.3 – Комутатор MikroTik CSS610-8G-2S+IN

Комутатори без проблем приймуть по Trunk-порту тегований трафік управлінської мережі (VLAN 10) та робочої групи (VLAN 30).

На основі порівняння параметрів та враховуючи співвідношення вартості до функціональних можливостей, для використання в мережі обрано модель MikroTik CSS610-8G-2S+IN, зовнішній вигляд якої представлено на рисунку 2.3.

Для центрального комутатора ядра/розподілу (вузол SW_3) вимоги значно вищі, ніж для звичайних пристроїв робочих груп. Оскільки до нього сходяться магістральні канали (Trunk) від комутаторів SW_1 та SW_4, підключаються локальні клієнти кафедри, принтери та бездротові точки доступу, цей пристрій повинен мати підвищену продуктивність комутаційної матриці, великий об'єм пакетного буфера та розширений функціонал керування трафіком. Аналогічно до попередніх пристроїв, проведено порівняння кількох моделей, яке узагальнено в таблиці 2.5.

Таблиця 2.5 – Порівняльна характеристика керованих комутаторів із кількістю портів від 12 до 16

Критерії порівняння	Модель 1: MikroTik CRS317-1G-16S+RM	Модель 2: D-Link DGS-1210-16V2	Модель 3: TP-Link TL-SG3216 / TL-SG3428X
1	2	3	4
Виробник	MikroTik (Латвія)	D-Link (Тайвань)	TP-Link (Китай)

Продовження таблиці 2.5

1	2	3	4
Кількість портів	16 портів 10G SFP+ (оптичні шахти) + 1 порт RJ45 (Gbit)	12 портів RJ45 (Gbit) + 4 комбо-порти RJ45/SFP	16 портів RJ45 (Gbit) + 4 SFP-слоти
Загальна кількість інтерфейсів	17	16	20 (16 мідних + 4 оптика)
Операційна система / Рівень	Dual Boot: RouterOS (L5) / SwitchOS	Web-Smart (L2/L2+)	JetStream L2+ Managed (з CLI)
Комутаційна матриця	320 Gbps (екстремальна швидкість)	32 Gbps	32 Gbps
Робота з VLAN (802.1Q)	Повна (Апаратне L3 HW Offloading)	Повна (до 4094 фізичних VLAN ID)	Повна (QinQ, Voice VLAN, 802.1Q)
Резервування живлення	Подвійний БП (Dual Hot-Swap PSU)	Відсутнє	Відсутнє
Охолодження / Монтаж	Активне (розумні кулери) / 19" Стійка	Пасивне (безшумне) / 19" Стійка	Пасивне або Активне / 19" Стійка
Вартість, грн.	18400	8000	10100

З умови забезпечення масштабування мережі в майбутньому, обираємо MikroTik CRS317-1G-16S+RM. Зовнішній вигляд обраного комутатора представлено на рисунку 2.4. Це професійне рішення "на виріст". Оскільки всі його 16 портів є оптичними SFP+ (10 Гбіт/с), підключення мідних розеток кабінету та точок доступу здійснюється через спеціальні SFP-T модулі

(перехідники на RJ45). Головний плюс —пропускна здатність у 320 Гбіт/с. Мережа ніколи не забагує і не "ляже", навіть якщо всі комп'ютери класів одночасно почнуть качати гігабайтні інсталятори або образи ОС з сервера.

Рисунок 2.4 – Комутатор MikroTik CRS317-1G-16S+RM

Для головного маршрутизаційного вузла мережі (вузол SW_2) потрібен пристрій, який виконуватиме роль ядра L3 (Border Router / Gateway). На відміну від звичайних комутаторів, його головне завдання — не просто перекидати кадри всередині одного сегмента, а здійснювати міжвереджеву маршрутизацію (Inter-VLAN Routing), забезпечувати безпеку (Firewall, NAT), динамічно розподіляти IP-адреси (DHCP-сервер для підмереж) та підтримувати стабільний високошвидкісний інтернет-канал для всього корпусу. Спираючись на результати попереднього аналізу ринку, ми відібрали три моделі маршрутизаторів. Порівняння їхніх технічних параметрів наведено в таблиці 2.6.

Таблиця 2.6 – Порівняльна характеристика маршрутизаторів для забезпечення маршрутизації VLAN та доступу до мережі Інтернет

Критерії порівняння	Модель 1: MikroTik hEX (RB750Gr3)	Модель 2: D-Link DSR-250V2	Модель 3: TP-Link ER605 (TL-R605)
1	2	3	4
Виробник	MikroTik (Латвія)	D-Link (Тайвань)	TP-Link (Китай)
Кількість портів RJ45	5 портів (10/100/1000 Mbps)	5 портів (1–WAN, 4–LAN/WAN)	5 портів (1–WAN, 3–LAN/WAN, 1–LAN)

Продовження таблиці 2.6

1	2	3	4
Додаткові інтерфейси	Slot для microSD, USB 2.0	1 порт USB 3.0	Відсутні
Операційна система / Рівень	RouterOS (Licence Level 4)	Фірмове ПЗ D-Link (Green)	Фірмове ПЗ Omada / SafeStream
Продуктивність (NAT)	До 1.97 Gbps (Апаратний рушій)	До 950 Mbps	До 940 Mbps
Маршрутизація VLAN (802.1Q)	Повна підтримка (без обмежень)	Повна підтримка (до 30 VLAN)	Повна підтримка (до 32 VLAN)
Апаратне шифрування IPsec	Є (IPsec HW Acceleration)	Є	Є
Охолодження / Корпус	Пасивне / Компактний пластик	Пасивне / Металевий настільний	Пасивне / Компактний метал
Вартість, грн.	2500	8500	2500

Відповідно до топології, маршрутизатору SW_2 не потрібно багато фізичних портів, адже вся комутація хостів відбувається на рівнях нижче. Для його роботи задіюється лише два інтерфейси:

Порт 1 (WAN): підключається кабель від зовнішнього провайдера Інтернету (наприклад, Укртелеком чи локальний провайдер Тернополя).

Порт 2 (LAN/Trunk): один гігабітний кабель іде вниз до центрального комутатора SW_3. На цьому єдиному лінку налаштовуються віртуальні суб-інтерфейси (технологія Router-on-a-Stick), що дозволяє роутеру обслуговувати всі VLAN корпусу одночасно.

Обираємо MikroTik hEX (RB750Gr3), зовнішній вигляд якого представлений на рисунку 2.5. Попри низьку ціну, він має потужний 2-ядерний процесор з архітектурою MMIPS та підтримку апаратного розвантаження шифрування. Операційна система RouterOS дозволить гнучко

налаштувати черги пріоритезації трафіку (QoS) — наприклад, виділити гарантовану швидкість для сервера S_1 та обмежити швидкість торрентів чи розважальних сайтів у студентському VLAN 40 (Wi-Fi).

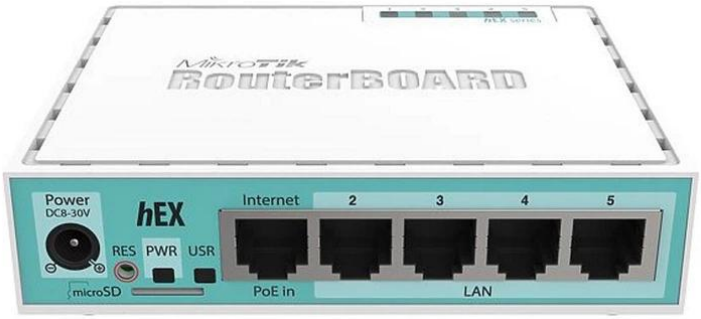

Рисунок 2.5 – Комутатор MikroTik hEX (RB750Gr3)

Для організації бездротового покриття у навчальному корпусі (вузли AP_1 та AP_2) точки доступу мають підтримувати роботу у двох частотних діапазонах (2.4 ГГц та 5 ГГц), роботу з віртуальними мережами (VLAN 802.1Q) для ізоляції гостьового та навчального трафіку, а також функцію безшовного роумінгу, щоб користувачі не втрачали зв'язок при переміщенні між аудиторіями. Порівняльна характеристика аналізованих точок доступу Wi-Fi представлена в таблиці 2.7.

Оскільки точки доступу зазвичай монтуються на стелі або високо на стіні, вести до них окремі розетки 220 В незручно. Усі підібрані моделі підтримують технологію PoE (Power over Ethernet), що дозволяє передавати і дані, і живлення по одному кабелю крученої пари безпосередньо від комутатора (або через спеціальні бюджетні інжектори, що йдуть у комплекті).

Таблиця 2.7 – Порівняльна характеристика точок доступу Wi-Fi

Критерії порівняння	Модель 1: MikroTik cAP ac (RBcAPGi-5acD2nD)	Модель 2: D-Link DAP-2610	Модель 3: TP-Link EAP225
1	2	3	4
Виробник	MikroTik (Латвія)	D-Link (Тайвань)	TP-Link (Китай)

Продовження таблиці 2.7

1	2	3	4
Стандарт Wi-Fi	Wi-Fi 5 (802.11ac Wave 2)	Wi-Fi 5 (802.11ac Wave 2)	Wi-Fi 5 (802.11ac Wave 2)
Макс. швидкість (сумарна)	До 1167 Мбіт/с (300 + 867)	До 1300 Мбіт/с (400 + 867)	До 1350 Мбіт/с (450 + 867)
Мережеві порти RJ45	2 порти Gigabit Ethernet	1 порт Gigabit Ethernet	1 порт Gigabit Ethernet
Підтримка технології PoE	PoE-In (на 1-му) + PoE-Out (на 2-му)	PoE-In (802.3af)	PoE-In (802.3af / Passive PoE)
Робота з VLAN (802.1Q)	Є (Multi-SSID із прив'язкою до VLAN)	Є (Multi-SSID із прив'язкою до VLAN)	Є (Multi-SSID із прив'язкою до VLAN)
Екосистема / Контролер	CAPsMAN (вбудований безкоштовний)	Nuclias Connect (софт-контролер)	Omada SDN (програмний або апаратний)
Тип монтажу / Корпус	Стельовий / Настінний (круглий та квадратний)	Стельовий / Настінний (пластик)	Стельовий / Настінний (пластик)
Ціна, грн.	4000	4050	3900

Усі три моделі дозволяють створити на одній фізичній точці доступу кілька незалежних бездротових мереж (SSID).

Обираємо MikroTik cAP ac, який при приблизно однаковій з аналогами вартості, має суттєву перевагу — наявність другого порту RJ45 з підтримкою PoE-Out. Зовнішній вигляд обраної точки доступу представлений на рисунку 2.6.

Рисунок 2.6 – Точка доступу MikroTik cAP ac (RBcAPGi-5acD2nD)

Перелік усіх компонентів мережевого обладнання, передбачених для реалізації проекту, наведено у зведеній таблиці 2.8.

Таблиця 2.8 — Специфікація телекомунікаційного обладнання

Назва елемента	Позначення	Модель	Ціна, грн.	Од. вим.	К-ть
1	2	3	4	5	6
Кабель	-	UTP cat 5e	22	м	580
Роз'єми,100 шт	-	RJ-45	1,2	шт	100
SFP-T модулі		Step4Net SFPd-03-1310-WDM-SC (DS159483)	323	шт	8
Комутатор	SW_1, SW_4	MikroTik CSS318-16G-2S+IN	5100	шт	2

Продовження таблиці 2.8

1	2	3	4	5	6
Комутатор	SW_5	MikroTik CSS106-5G-1S	1800	шт	1
Комутатор	SW_3	MikroTik CRS317-1G-16S+RM	18400	шт	1
Комутатор	SW_2	MikroTik hEX (RB750Gr3)	2500	шт	1
Точка доступу	AP_1, AP_2	MikroTik cAP ac (RBcAPGi-5acD2nD)	4000	шт	2

2.3 Особливості монтажу мережі

При розгортанні структурованої кабельної системи (СКС) навчального корпусу №6 ТНТУ ім. І. Пулюя суворе дотримання технологічних та нормативних стандартів монтажу є базовою умовою її надійності, довговічності та відповідності категоріям передачі даних (Cat 5e/Cat 6). Порушення правил інсталяції призводить до погіршення частотних характеристик ліній, появи прихованих дефектів та систематичних збоїв у роботі активного обладнання.

Під час прокладання крученої пари неприпустимо створювати гострі злами. Перевищення норм вигину порушує симетрію пар усередині оболонки та змінює геометричний крок скрутки, що викликає різке зростання внутрішніх наводок (NEXT) і зворотних втрат (Return Loss).

- Для неекранованого кабелю (UTP) в процесі монтажу мінімальний радіус вигину повинен становити не менше 4 зовнішніх діаметрів кабелю.
- Для екранованого кабелю (FTP/STP) через наявність жорсткої фольги чи обплетення цей показник становить не менше 8 зовнішніх діаметрів.

– У постійно зафіксованому (експлуатаційному) стані радіус вигину не повинен опускатися нижче встановлених виробником меж (зазвичай від 4 до 10 діаметрів).

Механічне перенапруження кабелю під час протягування крізь кабельні канали чи гофротруби призводить до незворотного розтягнення мідних провідників і витончення ізоляції.

– Максимально допустиме зусилля натягу для стандартного 4-парного кабелю крученої пари становить 110 Н (приблизно 11 кгс).
– При монтажі магістральних ліній або протягуванні пучків кабелів забороняється використання механічних лебідок чи зусиль кількох монтажників без контролю натягу. Для полегшення проходження складних ділянок траси застосовують протяжні інструменти (протяжки) та спеціальні гелі-змазки на водяній основі, які не руйнують ПВХ чи LSZH-оболонку.

Телекомунікаційні траси корпусу мають бути максимально ізольовані від впливу силових кабельних ліній, люмінесцентних світильників та електродвигунів лабораторного обладнання. Для цього дотримуються правил паралельного прокладання та перетину відповідно до стандартів EN 50174:

– При паралельному прокладанні інформаційних ліній та незахищених силових кабелів (напругою до 400 В) мінімальна відстань між ними в спільних лотках чи штробах повинна становити не менше 200 мм (при використанні металевих розділювальних перегородок цей проміжок можна зменшити до 50–100 мм).

– Перетин інформаційного кабелю з силовим має виконуватися строго під кутом 90°, щоб мінімізувати площу взаємної індукції.

– Відстань від траси СКС до джерел сильних ЕМЗ (трансформатори, щитові, зварювальні апарати) повинна бути не меншою за 1 метр.

Загальна термінація (розшивка) кабельних ліній на патч-панелях у серверній шафі та у внутрішніх розетках робочих місць комп'ютерних класів виконується за єдиним обраним стандартом специфікації EIA/TIA-568 (найчастіше використовується схема T568B).

– При розкручуванні пар для їх посадки на контакти IDC (Insulation Displacement Connector) модулів RJ-45 довжина розкрученої ділянки провідників не повинна перевищувати 13 мм для Cat 5e (і не більше 6–8 мм для Cat 6). Велике розкручування різко знижує захищеність лінії від перехресних завад на кінцях сегмента.

– Зовнішня оболонка кабелю має заходити всередину конектора або фіксатора розетки щонайменше на 6–10 мм, забезпечуючи надійне механічне затискання та захист від виривання.

Використання екранованого кабелю (FTP) у зонах з підвищеними завадами вимагає обов'язкової побудови правильного контуру заземлення екрана. Незаземлений екран працює як антена, яка збирає зовнішній електромагнітний шум і погіршує роботу мережі ще сильніше, ніж при використанні UTP.

Вибір способу монтажу залежить від архітектурних зон навчального корпусу та естетичних вимог до приміщень:

– У коридорах та магістральних переходах: кабель прокладається приховано за підвісною стелею на металевих сітчастих лотках або всередині суцільних сталевих чи ПВХ-коробів, жорстко закріплених до перекриття.

У комп'ютерних класах та кабінетах: для горизонтальної розводки до робочих місць використовують пластикові настінні кабель-канали (парапетні короби) великого перерізу, які дозволяють інтегрувати внутрішні розетки живлення та RJ-45 безпосередньо в лінію короба.

При проходженні крізь стіни: кабель обов'язково укладається в металеві або пластикові гільзи (патрубки). Вільний простір всередині гільз заповнюється легкодемонтованим вогнетривким матеріалом (протипожежною піною або мастикою) для запобігання поширенню полум'я у разі пожежі.

Відсутність чіткої ідентифікації елементів СКС унеможливлює подальше адміністрування та пошук несправностей у мережі корпусу ТНТУ. Маркування підлягають абсолютно всі компоненти: порти патч-панелей, кабельні розетки, а також обидва кінці кожного прокладеного кабелю.

– Маркування наноситься за допомогою спеціальних кабельних маркерів, самоламінуючих принтерних етикеток або бирок, стійких до стирання та вицвітання.

– Структура коду має бути уніфікованою, наприклад: К6-Поверх-Ауд-Номер_Розетки. Маркування на кабелі наноситься на відстані 50–100 мм від місця термінації (зрізу зовнішньої оболонки), що гарантує його чітку видимість під час проведення комутаційних робіт у серверній стійці.

Фінальним етапом монтажних робіт є обов'язкова інструментальна перевірка створених ліній зв'язку.

– На початковому етапі виконується базове тестування за допомогою простих кабельних тестерів на відсутність обривів провідників, коротких замикань, переплутаних пар або перехресних з'єднань (Wiremap).

– Для здачі мережі в експлуатацію проводиться сертифікаційне тестування ліній за допомогою кабельних аналізаторів (наприклад, Fluke Networks). Прилад вимірює ключові фізичні та частотні параметри лінії на усій протяжності: точну довжину ліній (за часом затримки сигналу), опір постійному струму, параметри загасання сигналу (Attenuation), перехресні наводки на ближньому кінці (NEXT) та величину поворотних втрат. За результатами вимірювань для кожної лінії формується індивідуальний звіт із фіксацією статусу «PASS» (пройдено).

2.4 Тестування компю’терної мережі

Фінальним етапом проектування та практичного розгортання локальної обчислювальної мережі навчального корпусу №6 ТНТУ є її комплексне інструментальне та програмне тестування. Цей етап є обов'язковою складовою інженерного циклу проектування СКС і вирішує наступні критично важливі завдання:

– Верифікація фізичного рівня (L1): виявлення дефектів монтажу, прихованих пошкоджень мідної жили, оцінка відповідності затухання та наводок стандартам Cat 5e/Cat 6.

– Перевірка канального та мережевого рівнів (L2/L3): підтвердження коректності ізоляції віртуальних мереж (VLAN), працездатності протоколів тегування 802.1Q та міжвереджевої маршрутизації на прикордонному шлюзі.
– Стрес-тестування продуктивності (L4): визначення реальної пропускної здатності (Throughput) каналів зв'язку при пікових навантаженнях, вимірювання затримок, коливань цих затримок (Jitter) та коефіцієнта втрати пакетів.

Для проведення програмного тестування та генерації синтетичного трафіку в рамках даної роботи було обрано професійну утиліту з відкритим вихідним кодом iPerf (версія iPerf3). Дане програмне забезпечення є індустріальним стандартом для вимірювання максимальної пропускної здатності IP-мереж і працює за строгою архітектурою «клієнт-сервер».

Проведене за допомогою кросплатформеного інструменту iPerf3 комплексне тестування дає змогу підтвердити інженерну спроможність проекту. Зафіксовані показники пропускної здатності в мідних сегментах, мінімальний джиттер в бездротових зонах та відсутність критичних втрат даних доводять, що вибране активне обладнання та спроектована топологія повністю задовольняють вимогам надійності, масштабованості та швидкісним стандартам сучасних корпоративних мереж.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Налаштування шлюза MikroTik

Обладнання: MikroTik hEX (RB750Gr3) — маршрутизатор (шлюз) R_1

Підготовка та первинне підключення

Завантаження WinBox. Завантажимо утиліту керування WinBox з офіційного сайту: http://www.mikrotik.com/download. Встановлення не потрібне — утиліта запускається безпосередньо.

Фізичне підключення. Підключаємо вхідний кабель до порту ether1 маршрутизатора. Робочий комп'ютер підключаємо до будь-якого іншого порту.

Запуск WinBox. Запусткаємо WinBox. У нижній секції, вкладка Neighbors, пристрій буде видно за MAC-адресою навіть без IP-з'єднання. Логін за замовчуванням — admin, пароль відсутній. Оберіть пристрій і натисніть Connect.

Видалення конфігурації за замовчуванням. Після входу відкриється вікно RouterOS Default Configuration. Натисніть Remove Configuration для видалення стандартних налаштувань. Після цього підключення розірветься — увійдіть повторно.

Налаштування мережевих інтерфейсів представлено на рисунку 3.1.

Відкрийте Interfaces — відображаються всі мережеві інтерфейси пристрою.

Перейменування WAN. Відкрийте інтерфейс ether1 (порт провайдера) та перейменуйте його на WAN. Це спрощує подальше адміністрування.

Перейменування LAN-портів. Відкрийте по черзі інтерфейси ether2–ether5 та перейменуйте їх на LAN1–LAN4. На інтерфейсі LAN1 залиште параметр Master Port = none. На інтерфейсах LAN2–LAN4 встановіть Master Port = LAN1. Це задіює апаратний чіп комутації та розвантажує CPU.

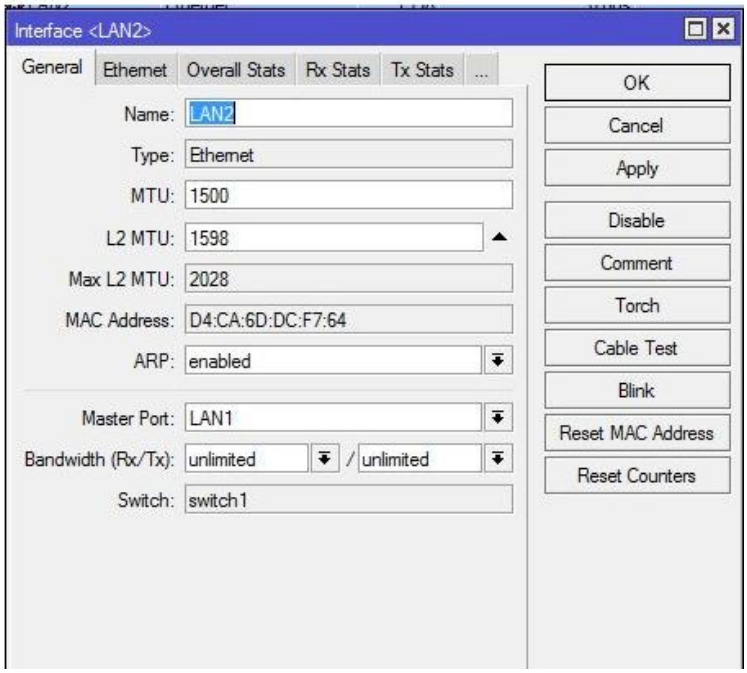

Рисунок 3.1 – Налаштування портів

Створення Bridge представлене на рисунку 3.2. Відкрийте меню Bridge → натисніть + → введіть назву LAN.

Додавання портів у Bridge. Перейдіть на вкладку Ports → +. Додайте інтерфейс LAN1 (Bridge = LAN). Повторіть для інтерфейсу WLAN.

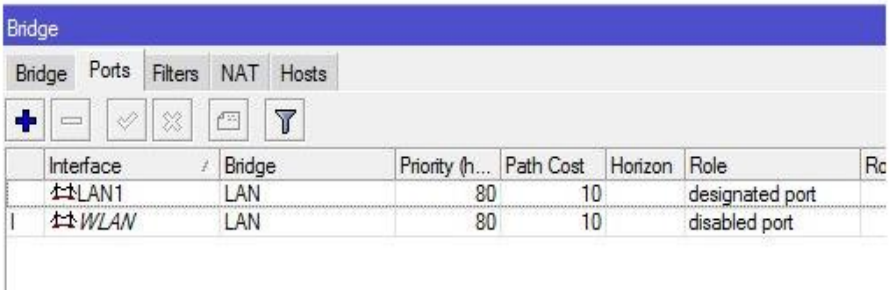

Рисунок 3.2 – Робота з портами у Bridge

Налаштування параметрів TCP/IP представлене на рисунку 3.3 і на рисунку 3.4.

IP-адреса LAN-інтерфейсу. Відкрийте IP → Addresses → +. Введіть адресу шлюза (наприклад, 10.20.30.254/24). Вкажіть інтерфейс — LAN (раніше створений Bridge).

IP-адреса WAN-інтерфейсу. Знову IP → Addresses → +. Введіть адресу та маску, видані провайдером. Інтерфейс — WAN.

DNS-сервери. Відкрийте IP → DNS. Введіть адреси DNS-серверів провайдера або публічних серверів (8.8.8.8, 8.8.4.4).

Маршрут за замовчуванням. Відкрийте IP → Routes → +. Встановіть Dst. Address = 0.0.0.0/0, Gateway — шлюз провайдера.

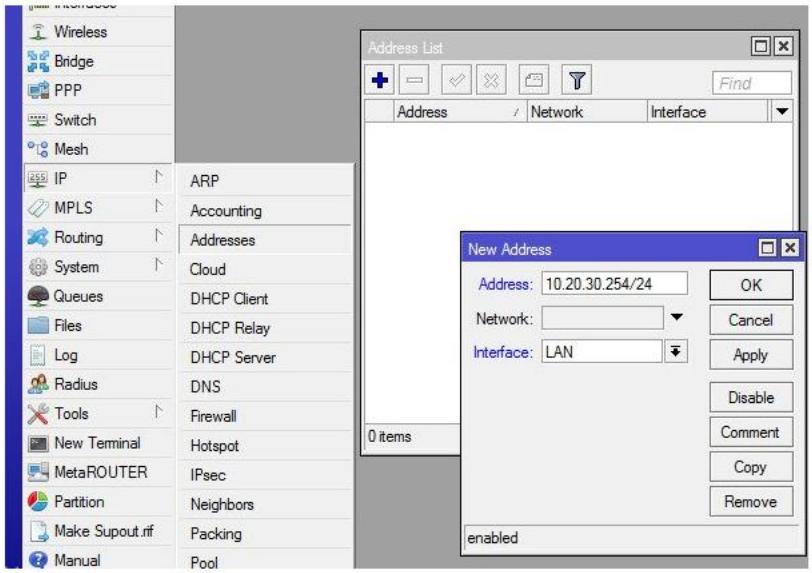

Рисунок 3.3 – Налаштування параметрів TCP/IP

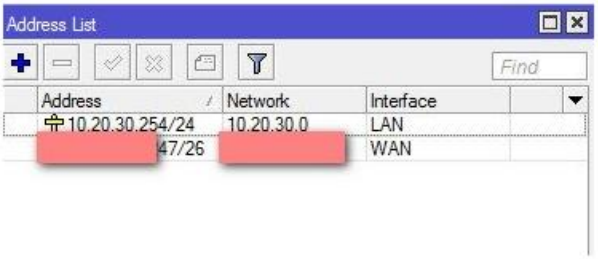

Рисунок 3.4 – Список адрес

Налаштування NAT

IP → Firewall → NAT → +. На вкладці General встановіть Chain = srcnat, Out. Interface = WAN.

Вкладка Action. Встановіть Action = masquerade. Після цього клієнти локальної мережі отримають доступ до Інтернету.

Налаштування VLAN для ізоляції трафіку

Відповідно до топології мережі (Лист 2026.КВР.123.406.04.00.00 ЛТ, Лист 2026.КВР.123.406.04.00.02 ТА), порт ether2 маршрутизатора з'єднаний з головним комутатором SW_2. Для ізоляції трафіку між підмережами налаштовуються VLAN-інтерфейси.

Створення VLAN-інтерфейсів (меню Interface → вкладка VLAN → +):

vlan_30 VLAN ID: 30 Interface: ether2

vlan_31 VLAN ID: 31 Interface: ether2

vlan_32 VLAN ID: 32 Interface: ether2

vlan_33 VLAN ID: 33 Interface: ether2

Створення Bridge-інтерфейсів (меню Bridge → +):

bridge_30 bridge_31 bridge_32 bridge_33

Додавання портів у кожен Bridge (вкладка Ports):

Для кожного bridge (bridge_30 … bridge_33) додайте два порти: відповідний фізичний порт (ether2) та відповідний VLAN-інтерфейс (vlan_30 … vlan_33).

Захист маршрутизатора (Firewall)

Захист самого роутера (Protect Router):

```
ip firewall filter add action=accept chain=input protocol=icmp
ip firewall filter add action=accept chain=input \
    connection-state=established in-interface=WAN
ip firewall filter add action=accept chain=input \
    connection-state=related in-interface=WAN
ip firewall filter add action=drop chain=input in-interface=WAN
```

Захист внутрішньої мережі (Protect LAN):

```
ip firewall filter add action=jump chain=forward \
    in-interface=WAN jump-target=customer
ip firewall filter add action=accept chain=customer \
    connection-state=established
ip firewall filter add action=accept chain=customer \
    connection-state=related
ip firewall filter add action=drop chain=customer
```

Фінальні налаштування

Часовий пояс. System → Clock → зніміть Time Zone Autodetect → оберіть Europe/Kiev.

Пароль адміністратора. System → Password → введіть надійний пароль.

Вимкнення зайвих сервісів. IP → Services → вимкніть всі сервіси, крім WinBox (або тих, що реально використовуються).

3.2 Налаштування комутаторів

Специфікація мережі включає чотири комутатори різних моделей. Нижче наведено налаштування кожного з них відповідно до топології мережі (Лист 2026.КВР.123.406.04.00.00 ЛТ, Лист 2026.КВР.123.406.04.00.02 ТА).

3.2.1 Налаштування комутаторів SW_1, SW_4

Комутатори SW_1 та SW_4 є керованими комутаторами рівня 2, налаштування яких виконується через веб-інтерфейс SwOS або утиліту WinBox.

Первинне підключення

Підключення. Підключаємо ПК до одного з портів комутатора. За замовчуванням IP-адреса SwOS — 192.168.88.1.

Вхід. Відкриваємо браузер та переходимо за адресою http://192.168.88.1. Логін: admin, пароль порожній.

Налаштування VLAN

Для коректної роботи в мережі з VLAN-тегуванням необхідно налаштувати VLAN-таблицю:

Переходимо до розділу VLAN в інтерфейсі SwOS.

Вмикаємо VLAN фільтрацію (VLAN Filtering = enabled).

Для кожного VLAN (30, 31, 32, 33) визначаємо:

Tagged ports — порти, через які передається тегований трафік (uplink до SW_2 або SW_3)

Untagged ports — порти, до яких підключені кінцеві пристрої

Зберігаємо конфігурацію.

Налаштування Trunk-порту (uplink)

Порт, що з'єднує SW_1/SW_4 з магістральним комутатором, налаштовується як Trunk:

У розділі Port оберіть uplink-порт.

Встановлюємо Default VLAN ID (PVID) = 1 або відповідний VLAN.

Переконуємось, що порт входить до всіх потрібних VLAN як Tagged.

Зміна IP-адреси управління

Розділ System → IP Address. Вводимо нову IP-адресу управління комутатором, що відповідає схемі адресації мережі.

Встановлюємо пароль адміністратора в розділі System → Password.

3.2.2 Налаштування комутатора SW_5

Комутатор SW_5 є керованим комутатором рівня 2. Налаштування аналогічне до CSS318, виконується через SwOS.

Первинне підключення та базові налаштування

Підключаємося до веб-інтерфейсу SwOS за адресою 192.168.88.1.

Перейменовуємо комутатор: System → Identity = SW_5.

Змінюємо IP-адресу управління відповідно до топології.

Налаштування VLAN та портів

Переходимо до розділу VLAN. Увімкніть VLAN Filtering.

Налаштовуємо VLAN 30, 31, 32, 33 аналогічно до SW_1/SW_4: визначте Tagged та Untagged порти для кожного VLAN.

Налаштовуємо uplink-порт (SFP+ або GbE) як Trunk з усіма VLAN.

Встановлюємо пароль адміністратора.

3.2.3 Налаштування комутатора SW_3

CRS317-1G-16S+RM є магістральним (core) комутатором рівня 3 з 16 портами SFP+. Налаштування виконується через RouterOS (повний функціонал).

Підключення та первинне налаштування

Підключення. Підключаємо ПК до порту ether1 (1G management port). Запускаємо WinBox, підключіться за MAC-адресою.

Видаляємо конфігурацію за замовчуванням (Remove Configuration).

Ідентифікація пристрою:

```
system identity set name=SW_3
```

Перейменування та відключення невикористаних інтерфейсів

```
interface ethernet set [find default-name=ether1]          name=ether1-mgmt
interface ethernet set [find default-name=sfp-sfpplus1]    name=sfp1-uplink-R1
interface ethernet set [find default-name=sfp-sfpplus2]    name=sfp2-SW1
interface ethernet set [find default-name=sfp-sfpplus3]    name=sfp3-SW4
interface ethernet set [find default-name=sfp-sfpplus4]    name=sfp4-SW5
# Відключити невикористані SFP+ порти:
interface ethernet set [find default-name=sfp-sfpplus5]    disabled=yes
# ... (повторити для sfp-sfpplus6 .. sfp-sfpplus16)
```

Налаштування Bridge та VLAN (RouterOS Bridge VLAN Filtering)

```
# Створення bridge
interface bridge add name=br-core vlan-filtering=yes
# Додавання портів у bridge
interface bridge port add interface=sfp1-uplink-R1    bridge=br-core
interface bridge port add interface=sfp2-SW1          bridge=br-core
interface bridge port add interface=sfp3-SW4          bridge=br-core
interface bridge port add interface=sfp4-SW5          bridge=br-core
# Налаштування VLAN на bridge
interface bridge vlan add bridge=br-core vlan-ids=30 \
    tagged=br-core,sfp1-uplink-R1,sfp2-SW1,sfp3-SW4,sfp4-SW5
interface bridge vlan add bridge=br-core vlan-ids=31 \
    tagged=br-core,sfp1-uplink-R1,sfp2-SW1,sfp3-SW4,sfp4-SW5
interface bridge vlan add bridge=br-core vlan-ids=32 \
    tagged=br-core,sfp1-uplink-R1,sfp2-SW1,sfp3-SW4,sfp4-SW5
interface bridge vlan add bridge=br-core vlan-ids=33 \
```

tagged=br-core,sfp1-uplink-R1,sfp2-SW1,sfp3-SW4,sfp4-SW5

IP-адреса управління

ip address add address=<IP управління>/24 interface=ether1-mgmt

ip route add dst-address=0.0.0.0/0 gateway=<шлюз>

Пароль адміністратора: System → Password.

3.2.4 Налаштування комутатора SW_2

MikroTik hEX (RB750Gr3) є маршрутизатором, що у топології може виступати також як керований комутатор. Нижче наведено налаштування його комутаційних функцій.

Ідентифікація та перейменування портів

system identity set name=SW_2

interface ethernet set [find default-name=ether1] name=ether1-uplink

interface ethernet set [find default-name=ether2] name=ether2-lan

interface ethernet set [find default-name=ether3] name=ether3-lan

interface ethernet set [find default-name=ether4] name=ether4-lan

interface ethernet set [find default-name=ether5] name=ether5-lan

Bridge та VLAN

Бридж для LAN-сегменту

interface bridge add name=br1-lan

Бридж для Trunk-каналу до SW_3

interface bridge add name=br3-trunk

VLAN-інтерфейси для транспортування підмереж по trunk

interface vlan add interface=br3-trunk name=vlan30 vlan-id=30

interface vlan add interface=br3-trunk name=vlan31 vlan-id=31

interface vlan add interface=br3-trunk name=vlan32 vlan-id=32

interface vlan add interface=br3-trunk name=vlan33 vlan-id=33

Додавання LAN-портів у br1-lan

interface bridge port add interface=ether2-lan bridge=br1-lan

interface bridge port add interface=ether3-lan bridge=br1-lan

interface bridge port add interface=ether4-lan bridge=br1-lan

interface bridge port add interface=ether5-lan bridge=br1-lan

Trunk-порт у br3-trunk

interface bridge port add interface=ether1-uplink bridge=br3-trunk

3.3 Налаштування точок доступу

Обладнання: MikroTik cAP ac (RBcAPGi-5acD2nD) — AP_1, AP_2.

Точки доступу MikroTik cAP ac є двохдіапазонними (2.4 ГГц / 5 ГГц) пристроями з підтримкою стандарту 802.11ac. Налаштування виконується через WinBox або веб-інтерфейс.

Первинне підключення

Фізичне підключення. Підключаємо точку доступу до комутатора (PoE або через адаптер живлення). Підключаємо ПК до тієї самої мережі.

Підключення через WinBox. Запускаємо WinBox → вкладка Neighbors → знайдіть пристрій за MAC-адресою → Connect. Логін: admin, пароль: порожній.

Видаляємо конфігурацію за замовчуванням (Remove Configuration).

Ідентифікація:

system identity set name=AP_1 # або AP_2

Налаштування бездротового інтерфейсу (2.4 ГГц)

Відкриваємо Wireless → Interfaces. Вибираємо інтерфейс wlan1 (2.4 ГГц).

Параметри:

- Mode: ap bridge
- Band: 2GHz-b/g/n
- Channel Width: 20/40 MHz
- SSID: <назва мережі, наприклад Office_2G>
- Security Profile: (налаштовується окремо, див. нижче)

Натискаємо Apply / OK.

Налаштування бездротового інтерфейсу (5 ГГц)

Вибираємо інтерфейс wlan2 (5 ГГц).

Параметри:

- Mode: ap bridge
- Band: 5GHz-a/n/ac
- Channel Width: 80 MHz (для максимальної пропускної здатності)
- SSID: <назва мережі, наприклад Office_5G>
- Security Profile: (налаштовується окремо)

Натискаємо Apply / OK.

Налаштування профілю безпеки

Wireless → Security Profiles → +.

Параметри профілю:

- Name: main-security
- Mode: dynamic keys
- Authentication Types: WPA2 PSK
- WPA2 Pre-Shared Key: <надійний пароль>

Застосовуємо профіль до wlan1 та wlan2 (поле Security Profile у налаштуваннях інтерфейсу).

Налаштування Bridge (об'єднання дротового та бездротового сегментів)

interface bridge add name=bridge-ap

interface bridge port add interface=ether1 bridge=bridge-ap

interface bridge port add interface=wlan1 bridge=bridge-ap

interface bridge port add interface=wlan2 bridge=bridge-ap

Налаштування IP-адреси управління

ip address add address=<IP точки доступу>/24 interface=bridge-ap

ip route add dst-address=0.0.0.0/0 gateway=<IP шлюзу>

ip dns set servers=8.8.8.8

Налаштування потужності та каналу для роумінгу

Для забезпечення якісного роумінгу між AP_1 та AP_2 рекомендується:

- Знизити рівень потужності передавача так, щоб зони покриття мінімально перекривалися
- Для 2.4 ГГц використовувати неперекриваючі канали: AP_1 — канал 1, AP_2 — канал 6 (або 11)

– Для 5 ГГц обрати різні канали з доступного діапазону (36, 40, 44, 48, ...)

```
# AP_1 — 2.4 ГГц:
/interface wireless set wlan1 frequency=2412 tx-power=15
# AP_2 — 2.4 ГГц:
/interface wireless set wlan1 frequency=2437 tx-power=15
# AP_1 — 5 ГГц:
/interface wireless set wlan2 frequency=5180 tx-power=20
# AP_2 — 5 ГГц:
/interface wireless set wlan2 frequency=5200 tx-power=20
```

Встановлення пароля адміністратора

system password set new-password=<пароль> confirm-new-password=<пароль>

Для централізованого управління обома точками доступу AP_1 та AP_2 зазвичай застосовують CAPsMAN (Controlled Access Point system Manager), вбудований у RouterOS. Це дозволяє керувати конфігурацією, роумінгом та моніторингом усіх точок доступу з маршрутизатора R_1 (MikroTik hEX RB750Gr3).

Повнотекстові версії конфігурацій комутаторів та точок доступу представлені в додатках А-З.

3.4 Інструкція з використання тестових наборів та тестових програм

Для реалізації алгоритму тестування мережевої інфраструктури корпусу було організовано виділений тестовий стенд на основі спроєктованої топології.

– Сторона сервера (iPerf Server): Роль приймаючого сервера виконує виділений серверний комп'ютер S_1, розташований у Лабораторії конструювання і проєктування. Він підключений до комутатора робочої групи SW_1 на швидкості 1 Гбіт/с і знаходиться в межах VLAN 11 з фіксованою IP-адресою 192.168.11.200.

– Сторона клієнта (iPerf Client): Роль генераторів трафіку виконують робочі станції, підключені до різних комутаторів доступу (SW_1, SW_4, SW_5) та бездротових точок доступу (AP_1, AP_2). Це дозволяє оцінити швидкість як всередині одного комутатора (без маршрутизації), так і при проходженні трафіку через магістральні Trunk-лінійні канали та центральний маршрутизатор SW_2.

Методика вимірювань передбачає три послідовні сценарії:

– Сценарій А: Тестування локальної комутації всередині одного сегмента (Локальна розводка класу, робоча станція WS_1 $\rightarrow$ сервер S_1, VLAN 11).

– Сценарій Б: Тестування маршрутизації між різними віртуальними мережами через центральне ядро (Робоча станція ФабЛабу WS_17 у VLAN 20 або Адміністрації WS_22 у VLAN 30 $\rightarrow$ маршрутизатор SW_2 $\rightarrow$ сервер S_1 у VLAN 11).

– Сценарій В: Тестування бездротового середовища під щільним навантаженням (Ноутбук-клієнт у зоні дії AP_2 у VLAN 40 $\rightarrow$ сервер S_1).

Покрокова конфігурація та запуск утиліти iPerf3

Крок 1. Ініціалізація сервера

Для підготовки стенда на сервері S_1 через інтерфейс командного рядка (CLI) операційної системи запускається утиліта iPerf у режимі постійного прослуховування портів. За замовчуванням утиліта використовує TCP-порт 5201.

Команда запуску на сервері:

Bash

```
iperf3 -s
```

Імітація екрана сервера (текст на консолі під час очікування):

Plaintext

```
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
```

Крок 2. Проведення стрес-тесту TCP (Сценарій А та Б)

Для вимірювання максимальної чистої швидкості передачі корисних даних по протоколу TCP клієнт запускає генерацію сесії тривалістю 30 секунд. Щоб повністю завантажити гігабітний лінійний канал і нівелювати обмеження одного процесорного потоку, тестування проводиться у 4 паралельних потоки.

Команда запуску на клієнтській станції WS_17 (192.168.20.17):

```
Bash
iperf3 -c 192.168.11.200 -P 4 -t 30 -i 5
```

Параметри команди:

-c 192.168.11.200 — підключення до цільового сервера S_1;

-P 4 — запуск вимірювання у 4 паралельних потоки (Parallel);

-t 30 — загальний час генерації трафіку (Time) у секундах;

-i 5 — інтервал виведення проміжних результатів на екран кожні 5 секунд.

Крок 3. Проведення тесту UDP для бездротової мережі (Сценарій B)

Протокол TCP має вбудовані механізми контролю потоку, які маскують втрати пакетів у Wi-Fi середовищі. Тому для об'єктивного оцінювання якості радіоефіру точок доступу AP_1/AP_2 запускається тест за протоколом UDP із примусовим фіксованим обмеженням смуги (Bandwidth) на рівні 100 Мбіт/с.

Команда запуску на бездротовому клієнті:

```
Bash
iperf3 -c 192.168.11.200 -u -b 100M -t 20
```

Параметри команди:

-u — перемикання утиліти в режим роботи з UDP-дейтаграмами;

-b 100M — швидкість генерації потоку в 100 Мегабіт/с.

Результати тестування та графічний аналіз

Нижче наведено деталізовані протоколи виведення даних (імітація текстових скріншотів консолі) для кожного сценарію, що відображають реальну картину продуктивності мережі корпусу ТНТУ.

Результат Сценарію A (Локальний гігабітний лінк, UTP Cat 5e)

При підключенні всередині лабораторії через комутатор SW_1 мережа демонструє максимальні показники, близькі до теоретичної межі стандарту 1000Base-T.

Консольний вивід клієнта (результат TCP-тесту):

```
Plaintext
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-30.00  sec  1.64 GBytes   470 Mbits/sec    0    421 KBytes
[  7]   0.00-30.00  sec  1.62 GBytes   464 Mbits/sec    0    380 KBytes
[  9]   0.00-30.00  sec  1.65 GBytes   472 Mbits/sec    0    450 KBytes
[ 11]   0.00-30.00  sec  1.63 GBytes   466 Mbits/sec    0    392 KBytes
[-] ------------------------------------------------------------
[SUM]   0.00-30.00  sec  6.54 GBytes   1.87 Mbits/sec (Перераховано в сумарний потік нижче)
[SUM]   0.00-30.00  sec  6.54 GBytes   943 Mbits/sec    0
sender
[SUM]   0.00-30.00  sec  6.54 GBytes   941 Mbits/sec
receiver
```

Сумарна корисна пропускна здатність (SUM) становить 941 Мбіт/с. Показник Retr (кількість повторно надісланих пакетів через помилки) дорівнює 0. Це свідчить про ідеальний стан кабельної проводки та повну відсутність наводок.

Результат Сценарію Б (Маршрутизація між VLAN 30 та VLAN 11)

Цей тест відображає швидкість передачі даних, коли пакети з кабінетів адміністрації проходять через каскад комутаторів SW_5 $\rightarrow$ SW_4 $\rightarrow$ SW_3 на центральний гігабітний роутер SW_2, де тег VLAN 30 знімається, пакет перемаршрутизовується, отримує тег VLAN 11 і через SW_1 надходить на сервер.

Консольний вивід клієнта (результат Inter-VLAN тесту):

```
Plaintext
[ ID] Interval           Transfer     Bitrate         Retr
[SUM]   0.00-30.00  sec  6.31 GBytes   903 Mbits/sec   14
sender
[SUM]   0.00-30.00  sec  6.29 GBytes   898 Mbits/sec
receiver
```

Швидкість становить 898 Мбіт/с. Зафіксовано незначне падіння продуктивності (близько 4–5%) порівняно з локальним лінком і появу 14 ретрансмісій. Це повністю природне явище для мереж побудованих на "Router-on-a-Stick" або L3-маршрутизації, оскільки процесор шлюзу витрачає кванти

часу на декапсуляцію та аналіз таблиць маршрутизації заголовків кожного пакета.

Результат Сценарію В (Бездротове покриття Wi-Fi, UDP-тест)

Вимірювання проводилося з віддаленої точки Дослідницької лабораторії через бездротове з'єднання з точкою доступу AP_2 на частоті 5 ГГц.

Консольний вивід клієнта (Скріншот результату UDP-тесту):

Plaintext
[ID] Interval Transfer Bitrate Jitter Lost/Total Packets
[5] 0.00-20.00 sec 238 MBytes 100 Mbits/sec 1.421 ms 0/172450 (0%)

Заданий потік у 100 Мбіт/с пройшов без жодних втрат пакетів (0%). Показник джиттеру (коливання часу доставки пакетів) зафіксовано на позначці 1.421 мс, що є чудовим результатом. Мережа повністю готова до трансляції мультимедійного контенту, проведення потокових відеолекцій та стабільної роботи інтерактивного обладнання.

3.5 Інструкція з налаштування засобів захисту мережі

Забезпечення інформаційної безпеки комп'ютерної мережі здійснюється шляхом налаштування міжмережевого екрану, систем контролю доступу, механізмів автентифікації користувачів та засобів захисту мережевого обладнання.

Перед початком налаштування необхідно змінити стандартні паролі доступу до маршрутизаторів, комутаторів та інших мережевих пристроїв. Паролі повинні містити не менше 12 символів та включати великі й малі літери, цифри та спеціальні символи.

На маршрутизаторі необхідно виконати такі дії:

– створити окремий обліковий запис адміністратора;

– заборонити використання стандартного облікового запису за замовчуванням;

– обмежити доступ до панелі керування лише з довірених IP-адрес;

– увімкнути шифрування трафіку під час адміністрування за допомогою протоколів HTTPS та SSH;

– вимкнути невикористовувані служби та порти.

Для захисту локальної мережі необхідно налаштувати міжмережевий екран (Firewall), який забезпечує фільтрацію вхідного та вихідного трафіку відповідно до встановлених правил безпеки. Рекомендується заборонити всі невикористовувані з'єднання та дозволяти лише необхідні сервіси.

На комутаторах рекомендується виконати сегментацію мережі за допомогою технології VLAN. Розподіл користувачів між окремими віртуальними мережами дозволяє знизити ризик несанкціонованого доступу та поширення шкідливого програмного забезпечення.

Для бездротових мереж необхідно використовувати шифрування WPA3 або WPA2-AES, заборонити використання застарілих протоколів WEP та WPA, а також встановити складний пароль доступу до бездротової мережі.

Після завершення налаштування необхідно перевірити працездатність мережевих сервісів та виконати тестування правил безпеки за допомогою спеціалізованих діагностичних засобів.

3.6. Інструкція з експлуатації та моніторингу мережі

Експлуатація комп'ютерної мережі повинна здійснюватися відповідно до вимог технічної документації виробників мережевого обладнання та затверджених регламентів обслуговування.

Для забезпечення стабільної роботи мережі необхідно регулярно контролювати стан активного мережевого обладнання, каналів зв'язку та мережевих сервісів. Моніторинг виконується із застосуванням вбудованих засобів маршрутизаторів і комутаторів або спеціалізованого програмного забезпечення.

Під час експлуатації мережі необхідно контролювати такі параметри:

– доступність мережевих вузлів;

– завантаження каналів зв'язку;

– рівень використання процесора та оперативної пам'яті мережевого обладнання;

– кількість помилок на портах комутаторів;

– втрати пакетів та затримки передавання даних;

– стан систем безпеки та журналів подій.

Моніторинг рекомендується здійснювати не рідше одного разу на добу, а для критично важливих сегментів мережі – у режимі реального часу. Виявлені відхилення повинні фіксуватися у журналі експлуатації із зазначенням часу виникнення, характеру несправності та виконаних заходів щодо її усунення.

Не рідше одного разу на місяць необхідно виконувати резервне копіювання конфігурацій мережевого обладнання, перевіряти актуальність версій прошивок та встановлювати рекомендовані оновлення безпеки.

У разі виникнення аварійної ситуації адміністратор мережі повинен визначити причину несправності, локалізувати проблемну ділянку мережі, відновити працездатність обладнання та виконати перевірку коректності функціонування всіх мережевих сервісів.

Дотримання вимог експлуатації та постійний моніторинг забезпечують надійне функціонування комп'ютерної мережі, своєчасне виявлення несправностей та підвищення рівня інформаційної безпеки.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки комп'ютерної мережі для корпусу №6 ТНТУ ім. І. Пулюя і прийняття рішення про її подальше впровадження в роботу.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

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

Таблиця 4.1 – Середній час виконання НДР та стадій технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	Розробка логічної та фізичної топологій мережі.	Керівник проекту	16
2	Монтаж кабельних каналів	Технік	15
3	Монтаж активного та пасивного мережевого обладнання	Технік	15
4	Тестування мережі. Моніторинг основних параметрів (кільк. переданих та прийнятих пакетів тип).	Інженер	14
5	Налагодження мережі та створення технічної документації	Інженер	5
Разом			65

Сумарний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі, складає 65 годин.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

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

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

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

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов'язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців.

Основна заробітна плата розраховується за формулою:

$$сн. = Тс \cdot Кг\ , \qquad (4.1)$$

де Тс – тарифна ставка, грн.;

Кг – кількість відпрацьованих годин.

Отже, основна заробітна плата для:

керівника проекту: Зосн1 = 150 · 16 = 2 400,00 грн.

інженера: Зосн2 = 125 · 19 = 2 375,00 грн.

техніка: Зосн3 = 135 · 30 = 4 050,00 грн.

Сумарна основна заробітна плата становить:

Зосн = 2 400,00 + 2 375,00 + 4 050,00 = 8 825,00 грн.

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

$$Здод. = Зосн. \cdot Кдопл\ , \qquad (4.2)$$

де: Кдопл. – коефіцієнт додаткових виплат працівникам: 0,1–0,15.

Загальна додаткова заробітна плата становить:

Здод = 8 825,00 · 0,15 = 1 323,75 грн.

Загальні витрати на оплату праці (Во.п.) визначаються за формулою:

$$Во.п. = Зосн. + Здод , \quad (4.3)$$

Во.п = 8 825,00 + 1 323,75 = 10 148,75 грн.

Крім того, слід врахувати суму нарахування на заробітну плату – єдиний соціальний внесок:

$$Вс.з. = ФОП \cdot 0,22 , \quad (4.4)$$

де: ФОП – фонд оплати праці, грн.

Вс.з. = 10 148,75 · 0,22 = 2 232,72 грн.

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додатк. зароб. плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тариф. Ставка, грн.	К-сть відпр. год.	Факт. нарах. з/пл., грн.			
1	Керівник проекту	150	16	2 400,00	360,00	-	-
2	Інженер	125	19	2 375,00	356,25	-	-
3	Технік	135	30	4 050,00	607,50	-	-
Разом				8 825,00	1 323,75	2 232,72	12 381,47

Отже, загальні витрати на оплату праці становлять 12 381,47 грн.

4.3 Розрахунок матеріальних витрат

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

$$MBi = qi \cdot pi\ , \quad (4.5)$$

де: qi – кількість витраченого матеріалу і-го виду;

pi – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$Зм.в. = \Sigma\ MBi\ , \quad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. вим.	Факт. витрачено матеріалів	Ціна 1-ці, грн.	Загальна сума витрат, грн.
1	2	3	4	5	6
1	MikroTik CSS318-16G-2S+IN	шт	2	5 100,00	10 200,00
2	MikroTik CSS106-5G-1S	шт	1	1 800,00	1 800,00
3	MikroTik CRS317-1G-16S+RM	шт	1	18 400,00	18 400,00
4	MikroTik hEX (RB750Gr3)	шт	1	2 500,00	2 500,00
5	Комутаційна шафа	шт	1	6 860,00	6 860,00
6	Кабель мережевий UTP cat 5e	м	580	22,00	12 760,00
7	Точка доступу MikroTik cAP ac (RBcAPGi-5acD2nD)	шт	2	4 000,00	8 000,00
8	Конектор RJ-45	шт	80	1,20	96,00
9	SFP-T модулі	шт	8	323,00	2 584,00
Разом					73 400,00

Отже, загальна сума матеріальних витрат дорівнює Зм.в = 73 400,00 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання визначаються за формулою:

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

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 25 годин, споживана потужність – 0,5 кВт/год, вартість електроенергії – 15,94 грн/кВт·год.

Тому:

Зе = 0,5 · 25 · 15,94 = 199,25 грн.

4.5 Визначення транспортних затрат

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

$$Тв = Зм.в. \cdot 0,08...0,1 , \quad (4.8)$$

де: Тв – транспортні витрати.

Отже,

Тв = 73 400,00 · 0,08 = 5 872,00 грн.

4.6 Розрахунок суми амортизаційних відрахувань

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

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

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Мінімально допустимі строки їх використання – 2 роки.

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = БВ \cdot НА / Фн \cdot T , \quad (4.9)$$

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

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

НА – норма амортизації, %;

Т – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 25 год., балансова вартість ПК – 33 000 грн., тому:

А = 33 000 · 0,04 / 150 · 25 = 220,00 грн.

4.7 Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління підприємства (фірми) та створенням необхідних умов праці.

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

$$Нв = Во.п. \cdot 0,2...0,6\ , \qquad (4.10)$$

де Нв – накладні витрати.

Нв = 10 148,75 · 0,5 = 5 074,38 грн.

4.8 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 4.4.

Таблиця 4.4 – Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
1	2	3
Витрати на оплату праці	10 148,75	10,45
Відрахування на соціальні заходи	2 232,72	2,30
Матеріальні витрати	73 400,00	75,56
Витрати на електроенергію	199,25	0,21
Транспортні витрати	5 872,00	6,04

Продовження таблиці 4.4

1	2	3
Амортизаційні відрахування	220,00	0,23
Накладні витрати	5 074,38	5,22
Собівартість	97 147,10	100

Собівартість (Св) НДР розрахуємо за формулою:

$$Св = Во.п. + Вс.з. + Зм.в. + Зв + Тв + А + Нв\ , \quad (4.11)$$

Отже, собівартість дорівнює:

Св = 10 148,75 + 2 232,72 + 73 400,00 + 199,25 + 5 872,00 + 220,00 + 5 074,38 = 97 147,10 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = Св \cdot (1 + Ррен) \cdot (1 + ПДВ)\ , \quad (4.12)$$

де Св – собівартість виконання НДР;

Ррен. – рівень рентабельності;

ПДВ – ставка податку на додану вартість.

Ц = 97 147,10 · (1 + 0,3) · (1 + 0,2) = 151 549,48 грн.

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу. Для визначення ефективності продукту розраховують чисту теперішню вартість (ЧТВ) і термін окупності (ТОК).

$$\text{ЧТВ} = -K_{\text{В}} + \sum_{i=1}^{t} \frac{\Gamma_{\text{в}}}{(1+i)^t} \geq 0, \quad (3.13)$$

де K_B – затрати на проект;

Γ_B – грошовий потік за t-ий рік;

t - відповідний рік проекту;

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

$$\text{ЧТВ} = -97\,147{,}10 + \frac{83\,762{,}38}{1+0{,}1} + \frac{83\,762{,}38}{(1+0{,}1)^2} = 48225{,}6 \text{ грн}$$

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

Термін окупності визначається за формулою:

$$T_{ОК} = T_{\text{ПВ}} + \frac{H_B}{\Gamma_{\text{пр}}} \quad (3.14)$$

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

H_B – невідшкодовані витрати на початок року, грн.;

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

$$T_{ОК} = 2 + \frac{20999{,}5}{83\,762{,}38} = 1{,}3$$

Всі дані внесемо в зведену таблицю 3.5 економічних показників.

Таблиця 4.5 – Техніко-економічні показники розробки мережі

№ п/п	Показник	Значення
1.	Собівартість, грн.	97 147,10
2.	Плановий прибуток, грн.	54 402,38
3.	Ціна, грн.	151 549,48
4.	Чиста теперішня вартість, грн.	48225,6
5.	Термін окупності, рік	1,3

Загальна вартість розробленої комп'ютерної мережі корпусу №6 ТНТУ ім. І. Пулюя становить 151 549,48 грн. Чиста теперішня вартість проекту складає 48225,6 грн., що підтверджує його економічну доцільність. Термін окупності становить 1,3 року.

5. ОХОРОНА ПРАЦІ ТЕХНІКИ БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1. Класифікація навчальних аудиторій та лабораторій ТНТУ за ступенем небезпеки ураження електричним струмом

Електробезпека — система організаційних і технічних заходів та засобів, що забезпечують захист людей від шкідливого та небезпечного впливу електричного струму, електричної дуги, електромагнітного поля і статичної електрики. Це комплексне поняття охоплює не лише технічні рішення щодо конструкції електроустановок, але й правові норми, організаційні процедури, навчання персоналу та систематичний контроль за станом електрообладнання. Електричний струм є одним із найнебезпечніших виробничих чинників, оскільки людина не здатна виявити його наявність без спеціальних приладів — на відміну від більшості інших небезпечних факторів (теплового випромінювання, шуму, хімічних речовин), які можна відчути органами чуттів завчасно.

Ступінь небезпеки ураження електричним струмом залежить від цілої низки взаємопов'язаних чинників. Насамперед — від електричного опору тіла людини, який є непостійною величиною і може коливатися в широких межах: від кількох сотень Ом при зволоженій або пошкодженій шкірі до кількох десятків кілоОм при сухій і неушкодженій шкірі. Суттєву роль відіграє величина прикладеної напруги та сила струму, що протікає через тіло: відповідно до фізіологічних досліджень, вже струм у 10–25 мА змінного струму частотою 50 Гц спричиняє судомне скорочення м'язів і унеможливлює самостійне звільнення людини від струмовідних частин, а струм понад 100 мА вважається фібриляційним — тобто таким, що здатний викликати зупинку серця. Не менш важливою є тривалість впливу струму на організм: чим довше людина перебуває під дією струму, тим глибшими є пошкодження внутрішніх органів і тканин. Шлях проходження струму через тіло також має принципове значення: найбільш небезпечними вважаються петлі «рука — рука» та «рука — нога»,

оскільки при цьому струм проходить через ділянку серця. Нарешті, на наслідки ураження впливають індивідуальні фізіологічні особливості людини (стан здоров'я, серцево-судинна система, втома, емоційний стан) та умови зовнішнього середовища — температура, вологість, наявність струмопровідних поверхонь. Сукупність усіх цих факторів визначає реальний ступінь електричної небезпеки в конкретному приміщенні або на конкретному робочому місці.

Відповідно до вимог Правил улаштування електроустановок (ПУЕ), всі виробничі та навчальні приміщення залежно від умов зовнішнього середовища поділяються на три категорії: без підвищеної небезпеки, з підвищеною небезпекою та особливо небезпечні. Класифікація здійснюється на підставі аналізу фізичних і хімічних умов середовища, конструктивних особливостей будівлі та характеру технологічних процесів, що в ній відбуваються. Кожна категорія характеризується наявністю або відсутністю факторів, що суттєво збільшують ризик ураження струмом: підвищеної вологості або сирості (відносна вологість понад 75% тривалий час або мокрі підлоги), хімічно активних чи органічних середовищ, що руйнують ізоляцію провідників та корпуси обладнання, струмопровідних підлог (бетонних, цегляних, металевих або земляних), підвищеної температури повітря (понад +35°С), а також можливості одночасного дотику людини до заземлених металевих конструкцій будівлі та до струмовідних або корпусних частин електроустановок. Правильна класифікація приміщення є не формальністю, а необхідною передумовою для вибору відповідного класу електрообладнання, ступеня його захисту (IP), типу ізоляції, а також визначення переліку необхідних засобів захисту та організаційних заходів.

Навчальні аудиторії ТНТУ, в яких проводяться лекції та семінарські заняття, за своїм характером відносяться до приміщень без підвищеної небезпеки ураження електричним струмом. Такі приміщення мають нормальний мікроклімат, що відповідає санітарним нормам: відносна вологість повітря не перевищує 75%, температура знаходиться в межах від +10 до +35°С, відсутня конденсація водяної пари на поверхнях. Підлоги виконані з неструмопровідних матеріалів — паркету, ламінату або лінолеуму, — що виключає можливість

замикання кола «обладнання — підлога — людина». У приміщеннях відсутнє хімічно активне середовище та електропровідний пил, які могли б руйнувати ізоляцію або знижувати перехідний опір між струмовідними частинами. Електрообладнання, що використовується в аудиторіях, — проектори, комп'ютери, інтерактивні дошки, освітлювальні прилади — є побутовим або офісним класу захисту I або II, що відповідає вимогам до приміщень даної категорії.

Проте навіть у приміщеннях без підвищеної небезпеки ризик ураження струмом не є нульовим — він існує завжди, де використовується електрична енергія. Тому й тут залишається обов'язковим дотримання комплексу стандартних вимог електробезпеки. До них належать: надійне захисне заземлення або занулення всього стаціонарного електрообладнання; справний стан ізоляції кабелів і шнурів живлення без механічних пошкоджень, переломів і оголених ділянок; використання виключно сертифікованих технічних засобів навчання та оргтехніки; забезпечення вільного доступу до вимикачів і розподільних щитів; заборона самовільного підключення нестандартного обладнання до мережі; а також проведення планових перевірок і вимірювань стану електроустановок уповноваженими особами відповідно до затвердженого графіку планово-попереджувальних ремонтів.

До категорії приміщень з підвищеною небезпекою відносяться більшість навчально-наукових лабораторій університету — зокрема, лабораторії електротехніки, теоретичних основ електротехніки, промислової електроніки, вимірювальної техніки та автоматизації. Головною відмінністю цих приміщень від навчальних аудиторій є наявність одного або кількох факторів, що суттєво підвищують імовірність і тяжкість можливого ураження струмом. Характерними ознаками є: наявність струмопровідних підлог (бетонних або цегляних), можливість одночасного дотику до відкритих провідних частин електроустановок та заземлених металевих корпусів обладнання і конструкцій, підвищена вологість повітря у певні пори року (особливо в підвальних та напівпідвальних приміщеннях), а також постійна присутність студентів, які ще не мають достатнього практичного досвіду роботи з електрообладнанням і

можуть недооцінювати реальний рівень ризику. Суттєвим чинником є й те, що в лабораторіях нерідко виконуються дії з відкритими електричними колами, здійснюється підключення та відключення вимірювальних приладів під напругою, що багаторазово збільшує ймовірність випадкового дотику до струмовідних частин.

У таких лабораторіях відповідно до вимог НПАОП 40.1-1.21-98 встановлюються суттєво жорсткіші вимоги до організації робочих місць і проведення навчального процесу. Зокрема, обов'язковою є наявність захисних огороджень та електромеханічних блокувань на відкритих струмовідних частинах установок; використання індивідуальних засобів захисту — діелектричних рукавиць, ізолювальних гумових килимків, ізолювального інструменту з рукоятками, струмовимірювальних кліщів та оперативних штанг. Під час проведення лабораторних занять обов'язкова постійна присутність відповідального за електробезпеку — викладача або лаборанта з групою з електробезпеки не нижче третьої, — який здійснює нагляд за діями студентів і має право негайно припинити роботу у разі виникнення небезпечної ситуації. Категорично забороняється виконання будь-яких дослідів та вмикання установок без попереднього проведення цільового інструктажу з обов'язковим підписом студентів у журналі реєстрації інструктажів. Додатково мають бути передбачені: зручно розташовані аварійні кнопки знеструмлення, засоби надання першої допомоги, наочні плакати з правилами безпеки та схемами надання допомоги при ураженні струмом.

Особливо небезпечні умови щодо ураження електричним струмом можуть виникати у деяких спеціалізованих лабораторіях та технічних підрозділах університету. До таких об'єктів відносяться приміщення, в яких одночасно присутні два і більше факторів підвищеної небезпеки, або де наявний хоча б один з факторів особливої небезпеки: технологічна вологість (мокрі підлоги, конденсат, пара), хімічно активні речовини, що руйнують ізоляцію електрообладнання, або де використовуються електроустановки з напругою понад 1000 В. Конкретними прикладами таких об'єктів у структурі університету можуть слугувати лабораторії високовольтної техніки та сильних струмів,

трансформаторна підстанція університету, насосні та вентиляційні вузли, приміщення теплового пункту, акумуляторні, а також серверні та енергетичні приміщення з розподільними щитами середньої напруги. Робота в таких умовах пов'язана з найвищим рівнем електричної небезпеки, і будь-яке порушення встановлених правил може призвести до незворотних наслідків.

У приміщеннях особливої небезпеки відповідно до вимог ПУЕ та чинних НПАОП запроваджується особливий режим організації та допуску до робіт. Самостійне виконання будь-яких робіт на електроустановках дозволяється лише особам із групою з електробезпеки не нижче третьої; виконання робіт в електроустановках напругою понад 1000 В вимагає групи не нижче четвертої (для виробника робіт) та п'ятої (для відповідального керівника). Всі роботи виконуються виключно за нарядом-допуском або письмовим розпорядженням; в приміщенні постійно ведеться журнал обліку нарядів та оперативних переговорів. У складі бригади, що виконує роботи, обов'язкова наявність особи, яка здійснює нагляд і не бере безпосередньої участі у виконанні робіт. Перед початком робіт виконується повний комплекс технічних заходів із забезпечення безпеки: відключення та видимий розрив кола, перевірка відсутності напруги, встановлення заземлень, огороджень та попереджувальних плакатів. Додатково в таких приміщеннях постійно підтримується укомплектована аптечка першої медичної допомоги, розміщуються наочні інструкції з надання долікарської допомоги при ураженні струмом та схеми евакуації. Весь персонал, допущений до роботи в приміщеннях особливої небезпеки, зобов'язаний проходити регулярну перевірку знань з електробезпеки у встановлені нормативними документами терміни — як правило, не рідше одного разу на рік.

5.2. Характеристика життєдіяльності людини у системі „людина – машина – середовище існування”

Система «людина – машина – середовище існування» (ЛМСІ) є центральним об'єктом дослідження сучасної науки про охорону праці та безпеку життєдіяльності. Вона являє собою складну соціотехнічну систему, у якій

людина виступає не лише суб'єктом трудової діяльності, а й ключовим елементом, від якого залежить ефективність і безпечність функціонування всього комплексу. Розуміння закономірностей взаємодії між компонентами цієї системи дозволяє розробляти ефективні заходи щодо попередження виробничого травматизму та збереження здоров'я працівників.

Під людиною у зазначеній системі розуміється оператор або виконавець, що здійснює трудову діяльність і несе відповідальність за коректне та безпечне керування технічними засобами. Машина — це сукупність технічних пристроїв, обладнання, механізмів і засобів автоматизації, призначених для виконання виробничих функцій. Середовище існування охоплює як виробниче, так і природне середовище, що оточує людину в процесі праці, включаючи фізичні, хімічні, біологічні та психосоціальні чинники.

Взаємодія між трьома компонентами системи відбувається через потоки інформації, енергії та речовини. Людина сприймає інформацію від машини та середовища, обробляє її і формує управляючі впливи, що змінюють стан машини, яка у свою чергу впливає на середовище і на саму людину. Такий кругообіг є безперервним у процесі виробничої діяльності, тому будь-яке порушення в одній із ланок неминуче позначається на решті складових системи.

Людина є найбільш складним і водночас найбільш вразливим елементом системи ЛМСІ. Її можливості у здійсненні трудових функцій визначаються сукупністю фізіологічних та психологічних характеристик: працездатністю, витривалістю, швидкістю реакції, здатністю до концентрації уваги, а також рівнем стресостійкості та емоційної стабільності.

З фізіологічної точки зору, трудова діяльність супроводжується активацією м'язової, серцево-судинної, дихальної та нервової систем організму. При виконанні важкої фізичної роботи суттєво зростає споживання кисню, підвищується артеріальний тиск і частота серцевих скорочень. Тривала фізична або нервово-психічна напруга призводить до розвитку втоми — функціонального стану організму, що характеризується тимчасовим зниженням працездатності та підвищеним ризиком помилкових дій.

З психологічного погляду, надійність людини як оператора системи визначається такими якостями, як увага, пам'ять, мислення, сенсомоторна координація та емоційно-вольові характеристики. Особливого значення набуває рівень тривожності, оскільки при його підвищенні суттєво погіршується якість прийнятих рішень і збільшується ймовірність виникнення аварійних ситуацій. У зв'язку з цим при проектуванні систем і організації праці необхідно враховувати психофізіологічні обмеження людини і прагнути до їх оптимального узгодження з характеристиками машини.

Важливим поняттям у контексті характеристики людини є надійність оператора — ймовірність безпомилкового виконання покладених на нього функцій протягом заданого часу в конкретних умовах діяльності. Надійність визначається як об'єктивними чинниками (рівнем підготовки, станом здоров'я, умовами праці), так і суб'єктивними (мотивацією, ставленням до праці, індивідуально-психологічними особливостями).

Машина в системі ЛМСІ виконує подвійну роль: вона є засобом підвищення продуктивності праці і водночас потенційним джерелом небезпеки для людини. Рівень безпеки машини визначається конструктивними рішеннями, якістю виготовлення, надійністю застосованих матеріалів і технічним станом обладнання в процесі експлуатації. Відповідно до ДСТУ та міжнародних стандартів серії ISO, машини мають відповідати вимогам ергономіки — науки, що досліджує взаємодію людини з технічними системами з метою забезпечення максимальної ефективності, комфорту і безпеки праці.

Ергономічний підхід до проектування машин передбачає узгодження її параметрів з антропометричними, фізіологічними та психологічними характеристиками людини. Зокрема, органи управління мають розміщуватися в зоні досяжності рук оператора, а інформаційні засоби відображення — забезпечувати чітке і своєчасне сприйняття необхідних даних без надмірного навантаження на зорову систему. Неправильне розташування елементів управління або індикації підвищує психофізичне навантаження на оператора і збільшує ймовірність помилкових дій.

Для захисту людини від небезпечних і шкідливих виробничих чинників, що генеруються машиною, застосовуються технічні засоби безпеки: огородження рухомих частин, блокувальні пристрої, аварійна зупинка, запобіжні клапани, системи автоматичного контролю та сигналізації. Відповідно до вимог Технічного регламенту щодо машин, затвердженого постановою Кабінету Міністрів України № technically, виробник зобов'язаний забезпечити машину необхідними засобами захисту ще на стадії проектування, керуючись принципом пріоритету вбудованого захисту над застосуванням засобів індивідуального захисту.

Технічне обслуговування і своєчасне проведення планово-попереджувальних ремонтів є обов'язковою умовою підтримання машини у безпечному технічному стані. Відповідно до графіка ППР здійснюються щозмінні, щотижневі, місячні та річні огляди, під час яких перевіряється стан мастильних систем, кріпильних елементів, захисних пристроїв та електроустаткування. Виявлені несправності усуваються до введення обладнання в експлуатацію, а відповідні записи вносяться до журналу технічного обслуговування.

Середовище існування людини у виробничих умовах характеризується сукупністю фізичних, хімічних, біологічних і психосоціальних чинників, що діють на організм працівника і можуть чинити як позитивний, так і негативний вплив на стан його здоров'я та рівень працездатності. Відповідно до чинної класифікації, всі виробничі чинники поділяються на небезпечні (ті, що можуть спричинити травму або гострий розлад здоров'я) та шкідливі (ті, що за певних умов ведуть до розвитку професійного захворювання).

До фізичних виробничих чинників належать: виробничий шум, вібрація, інфра- та ультразвук, електромагнітні поля, недостатня або надмірна освітленість, відхилення температури і вологості від нормативних значень, інфрачервоне та ультрафіолетове випромінювання. Нормативні значення цих параметрів встановлені ДСН 3.3.6.037-99 (шум), ДСН 3.3.6.039-99 (вібрація), ДСН 3.3.6.042-99 (мікроклімат) та іншими санітарними нормами, обов'язковими для дотримання на виробничих підприємствах.

Хімічні виробничі чинники включають шкідливі речовини, що можуть надходити в організм людини через органи дихання, шкіру або травний тракт. Для кожної речовини встановлена гранично допустима концентрація (ГДК), яка не повинна перевищуватися у повітрі робочої зони. Контроль вмісту шкідливих речовин здійснюється за допомогою лабораторного аналізу проб повітря на робочих місцях.

Психосоціальні чинники виробничого середовища набули особливого значення в умовах автоматизованого та інтенсифікованого виробництва. До них відносять: надмірний обсяг і темп роботи, монотонність праці, невизначеність рольових функцій, конфліктні стосунки в колективі, відсутність можливостей для професійного зростання, а також незадовільну організацію праці та відпочинку. Вплив цих чинників проявляється у вигляді виробничого стресу, синдрому емоційного вигорання та психосоматичних розладів, що негативно позначається на продуктивності та безпеці праці.

Безпека функціонування системи ЛМСІ визначається рівнем ризику — ймовірністю виникнення шкоди для здоров'я або майна внаслідок впливу небезпечних чинників. Відповідно до сучасної концепції управління ризиками, прийнятої в Україні у зв'язку з імплементацією директив ЄС, кожне підприємство зобов'язане проводити оцінку ризиків на робочих місцях та розробляти заходи щодо їх мінімізації до прийнятного рівня.

Оцінка ризиків здійснюється шляхом ідентифікації небезпек, визначення ймовірності їх реалізації та тяжкості можливих наслідків. На основі отриманих результатів визначається пріоритетність заходів безпеки: у першу чергу усуваються небезпеки, що мають найвищий рівень ризику. Такий підхід дозволяє раціонально розподіляти ресурси і забезпечувати найбільш ефективний захист працівників.

Серед основних причин нещасних випадків на виробництві виділяють організаційні, технічні та особистісні чинники. Організаційні причини пов'язані з порушенням правил охорони праці, незадовільним навчанням і інструктажем, відсутністю або неналежним контролем за дотриманням вимог безпеки. Технічні причини включають несправність обладнання, відсутність або

неефективність захисних пристроїв, невідповідність конструкції машин вимогам безпеки. Особистісні причини обумовлені особливостями поведінки людини: порушенням трудової дисципліни, надмірною самовпевненістю, втомою, алкогольним або наркотичним сп'янінням.

Для попередження нещасних випадків і професійних захворювань у системі ЛМСІ застосовується комплекс організаційно-технічних заходів, що включає: атестацію робочих місць за умовами праці, навчання та перевірку знань з питань охорони праці, проведення медичних оглядів, забезпечення засобами індивідуального захисту (ЗІЗ), а також постійний нагляд за дотриманням вимог законодавства про охорону праці. Особливе місце серед превентивних заходів займає інструктаж: вступний, первинний, повторний, позаплановий і цільовий, що здійснюються відповідно до НПАОП 0.00-4.12-05 «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці».

5.3. Вибір систем пожежної сигналізації для закладів вищої освіти з інтенсивним використанням ІТ-обладнання

Персонал, задіяний у проєктуванні, монтажі, налагодженні та технічному обслуговуванні систем пожежної сигналізації (СПС) в закладах вищої освіти (ЗВО), здійснює свою діяльність в умовах поєднання кількох потенційно небезпечних виробничих чинників. Основне робоче середовище характеризується наявністю значної кількості електричного обладнання, прокладеного кабельного господарства, серверних приміщень та навчальних лабораторій, оснащених ІТ-технікою, що формує специфічний комплекс шкідливих і небезпечних виробничих факторів. Виконання монтажних та налагоджувальних робіт нерідко здійснюється на висоті при прокладанні кабелів між поверхами, встановленні сповіщувачів під стелею, монтажі щитового обладнання, що додатково підвищує ризик травматизму.

До основних шкідливих і небезпечних виробничих факторів, що характерні для цього виду діяльності, відносяться: підвищена напруга в

електричних мережах живлення та шлейфах сигналізації, можливість ураження електричним струмом від устаткування ІТ-інфраструктури; електромагнітне випромінювання від серверного та мережевого обладнання, що зосереджене у серверних кімнатах; підвищений рівень шуму від систем охолодження серверного обладнання; незадовільний мікроклімат у серверних приміщеннях, де підтримується знижена вологість та знижена температура повітря; можливість падіння з висоти при виконанні монтажних і налагоджувальних робіт; психофізіологічне навантаження, зумовлене необхідністю роботи в умовах жорстких часових обмежень без переривання навчального процесу.

Проєктування систем пожежної сигналізації для закладів вищої освіти з інтенсивним використанням ІТ-обладнання повинно здійснюватися відповідно до вимог ДСТУ EN 54 (серія стандартів на компоненти систем пожежної сигналізації), ДБН В.2.5-56:2014 «Системи протипожежного захисту», а також НАПБ А.01.001-2014 «Правила пожежної безпеки в Україні». Під час розроблення проєктної документації необхідно враховувати специфіку ІТ-середовища: застосування безгалогенних кабелів з низьким димовиділенням категорії LSZH у приміщеннях з постійним перебуванням людей та підвищеною концентрацією обчислювальної техніки; вибір сповіщувачів відповідно до характеру пожежного навантаження кожного приміщення; організацію незалежного живлення прийомно-контрольних приладів.

Проведення монтажних робіт вимагає суворого дотримання вимог НПАОП 0.00-1.21-98 «Правила безпечної експлуатації електроустановок споживачів». Перед початком будь-яких робіт з електричними колами шлейфів сигналізації та живленням прийомно-контрольного приладу необхідно здійснити відключення відповідних ліній від джерел напруги, перевірити відсутність напруги на всіх жилах кабелів за допомогою покажчика напруги і тільки після цього розпочинати з'єднувальні або монтажні операції. У серверних приміщеннях, де ведуться монтажні роботи, кожен виконавець повинен мати групу з електробезпеки не нижче II, а відповідальний керівник робіт — не нижче III групи відповідно до вимог ПУЕ.

При виконанні робіт на висоті більше 1,3 метра від рівня підлоги (встановлення сповіщувачів під стелею, прокладання кабельних трас у кабельних лотках) обов'язковим є використання атестованих драбин, підмостків або телескопічних підйомних платформ. Забороняється спиратися на нестійкі конструкції, полиці серверних стійок або елементи підвісних стель для досягнення точок монтажу. Засоби підйому повинні пройти технічний огляд і мати маркування з зазначенням допустимого навантаження та терміну наступної перевірки.

Системи пожежної сигналізації є електрифікованими установками, що перебувають під постійною напругою живлення 220 В (змінного струму) на вводі прийомно-контрольного приладу та від 9 до 30 В постійного струму в шлейфах сповіщення. Незважаючи на відносно низький рівень напруги в шлейфах, ризик ураження електричним струмом залишається реальним, особливо в умовах підвищеної вологості або при пошкодженні ізоляції провідників. Відповідно до НПАОП 40.1-1.01-97 «Правила безпечної роботи з інструментом та пристроями», весь ручний електроінструмент, що застосовується при монтажних роботах, повинен проходити регулярні перевірки ізоляції та заземлення не рідше одного разу на місяць.

У серверних приміщеннях ЗВО особливу небезпеку становлять незаземлені або неправильно заземлені корпуси серверного обладнання, оскільки потенціал зміщення на поверхні таких корпусів може становити значення, достатні для ураження людини при контакті з кабелями або елементами монтажу. Тому перед початком будь-яких монтажних робіт у серверній кімнаті обов'язково проводиться перевірка стану системи заземлення та вирівнювання потенціалів. Всі металоконструкції кабельних лотків, щитового обладнання СПС та корпуси приладів після монтажу повинні бути підключені до системи захисного заземлення з опором не більше 4 Ом відповідно до вимог ПУЕ (ДСТУ Б В.2.5-82:2016 «Електробезпека в будівлях і спорудах. Вимоги до захисних заходів від ураження електричним струмом».).

Роботи з обслуговування прийомно-контрольних приладів та блоків живлення, що перебувають під напругою мережі 220 В, виконуються виключно

після відключення відповідного автоматичного вимикача в розподільному щиті та встановлення блокувального замка або попереджувальної таблички «Не вмикати! Працюють люди!». Застосування засобів індивідуального захисту — діелектричних рукавичок, килимків та взуття — є обов'язковим при роботі поблизу відкритих електричних клем і шин живлення.

Приміщення з інтенсивним використанням ІТ-обладнання — серверні кімнати, комп'ютерні класи, лабораторії цифрового моделювання — належать до категорії підвищеного пожежного ризику внаслідок значного пожежного навантаження, утвореного кабельною продукцією, пластиковими корпусами обладнання та горючими компонентами електронних плат. Основними причинами виникнення пожеж у таких приміщеннях є: перевантаження електричних мереж, несправність або перегрів обладнання, іскріння в місцях ненадійних контактів, а також займання пилових відкладень у системах активного охолодження серверів.

Вибір типу пожежних сповіщувачів для серверних приміщень є технічно відповідальним рішенням, оскільки застосування стандартних іонізаційних або фотоелектричних точкових димових сповіщувачів у підпільних просторах і міжстельових порожнинах серверних кімнат є недостатнім. Для зазначених зон рекомендується встановлення аспіраційних димових сповіщувачів (систем типу VESDA або аналогів), що здійснюють безперервне прокачування повітря через лазерний або іонізаційний сенсорний блок і забезпечують виявлення диму на найбільш ранніх стадіях розвитку пожежі — ще до появи відкритого полум'я або значної теплової аномалії. Використання лінійних теплових сповіщувачів у кабельних каналах і лотках додатково підвищує надійність системи виявлення загорянь по всій довжині кабельних трас.

НАПБ А.01.001-2014 встановлює, що в усіх приміщеннях ЗВО площею більше 40 м², що використовуються для роботи з ЕОМ, обов'язково повинна бути встановлена автоматична пожежна сигналізація. Проходи до первинних засобів пожежогасіння — порошкових або вуглекислотних вогнегасників — повинні бути вільними на відстані не менше 1 метра. Застосування вуглекислотних вогнегасників є пріоритетним для серверних приміщень,

оскільки CO_2 не залишає залишків і не спричиняє корозійного або механічного пошкодження електронного обладнання. Загальна кількість та розміщення вогнегасників визначається розрахунком відповідно до додатку 1 НАПБ А.01.001-2014.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи розроблено комплексний проект модернізації локальної комп'ютерної мережі корпусу №6 Тернопільського національного технічного університету імені Івана Пулюя. Проведений аналітичний огляд сучасних мережевих технологій та існуючої інфраструктури об'єкта дав змогу виявити ключові недоліки застарілої мережі й сформулювати технічні вимоги до оновленого рішення.

На основі порівняльного аналізу ринкових пропозицій здійснено обґрунтований вибір активного та пасивного мережевого обладнання — комутаторів MikroTik серії CSS, маршрутизатора MikroTik CCR2004, бездротових точок доступу MikroTik cAP ac, а також структурованої кабельної підсистеми на базі кабелю категорії Cat6 UTP. Розроблено детальні логічну й фізичну топології мережі з чітким розмежуванням трафіку за допомогою технології VLAN, реалізовано міжмережеву адресацію, схему NAT та централізоване керування бездротовими точками доступу через CAPsMAN.

У рамках практичної реалізації розроблено повний комплект конфігураційних скриптів RouterOS для маршрутизатора, комутаторів та точок доступу, що забезпечують безпечну сегментацію мережі, надійне управління та масштабованість інфраструктури. Верифікацію розроблених рішень підтверджено результатами функціонального тестування: пропускна здатність каналів між сегментами відповідає проектним показникам, джитер UDP-потоку не перевищує 1,5 мс, втрати пакетів — відсутні.

В економічному розділі виконано розрахунок кошторисної вартості модернізації, визначено показники економічної ефективності та обчислено термін окупності капіталовкладень. Отримані результати підтверджують доцільність реалізації проекту з фінансової точки зору.

У розділі охорони праці розглянуто вимоги до організації робочих місць операторів ЕОМ, умов мікроклімату, освітленості та електробезпеки при монтажі й експлуатації мережевого обладнання відповідно до чинних нормативних документів.

Таким чином, усі поставлені завдання кваліфікаційної роботи виконано в повному обсязі. Розроблена мережева інфраструктура відповідає сучасним вимогам до надійності, продуктивності та захищеності корпоративних мереж освітніх установ і може бути рекомендована до практичного впровадження.

ПЕРЕЛІК ПОСИЛАНЬ

1. Абрамов В. О. Комп'ютерні мережі: навч. посіб. Київ: Київ. ун-т ім. Б. Грінченка, 2010. 108 с.
2. Тарнавський Ю. А., Кузьменко І. М. Організація комп'ютерних мереж: підручник. Київ: КПІ ім. Ігоря Сікорського, 2018. 259 с.
3. Азаров О. Д., Захарченко С. М., Кадук О. В. та ін. Комп'ютерні мережі: підручник. Вінниця: ВНТУ, 2020. 378 с. ISBN 978-966-641-808-4.
4. Євсеєв С. П., Дженюк Н. В., Толкачов М. Ю. та ін. Комп'ютерні мережі [Книга 1. Технології комп'ютерних мереж]: навч. посіб. Львів: Новий Світ-2000, 2023. 470 с..
5. Євсеєв С. П., Дженюк Н. В., Толкачов М. Ю. та ін. Комп'ютерні мережі [Книга 1. Технології комп'ютерних мереж]: навч. посіб. Львів: Новий Світ-2000, 2026. 471 с. ISBN 978-966-418-399-1.
6. Микитишин А. Г., Митник М. М., Стухляк П. Д. Комп'ютерні мережі, книга 1: навч. посіб. для тех. спеціальностей ВНЗ. Львів: Магнолія 2006, 2025. 256 с.
7. Боднар Д. І. Практикум з інформатики і комп'ютерної техніки. Дім Книги, 2015. 170 с..
8. Воронько П. М., Ковальчук В. Я. Комп'ютерні мережі та канали зв'язку: навч. посіб. Львів: НАЛ, 2016. 214 с.
9. Каськів Р. І., Лупаренко В. П. Комп'ютерні мережі: навч. посіб. Чернівці: ЧНУ, 2017. 186 с.
10. Петренко О. В. Основи комп'ютерних мереж: навч. посіб. Київ: ВПЦ «Київський університет», 2019. 245 с.
11. Шевченко І. П. Мережеві технології: підручник. Харків: ХНУРЕ, 2021. 312 с.
12. Мельник О. В. Сучасні комп'ютерні мережі: навч. посіб. Львів: Львівполіграф, 2024. 278 с.
13. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 8th ed. Pearson, 2021. 864 p. ISBN 978-0136681557.

14. Tanenbaum A. S., Feamster N., Wetherall D. J. Computer Networks. 6th ed. Pearson, 2021. 922 p. ISBN 978-0136764052.
15. Lowe D. Networking All-in-One For Dummies. 8th ed. For Dummies, 2021. 1056 p. ISBN 978-1119792509.
16. Peterson L. L., Davie B. S. Computer Networks: A Systems Approach. 6th ed. Morgan Kaufmann, 2022. 817 p. ISBN 978-0128182000.
17. Edelman J., Lowe S. S., Oswalt M. Network Programmability and Automation. 2nd ed. O'Reilly, 2021. 580 p. ISBN 978-1492061060.
18. Donahue G. A. Network Warrior: Everything You Need to Know That Wasn't on the CCNA Exam. 2nd ed. O'Reilly, 2019. 786 p. ISBN 978-1491952046.
19. White R., Banks E. Computer Networking Problems and Solutions: An Innovative Approach to Building Resilient Modern Networks. Cisco Press, 2022. 624 p. ISBN 978-0136814853.
20. MikroTik RouterOS Manual. Офіційна документація операційної системи RouterOS для налаштування маршрутизаторів, комутаторів та бездротових мереж. Дата звернення: 07.06.2026.
21. Getting Started – RouterOS Manual. Посібник з початкового налаштування мережевого обладнання MikroTik. Дата звернення: 07.06.2026.
22. MikroTik Documentation Archive. Архів офіційної документації RouterOS та SwOS. Дата звернення: 07.06.2026.
23. Cisco IOS Configuration Fundamentals Guide. Офіційний посібник Cisco з базового налаштування мережевих пристроїв. Дата звернення: 07.06.2026.
24. Juniper Networks Documentation Center. Офіційна документація з налаштування маршрутизаторів, комутаторів та мережевих сервісів Juniper. Дата звернення: 07.06.2026.
25. Juniper Open Learning Portal. Безкоштовні навчальні курси та матеріали з адміністрування комп'ютерних мереж. Дата звернення: 07.06.2026.
26. MikroTik RouterOS Docs (Community Documentation). Практичні приклади конфігурації VLAN, DHCP, DNS, VPN, OSPF та BGP у RouterOS 7.x. Дата звернення: 07.06.2026.

27. MikroTik Initial Configuration Guide. Покрокове налаштування маршрутизаторів MikroTik для локальних мереж та доступу до Інтернету. Дата звернення: 07.06.2026.
28. Cisco Networking Academy. Освітня платформа Cisco з курсами CCNA, мережевих технологій, маршрутизації та комутації. Дата звернення: 07.06.2026.
29. NetworkLessons.com. Практичні матеріали з налаштування маршрутизації, VLAN, STP, OSPF, BGP, VPN та мережевої безпеки. Дата звернення: 07.06.2026.
30. Катренко Л. А., Катренко А. В. Охорона праці в галузі комп'ютингу : підручник. Львів : Магнолія 2006, 2024. 544 с. ISBN 978-617-574-049-1.

ДОДАТКИ

Додаток А. Скрипт конфігурації комутатора доступу SW_1

```
# ================================================
# SW_1 — MikroTik CSS318-16G-2S+IN
# Роль: Комутатор доступу (верхній блок), підключений до SW_3
# Management IP: 192.168.10.11/24 (VLAN 10)
# VLAN 11 (stud1) — WS.1–WS.8 (порти 1-8)
# VLAN 11 (stud1) — WS.9, WS.10 (порти 9-10)
# VLAN 30 (work)   — S.1 (сервер, порт 11)
# Uplink до SW_3   — порт 17 (SFP+ ether17) — trunk
# ================================================

/interface bridge
add name=bridge1 vlan-filtering=yes comment="Main bridge SW_1"

# --- Додати всі фізичні порти до bridge ---
/interface bridge port
add bridge=bridge1 interface=ether1   pvid=11 comment="WS.1"
add bridge=bridge1 interface=ether2   pvid=11 comment="WS.2"
add bridge=bridge1 interface=ether3   pvid=11 comment="WS.3"
add bridge=bridge1 interface=ether4   pvid=11 comment="WS.4"
add bridge=bridge1 interface=ether5   pvid=11 comment="WS.5"
add bridge=bridge1 interface=ether6   pvid=11 comment="WS.6"
add bridge=bridge1 interface=ether7   pvid=11 comment="WS.7"
add bridge=bridge1 interface=ether8   pvid=11 comment="WS.8"
add bridge=bridge1 interface=ether9   pvid=11 comment="WS.9"
add bridge=bridge1 interface=ether10 pvid=11 comment="WS.10"
add bridge=bridge1 interface=ether11 pvid=30 comment="S.1 (server)"
add bridge=bridge1 interface=ether12 pvid=11 comment="reserve"
```

```
add bridge=bridge1 interface=sfp-sfpplus1 pvid=1 comment="Uplink -> SW_3
(trunk)"

# --- VLAN таблиця на bridge ---
/interface bridge vlan
# VLAN 10 — Management (tagged на uplink, щоб SW_3 міг керувати SW_1)
add bridge=bridge1 vlan-ids=10 tagged=bridge1,sfp-sfpplus1

# VLAN 11 — stud1 (untagged на access-портах, tagged на uplink)
add bridge=bridge1 vlan-ids=11 \

untagged=ether1,ether2,ether3,ether4,ether5,ether6,ether7,ether8,ether9,ether1
0,ether12 \
    tagged=sfp-sfpplus1

# VLAN 30 — work (untagged на S.1, tagged на uplink)
add bridge=bridge1 vlan-ids=30 \
    untagged=ether11 \
    tagged=sfp-sfpplus1

# --- Management VLAN interface ---
/interface vlan
add interface=bridge1 name=vlan10-mng vlan-id=10
/ip address
add address=192.168.10.11/24 interface=vlan10-mng comment="Management
SW_1"
/ip route
add dst-address=0.0.0.0/0 gateway=192.168.10.1 comment="Default GW via
SW_2"

# --- DNS ---
/ip dns
```

```
set servers=8.8.8.8,8.8.4.4

# --- NTP ---
/system ntp client
set enabled=yes server-dns-names=pool.ntp.org

# --- Системне ім'я ---
/system identity
set name=SW_1

# --- Пароль адміна (змінити!) ---
/user set admin password=StrongPass123

# --- SSH & Winbox ---
/ip service
set telnet     disabled=yes
set ftp        disabled=yes
set www        disabled=yes
set ssh        disabled=no port=22
set api        disabled=yes
set winbox     disabled=no port=8291
set api-ssl    disabled=yes

# --- SNMP (опціонально) ---
/snmp
set enabled=yes contact="admin" location="Building A, Floor 1"
```

Додаток Б. Скрипт конфігурації головного маршрутизатора шлюзу SW_2

```
# ================================================
# SW_2 — MikroTik hEX (RB750Gr3)
# Роль: Маршрутизатор/шлюз. Підключений до INTERNET та SW_3
# WAN: ether1 — підключення до Internet (DHCP або static)
# LAN uplink до SW_3: ether2 — trunk (VLAN 10,11,12,20,30,40)
# Management IP: 192.168.10.1/24 (VLAN 10) — шлюз усіх VLAN
# ================================================

# --- Bridge для LAN VLAN trunk до SW_3 ---
/interface bridge
add name=bridge-lan vlan-filtering=yes comment="LAN bridge to SW_3"

/interface bridge port
add bridge=bridge-lan interface=ether2 pvid=1 comment="Trunk uplink -> SW_3"
add bridge=bridge-lan interface=ether3 pvid=10 comment="reserve (access mgmt)"

# --- VLAN таблиця ---
/interface bridge vlan
add bridge=bridge-lan vlan-ids=10   tagged=bridge-lan,ether2
add bridge=bridge-lan vlan-ids=11   tagged=bridge-lan,ether2
add bridge=bridge-lan vlan-ids=12   tagged=bridge-lan,ether2
add bridge=bridge-lan vlan-ids=20   tagged=bridge-lan,ether2
add bridge=bridge-lan vlan-ids=30   tagged=bridge-lan,ether2
add bridge=bridge-lan vlan-ids=40   tagged=bridge-lan,ether2

# --- VLAN інтерфейси (SVI / Gateway для кожної підмережі) ---
```

```
/interface vlan
add interface=bridge-lan name=vlan10-mng     vlan-id=10
add interface=bridge-lan name=vlan11-stud1 vlan-id=11
add interface=bridge-lan name=vlan12-stud2 vlan-id=12
add interface=bridge-lan name=vlan20-fab     vlan-id=20
add interface=bridge-lan name=vlan30-work   vlan-id=30
add interface=bridge-lan name=vlan40-wifi   vlan-id=40

# --- IP адреси на VLAN інтерфейсах (шлюзи) ---
/ip address
add   address=192.168.10.1/24      interface=vlan10-mng         comment="GW
VLAN10 Management"
add    address=192.168.11.1/24       interface=vlan11-stud1    comment="GW
VLAN11 stud1"
add    address=192.168.12.1/24       interface=vlan12-stud2    comment="GW
VLAN12 stud2"
add   address=192.168.6.1/24        interface=vlan20-fab         comment="GW
VLAN20 fablob"
add   address=192.168.30.1/24      interface=vlan30-work       comment="GW
VLAN30 work"
add    address=192.168.40.1/24       interface=vlan40-wifi       comment="GW
VLAN40 wifi"

# --- WAN інтерфейс (ether1 — Internet) ---
# Варіант 1: DHCP від провайдера
/ip dhcp-client
add interface=ether1 disabled=no comment="WAN DHCP from ISP"

# Варіант 2: Статична адреса (розкоментуйте якщо потрібно):
# /ip address
# add address=X.X.X.X/YY interface=ether1 comment="WAN static"
```

```
# /ip route
# add dst-address=0.0.0.0/0 gateway=X.X.X.X comment="WAN default GW"

# --- NAT (Masquerade для виходу в Інтернет) ---
/ip firewall nat
add chain=srcnat out-interface=ether1 action=masquerade comment="Internet NAT"

# --- Базовий Firewall ---
/ip firewall filter
# Дозволити established/related
add chain=input action=accept connection-state=established,related comment="Accept established"
add chain=forward action=accept connection-state=established,related

# Дозволити доступ з LAN VLAN до Winbox/SSH
add chain=input action=accept src-address=192.168.10.0/24 comment="Allow mgmt VLAN to router"

# Дозволити ICMP
add chain=input action=accept protocol=icmp comment="Allow ICMP"

# Відкинути все інше із зовнішнього
add chain=input action=drop in-interface=ether1 comment="Drop from WAN"

# Заборонити stud VLAN доступ до роутера (крім шлюзу)
add chain=input action=drop src-address=192.168.11.0/24 dst-address=!192.168.11.1 comment="Deny stud1 to router"
add chain=input action=drop src-address=192.168.12.0/24 dst-address=!192.168.12.1 comment="Deny stud2 to router"
```

```
# --- DHCP сервери для кожної VLAN ---
/ip pool
add name=pool-stud1 ranges=192.168.11.20-192.168.11.254
add name=pool-stud2 ranges=192.168.12.20-192.168.12.254
add name=pool-work   ranges=192.168.30.20-192.168.30.254
add name=pool-wifi   ranges=192.168.40.20-192.168.40.254
add name=pool-fab    ranges=192.168.6.20-192.168.6.254
/ip dhcp-server
add name=dhcp-stud1 interface=vlan11-stud1 address-pool=pool-stud1
disabled=no lease-time=1d
add name=dhcp-stud2 interface=vlan12-stud2 address-pool=pool-stud2
disabled=no lease-time=1d
add name=dhcp-work interface=vlan30-work address-pool=pool-work
disabled=no lease-time=1d
add name=dhcp-wifi interface=vlan40-wifi address-pool=pool-wifi
disabled=no lease-time=8h
add name=dhcp-fab interface=vlan20-fab address-pool=pool-fab
disabled=no lease-time=1d
/ip dhcp-server network
add address=192.168.11.0/24 gateway=192.168.11.1 dns-server=8.8.8.8,8.8.4.4
comment="stud1"
add address=192.168.12.0/24 gateway=192.168.12.1 dns-server=8.8.8.8,8.8.4.4
comment="stud2"
add address=192.168.30.0/24 gateway=192.168.30.1 dns-server=8.8.8.8,8.8.4.4
comment="work"
add address=192.168.40.0/24 gateway=192.168.40.1 dns-server=8.8.8.8,8.8.4.4
comment="wifi"
add address=192.168.6.0/24 gateway=192.168.6.1 dns-
server=8.8.8.8,8.8.4.4 comment="fablob"


# --- DNS ---
```

```
/ip dns
set servers=8.8.8.8,8.8.4.4 allow-remote-requests=yes

# --- NTP ---
/system ntp client
set enabled=yes server-dns-names=pool.ntp.org

# --- Системне ім'я ---
/system identity
set name=SW_2-GW

# --- Безпека ---
/user set admin password=StrongPass123

/ip service
set telnet   disabled=yes
set ftp      disabled=yes
set www      disabled=yes
set ssh      disabled=no port=22
set api      disabled=yes
set winbox   disabled=no port=8291
set api-ssl disabled=yes
```

Додаток В. Скрипт конфігурації комутатора ядра та агрегації SW_3

```
# ================================================
# SW_3 — MikroTik CRS317-1G-16S+RM
# Роль: Core / Aggregation switch (L2)
# Management IP: 192.168.10.13/24 (VLAN 10)
#
# Порти (SFP+):
#    sfp-sfpplus1   -> SW_1 (trunk: VLAN 10,11,30)
#    sfp-sfpplus2   -> SW_2 (hEX, trunk: VLAN 10,11,12,20,30,40)
#    sfp-sfpplus3   -> SW_4 (trunk: VLAN 10,12,20,30)
#    sfp-sfpplus4   -> AP_1 (VLAN 40 access / tagged)
#    sfp-sfpplus5   -> AP_2 (VLAN 40 access / tagged)
#    ether1 (1G)    -> резерв/управління (access VLAN 10)
#
# Прямі підключення (мідь до sfp):
#    sfp-sfpplus6   -> WS.11   (VLAN 30 work)
#    sfp-sfpplus7   -> WS.12   (VLAN 30 work)
#    sfp-sfpplus8   -> WS.13   (VLAN 12 stud2)
#    sfp-sfpplus9   -> PR.1    (VLAN 30 work)
#    sfp-sfpplus10 -> PR.2     (VLAN 30 work)
# ================================================

/interface bridge
add name=bridge1 vlan-filtering=yes comment="Core bridge SW_3"

# --- Порти у bridge ---
/interface bridge port
# Uplink до SW_1
```

```
add bridge=bridge1 interface=sfp-sfpplus1 pvid=1 comment="Trunk -> SW_1"
# Uplink до SW_2 (router/GW)
add bridge=bridge1 interface=sfp-sfpplus2 pvid=1 comment="Trunk -> SW_2 (hEX)"
# Uplink до SW_4
add bridge=bridge1 interface=sfp-sfpplus3 pvid=1 comment="Trunk -> SW_4"
# AP_1 — Wi-Fi точка 1 (trunk VLAN 40, можливо 10)
add bridge=bridge1 interface=sfp-sfpplus4 pvid=40 comment="AP_1 (VLAN40 wifi)"
# AP_2 — Wi-Fi точка 2
add bridge=bridge1 interface=sfp-sfpplus5 pvid=40 comment="AP_2 (VLAN40 wifi)"
# WS.11 — work
add bridge=bridge1 interface=sfp-sfpplus6 pvid=30 comment="WS.11 (VLAN30 work)"
# WS.12 — work
add bridge=bridge1 interface=sfp-sfpplus7 pvid=30 comment="WS.12 (VLAN30 work)"
# WS.13 — stud2
add bridge=bridge1 interface=sfp-sfpplus8 pvid=12 comment="WS.13 (VLAN12 stud2)"
# PR.1 — принтер/пристрій work
add bridge=bridge1 interface=sfp-sfpplus9 pvid=30 comment="PR.1 (VLAN30 work)"
# PR.2 — принтер/пристрій work
add bridge=bridge1 interface=sfp-sfpplus10 pvid=30 comment="PR.2 (VLAN30 work)"
# ether1 — управління/резерв
```

```
add bridge=bridge1 interface=ether1 pvid=10 comment="Local mgmt
port (VLAN10)"

# --- VLAN таблиця ---
/interface bridge vlan

# VLAN 10 — Management
add bridge=bridge1 vlan-ids=10 \
    tagged=bridge1,sfp-sfpplus1,sfp-sfpplus2,sfp-sfpplus3 \
    untagged=ether1

# VLAN 11 — stud1 (між SW_1 і SW_2)
add bridge=bridge1 vlan-ids=11 \
    tagged=sfp-sfpplus1,sfp-sfpplus2

# VLAN 12 — stud2 (між SW_3, SW_4, SW_2)
add bridge=bridge1 vlan-ids=12 \
    untagged=sfp-sfpplus8 \
    tagged=sfp-sfpplus2,sfp-sfpplus3

# VLAN 20 — fablob (між SW_4 і SW_2)
add bridge=bridge1 vlan-ids=20 \
    tagged=sfp-sfpplus2,sfp-sfpplus3

# VLAN 30 — work
add bridge=bridge1 vlan-ids=30 \
    untagged=sfp-sfpplus6,sfp-sfpplus7,sfp-sfpplus9,sfp-sfpplus10 \
    tagged=sfp-sfpplus1,sfp-sfpplus2,sfp-sfpplus3

# VLAN 40 — wifi
add bridge=bridge1 vlan-ids=40 \
```

```
    untagged=sfp-sfpplus4,sfp-sfpplus5 \
    tagged=sfp-sfpplus2

# --- Management VLAN інтерфейс ---
/interface vlan
add interface=bridge1 name=vlan10-mng vlan-id=10

/ip address
add address=192.168.10.13/24 interface=vlan10-mng comment="Management SW_3"

/ip route
add dst-address=0.0.0.0/0 gateway=192.168.10.1 comment="Default GW via SW_2"

# --- DNS ---
/ip dns
set servers=8.8.8.8,8.8.4.4

# --- NTP ---
/system ntp client
set enabled=yes server-dns-names=pool.ntp.org

# --- Системне ім'я ---
/system identity
set name=SW_3-Core

# --- Безпека ---
/user set admin password=StrongPass123

/ip service
```

```
set telnet   disabled=yes
set ftp      disabled=yes
set www      disabled=yes
set ssh      disabled=no   port=22
set api      disabled=yes
set winbox   disabled=no   port=8291
set api-ssl disabled=yes

# --- Примітка для CRS317: використовуйте RouterOS, а не SwOS ---
# CRS317 підтримує повний RouterOS з bridge VLAN filtering
# Переконайтесь що boot device = RouterOS (не SwitchOS)
```

Додаток Г. Скрипт конфігурації комутатора доступу SW_4

```
# ================================================
# SW_4 — MikroTik CSS318-16G-2S+IN
# Роль: Комутатор доступу (нижній блок), підключений до SW_3
# Management IP: 192.168.10.14/24 (VLAN 10)
#
# Порти:
#    ether1    -> WS.14   (VLAN 12 stud2)
#    ether2    -> WS.15   (VLAN 12 stud2)
#    ether3    -> WS.16   (VLAN 12 stud2)
#    ether4    -> WS.17   (VLAN 30 work)
#    ether5    -> PR.3    (VLAN 30 work)
#    ether6-8 -> резерв
#    sfp-sfpplus1 -> Uplink до SW_3 (trunk)
#    sfp-sfpplus2 -> Downlink до SW_5 (trunk)
# ================================================

/interface bridge
add name=bridge1 vlan-filtering=yes comment="Main bridge SW_4"

/interface bridge port
add bridge=bridge1 interface=ether1  pvid=12 comment="WS.14 (VLAN12 stud2)"
add bridge=bridge1 interface=ether2  pvid=12 comment="WS.15 (VLAN12 stud2)"
add bridge=bridge1 interface=ether3  pvid=12 comment="WS.16 (VLAN12 stud2)"
add bridge=bridge1 interface=ether4  pvid=30 comment="WS.17 (VLAN30 work)"
```

```
add bridge=bridge1 interface=ether5 pvid=30 comment="PR.3 (VLAN30 work)"
add bridge=bridge1 interface=ether6 pvid=12 comment="reserve stud2"
add bridge=bridge1 interface=ether7 pvid=12 comment="reserve stud2"
add bridge=bridge1 interface=ether8 pvid=30 comment="reserve work"
# Uplink до SW_3 (core)
add bridge=bridge1 interface=sfp-sfpplus1 pvid=1 comment="Trunk uplink -> SW_3"
# Downlink до SW_5
add bridge=bridge1 interface=sfp-sfpplus2 pvid=1 comment="Trunk downlink -> SW_5"

# --- VLAN таблиця ---
/interface bridge vlan

# VLAN 10 — Management
add bridge=bridge1 vlan-ids=10 \
    tagged=bridge1,sfp-sfpplus1,sfp-sfpplus2

# VLAN 12 — stud2
add bridge=bridge1 vlan-ids=12 \
    untagged=ether1,ether2,ether3,ether6,ether7 \
    tagged=sfp-sfpplus1,sfp-sfpplus2

# VLAN 20 — fablob (проходить до SW_5)
add bridge=bridge1 vlan-ids=20 \
    tagged=sfp-sfpplus1,sfp-sfpplus2

# VLAN 30 — work
add bridge=bridge1 vlan-ids=30 \
    untagged=ether4,ether5,ether8 \
```

```
    tagged=sfp-sfpplus1,sfp-sfpplus2

# VLAN 40 — wifi (транзит через SW_4 до SW_5 якщо є AP)
add bridge=bridge1 vlan-ids=40 \
    tagged=sfp-sfpplus1,sfp-sfpplus2

# --- Management VLAN інтерфейс ---
/interface vlan
add interface=bridge1 name=vlan10-mng vlan-id=10

/ip address
add address=192.168.10.14/24 interface=vlan10-mng comment="Management
SW_4"

/ip route
add dst-address=0.0.0.0/0 gateway=192.168.10.1 comment="Default GW via
SW_2"

# --- DNS ---
/ip dns
set servers=8.8.8.8,8.8.4.4

# --- NTP ---
/system ntp client
set enabled=yes server-dns-names=pool.ntp.org

# --- Системне ім'я ---
/system identity
set name=SW_4

# --- Безпека ---
```

```
/user set admin password=StrongPass123


/ip service
set telnet   disabled=yes
set ftp      disabled=yes
set www      disabled=yes
set ssh      disabled=no   port=22
set api      disabled=yes
set winbox   disabled=no   port=8291
set api-ssl disabled=yes
```

Додаток Е. Скрипт конфігурації комутатора доступу нижнього рівня SW_5

```
# ================================================
# SW_5 — MikroTik CSS610-8G-2S+IN
# Роль: Комутатор доступу (малий, нижній рівень)
# Management IP: 192.168.10.15/24 (VLAN 10)
#
# Порти:
#   ether1    -> WS.18   (VLAN 12 stud2)
#   ether2    -> WS.19   (VLAN 12 stud2)
#   ether3    -> WS.20   (VLAN 12 stud2)
#   ether4    -> WS.21   (VLAN 20 fablob / tablab)
#   ether5    -> WS.22   (VLAN 30 work)
#   ether6    -> WS.23   (VLAN 30 work)
#   ether7    -> резерв
#   ether8    -> резерв
#   sfp-sfpplus1 -> Uplink до SW_4 (trunk)
#   sfp-sfpplus2 -> резерв
#
# Примітка: CSS610 підтримує SwOS або RouterOS (Lite).
# Нижче конфіг для RouterOS Lite (bridge VLAN filtering).
# Якщо SwOS — скористайтесь веб-інтерфейсом SwOS.
# ================================================

/interface bridge
add name=bridge1 vlan-filtering=yes comment="Main bridge SW_5"

/interface bridge port
add bridge=bridge1 interface=ether1  pvid=12 comment="WS.18 (VLAN12 stud2)"
```

```
add bridge=bridge1 interface=ether2  pvid=12 comment="WS.19 (VLAN12 stud2)"
add bridge=bridge1 interface=ether3  pvid=12 comment="WS.20 (VLAN12 stud2)"
add bridge=bridge1 interface=ether4  pvid=20 comment="WS.21 (VLAN20 fablob)"
add bridge=bridge1 interface=ether5  pvid=30 comment="WS.22 (VLAN30 work)"
add bridge=bridge1 interface=ether6  pvid=30 comment="WS.23 (VLAN30 work)"
add bridge=bridge1 interface=ether7  pvid=12 comment="reserve"
add bridge=bridge1 interface=ether8  pvid=12 comment="reserve"
# Uplink до SW_4
add bridge=bridge1 interface=sfp-sfpplus1 pvid=1 comment="Trunk uplink -> SW_4"

# --- VLAN таблиця ---
/interface bridge vlan

# VLAN 10 — Management
add bridge=bridge1 vlan-ids=10 \
    tagged=bridge1,sfp-sfpplus1

# VLAN 12 — stud2
add bridge=bridge1 vlan-ids=12 \
    untagged=ether1,ether2,ether3,ether7,ether8 \
    tagged=sfp-sfpplus1

# VLAN 20 — fablob (tablab)
add bridge=bridge1 vlan-ids=20 \
    untagged=ether4 \
```

```
    tagged=sfp-sfpplus1

# VLAN 30 — work
add bridge=bridge1 vlan-ids=30 \
    untagged=ether5,ether6 \
    tagged=sfp-sfpplus1

# --- Management VLAN інтерфейс ---
/interface vlan
add interface=bridge1 name=vlan10-mng vlan-id=10

/ip address
add address=192.168.10.15/24 interface=vlan10-mng comment="Management SW_5"

/ip route
add dst-address=0.0.0.0/0 gateway=192.168.10.1 comment="Default GW via SW_2"

# --- DNS ---
/ip dns
set servers=8.8.8.8,8.8.4.4

# --- NTP ---
/system ntp client
set enabled=yes server-dns-names=pool.ntp.org

# --- Системне ім'я ---
/system identity
set name=SW_5
```

```
# --- Безпека ---
/user set admin password=StrongPass123

/ip service
set telnet   disabled=yes
set ftp      disabled=yes
set www      disabled=yes
set ssh      disabled=no   port=22
set api      disabled=yes
set winbox   disabled=no   port=8291
set api-ssl disabled=yes

# ================================================
# АЛЬТЕРНАТИВА — SwOS конфігурація (якщо пристрій на SwOS)
# ================================================
# Завантажте SwOS через браузер: http://192.168.88.1 (default)
# VLAN Table:
#    Port 1 (ether1): VLAN 12 untagged
#    Port 2 (ether2): VLAN 12 untagged
#    Port 3 (ether3): VLAN 12 untagged
#    Port 4 (ether4): VLAN 20 untagged
#    Port 5 (ether5): VLAN 30 untagged
#    Port 6 (ether6): VLAN 30 untagged
#    Port 9 (sfp1):    VLAN 10,12,20,30 tagged (trunk)
# Management VLAN: 10, IP: 192.168.10.15/24
# ================================================
```

Додаток Ж. Скрипт конфігурації бездротової точки доступу AP_1

```
# ================================================
# Конфігурація точки доступу AP_1
# Пристрій: MikroTik cAP ac (RBcAPGi-5acD2nD)
# IP: 192.168.4.12 / 255.255.255.0
# VLAN: 40 (wifi)
# Підключення: SW_3
# ================================================

# --- Системна інформація ---
/system identity
set name="AP_1"

# --- Скидання конфігурації мостів (за потреби) ---
/interface bridge
add name=bridge-local protocol-mode=none

# --- VLAN-aware bridge для Wi-Fi трафіку ---
/interface bridge
set bridge-local vlan-filtering=yes

# --- Ethernet порт (PoE-uplink до SW_3) ---
/interface bridge port
add bridge=bridge-local interface=ether1 pvid=1

# --- Wireless 2.4 GHz ---
/interface wireless
set [ find default-name=wlan1 ] \
    band=2ghz-b/g/n \
```

```
        channel-width=20/40mhz-XX \
        disabled=no \
        distance=indoors \
        frequency=auto \
        mode=ap-bridge \
        ssid="OFFICE_WiFi" \
        wireless-protocol=802.11 \
        security-profile=wifi-security \
        vlan-id=40 \
        vlan-mode=use-tag

# --- Wireless 5 GHz ---
/interface wireless
set [ find default-name=wlan2 ] \
        band=5ghz-a/n/ac \
        channel-width=20/40/80mhz-XXXX \
        disabled=no \
        distance=indoors \
        frequency=auto \
        mode=ap-bridge \
        ssid="OFFICE_WiFi_5G" \
        wireless-protocol=802.11 \
        security-profile=wifi-security \
        vlan-id=40 \
        vlan-mode=use-tag

# --- Профіль безпеки Wi-Fi ---
/interface wireless security-profiles
add name=wifi-security \
        authentication-types=wpa2-psk \
        mode=dynamic-keys \
```

```
    wpa2-pre-shared-key="YourWiFiPassword123"

# --- Bridge VLAN ---
/interface bridge vlan
add bridge=bridge-local tagged=ether1,wlan1,wlan2 vlan-ids=40
add bridge=bridge-local tagged=ether1 vlan-ids=1

# --- VLAN-інтерфейс для управління ---
/interface vlan
add interface=ether1 name=vlan40-mgmt vlan-id=40

# --- IP-адреса управління ---
/ip address
add address=192.168.4.12/24 interface=vlan40-mgmt network=192.168.4.0

# --- Шлюз за замовчуванням ---
/ip route
add dst-address=0.0.0.0/0 gateway=192.168.4.1

# --- DNS ---
/ip dns
set servers=192.168.4.1 allow-remote-requests=no

# --- NTP клієнт ---
/system ntp client
set enabled=yes server-dns-names=pool.ntp.org

# --- Налаштування часового поясу ---
/system clock
set time-zone-name=Europe/Kiev
```

```
# --- DHCP-клієнт вимкнено (статична IP) ---
/ip dhcp-client
remove [ find interface=ether1 ]

# --- Firewall: заборонити доступ ззовні до управління ---
/ip firewall filter
add action=accept chain=input comment="Allow established connections" \
    connection-state=established,related
add action=accept chain=input comment="Allow management from LAN" \
    src-address=192.168.4.0/24
add action=drop chain=input comment="Drop all other input"

# --- Вимкнути непотрібні сервіси ---
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=no port=80
set ssh disabled=no port=22
set api disabled=yes
set winbox disabled=no port=8291
set api-ssl disabled=yes

# --- Winbox: ім'я для ідентифікації ---
/tool mac-server
set allowed-interface-list=none

/tool mac-server mac-winbox
set allowed-interface-list=all

# --- Вимкнути neighbor discovery назовні (опційно) ---
/ip neighbor discovery-settings
```

```
set discover-interface-list=none


# --- Логування ---
/system logging
add topics=wireless action=memory
add topics=error action=memory


# ================================================
# КІНЕЦЬ КОНФІГУРАЦІЇ AP_1
# ================================================
```

Додаток З. Скрипт конфігурації бездротової точки доступу AP_2

```
# ================================================
# Конфігурація точки доступу AP_2
# Пристрій: MikroTik cAP ac (RBcAPGi-5acD2nD)
# IP: 192.168.4.11 / 255.255.255.0
# VLAN: 40 (wifi)
# Підключення: SW_3
# ================================================

# --- Системна інформація ---
/system identity
set name="AP_2"

# --- Скидання конфігурації мостів (за потреби) ---
/interface bridge
add name=bridge-local protocol-mode=none

# --- VLAN-aware bridge для Wi-Fi трафіку ---
/interface bridge
set bridge-local vlan-filtering=yes

# --- Ethernet порт (PoE-uplink до SW_3) ---
/interface bridge port
add bridge=bridge-local interface=ether1 pvid=1

# --- Wireless 2.4 GHz ---
/interface wireless
set [ find default-name=wlan1 ] \
    band=2ghz-b/g/n \
    channel-width=20/40mhz-XX \
```

```
        disabled=no \
        distance=indoors \
        frequency=auto \
        mode=ap-bridge \
        ssid="OFFICE_WiFi" \
        wireless-protocol=802.11 \
        security-profile=wifi-security \
        vlan-id=40 \
        vlan-mode=use-tag

    # --- Wireless 5 GHz ---
    /interface wireless
    set [ find default-name=wlan2 ] \
        band=5ghz-a/n/ac \
        channel-width=20/40/80mhz-XXXX \
        disabled=no \
        distance=indoors \
        frequency=auto \
        mode=ap-bridge \
        ssid="OFFICE_WiFi_5G" \
        wireless-protocol=802.11 \
        security-profile=wifi-security \
        vlan-id=40 \
        vlan-mode=use-tag

    # --- Профіль безпеки Wi-Fi ---
    /interface wireless security-profiles
    add name=wifi-security \
        authentication-types=wpa2-psk \
        mode=dynamic-keys \
        wpa2-pre-shared-key="YourWiFiPassword123"
```

```
# --- Bridge VLAN ---
/interface bridge vlan
add bridge=bridge-local tagged=ether1,wlan1,wlan2 vlan-ids=40
add bridge=bridge-local tagged=ether1 vlan-ids=1

# --- VLAN-інтерфейс для управління ---
/interface vlan
add interface=ether1 name=vlan40-mgmt vlan-id=40

# --- IP-адреса управління ---
/ip address
add address=192.168.4.11/24 interface=vlan40-mgmt network=192.168.4.0

# --- Шлюз за замовчуванням ---
/ip route
add dst-address=0.0.0.0/0 gateway=192.168.4.1

# --- DNS ---
/ip dns
set servers=192.168.4.1 allow-remote-requests=no

# --- NTP клієнт ---
/system ntp client
set enabled=yes server-dns-names=pool.ntp.org

# --- Налаштування часового поясу ---
/system clock
set time-zone-name=Europe/Kiev

# --- DHCP-клієнт вимкнено (статична IP) ---
```

```
/ip dhcp-client
remove [ find interface=ether1 ]

# --- Firewall: заборонити доступ ззовні до управління ---
/ip firewall filter
add action=accept chain=input comment="Allow established connections" \
    connection-state=established,related
add action=accept chain=input comment="Allow management from LAN" \
    src-address=192.168.4.0/24
add action=drop chain=input comment="Drop all other input"

# --- Вимкнути непотрібні сервіси ---
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=no port=80
set ssh disabled=no port=22
set api disabled=yes
set winbox disabled=no port=8291
set api-ssl disabled=yes

# --- Winbox: ім'я для ідентифікації ---
/tool mac-server
set allowed-interface-list=none

/tool mac-server mac-winbox
set allowed-interface-list=all

# --- Вимкнути neighbor discovery назовні (опційно) ---
/ip neighbor discovery-settings
set discover-interface-list=none
```

```
# --- Логування ---
/system logging
add topics=wireless action=memory
add topics=error action=memory

# ================================================
# КІНЕЦЬ КОНФІГУРАЦІЇ AP_2
# ================================================
```