Форма № Н-9.02

Міністерство освіти і науки України

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

(повне найменування вищого навчального закладу)

Відділення інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра

(освітньо-професійного ступеня)

на тему: **Розробка проєкту комп'ютерної мережі ПП "СТО сорок"**

Виконав: студент IV курсу, групи КІ-412

Спеціальності 123 Комп'ютерна інженерія

(шифр і назва спеціальності)

_____ **Андрій ЦЯПУТА**

(ім'я та прізвище)

Керівник **Василь ПИЖ**

(ім'я та прізвище)

Рецензент _____

(ім'я та прізвище)

Тернопіль – 2026

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

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

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

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

Цяпуті Андрію Івановичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту комп'ютерної мережі ПП "СТО сорок"**

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

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

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

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

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Загальний розділ. Розробка технічного та робочого проєкту.

Спеціальний розділ. Економічний розділ. Охорона праці та безпека життєдіяльності.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

- план приміщень;
- фізична топологія мережі;
- логічна топологія;
- таблиця IP-адрес;
- таблиця техніко-економічних показників.

6. Консультанти розділів роботи

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

КАЛЕНДАРНИЙ ПЛАН

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

7. Дата видачі завдання: 31 березня 2026 року

Студент _____ Андрій ЦЯПУТА
(підпис) (ім'я та прізвище)

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

АНОТАЦІЯ

Цяпута А І. - Розробка проєкту комп’ютерної мережі ПП “СТО сорок”: кваліфікаційна робота на здобуття освітньо-професійного ступеня фахового молодшого бакалавра, за спеціальністю 123 Комп’ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2026. -78с.

У кваліфікаційній роботі представлено опис методології та всіх стадій проєктування комп’ютерної мережі на прикладі теми: «Розробка проєкту комп’ютерної мережі ПП «СТО сорок».

Метою дослідження є створення проєкту мережевої інфраструктури підприємства згідно з технічними вимогами, що забезпечить необхідну швидкість обміну даними, спільний доступ до ресурсів і вихід у глобальну мережу Інтернет.

У роботі обґрунтовано вибір мережевих технологій і топології, а також підібрано відповідне комутаційне обладнання.

У межах проєкту виконано детальний аналіз апаратних засобів, які застосовуються для розгортання сучасних обчислювальних мереж.

Розглянуто методику розрахунку кошторису на виконання робіт, а також висвітлено правила техніки безпеки під час монтажу й налаштування мережевих компонентів.

ABSTRACT

A. I. Tsiaputa - Development of a computer network project of the "STO Sorok" PE: qualifying work for obtaining an educational and professional degree of a professional junior bachelor, specialty 123 Computer engineering. Ternopil: VSP "TFC TNTU", 2026. -78p.

The qualification work presents a description of the methodology and all stages of designing a computer network using the example of the topic: "Development of a computer network project of the STO Sorok PE."

The purpose of the study is to create a project of the network infrastructure of the enterprise in accordance with the technical requirements, which will ensure the necessary speed of data exchange, shared access to resources and access to the global Internet.

The work substantiates the choice of network technologies and topology, as well as selects the appropriate switching equipment. Within the scope of the project, a detailed analysis of the hardware used to deploy modern computer networks was performed.

The method of calculating the estimate for the performance of works is considered, as well as the safety rules during the installation and configuration of network components are highlighted.

ЗМІСТ

					2026.КВР.123.412.14.00.00 ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Цяпута А І			Розробка проєкту комп'ютерної мережі ПП "СТО сорок" Пояснювальна записка	Літ.	Арк. / Аркушів
Перевір.		Пиж В С					
Реценз.						ВСП ТФК ТНТУ КІ-412 м. Тернопіль	
Н. Контр.							
Затверд.							

ВСТУП

У теперішній час власна ІТ-інфраструктура є невіддільною частиною функціонування більшості організацій, офісів та життєдіяльності приватних осіб. Зокрема, на базі типового офісу робоче місце кожного працівника зазвичай оснащене персональним комп’ютером або ноутбуком, а також допоміжними мобільними гаджетами — смартфонами й планшетами. Подібна тенденція простежується і на побутовому рівні, де до цифрового простору змалечку залучаються навіть діти.

Процес об’єднання всіх наявних пристроїв у межах квартири, офісного приміщення чи установи навколо єдиної бездротової точки доступу Wi-Fi фактично знаменує собою створення базової локальної мережі. Проте функціонал такої структури не обмежується лише наданням доступу до глобальної мережі. У межах підприємств локальні обчислювальні мережі (ЛОМ) розгортаються насамперед для централізованого керування інформаційними ресурсами та організації розмежованого доступу співробітників до корпоративних даних.

Правильна архітектура та професійне налаштування ЛОМ дозволяють суттєво модернізувати бізнес-процеси, підвищити якість менеджменту, оптимізувати моніторинг діяльності персоналу та зміцнити контур інформаційної безпеки. Водночас інтеграція локальної мережі не завжди є виправданою, зокрема для суб'єктів малого підприємництва, які мають обмежений бюджет на розвиток ІТ.

Впровадження локальної мережі виступає раціональним кроком для підвищення ефективності роботи компанії. Найпростіший її варіант можна побудувати навіть для двох робочих станцій за допомогою провідного або бездротового каналу зв'язку. За своєю суттю ЛОМ є комплексною інформаційною системою, що перебуває у власності конкретного суб’єкта господарювання. Ключове призначення цієї інфраструктури полягає у забезпеченні повного життєвого циклу даних: їх генерації, збереження, модифіка-

ції, захисту та утилізації. Разом з тим критично важливо досягти балансу між раціональним розподілом ресурсів, швидкістю отримання потрібних відомостей та високим рівнем безпеки комерційної та особистої інформації.

Функціонування мережевого середовища суттєво полегшує інформаційний обмін та інтенсифікує внутрішні операції, що безпосередньо конвертується у зростання загальної продуктивності праці. У корпоративному секторі нерідко застосовуються однорангові (розподілені) мережі, де кожна робоча станція має однакові права, а єдиний керуючий вузол відсутній. За такої конфігурації користувачі в індивідуальному порядку визначають рівень доступу інших учасників до власних локальних ресурсів.

Іншим варіантом є впровадження архітектури «клієнт-сервер», де функції адміністрування та координації покладаються на виділений комп’ютер (сервер). Саме він здійснює централізований контроль за розподілом прав доступу, що дозволяє гнучко й безпечно керувати інформаційними потоками всередині підприємства.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Тематика цієї кваліфікаційної роботи присвячена проєктуванню та розгортанню комп’ютерної мережі для приватного підприємства «СТО сорок».

Розроблювана мережева інфраструктура має гарантувати високу пропускну здатність інформаційного обміну між робочими станціями (на рівні до 1000 Мбіт/с). Це дозволить забезпечити стабільний і швидкий доступ користувачів до розподілених корпоративних ресурсів, зокрема до мережевих сховищ даних (NAS), розташованих на виділеному сервері.

Для побудови надійної архітектури зв'язку передбачено впровадження сучасних і завадостійких середовищ передавання сигналів. Основними компонентами кабельної системи підприємства стануть мідні кабелі типу «вита пара» та волоконно-оптичні лінії зв’язку, які на сьогодні є стандартами де-факто під час створення локальних обчислювальних мереж.

Невіддільним елементом проєкту є організація захищеного шлюзу до глобальної мережі Інтернет із подальшим збалансованим розподілом трафіка між усіма клієнтськими пристроями компанії.

Створювана інфраструктура покликана забезпечити комплекс таких ключових переваг:

– максимальну пропускну здатність та інтенсивність обміну даними між мережевими вузлами;

– порівняно високу швидкість та економічність процесів монтажу й конфігурування обладнання;

– оптимальний рівень складності під час безпосереднього впровадження технологій передавання інформації;

– можливість подальшого масштабування та інтеграції з іншими високопродуктивними мережевими архітектурами.

1.1.2 Призначенння розробки

Розроблювана комп’ютерна мережа призначена для забезпечення ефективної та координованої діяльності всіх структурних підрозділів ПП «СТО сорок», що функціонує у сфері правових послуг.

До створеної мережевої інфраструктури висуваються такі базові вимоги:

– надання високошвидкісного та відмовостійкого доступу до корпоративних файлів, внутрішніх сервісів і публічних інформаційних масивів;

– організація системи мережевого друку для оперативного виготовлення паперових копій документів;

– гарантування безперебійного підключення до глобальної мережі Інтернет для всього персоналу установи;

– використання високошвидкісних каналів зв'язку із пропускною здатністю на рівні 100/1000 Мбіт/с.

– інтенсифікація електронного документообігу та оптимізація взаємодії між різними відділами підприємства.

Архітектура мережі розрахована виключно на корпоративне (офісне) застосування, яке охоплює міжузловий обмін даними, роботу з веб-ресурсами, сумісне використання периферійного обладнання (зокрема принтерів та БФП) і підтримку єдиного інформаційного простору.

Окрему увагу в проєкті приділено питанням інформаційної безпеки та захисту даних. Передбачено комплекс заходів для запобігання несанкціонованому втручанню в роботу системи як з боку внутрішніх користувачів, так і від зовнішніх загроз із глобальної мережі. Реалізація цього завдання покладається на механізми суворої автентифікації користувачів за допомо-

гою парольних політик, а також на впровадження моделі розмежування прав доступу до конфіденційної та службової інформації.

1.1.3 Вимоги до апаратного та програмного забезпечення

Для створення оптимальних умов роботи підприємства проєктована мережа має відповідати таким критеріям:

– Структуризація: поділ інфраструктури на логічні робочі групи для ефективного керування доступом до ресурсів.

– Пропускна здатність: підтримка швидкості передавання даних на рівні 100/1000 Мбіт/с для забезпечення стабільної роботи всіх сервісів.

– Доступність обладнання: використання поширених на ринку апаратних компонентів із оптимальним співвідношенням ціни та надійності.

– Ефективність апаратної частини: мережеві пристрої (активне обладнання) мають бути економічно вигідними, підтримувати цільову швидкість, легко піддаватися ремонту чи заміні та підтримувати централізоване адміністрування.

– Програмне забезпечення: використання клієнтських мережевих операційних систем Windows 11 на робочих станціях персоналу.

– Бездротовий зв'язок: захист бездротового сегмента за допомогою протоколів безпеки WPA-PSK / WPA2-PSK та підтримка стандарту IEEE 802.11n.

– Архітектура та сервери: побудова мережі на базі некерованих комутаторів для робочих груп та одного керованого комутатора для ядра мережі. Додатково передбачено розгортання окремого файлового сервера та виділеного ПК для бухгалтерського софту.

1.1.4 Стадії та етапи розробки

Проєктування інфраструктури та підготовка документації є критично важливими для стабільної роботи мережі. Спрощений підхід без креслень припустимий лише для мінімальних конфігурацій (наприклад, з двох ПК), тоді як складні системи вимагають повного пакета проєктних рішень.

Процес розробки складається з таких послідовних етапів:

1. Передпроєктне дослідження та огляд території. Передбачає багаторівневий аналіз майбутньої мережі:

– Фізичний рівень: кабельне господарство, крос-панелі, монтажні шафи та стійки;

– Канальний рівень: комутатори, архітектура ЛОМ та внутрішньомережеві протоколи;

– Мережевий рівень: маршрутизація, IP-адресація, шлюзи та вихід в Інтернет;

– Програмний рівень: мережеве ПЗ, СУБД, проксі-сервери тощо.

2. Аналіз завдань і трафіка. Визначення функціональних вимог до мережі, оцінка інтенсивності й напрямків потоків даних, розміщення користувачів і ресурсів, а також розробка політик безпеки та аудиту наявної інфраструктури будівлі.

3. Технічне проєктування інфраструктури. Основна стадія, що включає:

– розробку структурованої кабельної системи (СКС);

– план розміщення та комутації активного й пасивного обладнання;

– вибір конкретних апаратних засобів;

– конфігурування магістральних каналів і зовнішньої маршрутизації;

– розрахунок адресного простору (IP-плану) та параметрів мережевих сервісів.

4. Підбір програмного забезпечення. Вибір серверних і клієнтських операційних систем, платформ моніторингу, захисту та адміністрування відповідно до архітектурних вимог підприємства.

1.1.5 Вимоги до документації

Мережева документація (зокрема кабельний журнал) є критично важливою для мінімізації часу простою інфраструктури, ліквідації аварій та забезпечення безпеки.

Вона виконує три ключові функції:

– Діагностика: слугує інструкцією для швидкого пошуку й усунення несправностей.

– Адаптація: прискорює ознайомлення нового персоналу з архітектурою ЛОМ.

– Аутсорсинг: оптимізує витрати часу та коштів під час залучення зовнішніх IT-консультантів.

Незалежно від специфіки підприємства, стандартний пакет документації містить:

1. Топологію мережі: схематичне зображення взаємозв'язків між ядрами мережі (роутери, комутатори, фаєрволи, сервери) без деталізації кінцевих ПК.

2. Паспорт серверів: системні імена, IP-адреси, ролі, конфігурація дискових масивів, версії ОС та гарантійні дані.

3. Комутаційну карту: схему розподілу портів активного обладнання, налаштування WAN/VLAN та кросування на патч-панелях.

4. Параметри сервісів: конфігурацію базових служб інфраструктури (DNS, DHCP, RAS тощо).

5. Політики доменів: налаштування безпеки, прав доступу та конфігурацію мережевих профілів користувачів.

6. Реєстр критичного ПЗ: перелік бізнес-додатків із інструкціями щодо їх підтримки та відновлення.

7. Регламенти: правила парольної та фізичної безпеки, налаштування брандмауерів, процедури ТО серверів та обробки заявок.

Для детального опису ліній зв'язку до журналу обов'язково вносять:

– IP-адресу або ідентифікатор каналу;

– вендора обладнання та опис кінцевих пристроїв на обох вузлах з'єднання;

– топологію траси («точка-точка») із зазначенням точок вводу в будівлю;

– тип середовища передавання (мідь, оптика, радіоканал);

– контакти провайдера та ПІБ відповідального співробітника.

1.1.6 Техніко-економічні показники

Проєктована мережева інфраструктура має відповідати таким технічним та експлуатаційним критеріям:

– Економічна ефективність: використання актуальних технологій для досягнення максимальної продуктивності за мінімальних капіталовкладень.

– Висока пропускна здатність: підтримання швидкісних режимів 100/1000 Мбіт/с для інтенсифікації внутрішнього обміну даними.

– Масштабованість та модульність: архітектура ЛОМ повинна забезпечувати швидке підключення нових вузлів і гнучку адаптацію до структурних змін підприємства без значних витрат.

– Глобальна інтеграція: організація безперешкодного та збалансованого доступу до мережі Інтернет для всього персоналу.

– Мобільність сегментів: розгортання бездротової мережі Wi-Fi для забезпечення зручного зв'язку мобільних пристроїв співробітників та готівкових клієнтів.

– Інформаційна безпека: впровадження сучасних протоколів шифрування й автентифікації для захисту конфіденційних даних від несанкціонованого доступу.

– Централізований менеджмент: інтеграція засобів моніторингу для оперативного адміністрування, виявлення та усунення мережевих інцидентів.

– Зворотна сумісність: гарантування коректної інтеграції нових рішень із наявним парком комп'ютерного та периферійного обладнання.

– Відмовостійкість: висока надійність системи та здатність до швидкого самовідновлення після апаратних чи програмних збоїв.

1.1.7 Порядок контролю та прийому

Після завершення монтажу ЛОМ виконавець проводить комплексний аудит системи. Його результатом є звіт із фіксацією дефектів та рекомендаціями щодо оптимізації, ремонту чи модернізації інфраструктури.

Приймальне тестування та аудит мережі вирішують такі завдання:

– Локалізація несправностей: визначення причин нестабільної роботи (на боці провайдера чи обладнання) та вирішення технічних конфліктів.

– Метрологічний контроль: оцінка реальної швидкості, затримок і пропускної здатності каналів.

– Менеджмент витрат: оптимізація бюджету на технічне обслуговування.

– Модернізація: збір вихідних даних перед модернізацією та оцінка її фінальної ефективності.

– Відчуження системи: аудит інфраструктури перед передачею новому персоналу чи IT-аутсорсингу.

Об'єктами суцільної діагностики є: активне обладнання (роутери, комутатори, точки доступу), сервери, канали зв'язку, мережеве ПЗ та периферійні пристрої.

Сам процес технічного аудиту та здачі системи складається з трьох ключових блоків:

1. Аналіз документації: перевірка наявної та формування нової виконавчої техдокументації відповідно до реальної конфігурації.

2. Інструментальна перевірка працездатності:

– візуальний огляд, контроль стану кабельних трас та коректності маркування;

– аналіз відповідності ЛОМ стандартам, оцінка конфігурації пристроїв та Wi-Fi;

– проведення стрес-тестування, тестів на проникнення (pentest) та оцінка відмовостійкості.

3. Введення в експлуатацію: підрядник письмово сповіщає замовника про готовність і надає погоджений пакет документів. Замовник протягом 5 днів створює профільну комісію для приймання мережі, за результатами роботи якої підписується фінальний Акт введення ЛОМ в експлуатацію.

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

Метою цієї кваліфікаційної роботи є розробка проєкту комп’ютерної мережі, що об’єднає в єдину інфраструктуру всі робочі станції компанії. Організація спеціалізується на наданні комплексних юридичних послуг фізичним та юридичним особам у сферах цивільного, господарського, адміністративного та трудового права. Основні бізнес-процеси компанії охоплюють представництво інтересів клієнтів у судах, правову експертизу й розробку договорів, реєстрацію та ліквідацію бізнесу, супровід угод із нерухомістю, а також комплексний правовий аудит підприємств (due diligence). Діяльність фірми вимагає високої оперативності та суворого дотримання адвокатської таємниці й конфіденційності.

Комп'ютерне обладнання персоналу буде розміщене у трьох робочих залах та кабінеті керівника. Для концентрації мережевих ресурсів та зведення всіх комунікаційних ліній у проєкті передбачено організацію виділеного приміщення серверної кімнати.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЄКТУ

2.1 Розробка та обґрунтування логічної та фізичної схем мережі

Під час проєктування архітектури сучасних локальних обчислювальних мереж (ЛОМ) фундаментальним етапом є вибір геометричного та логічного способу взаємозв'язку робочих станцій, тобто мережевої топології. У телекомунікаційній інженерії виділяють три класичні базові конфігурації: шинну (bus), кільцеву (ring) та радіальну, відому як «зірка» (star). Кожна з цих моделей характеризується унікальними інженерними та структурними паттернами, безпосередньо впливає на логіку комутації кадрів, розподіл пропускної здатності, стійкість до відмов та загальну продуктивність системи.

У реальних проєктах, орієнтованих на стандарти Ethernet (IEEE 802.3), для досягнення компромісу між капітальними витратами (CAPEX) та технічними характеристиками часто інтегрують гібридні (комбіновані) архітектурні рішення. Це дозволяє нівелювати системні недоліки однієї топологічної моделі за рахунок переваг іншої. Графічне представлення базових топологічних схем, що відображає архітектуру фізичних з'єднань між мережевими інтерфейсами, наведено нижче (див. Рис. 2.1–2.3).

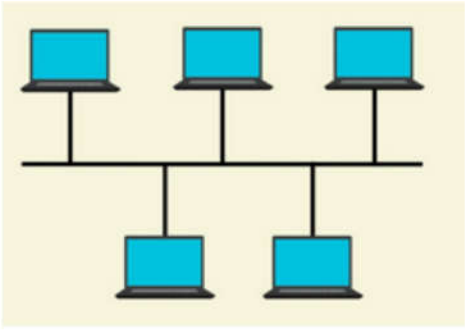


Рисунок 2.1 – Топологія типу шина

Топологія типу «шина» (див. рис. 2.1) історично відноситься до першим архітектурним концепціям побудови розподілених систем збору та обробки даних. Конструктивно вона є моноканалом — єдиною магістральною лінією передавання сигналів, до якої паралельно за допомогою Т-конекторів або відгалужень підключаються всі мережеві вузли (сервери, робочі станції, периферія). Ця топологія сформувала технологічний фундамент для ранніх специфікацій сімейства Ethernet, зокрема 10BASE-5 («товстий» коаксіальний кабель RG-8) та 10BASE-2 («тонкий» коаксіальний кабель RG-58).

З погляду передавання сигналів, шина функціонує в режимі напівдуплексу (Half-Duplex) у загальному домені колізій. Будь-який інформаційний кадр, згенерований мережевим адаптером вузла, дифузно поширюється в обидва боки магістралі, стаючи доступним для детектування всіма фізичними інтерфейсами мережі. Кожна робоча станція самостійно аналізує заголовок кадру (MAC-адресу одержувача) для ухвалення рішення про його подальший запуск у стек протоколів ОС або ігнорування.

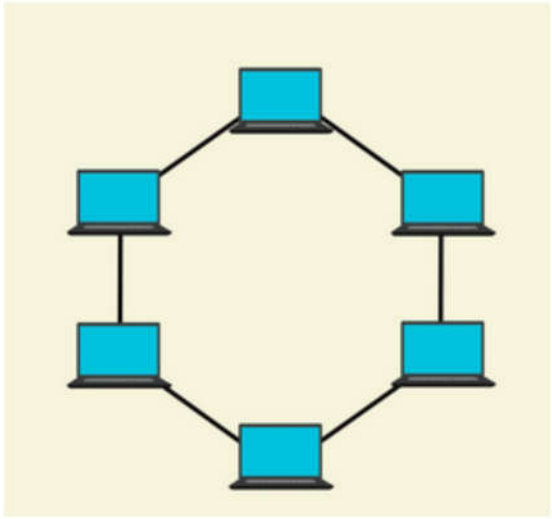


Рисунок 2.2 – Топологія типу кільце

Стабільність такої системи вимагає жорсткої координації доступу до фізичного середовища, регламентації довжини кабельних сегментів та обов'язкового встановлення термінаторів (узгоджених опорів, зазвичай на 50

Ом) на кінцях лінії для поглинання сигналів та запобігання їхнього відбиття. Для мінімізації конфліктів у спільному каналі використовується метод множинного доступу з контролем носійної та виявленням колізій — CSMA/CD. У сучасних ЛОМ шина у чистому вигляді практично не застосовується через критично низьку відмовостійкість (обрив кабелю паралізує всю мережу) та обмежену масштабованість, проте її логічні принципи закладені в основу багатьох промислових шин (CAN, Modbus) та бездротових технологій.

Топологія типу «кільце» (див. рис. 2.2) характеризується послідовним з'єднанням активних вузлів за замкненим контуром, де вихідний порт попереднього мережевого адаптера підключається до вхідного порту наступного. Трансляція пакетів здійснюється виключно в одному напрямку. Проходячи крізь кожен вузол, цифровий сигнал регенерується та очищується від фазових джиттерів, що дозволяє будувати мережі значної протяжності без втрати амплітуди імпульсів.

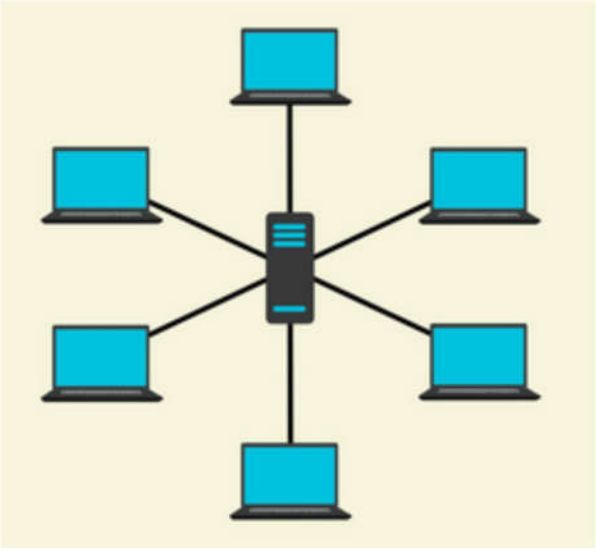


Рисунок 2.3 – Топологія типу зірка

Топологія типу «зірка» (див. рис. 2.3) на сьогодні є домінуючим галузевим стандартом під час розгортання локальних мереж будівель та офісів юрфірм. Її архітектурна суть полягає в тому, що кожна робоча станція або

сервер підключається окремим ізольованим променем (кабелем) безпосередньо до центрального комутаційного вузла. Раніше у ролі такого центру виступали пасивні багатопортові повторювачі — концентратори (хаби), які просто копіювали сигнал з одного порту на всі інші, створюючи єдиний домен колізій.

Сучасні рішення базуються виключно на багатопортових інтелектуальних пристроях — комутаторах (світчах L2/L3). Комутатор аналізує таблицю MAC-адрес і виконує адресне пересилання кадрів (Unicast) між конкретними портами. Це забезпечує повнодуплексний режим (Full-Duplex) роботи на швидкостях 100/1000 Мбіт/с та вище, повністю ізолюючи домени колізій для кожного окремого порту. Зіркова топологія має найвищий рівень експлуатаційної гнучкості: пошкодження лінії до одного з ПК ніяк не впливає на роботу інших користувачів, а діагностика несправностей зводиться до аналізу стану портів комутатора. Єдиною вразливою точкою (Single Point of Failure) є сам центральний комутатор, що вирішується шляхом дублювання обладнання та агрегації ліній зв'язку.

На практиці архітектура великих офісних мереж рідко обмежується однією базовою топологією. Найчастіше розробники використовують комбінований підхід, створюючи ієрархічні структури типу «дерево» (ієрархічна зірка) або комбінацію «зірка-шина» та «зірка-кільце».

Яскравим історичним та інженерним прикладом є технологія Token Ring. Фізично вона монтувалася за топологією «зірка»: усі кабелі від робочих станцій сходилися в центральні модулі багатостанційного доступу — MAU (Multistation Access Unit). Проте внутрішня мікросхема та релейна логіка самого MAU послідовно з'єднувала порти між собою, утворюючи замкнене логічне кільце. Таким чином досягалася висока надійність зірки (при вимкненні ПК модуль МАУ просто закорочував порт, не розриваючи мережу) при збереженні безколізійного маркерного доступу кільця.

Для проєкту мережі юридичної фірми, де розгортається сучасна інфраструктура Ethernet на базі структурованої кабельної системи (СКС) категорії

5е або 6, оптимальним вибором є топологія «розширена зірка». Робочі станції трьох залів та кабінету керівника утворюють локальні зірки, підключаючись до комутаторів доступу, які, своєю чергою, підключені до центрального комутатора ядра в серверній кімнаті. Це гарантує максимальну пропускну здатність 1 Гбіт/с для швидкого доступу до юридичних баз даних та файлового сервера компанії.

Порівняльна характеристика мережевих топологій наведена в таблиці 2.1

Таблиця 2.1 Порівняльна характеристика основних топологій:

Параметр порівняння	Топологія «Шина» (Bus)	Топологія «Кільце» (Ring)	Топологія «Зірка» (Star)
1	2	3	4
Складність проєктування та монтажу	Дуже низька; вимагає прокладання одного магістрального кабелю.	Середня; потребує послідовного закільцювання всіх вузлів.	Вища; вимагає прокладання окремої лінії зв'язку від кожного ПК до центру.
Витрати на кабельну інфраструктуру	Мінімальні (один загальний провід).	Низькі/Середні (залежно від геометрії приміщення).	Максимальні (великі витрати витої пари або оптики).
Потреба в активному обладнанні	Відсутня (підключення через пасивні Т-конектори).	Мінімальна (у класичному варіанті) або середня (при використанні MAU).	Висока (обов'язкова наявність комутаторів або маршрутизаторів).
Відмовостійкість (надійність)	Низька; будь-який обрив або відсутність термінатора руйнує	Низька; вихід з ладу одного вузла чи кабелю розриває контур зв'язку.	Висока; аварія на лінії одного користувача ізолюється і не впливає на

Продовження таблиці 2.1

1	2	3	4
	всю мережу.		інших.
Масштабованість (додавання нових ПК)	Обмежена; потребує розрізання магістралі, що тимчасово зупиняє роботу ЛОМ.	Середня; додавання вузла вимагає розриву кільця та перенаштування.	Відмінна; новий пристрій легко підключається до вільного порту комутатора.

Кабельна підсистема є фізичним фундаментом структурованої кабельної системи (СКС) підприємства, що визначає середовище передавання сигналів, завадостійкість та потенціал масштабованості мережі. Для побудови сучасних офісних ЛОМ, зокрема в інфраструктурі юридичних фірм, де пріоритетом є висока надійність та захист даних, базовим рішенням є використання чотирипарного мідного кабелю типу «вита пара» (Twisted Pair). Найчастіше застосовуються кабелі категорій Cat 5e або Cat 6 у неекранованому (UTP) або екранованому (FTP) виконанні. Останній забезпечує додатковий захист від зовнішніх електромагнітних завад і наведень.

Логічна архітектура та швидкісні характеристики такого середовища регламентуються стандартами Fast Ethernet (сімейство специфікацій IEEE 802.3u), які забезпечують пропускну здатність на рівні 100 Мбіт/с. Фізична реалізація Fast Ethernet у межах робочих залів та кабінетів найчастіше базується на двох ключових стандартах:

– 100BASE-TX: використовує дві пари провідників кабелю UTP/STP категорії 5 і вище. Максимальна довжина кабельного сегмента від комутатора до робочої станції обмежена стандартом і становить 100 метрів (90 метрів лінійної частини СКС + 10 метрів на патч-корди). Комунікація здійснюється у повнодуплексному режимі (Full-Duplex) завдяки розділенню ліній прийому (RX) та передачі (TX).

– 100BASE-FX: волоконно-оптичний стандарт, що використовує багатомодовий (MMF) або одномодовий (SMF) кабель. Застосовується переважно для організації магістральних вертикальних каналів (Up-link) між комутаційними шафами або для підключення віддалених серверів на відстанях від 2 до 40 км, гарантуючи повну гальванічну розв'язку та абсолютну захищеність від перехоплення інформації.

Кабельна підсистема Fast Ethernet є зворотно сумісною із технологією Gigabit Ethernet, яку ми оберемо для нашої роботи, що дозволяє без модернізації пасивної кабельної мережі перейти на гігабітні швидкості шляхом простої заміни активного обладнання (комутаторів та мережевих адаптерів).

Схема розведення кабелю 100BaseTX показана на рисунку 2.4

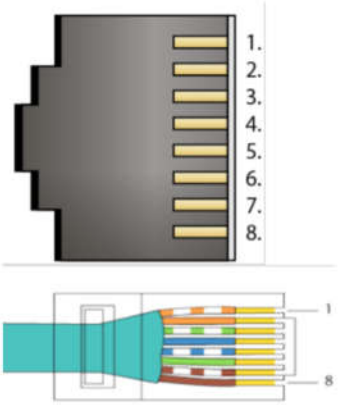


Рисунок 2.4 – Зображення розєму RJ45 та схема стандарту T568

Враховуючи специфіку функціонування юридичної фірми, вимоги до відмовостійкості та необхідність забезпечення високої пропускної здатності для роботи з корпоративними базами даних, для реалізації проєкту обрано гібридну (комбіновану) топологію. Вона поєднує в собі переваги ієрархічної зірки (розширеної зірки) для провідного сегмента та комірчастої топології (Mesh) для бездротової мережі Wi-Fi. Фізичним середовищем передавання обрано чотирипарний кабель «вита пара» категорії 5e (Cat 5e), а базовою

технологією — 1000BASE-T (Gigabit Ethernet), що гарантує швидкість обміну даними до 1_000 Мбіт/с.

Для побудови обраної комбінованої архітектури передбачено таку схему використання активного обладнання:

– Центральний вузол (Ядро мережі): встановлюється головний керований комутатор другого або третього рівня (L2/L3) на 16 портів. Він забезпечуватиме агрегацію трафіка, маршрутизацію між підмережами та централізоване керування всією інфраструктурою.

– Сегменти робочих груп: для підключення кінцевих пристроїв у трьох робочих залах та кабінеті керівника застосовуються комутатори рівня доступу. Зважаючи на економічну доцільність, обрано некеровані комутатори на 16 портів.

– Бездротовий сегмент: для організації Mesh-топології (комірчастої структури) вибирається сучасна бездротова точка доступу з підтримкою безшовного роумінгу, що забезпечить стабільне покриття для співробітників та клієнтів фірми.

Конструктивно від кожного комутатора робочої групи прокладаються окремі високошвидкісні аплінки (Up-link) до центрального керованого комутатора в серверній кімнаті.Така схема нівелює ризик утворення петель та оптимізує розподіл трафіка. Детальний опис та розподіл логічної топології проєктуємої мережі, а також параметри адресації й підключення обладнання наведено в таблицях 2.2 та 2.3.

Таблиця 2.3 – Логічна адресація в мережі

Позначення вузлів	Назва робочої групи	Кількість вузлів	Назва приміщення	Номер VLAN	Адреса підмережі / Маска
1	2	3	4	5	6
WS_1	Юристи-1	6	Робочий зал	100	192.168.100.0 /24

Продовження таблиці 2.3

1	2	3	4	5	6
— WS_6			№1		
WS_7 — WS_12	Юристи-2	6	Робочий зал №2	101	192.168.101.0 /24
WS_13 — WS_18	Юристи-3	6	Робочий зал №3	102	192.168.102.0 /24
WS_19 — WS_21	Керівництво	3	Кабінет керівника	103	192.168.103.0 /24
AP_1	Бездротова мережа	1	Коридор / Клієнт-зона	200	192.168.200.0 /24
SRV_1 (WS_22)	Адміністрування	1	Серверна кімната	300	192.168.60.0 /24
R_1	Адміністрування	1	Серверна кімната		192.168.0.0 /16

Таблиця 2.4 - Таблиця конфігурування VLAN

№ п/п	Назва пристрою	Номер порту	Тип (режим) порту	Назва підключеного пристрою або групи	Відданий порт	Цільовий VLAN / Дозволені VLAN (у режимі Trunk)
1	2	3	4	5	6	7
1	SW_1	1	Trunk	маршрутизатор	LAN 1	100, 101, 102,

Продовження таблиці 2.4

1	2	3	4	5	6	7
				(RTR_1)		103, 200, 300
2	SW_1	2 — 4	Access	Комп'ютери керівництва (WS_19 — WS_21)	NIC	103
3	SW_1	5 — 10	Резерв	Вільні порти для розширення ЛОМ	—	—
4	SW_1	11	Trunk	Комутатор доступу Робочого залу №1 (SW_2)	16	100, 101, 102, 103, 200, 300
5	SW_1	12	Trunk	Комутатор доступу Робочого залу №2 (SW_3)	16	100, 101, 102, 103, 200, 300
6	SW_1	13	Trunk	Комутатор доступу Робочого залу №3 (SW_4)	16	100, 101, 102, 103, 200, 300
7	SW_1	14	Access	Виділений файловий сервер фірми (SRV_1)	NIC	300
8	SW_1	15	Access	Бездротова точка доступу Wi-Fi (AP_1)	LAN	200

2.2 Обґрунтування вибору комунікаційного обладнання

Для практичної реалізації проєктованої комп'ютерної мережі фірми необхідно підібрати апаратні компоненти, що відповідатимуть критеріям продуктивності, надійності та економічної доцільності.

Розрахунок специфікації обладнання передбачає розгортання двох комутаторів рівня доступу (для кожної робочої групи в залах №1, №2), одного центрального керованого комутатора ядра мережі, а також бездротової точки доступу для забезпечення клієнтської Mesh-зони.

Наступним кроком є вибір комутаторів рівня доступу (SW_2, SW_3). Згідно з технічним завданням, ці пристрої мають бути некерованими, оснащеними 16 портами з підтримкою технології Gigabit Ethernet (10/100/1000 Мбіт/с) та мати високу сумарну пропускну здатність внутрішньої матриці комутації.

З метою обґрунтування вибору проведено порівняльний аналіз трьох ринкових аналогів від провідних виробників мережевого обладнання: TP-Link, D-Link та Netgear.

Детальні технічні характеристики розглянутих моделей наведено в таблиці 2.5.

Таблиця 2.5 – Порівняльна характеристика комутаторів

Критерій порівняння	TP-Link TL-SG1016D	D-Link DGS-1016D	Netgear GS316
1	2	3	4
Тип пристрою	Некерований	Некерований	Некерований
Кількість портів	16 × RJ-45	16 × RJ-45	16 × RJ-45
Швидкість інтерфейсів	10/100/1000 Мбіт/с	10/100/1000 Мбіт/с	10/100/1000 Мбіт/с

Продовження таблиці 2.5

1	2	3	4
Комутаційна матриця	32 Гбіт/с	32 Гбіт/с	32 Гбіт/с
Швидкість перенаправлення пакетів	23.8 Mpps	23.8 Mpps	23.8 Mpps
Таблиця MAC-адрес	8K записів	8K записів	8K записів
Буфер пакетів	4.1 Мбіт	512 КБ (4 Мбіт)	1 Мбіт
Енергоефективність	Підтримка Green Technology (IEEE 802.3az)	Підтримка D-Link Green (IEEE 802.3az)	Підтримка Energy Efficient Ethernet
Тип корпусу / Охолодження	Металевий (для стійки 19" або настільний) / Безвентиляторне	Металевий (для стійки 19" або настільний) / Безвентиляторне	Металевий (для стійки 19" або настільний) / Безвентиляторне
Цінова категорія	Доступна 3000 грн	Середня	Вища

Виходячи з таблиці 2.5, для побудови мережі обираємо комутатор моделі TP-Link TL-SG1016D. Його зовнішній вигляд представлено на рисунку 2.5.

Рисунок 2.5 –Вигляд комутатор TP-Link TL-SG1016D

Для координації внутрішнього трафіка, агрегації каналів від робочих груп (залів №1, №2) та логічної ізоляції підмереж за допомогою технології VLAN, у серверній кімнаті фірми необхідно встановити керований комутатор другого рівня (L2 Smart/Managed). Головними критеріями вибору є: наявність не менше 16 гігабітних портів, підтримка тегування трафіка стандарту IEEE 802.1Q (Trunking), висока швидкість внутрішньої матриці та зручний інтерфейс управління.Як модель обрано комутатор бізнес-серії Cisco Catalyst CBS250-16T-2G. Для підтвердження техніко-економічної доцільності цього рішення проведено порівняльний аналіз із двома ринковими аналогами від виробників HPE (Aruba) та TP-Link. Результати зіставлення наведено в таблиці 2.6. За результатами аналізу таблиці 2.6, модель Cisco Catalyst CBS250-16T-2G є оптимальним вибором для ядра мережі юридичної фірми. Пристрій забезпечує максимальну продуктивність (внутрішня шина 36 Гбіт/с повністю виключає затримки пакетів), підтримує всі необхідні функції безпеки (DHCP Snooping захищає від підміни IP-адрес, а ACL дозволяють гнучко розмежувати доступ між залами юристів). Серія CBS250 спеціально розроблена Cisco як доступне рішення для малого та середнього бізнесу, що дозволяє отримати фірмову надійність та стабільність роботи операційної системи Cisco IOS за помірну ціну. Наявність двох виділених SFP-портів дозволить у майбутньому підключити сервер за допомогою високошвидкісної оптики без втрати основних мідних портів.

Його зовнішній вигляд наведено на рисунку 2.6.

Таблиця 2.6 – Порівняльні характеристики комутаторів

Критерій порівняння	Cisco CBS250-16T-2G	Aruba Instant On 1930 16G	TP-Link JetStream TL-SG2216
1	2	3	4
Тип керування	Керований (L2 / Smart)	Керований (L2+ / Smart)	Керований (L2 / Smart)

Продовження таблиці 2.6

1	2	3	4
Кількість LAN портів	16 × 10/100/1000 Мбіт/с	16 × 10/100/1000 Мбіт/с	16 × 10/100/1000 Мбіт/с
Uplink-інтерфейси	2 × 1 Гбіт/с SFP (оптика)	2 × 1 Гбіт/с SFP (оптика)	2 × 1 Гбіт/с SFP (комбо)
Пропускна здатність шини	36 Гбіт/с	36 Гбіт/с	32 Гбіт/с
Швидкість комутації пакетів	26.78 Mpps	26.78 Mpps	23.8 Mpps
Функції VLAN / Стекування	IEEE 802.1Q (до 256 груп), Q-in-Q	IEEE 802.1Q, Voice VLAN	IEEE 802.1Q (до 512 груп), Port VLAN
Безпека та захист	ACL, IEEE 802.1X, DoS prevention, DHCP Snooping	ACL, Radius, 802.1X, SSL/TLS	ACL, Port Security, SSH/SSL
Охолодження / Корпус	Безвентиляторне / Метал 19"	Безвентиляторне / Метал 19"	Безвентиляторне / Метал 19"
Ціновий діапазон	11300 грн	9800 грн	6000 грн

Рисунок 2.6 – Зовнішній вигляд Cisco CBS250-16T-2G

Центральний маршрутизатор (R_1) є захистом мережі фірми та її шлюзом у глобальну мережу Інтернет. На цей пристрій покладаються критично важливі завдання: організація захищеного підключення до провайдера, міжвілання маршрутизація (Inter-VLAN routing), трансляція мережевих адрес (NAT), впровадження політик безпеки (Firewall) для захисту персональних даних клієнтів, а також підняття криптографічних VPN-тунелів (IPsec/ OpenVPN) для безпечного віддаленого доступу юристів до корпоративних ресурсів із суду чи дому.

Як базову модель обрано гігабітний маршрутизатор бізнес-класу MikroTik hEX S (RB760iGS). Для підтвердження оптимальності цього вибору виконано порівняльний аналіз із конкурентними шлюзами від Ubiquiti та TP-Link (дивися таблицю 2.7). Вартість цього маршрутизатора - 3200 грн.

Таблиця 2.7 – Порівняльні характеристики маршрутизаторів

Критерій порівняння	MikroTik hEX S	Ubiquiti EdgeRouter X	TP-Link TL-ER7206
1	2	3	4
Операційна система	RouterOS (Level 4)	EdgeOS	Omada OS
Кількість портів LAN/ WAN	5 × 10/100/1000 Мбіт/с	5 × 10/100/1000 Мбіт/с	1 × Fixed Gigabit WAN, 2 × Fixed Gigabit LAN, 3 × Changeable WAN/LAN
Оптичний інтерфейс	1 × SFP (1 Гбіт/с)	Відсутній	1 × SFP (1 Гбіт/с)
Апаратне шифрування	Є (IPsec HW Encryption)	Є	Є

Продовження таблиці 2.7

1	2	3	4
IPsec			
Пропускна здатність (NAT)	До 1.97 Гбіт/с	До 1 Гбіт/с	До 940 Мбіт/с
Функції безпеки (Firewall)	Повнофункціональний Stateful Firewall, NAT, Mangle	ACL, NAT, Firewall	SPI Firewall, DoS Defence, IP/MAC/URL Filtering
Живлення через PoE	PoE-in (пасивне/802.3af), 1 × PoE-out	PoE-in, 1 × PoE-out (пасивне)	Відсутнє

Для організації бездротового сегмента мережі (VLAN 200) в офісі фірми передбачено розгортання точки доступу AP_1, яка обслуговуватиме мобільні пристрої співробітників та ноутбуки чи смартфони відвідувачів у зоні очікування (коридорі).

Основними критеріями до вибору обладнання є: підтримка сучасних стандартів шифрування (WPA2/WPA3) для захисту від перехоплення трафіка, робота у двох частотних діапазонах, непомітний дизайн та можливість централізованого адміністрування.

На основі цих вимог для реалізації проєкту обрано бездротову точку доступу бізнес-класу MikroTik cAP ac (RBcAPGi-5acD2nD).

Технічне та архітектурне обґрунтування вибору моделі MikroTik cAP ac:

– Двохдіапазонний режим (Dual-Band): Пристрій одночасно функціонує на частотах 2.4 ГГц (стандарти 802.11b/g/n) та 5 ГГц (стандарти 802.11a/n/ac). Це дозволяє виділити швидкісний канал 5 ГГц для внутрішніх потреб

юристів (робота з документами та базами даних), а завадостійкий діапазон 2.4 ГГц залишити для гостьового клієнтського доступу.

– Інтеграція в екосистему MikroTik (CAPsMAN): Оскільки як головний маршрутизатор системи обрано MikroTik hEX S, управління точкою доступу відбуватиметься централізовано за допомогою фірмової технології CAPsMAN (Controlled Access Point system Manager). Це дозволяє адмініструвати бездротову мережу, оновлювати політики безпеки та керувати гостьовим доступом безпосередньо з головного роутера без потреби заходити на саму точку.

– Підтримка Multi-SSID та ізоляції: Точка доступу дозволяє підняти кілька незалежних бездротових мереж (SSID) на одному фізичному пристрої. Гостьова мережа Wi-Fi буде повністю ізольована від корпоративної мережі фірми на рівні віртуальних підмереж, що виключає ризик несанкціонованого доступу клієнтів до конфіденційних юридичних документів.

– Ергономіка та живлення (PoE): Пристрій виконано у круглому низькопрофільному корпусі для кріплення на стелю, що дозволяє організувати кругову діаграму спрямованості антен для максимального покриття приміщення. Модель підтримує технологію живлення PoE (Power over Ethernet) через перший LAN-порт, завдяки чому передача даних і живлення відбуваються по одному кабелю «вита пара» від інжектора або PoE-комутатора.

Таблиця 2.8 -Зведена таблиця обладнання мережі.

№ п\п	Тип обладнання	Марка	кі-лькість	ціна
1	2	3	4	5
1	Некерований комутатор	TP-Link TL-SG1016D	2	3000 грн
2	Керований комутатор	Cisco CBS250-16T-2G		11300 грн

Продовження таблиці 2.8

1	2	3	4	5
3	Точка доступу	MikroTik cAP ac (RBcAPGi-5acD2nD) EBA63 AX3000	1	3500 грн
4	Маршрутизатор	MikroTik hEX S	1	3200 грн

2.3 Особливості монтажу мережі

Під час проєктування та розгортання структурованої кабельної системи (СКС) фірми базовим нормативним вектором є суворе дотримання комплексу міжнародних, європейських та національних стандартів. Вони регламентують архітектуру, фізичні параметри ліній зв'язку та правила монтажу пасивного обладнання. Ключові вимоги до архітектурної побудови СКС та експлуатаційних параметрів середовища передавання даних акумульовані в таких нормативних документах:

– ISO/IEC 11801 — міжнародний стандарт, що визначає загальну методологію проектування інформаційних мереж загального призначення;

– EN 50173 — європейський стандарт, який адаптує загальні правила під специфіку регіональних телекомунікаційних систем;

– ANSI/EIA/TIA 568 («Commercial Building Telecommunications Wiring Standard») — американський стандарт, що деталізує вимоги до кабельних трас у комерційних будівлях;

– ANSI/EIA/TIA 569 («Commercial Building Standard for Telecommunications Pathways and Spaces») — нормативний документ, що регулює організацію технологічних каналів, просторів та кабельних проходів.

З метою мінімізації негативного впливу перехресних завад (NEXT, FEXT) та електромагнітних наведень на слабострумові лінії передавання ци-

фрових даних, стандартом ANSI/EIA/TIA 569A встановлено суворі просторові обмеження щодо сумісного прокладання інформаційних кабелів та ліній електроживлення:

– Не менше 12 см — просторова ізоляція від неекранованих силових ліній із сумарною потужністю до 2 кВА. У разі паралельного прокладання силових і слабкострумових кабелів усередині єдиного магістрального пластикового коробу (кабель-каналу) обов'язковим є встановлення внутрішньої суцільної діелектричної перегородки.

– Не менше 30 см — відстань від джерел флуоресцентного освітлення (люмінесцентних ламп) та промислових ліній, що здатні генерувати високовольтні імпульсні наведення.

– Не менше 90 см — дистанція від силових кабельних магістралей, робоча потужність яких перевищує показник 5 кВА.

– Не менше 100 см — безпечний радіус від ліній живлення силових трансформаторних підстанцій та індукційних електродвигунів систем вентиляції чи кондиціювання. При цьому допускається перетин трас «витої пари» з силовими електрокабелями виключно під прямим кутом (90°), що мінімізує площу взаємної індукції.

На кожному робочому місці передбачено монтаж двохпортової телекомунікаційної розетки (ТР), оснащеної уніфікованими коннекторами стандарту RJ-45 (8P8C). Дані порти є універсальними і можуть задіюватися як для передавання цифрових даних (Gigabit Ethernet), так і для потреб IP-телефонії. Спуск кабельних трас до розеток виконується всередині захисних пластикових коробів. Телекомунікаційні розетки інтегруються безпосередньо в корпус кабель-каналу (вбудований монтаж).

Для спрощення адміністрування та локалізації аварій кожен порт підлягає обов'язковому маркуванню з унікальним індексом згідно зі стандартом ANSI/TIA/EIA-606-B. Кінцеве обладнання (робочі станції, мережеві принтери, VoIP-телефони) підключається до розеток за допомогою фабричних гнучких патч-кордів категорії 5e довжиною від 1.5 до 3 метрів.

Центральний комутаційний вузол (ядро мережі) базується на базі підлогової телекомунікаційної шафи євростандарту висотою 12U, яка встановлюється у спеціально виділеній серверній кімнаті.

Внутрішня корисна відстань між монтажними вертикальними напрямними (профілями) становить 19 дюймів (482.6 мм). Габаритні розміри шафи (ширина — 600 мм, глибина — 845 мм) підібрані з урахуванням потреби в організації раціональних повітряних потоків для пасивного та активного охолодження обладнання.

Безперервність функціонування активного мережевого, серверного та комутаційного парку обладнання у разі повного аварійного знеструмлення первинної електромережі забезпечується архітектурою джерел безперебійного живлення (ДБЖ).

Автономна робота системи закладена на рівні не менше 20 хвилин, що є достатнім для коректного збереження баз даних та резервного копіювання інформації. Розрахунок номінальної потужності ДБЖ виконується на основі сумарного енергоспоживання всіх активних вузлів у шафі з обов'язковим додаванням 20% експлуатаційного запасу на випадок пікових навантажень або майбутнього розширення мережі.

Електроживлення АРМ реалізується через розподільчу побутову однофазну мережу напругою 220 В із частотою струму 50 Гц. Комп'ютерні силові розетки конструктивно відокремлені від загальних побутових розеткових груп та мають яскраве диференціювання або спеціальне маркування.

На кожному робочому місці монтується не менше двох силових абонентських розеток із обов’язковим виведенням окремого заземлювального контакту, підключеного до загального контуру захисного заземлення будівлі відповідно до норм ПУЕ.

Окремим критично важливим аспектом є забезпечення техногенної та пожежної безпеки персоналу та обладнання.

Серверне приміщення та робочі зали в обов'язковому порядку комплектуються сертифікованими засобами пожежогасіння. Кількість, тип та

ємність вогнегасників визначаються відповідно до чинних Правил пожежної безпеки в Україні (НАПБ А.01.001-2014) та нормативів ДСНС (раніше МНС) України, виходячи з площі приміщень та категорії пожежної небезпеки (для серверних кімнат регламентовано використання вуглекислотних вогнегасників типу ВВ, які не пошкоджують мікросхеми та цифрову апаратуру).

Відповідно до концептуальних вимог стандартів, архітектура проєктуємої СКС розподіляється на п'ять ключових, ієрархічно взаємопов'язаних підсистем:

– Horizontal Cabling (Горизонтальна кабельна підсистема) — охоплює простір від крос-панелей у телекомунікаційній кімнаті до інформаційних розеток АРМ у межах одного поверху будинку.

– Backbone Cabling (Магістральна кабельна підсистема) — забезпечує високошвидкісні вертикальні чи горизонтальні зв’язки між окремими телекомунікаційними приміщеннями в межах однієї споруди або між різними будівлями комплексу.

– Work Area (WA — Робоча область / робоче місце) — комплекс пасивних елементів (розетки, адаптери, сполучні шнури), що забезпечують безпосереднє підключення термінальних пристроїв користувача.

– Telecommunications Room (TR — Телекомунікаційна кімната / шафа) — технологічний простір для розміщення розподільчих пунктів поверху та комутаційного обладнання (згідно з ревізією стандарту ANSI/TIA/EIA-568-B, застарілий термін Telecommunications Closet (TC) було офіційно скасовано).

– Equipment Room (ER — Апаратна / серверна кімната) — виділене технічне приміщення, де зосереджено головне телекомунікаційне обладнання підвищеної складності (сервери, АТС, маршрутизатори ядра мережі та ДБЖ великої потужності).

2.4 Тестування мережі

Мережевий аналізатор EtherScope Series II значно спрощує та пришвидшує тестування LAN, забезпечуючи можливість перевірки, вимірювання та оцінки різноманітних параметрів мережевих конфігурацій, сервісів і характеристик каналу Ethernet.

Пристрій оснащений портом RJ-45 і підтримує волоконно-оптичні трансівери SFP для тестування стандартів 10/100/1000BASE-T і 100/1000BASE-X. Він дозволяє підключатися безпосередньо до тестованого каналу, перевіряти фізичні характеристики, такі як довжина та схема сполук, а також проводити налаштування TCP/IP, тестувати Ethernet-сигнали та PoE на відповідність стандарту 802.3af.

Крім того, аналізатор дозволяє ідентифікувати найближчий комутатор, слот та порт, а також моніторити локальний трафік і надавати статистичні дані, включаючи інформацію про VLAN, протоколи та активних користувачів.

Особливістю EtherScope є наявність спеціалізованих засобів для перевірки продуктивності мережевих сервісів, що дозволяє вимірювати час відгуку основних сервісів і встановлювати пороги для їх оцінки на основі принципу "пройшов/не пройшов".

Це спрощує сприйняття результатів тестування навіть для користувачів без глибоких технічних знань. Результати тестів можна зберігати у вигляді скриптів для подальших перевірок або передачі колегам, а також переглядати в табличному або графічному форматі для детального аналізу.

EtherScope також має можливості для тестування продуктивності мережі Ethernet з пропускною здатністю до 1 Гбіт/с. Для цього використовуються тести IETF RFC 2544 або інші розширені тести, що дозволяють оцінити наскрізні параметри каналу.

Для перевірки повних характеристик каналу потрібні два прилади, які підключаються до протилежних кінців каналу. Використовуючи EtherScope з одного боку каналу, можна підключити інший аналізатор EtherScope або рефлектор пакетів LinkRunner Pro з іншого боку. Така конфігурація дозволяє автоматично проводити повний тест параметрів мережі.

Переваги тестування LAN для IT-фахівців залежать від їхньої ролі та відповідальності. Для IT-спеціалістів, які займаються установкою або оновленням мереж, тестування забезпечує точність виконаних робіт і знижує ризики виникнення проблем у майбутньому.

Перевірка також вигідна для системних інтеграторів і постачальників IT-послуг, оскільки знижує ймовірність виникнення дорогих та трудомістких виправлень. Завдяки точним звітам про результати перевірки, виконання проекту можна підтвердити документально, що є важливим для вирішення спірних ситуацій. Наприклад, якщо виникнуть проблеми з доступом до Інтернету, звіт допоможе визначити відповідальну сторону та підтвердить правильність виконання налаштувань мережі.

Перевірка LAN важлива й для мережевих інженерів та адміністраторів, які використовують ці результати як доказ правильної інсталяції мережі. Звіт про виконану роботу може бути необхідним для підтвердження фінансових витрат у разі співпраці з зовнішніми підрядниками. Тестування також допомагає власникам мереж вимагати виконання конкретних дій за умовами контракту, що гарантує високий рівень якості монтажних робіт і мінімізує ймовірність проблем у майбутньому.

Методи тестування LAN включають вимірювання та аналіз ключових параметрів, таких як конфігурація мережі, доступність мережевих сервісів і швидкість відгуку, а також вимірювання продуктивності мережі Ethernet. Кожен параметр оцінюється з використанням порогових значень "пройшов/не пройшов".

Перевірка конфігурації мережі включає порівняння фактичних підключень з контрольним списком, а перевірка сервісів передбачає вимірювання

часу відгуку для критичних сервісів, таких як DHCP, DNS та Інтернет. Для перевірки продуктивності вимірюються параметри, такі як пропускна здатність, час затримки, рівень втрати кадрів і джиттер. Результати тестування дозволяють визначити відповідні порогові значення для кожного параметра, що гарантує успішне проходження перевірки.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Налаштування головного комутатора та маршрутизатора

Оскільки ми обрали професійний керований комутатор Cisco Catalyst CBS250-16T-2G, у цьому розділі нам потрібно навести реальні команди Cisco CLI (командного рядка), які створять наші віртуальні мережі (VLAN), налаштують порти доступу (Access) для керівництва, магістральні порти (Trunk) для комутаторів залів та маршрутизатора, а також увімкнуть базові функції безпеки.

Програмне налаштування центрального комутатора Cisco Catalyst CBS250-16T-2G є ключовим етапом проєкту, що забезпечує логічний розподіл мережевої структури фірми, безпеку внутрішнього трафіка та міжвеланну взаємодію. Конфігурування пристрою здійснюється через спеціалізований інтерфейс командного рядка (CLI) операційної системи Cisco IOS.

Процес налаштування розподіляється на кілька послідовних технологічних етапів:

– Ініціалізація та активація необхідних ідентифікаторів віртуальних локальних мереж (VLAN ID) відповідно до розробленої схеми логічної адресації.

– Конфігурування фізичних інтерфейсів комутатора в режим доступу (Access mode) для підключення кінцевих пристроїв керівництва, сервера та бездротової точки доступу.

– Налаштування магістральних інтерфейсів у режим тегування (Trunk mode) за стандартом IEEE 802.1Q для забезпечення транзиту трафіка між комутаторами робочих залів та центральним маршрутизатором.

– Впровадження базових сервісів безпеки для захисту від несанкціонованого доступу до системи керування пристроєм.

Нижче наведено лістинг команд конфігурації комутатора SW_1.

Блок 1: Створення віртуальних локальних мереж (VLAN) та присвоєння їм текстових міток

На цьому етапі створюються ізольовані широкомовні домени для кожної структурної групи підприємства:

```
SW_1# configure terminal
SW_1(config)# vlan 100
SW_1(config-vlan)# name Lawyers_Room_1
SW_1(config-vlan)# exit
SW_1(config)# vlan 101
SW_1(config-vlan)# name Lawyers_Room_2
SW_1(config-vlan)# exit
SW_1(config)# vlan 102
SW_1(config-vlan)# name Lawyers_Room_3
SW_1(config-vlan)# exit
SW_1(config)# vlan 103
SW_1(config-vlan)# name Management
SW_1(config-vlan)# exit
SW_1(config)# vlan 200
SW_1(config-vlan)# name Wi-Fi_Wireless
SW_1(config-vlan)# exit
SW_1(config)# vlan 300
SW_1(config-vlan)# name Server_Admin
SW_1(config-vlan)# exit
```

Блок 2: Конфігурування портів доступу (Access)

Згідно з розробленою специфікацією (див. табл. 2.4), порти 2, 3 та 4 виділяються для робочих станцій кабінету керівника (VLAN 103), порт 14 — для підключення файлового сервера (VLAN 300), а порт 15 — для бездротової точки доступу MikroTik cAP ac (VLAN 200):

```
SW_1(config)# interface range gigabitEthernet 0/2-4
SW_1(config-if-range)# description Access_to_Management
```

SW_1(config-if-range)# switchport mode access

SW_1(config-if-range)# switchport access vlan 103

SW_1(config-if-range)# no shutdown

SW_1(config-if-range)# exit

! Налаштування порту для підключення файлового сервера фірми (інтерфейс GigabitEthernet 0/14)

SW_1(config)# interface gigabitEthernet 0/14

SW_1(config-if)# description Access_to_FileServer

SW_1(config-if)# switchport mode access

SW_1(config-if)# switchport access vlan 300

SW_1(config-if)# no shutdown

SW_1(config-if)# exit

! Налаштування порту для бездротової точки доступу Wi-Fi (інтерфейс GigabitEthernet 0/15)

SW_1(config)# interface gigabitEthernet 0/15

SW_1(config-if)# description Access_to_Wireless_AP

SW_1(config-if)# switchport mode access

SW_1(config-if)# switchport access vlan 200

SW_1(config-if)# no shutdown

SW_1(config-if)# exit

Блок 3: Конфігурування магістральних портів (Trunk)

Для передавання маркованих (тегованих) кадрів усіх наявних підмереж між комутаторами доступу в залах та головним маршрутизатором, порти 1, 11, 12 та 13 переводяться в режим Trunk з явним визначенням інкапсуляції 802.1Q:

! Налаштування порту зв'язку з центральним маршрутизатором MikroTik (інтерфейс GigabitEthernet 0/1)

SW_1(config)# interface gigabitEthernet 0/1

SW_1(config-if)# description Trunk_to_Core_Router_RTR_1

SW_1(config-if)# switchport mode trunk

SW_1(config-if)# switchport trunk allowed vlan 100,101,102,103,200,300

SW_1(config-if)# no shutdown

SW_1(config-if)# exit

! Налаштування магістральних ліній до комутаторів робочих залів (інтерфейси GigabitEthernet 0/11 - 0/13)

SW_1(config)# interface range gigabitEthernet 0/11-13

SW_1(config-if-range)# description Trunk_Links_to_Access_Switches

SW_1(config-if-range)# switchport mode trunk

SW_1(config-if-range)# switchport trunk allowed vlan 100,101,102,103,200,300

SW_1(config-if-range)# no shutdown

SW_1(config-if-range)# exit

Блок 4: Налаштування безпеки та збереження конфігурації

Для запобігання несанкціонованому доступу зловмисників до інтерфейсу керування, невикористовувані порти (з 5 по 10) програмно де-активуються (переводяться в стан shutdown), встановлюється пароль на привілейований режим екрана та конфігурація переноситься з оперативної пам'яті (RAM) у постійну (NVRAM):

! Деактивація резервних інтерфейсів

SW_1(config)# interface range gigabitEthernet 0/5-10

SW_1(config-if-range)# description Reserved_Ports

SW_1(config-if-range)# shutdown

SW_1(config-if-range)# exit

! Встановлення криптографічного пароля на доступ до режиму адміністратора (Enable)

SW_1(config)# enable secret Security_LawFirm_2026

! Збереження поточної робочої конфігурації пристрою

SW_1(config)# exit

SW_1# copy running-config startup-config

Destination filename [startup-config]? [Enter]

SW_1#

Завдяки реалізації цієї програмної конфігурації, комутатор ядра SW_1 успішно розмежовує широкомовні шторми всередині залів юристів, захищає конфіденційний трафік керівництва від можливого перехоплення та забезпечує швидкісне проходження пакетів даних до серверної підмережі.

Опишимо скрипт налаштування маршрутизатора MikroTik hEX S (RTR_1).

Головне завдання MikroTik — прийняти через один фізичний порт (ether1) тегований трафік усіх наших VLAN від комутатора Cisco, створити під них віртуальні інтерфейси, підняти DHCP-сервери для автоматичної роздачі IP-адрес клієнтам та налаштувати захист (Firewall/NAT) для виходу в Інтернет.

Налаштування MikroTik здійснюється за допомогою операційної системи RouterOS через командний рядок (CLI).

Центральний маршрутизатор MikroTik hEX S (RTR_1) виступає основним шлюзом безпеки та координатором міжвеланної маршрутизації (Inter-VLAN routing). Програмне забезпечення пристрою функціонує під управлінням операційної системи RouterOS.

Для реалізації логічної структури мережі фірми конфігурація маршрутизатора передбачає виконання таких кроків:

– Конфігурування зовнішнього інтерфейсу (ether5) для отримання статичної або динамічної IP-адреси від інтернет-провайдера.

– Створення віртуальних sub-інтерфейсів (VLAN) на базі першого фізичного порту (ether1), підключеного до магістрального порту (Trunk) комутатора SW_1.

– Присвоєння IP-адрес створеним віртуальним інтерфейсам, які виступатимуть шлюзами за замовчуванням (Default Gateway) для кінцевих хостів у залах.

– Налаштування пулів адрес та DHCP-серверів для автоматизації процесу мережевої конфігурації робочих станцій юристів.

– Налаштування правил міжмережевого екрана (Firewall) та трансляції мережевих адрес (NAT/Masquerade) для безпечного виходу в Інтернет.

Блок 1: Створення віртуальних інтерфейсів VLAN стандарту IEEE 802.1Q

Усі віртуальні локальні мережі прив'язуються до фізичного інтерфейсу ether1, який приймає тегований трафік від Cisco SW_1:

```
/interface vlan
add name=vlan100-lawyers1 vlan-id=100 interface=ether1 comment="Lawyers Room 1"
add name=vlan101-lawyers2 vlan-id=101 interface=ether1 comment="Lawyers Room 2"
add name=vlan102-lawyers3 vlan-id=102 interface=ether1 comment="Lawyers Room 3"
add name=vlan103-mgmt vlan-id=103 interface=ether1 comment="Management"
add name=vlan200-wifi vlan-id=200 interface=ether1 comment="Wireless Network"
add name=vlan300-server vlan-id=300 interface=ether1 comment="Server and Admin Room"
```

Блок 2: Присвоєння IP-адрес інтерфейсам (Шлюзи підмереж)

Відповідно до розробленої Таблиці 2.3, кожному VLAN-інтерфейсу жорстко задається перша корисна IP-адреса підмережі:

```
/ip address
add address=192.168.100.1/24 interface=vlan100-lawyers1
add address=192.168.101.1/24 interface=vlan101-lawyers2
add address=192.168.102.1/24 interface=vlan102-lawyers3
add address=192.168.103.1/24 interface=vlan103-mgmt
add address=192.168.200.1/24 interface=vlan200-wifi
add address=192.168.60.1/24 interface=vlan300-server
```

Блок 3: Конфігурування пулів адрес та DHCP-серверів

Для забезпечення автоматичного отримання IP-адрес комп'ютерами, на кожному інтерфейсі (окрім серверного, де адреса сервера задається статично) розгортається служба DHCP. Діапазон видачі адрес встановлюється з .10 по .254, залишаючи перші адреси для мережевих принтерів та іншого стаціонарного обладнання:

```
# Створення пулів IP-адрес
/ip pool
add name=pool-vlan100 ranges=192.168.100.10-192.168.100.254
add name=pool-vlan101 ranges=192.168.101.10-192.168.101.254
add name=pool-vlan102 ranges=192.168.102.10-192.168.102.254
add name=pool-vlan103 ranges=192.168.103.10-192.168.103.254
add name=pool-vlan200 ranges=192.168.200.10-192.168.200.254
# Налаштування DHCP-серверів на інтерфейсах
/ip dhcp-server
add name=dhcp-vlan100 interface=vlan100-lawyers1 address-pool=pool-vlan100 disabled=no
add name=dhcp-vlan101 interface=vlan101-lawyers2 address-pool=pool-vlan101 disabled=no
add name=dhcp-vlan102 interface=vlan102-lawyers3 address-pool=pool-vlan102 disabled=no
add name=dhcp-vlan103 interface=vlan103-mgmt address-pool=pool-vlan103 disabled=no
add name=dhcp-vlan200 interface=vlan200-wifi address-pool=pool-vlan200 disabled=no
# Параметри мереж для DHCP (Шлюз та DNS-сервери)
/ip dhcp-server network
add address=192.168.100.0/24 gateway=192.168.100.1 dns-server=192.168.60.1,8.8.8.8
add address=192.168.101.0/24 gateway=192.168.101.1 dns-server=192.168.60.1,8.8.8.8
```

add address=192.168.102.0/24 gateway=192.168.102.1 dns-server=192.168.60.1,8.8.8.8

add address=192.168.103.0/24 gateway=192.168.103.1 dns-server=192.168.60.1,8.8.8.8

add address=192.168.200.0/24 gateway=192.168.200.1 dns-server=8.8.8.8

Блок 4: Налаштування безпеки, Firewall та NAT

Для захисту внутрішньої конфіденційної інформації фірми активується механізм динамічної трансляції адрес (скривання внутрішніх IP за однією зовнішньою адресою), а також налаштовуються базові правила безпеки: гостьовому Wi-Fi (VLAN 200) забороняється доступ до робочих залів та серверної кімнати:

Налаштування виходу в Інтернет за допомогою NAT (Маскарадинг на WAN-порті ether5)

/ip firewall nat

add chain=srcnat out-interface=ether5 action=masquerade comment="Internet NAT for LAN"

Налаштування правил фільтрації трафіка (Firewall)

/ip firewall filter

1. Дозволити вже встановлені та пов'язані з'єднання (прискорює роботу)

add chain=forward connection-state=established,related action=accept

2. Заборонити доступ з гостьового Wi-Fi (VLAN 200) до робочих підмереж юристів та серверів

add chain=forward src-address=192.168.200.0/24 dst-address=192.168.100.0/24 action=drop comment="Block Guest to Room 1"

add chain=forward src-address=192.168.200.0/24 dst-address=192.168.101.0/24 action=drop comment="Block Guest to Room 2"

add chain=forward src-address=192.168.200.0/24 dst-address=192.168.102.0/24 action=drop comment="Block Guest to Room 3"

```
add chain=forward src-address=192.168.200.0/24 dst-address=192.168.60.0/24  action=drop comment="Block Guest to Servers"
# 3. Заборонити всі інші некоректні пакети
add chain=forward connection-state=invalid action=drop
```

3.2 Налаштування точки доступу

На завершення конфігурування активного обладнання залишилося налаштувати бездротову точку доступу MikroTik cAP ac (AP_1).

Оскільки в ролі головного роутера ми використовуємо MikroTik hEX S, налаштування точки доступу найпростіше та найправильніше реалізувати через фірмову технологію централізованого управління CAPsMAN (Controlled Access Point system Manager). У такій архітектурі сама точка доступу переводиться в режим «ведомого» пристрою (CAP), а всі параметри бездротових мереж (назва Wi-Fi, паролі, розподіл по VLAN) автоматично передаються на неї з головного маршрутизатора.

Нижче наведено текст та лістинги команд для обох пристроїв.

Конфігурування бездротової підсистеми Wi-Fi за допомогою технології MikroTik CAPsMAN

Організація бездротового доступу в офісі фірми потребує створення безпечного радіосередовища. Завдяки інтеграції обладнання в єдину екосистему MikroTik, керування точкою доступу cAP ac здійснюється централізовано через контролер CAPsMAN, розгорнутий на базі маршрутизатора ядра мережі RTR_1. Це дозволяє розділити фізичний ефір на віртуальні бездротові мережі (SSID) із прив'язкою до відповідних VLAN та забезпечити централізований моніторинг.

Процес налаштування складається з двох етапів: конфігурування контролера на головному маршрутизаторі та переведення фізичної точки доступу в режим керованого агента.

Етап 1: Конфігурування контролера CAPsMAN на маршрутизаторі RTR_1

На головному роутері створюються профілі безпеки (паролі), конфігурації для частотних діапазонів (2.4 ГГц та 5 ГГц) та правила розподілу користувачів за віртуальними мережами. Нам необхідно підняти гостьову мережу для клієнтів (з прив'язкою до VLAN 200), параметри якої автоматично транслюватимуться на точку доступу:

1. Активація контролера CAPsMAN

/caps-man manager set enabled=yes

2. Налаштування профілю безпеки (Захист гостьової мережі шифруванням WPA2)

/caps-man security

add name=sec_guest authentication-types=wpa2-psk encryption=aes-ccm passphrase=LawFirmGuest2026

3. Конфігурування параметрів передачі даних та прив'язки до віртуальної мережі VLAN 200

/caps-man datapath

add name=datapath_guest vlan-mode=no-tag vlan-id=200 client-to-client-forwarding=no

4. Створення профілю конфігурації бездротової мережі (SSID та режим роботи пристрою)

/caps-man configuration

add name=cfg_guest sside="LawFirm_Guests" mode=ap security=sec_guest datapath=datapath_guest country=ukraine

5. Створення правила автоматичного налаштування радіоінтерфейсів для підключених точок доступу

/caps-man provisioning

add action=create-dynamic-enabled master-configuration=cfg_guest name-format=identity

Параметр client-to-client-forwarding=no є критично важливим для безпеки, оскільки він на апаратному рівні забороняє пристроям клієнтів у гостьовому Wi-Fi обмінюватися даними чи сканувати один одного, що локалізує потенційні загрози всередині бездротового сегмента.

Етап 2: Конфігурування точки доступу MikroTik cAP ac (AP_1)

Фізична точка доступу підключається кабелем до 15-го порту комутатора Cisco (налаштованого в режим Access під VLAN 200). Для введення її в експлуатацію необхідно повністю вимкнути стандартну заводську конфігурацію маршрутизатора та перевести радіоінтерфейси (вбудовані антени 2.4 GHz та 5 GHz) під управління контролера:

1. Скидання заводських налаштувань у нульовий режим (виконується через CLI точки доступу)

/system backup save name=factory_backup

/system reset-configuration no-defaults=yes skip-backup=yes

2. Після перезавантаження — активація режиму керованого клієнта (CAP)

Вказуємо внутрішній міст (bridge) та фізичний інтерфейс ether1 для пошуку контролера

/interface bridge

add name=bridge_cap

/interface bridge port

add bridge=bridge_cap interface=ether1

/interface wireless cap

Переведення бездротових інтерфейсів wlan1 та wlan2 під повне управління CAPsMAN

set discovery-interfaces=bridge_cap interfaces=wlan1,wlan2 enabled=yes

Після виконання цих команд точка доступу AP_1 виявить у локальній мережі контролер на маршрутизаторі RTR_1, отримає від нього створені налаштування і почне транслювати ізольовану бездротову мережу "Firm_Guests" у двох частотних діапазонах одночасно. Адміністратор мережі

зможе керувати потужністю сигналу, частотними каналами та бачити список підключених смартфонів чи ноутбуків безпосередньо через інтерфейс головного роутера.

3.3 Інструкція з використання тестових наборів та тестових програм

Для діагностики мережі використовуютьсянаступні команди:

PING Команда PING є однією з найосновніших і найбільш ефективних для тестування мережі. Вона допомагає визначити доступність іншого пристрою в мережі, перевіряючи, чи можуть дані пройти до цільової IP-адреси. Вона відправляє пакети і аналізує, скільки з них повернулося. Якщо деякі пакети не повертаються, то це вказує на проблеми з мережею, такі як втрати пакетів, що може знизити якість з’єднання, особливо для онлайн-ігор або відео трансляцій. Кількість пакетів та тайм-аут можна налаштовувати за допомогою додаткових параметрів.

– TRACERT, або Trace Route, є командою, що відслідковує шлях пакета до кінцевої точки. Вона не лише вимірює швидкість, але й показує весь маршрут, через який проходять дані, включаючи список маршрутизаторів, через які проходять пакети. Це дає змогу зрозуміти, де можуть виникати проблеми в мережі, так як команда також вказує час проходження кожного маршрутизатора.

– PATHPING поєднує функціональність PING і TRACERT. Вона аналізує маршрут пакета та визначає, на яких вузлах трапляються втрати пакетів. Ця команда потребує більше часу для виконання, але вона надає детальнішу інформацію про проблемні точки в мережі, що може бути корисно для виявлення причин затримок.

– Команда IPCONFIG дозволяє отримати основну інформацію про налаштування мережі на комп'ютері, зокрема IP-адреси, шлюзи та інші параметри мережевих адаптерів. Вона часто використовується для

діагностики та конфігурації, а також з допомогою параметра /flushdns дозволяє очистити кеш DNS, що може допомогти вирішити проблеми з доступом до деяких сайтів.

– GETMAC відображає унікальну MAC-адресу кожного мережевого адаптера вашого комп’ютера, що дозволяє ідентифікувати пристрої в мережі. Зазвичай, комп’ютери мають різні MAC-адреси для кожного з'єднання, наприклад, для Wi-Fi і Ethernet.

– NSLOOKUP — це інструмент для перевірки зв'язку між доменними іменами і IP-адресами. В основному ця команда дозволяє дізнатися IP-адресу за доменним іменем або навпаки, доменне ім’я за IP-адресою. Це корисно для діагностики проблем із з’єднанням з конкретними вебсайтами чи сервісами.

– NETSTAT — це потужна утиліта для збору статистики про мережеві з'єднання та порти, які використовуються на комп'ютері. Вона дозволяє отримати інформацію про відкриті порти, активні з’єднання і потоки даних, що надходять чи відправляються через вашу мережу. Цей інструмент корисний для виявлення небажаних з'єднань чи мережевих проблем.

Ці команди є основними інструментами для діагностики та налаштування мережі. Вони допомагають виявити й усунути проблеми в мережі, а також перевірити налаштування і продуктивність мережевих з'єднань.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки проекту локальної комп'ютерної мережі ПП "СТО сорок" і прийняття рішення про її подальший розвиток і впровадження або ж недоцільність проведення відповідної розробки.

Для розрахунку вартості НДР необхідно виконати наступні етапи:

– описати технологічний процес розробки із зазначенням трудомісткості кожної операції;

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

– визначити суму матеріальних затрат;

– обчислити витрати на електроенергію для науково-виробничих цілей;

– розрахувати транспортні витрати;

– нарахувати суму амортизаційних відрахувань;

– визначити суму накладних витрат;

– скласти кошторис та визначити собівартість НДР;

– розрахувати ціну НДР;

– визначити економічну ефективність та термін окупності продукту.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

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

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

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	2	3	4
1.	Підготовка	Інженер	5
2	Розробка проекту мережі	Інженер	19
3	Монтаж пасивного обладнання	Лаборант	20
4	Налаштування активного комутаційного обладнання	Технік	9
5	Встановлення та на лаштування програмного забезпечення	Технік	8
6	Тестування мережі	Технік	5
Р а з о м		–	66

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

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

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства.

Заробітна плата складається з основної та додаткової оплати праці.

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

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов'язані з виплатами за фактично відпрацьований час.

Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців.

Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

Основна заробітна плата розраховується за формулою:

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

де $Тс$ – тарифна ставка, грн.;

$Кг$ – кількість відпрацьованих годин.

$З_{осн.}$=150*24+140*22+120*20=9080,00 грн.

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

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

де $К_{допл.}$ – коефіцієнт додаткових виплат працівникам.

$З_{дод.}=9080,00$*0,15=1362,00 грн

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

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

$В_{о.п.} = 9080,00$+ 1362,00 =10442,00 грн.

Крім того, слід визначити відрахування на заробітну плату:

1.єдиний соціальний внесок .

Отже, сума відрахувань на соціальні заходи буде становити:

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

де $ФОП$ – фонд оплати праці, грн.

$В_{з.с.}$ = 10442,00 *$0,22$=3926,19 грн.

Проведені розрахунки зведемо у наступну таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Дод. заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на опл. пр., грн. 6=3+4+5
		Тарифна ставка, грн.	К-сть від-працьов. год.	Факт. нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1	Інженер	150	24	3600	540	-	-
2	Технік	140	22	3080	462	-	-
3	Лаборант	120	20	2400	360	-	-
	Разом	-	-	9080	1362	3926,19	14368,19

4.3 Розрахунок матеріальних витрат

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

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

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити:

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

$З_{м.в.}$= 40128,00 грн.

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. вимі-ру	Факт. витра-чено матері-алів	Ціна 1-ці, грн.	Загальна сума витрат, грн.
1	2	3	4	5	6
1	Кабель UTP Cat5e	м	750	15,00	11250,00
2	Роз’єми RJ-45	шт	175	2,00	350,00
3	Розетки RJ-45	шт	40	55,00	2200,00
4	Короб пластиковий 40*25*2м	шт	48	45,00	2160,00
5	Дюбель	шт	280	0,60	168,00
6	Некерований комутатор TP-Link TL-SG1016D	шт	2	3000,00	6000,00
7	Керований комутатор Cisco CBS250-16T-2G	шт	1	11300,00	11300,00
8	Точка доступу MikroTik cAP ac (RBcAPGi-5acD2nD) EBA63 AX3000	шт	1	3500,00	3500,00
9	Маршрутизатор MikroTik hEX S	шт	1	3200,00	3200,00
	Р а з о м				40128,00

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

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

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Для розробки проекту даної локальної комп'ютерної мережі використовується один ПК, потужність якого W = 0,5 кВт і який працює 16 годин.

$З_е$=0,50*16*15,94=127,60 грн.

4.5 Визначення транспортних затрат

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

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

де $Т_В$ – транспортні витрати.

$Т_В$ = 40128,00*0,08=3210,24 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. Комп'ютери та оргтехніка належать до четвертої групи основних фондів.

Мінімально допустимі строки їх корисного використання 2 роки.

Для визначення амортизаційних відрахувань застосовуємо формулу:

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

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

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

$Н_А$ – норма амортизації, %.

Для проектування даної комп'ютерної мережі використовується один комп'ютер (вартість якого становить 35000,00 грн.), який працює 16 годин.

Тоді:

$А$= 35000*0,04*16/150=149,33 грн.

4.7 Обчислення накладних витрат

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

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

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

де $Н_В$ – накладні витрати.

$Н_В$=10442,02 * 0,2=2088,4 грн.

4.8 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 4.4

Собівартість (СВ) НДР розрахуємо за формулою:

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

$С_в$= 60071,8 грн.

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до заг. суми
1	2	3
Витрати на оплату праці	10442,02	20,80
Відрахування на соціальні заходи	3926,19	5,68
Матеріальні витрати	40128,00	58,08
Витрати на електроенергію	127,6	0,18
Транспортні витрати	3210,24	4,65
Амортизаційні відрахування	149,33	0,22
Накладні витрати	2088,4	10,40
Собівартість	60071,8	100,00

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

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

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

$К$ – кількість замовлень, од.;

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

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

$Ц$=60071,8*(1+0,26)*(1+0,2)= 90828,5 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 ($T_{ОК}$).

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

де K_B – затрати на проект;

$Г_n$ – грошовий потік за t–ий рік;

t – відповідний рік проекту;

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

$ЧТВ = -60071,8 + 42756,7/(1+0,1) + 42756,7/(1+0,1)^2 = 19134,0$ (грн.)

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

Термін окупності визначається за формулою:

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

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

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

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

$T_{ОК}$=1+21202,1/42756,7=1,5

Економічні показники НДР зведено в таблицю 4.5

Таблиця 4.5 - Економічні показники НДР

№ п/п	Показник	Значення
1	2	3
1.	Собівартість, грн.	60071,8
2.	Плановий прибуток, грн.	30756,7
3.	Ціна, грн.	90828,5
4.	Чиста теперішня вартість, грн	14134,0
5.	Термін окупності, рік	1,5

В результаті аналізу економічних показників, розрахованих та зведених у таблицю 4.5, можна прийти до висновку, що при терміні окупності – 1,5 року проводити роботи по впровадженню даної мережі є доцільним та економічно вигідним.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

5.1 Інженерні засоби зниження виробничого шуму в зонах обслуговування клієнтів та роботи операторів в ПП “СТО сорок”

Ефективне вирішення проблем захисту від шуму, вібрацій, ультра- та інфразвука досягається проведенням комплексу заходів, що послабляють інтенсивність шкідливих виробничих факторів у їхніх джерелах, на шляху поширення. Зниження інтенсивності шуму в джерелах забезпечує кардинальне вирішення всіх цих проблем. Зниження інтенсивності шуму на шляху поширення нерідко буває дешевшим за вирішення проблеми в джерелі, але досить ефективним.

Наприклад, шум визначається, у першу чергу, їхніми силовими установками, тому для його зниження необхідне проведення заходів щодо зменшення шуму двигунів. При цьому можливі два шляхи: створення нових малошумних двигунів і модифікація існуючих.

При створенні нових малошумних двоконтурних турбореактивних двигунів (ТРД) необхідно вибирати такі параметри робочого процесу, двоконтурності, схем, програм регулювання й окремих конструктивних характеристик, які б забезпечували мінімальний шум. Модифікація існуючих конструкцій двигунів може передбачати додаткові заходи щодо зниження шуму, такі як: установку шумопоглинаючих сопел, регулювання площ перерізу реактивних сопел, акустичну обробку вхідних і вихідних каналів вентилятора та мотогондол та інш.

До методів зниження шуму силових установок можна віднести застосування стаціонарних і пересувних глушників шуму біля сопел усмоктування і вихлопу газів двигунів під час їхнього випробування у наземних умовах.

Стаціонарні шумоглушники встановлюються на випробувальних станціях двигунів, на спеціальних площадках чи в ангарах (боксах).

Методи ослаблення шуму від джерел, розташованих усередині приміщень, дуже різноманітні і залежать від типу устаткування. Наприклад, знизити шум електричних машин можна:

– усуненням неврівноваженості ротора, регулюванням підшипникових вузлів і щиткових контактів (для зменшення механічного шуму і вібрацій);

– акустичною оптимізацією вентиляторів охолодження (наприклад, збільшенням зазорів, зменшенням діаметра гвинта й колової швидкості), зменшенням витрат охолоджуваного повітря і, нарешті, вирішенням проблеми охолодження без використання вентиляторів, завдяки чому знижується аеродинамічний шум;

– усуненням асиметрій у магнітопроводах і обмотках, ослабленням інтенсивності перемінних радіальних магнітних сил низького порядку (для зменшення магнітного шуму і вібрації).

У випадку неможливості забезпечення колективного захисту робітників від впливу розглянутих факторів наведеними методами застосовуються засоби індивідуального захисту.

Засобами індивідуального захисту від шуму є протишумні шоломи, навушники і вкладиші.

Засоби захисту від вібрацій у джерелах вібрацій ґрунтуються на урівноважуванні діючих сил і моментів у машинах і механізмах, балансуванні обертових деталей, застосуванні матеріалів з підвищеним внутрішнім тертям, поліпшенні технології виготовлення і т.ін.

Зниження рівня вібрації на шляху її поширення досягається застосуванням віброізолюючих конструкцій і вібродемпфуючих матеріалів і покриттів, а також віброгасників. Для забезпечення віброізоляції влаштовують розриви між елементами конструкцій або усувають тверді зв’язки між ними, а також уникають подібності частот власних коливань системи і частот сил, що її збурюють.

Підвіска двигунів літаків на пружних амортизаторах забезпечує зниження вібрації і шуму в кабінах у всіх смугах звукового спектру від 5 до 8 дБ.

Для вібропоглинання на вібруючі елементи машини наносять в'язкі або пружні матеріали, яким притаманні значні внутрішні втрати. До таких матеріалів відносяться антивібрит, агат, сендвічні конструкції, СКЛ-25 та інш. Зниження вібрації таким чином досягає 2-10 дБ в смузі частот 31,5-8000 Гц.

Засобами індивідуального захисту від вібрації є: черевики, рукавиці, виготовлені із віброзахисних матеріалів цілком або в місцях з'єднання з вібруючою поверхнею.

Захист від ультра- та інфразвука. Захист від ультразвукових коливань здійснюється тими ж методами, що і захист від шуму. Основну увагу потрібно приділяти усуненню безпосереднього контакту робітників з коливними середовищами.

Для цього завантаження ультразвукових ванн, вивантаження й інші роботи виконують при виключених генераторах коливань, або використовують спеціальні пристосування з ручками, не зв'язаними вібруючими деталями. Ультразвукове технологічне устаткування ізолюють кожухами або звукоізолюючими камерами. Внутрішні поверхні камер облицьовуються звукопоглинаючими матеріалами. Робочі місця можна екранувати. Для поглинання енергії ультразвука рекомендуються матеріали, подібні до застосовуваних при зниженні шуму, але з більшою ефективністю на високих частотах.

Труднощі захисту від інфразвукових хвиль полягають в тому, що стіни і великі елементи конструкцій починають вібрувати в ритмі інфразвука і не чинять йому ніякого опору.

Інфразвук практично не послаблюється перешкодами, тому основною задачею захисту людини від шкідливого впливу інфразвука є виключення чи ослаблення його генерування в самому джерелі.

Ефективними заходами від інфразвука є також застосування методів зниження вібрацій.

5.2 Вимоги безпеки під час прокладання слабкострумових мереж поблизу технологічного обладнання

Очевидний факт: у більшості випадків як у житлових, так і у виробничих приміщеннях виникає необхідність прокладати не тільки електропроводку, а й мережі, що мають інше призначення. Це переважно слабострумові мережі: телефонні, телевізійні, мережі інтернет. Слабострумові кабелі. Звичайно, дані комунікації прокладаються згідно з такими ж основними правилами, як і силові мережі. Але є кілька нюансів, які слід враховувати під час спільного прокладання цих комунікацій.

Офіційних правил із цього питання ви не знайдете. Але фахівці, виходячи зі свого багаторічного досвіду, все ж таки наводять кілька рекомендацій, щоб підсумок робіт був максимально ефективним і надійним (особливо щодо правил пожежної безпеки).

Отже, силовий кабель разом із слабострумовим краще не прокладати, використовуючи лише один кабель-канал або одну штробу, щоб запобігти можливості перегріву і, в деяких випадках, займання кабелю. Як наслідок – поломка обладнання, пожежа. Використовуйте перегородки з негорючих матеріалів, щоб мінімізувати контакт різних видів кабелю між собою.

Добре використовувати також екрановану кручену пару або труби з металу для прокладання двох різних видів кабелю. Таким чином, значно знижується рівень негативного впливу зовнішнього поля на кабельну продукцію.

Іноді є можливість прокласти силовий кабель і кабель слабострумові на різних, протилежних стінах. Не нехтуйте нею. Це забезпечить повну їхню взаємодію та максимальну безпеку.

Перетин слабострумового кабелю та електропроводки краще проводити під кутом 90°. Рекомендується також прилади, які розподіляють та споживають електроенергію, розташовувати далі від слабкого кабелю. Таким чином надаватиметься мінімальна дія на кручену пару.

Як показує практика, перерахованих вище рекомендацій достатньо, щоб самостійно виконати ті чи інші роботи з проведення в будинку. У випадку ж з промисловими, виробничими приміщеннями все набагато суворіше. Адже йдеться про серйозні силові навантаження та безпеку людей вже щодо цих вихідних даних. У такому разі, з рекомендацій можна додати наступне: якщо відстань між кабелями менше 15 метрів, то їх, як правило, прокладають у лотках або в одному кабель-каналі, але з вогнетривкою перегородкою всередині та відстанню між ними не менше 50 мм, при напрузі поля не вищі за 3 В/м. Якщо кручена пара не має екрана, відстань від нього до будь-якого джерела електромагнітного випромінювання (більше 3 В/м) не повинна бути меншою за 1,5 метра. Люмінесцентні лампи, а також інші прилади, які мають розрядники, повинні розташовуватися від слабострумових мереж на відстані більше 125 мм.

Рекомендації щодо спільної прокладки силових та слабострумових мереж у різних видах приміщень дуже прості. Їх застосування на практиці – це додаткова впевненість у власній безпеці та безпеці інших людей. Також це і запорука гарної та довговічної роботи проводки та техніки. Завжди за будь-яких видів прокладки та роботи з електричним враховуйте всі правила пожежної безпеки.

5.3 Класифікація можливих надзвичайних ситуацій в ПП “СТО сорок” та пільги за роботу зі шкідливими умовами праці

В Україні щорічно виникають тисячі тяжких надзвичайних ситуацій природного та техногенного характеру, внаслідок яких гине велика кількість людей, а матеріальні збитки сягають кількох мільярдів гривень. Нині в багатьох областях України у зв’язку з небезпечними природними явищами, аваріями і катастрофами обстановка характеризується як дуже складна.

Як свідчить практика (Чорнобильська катастрофа; аварії з загибеллю людей на вугільних шахтах України; авіаційні катастрофи — АН-124 під

Києвом, АН-24 поблизу міста Салоніки в Греції та інші) для роботи в районі надзвичайної ситуації потрібне залучення значної кількості людських, матеріальних і технічних ресурсів.

15 липня 1998 року Постановою Кабінету Міністрів України № 1099 «Про порядок класифікації надзвичайних ситуацій" затверджено "Положення про класифікацію надзвичайних ситуацій».

Відповідно до характеру походження подій, що можуть зумовити виникнення надзвичайних ситуацій на території України, розрізняють:

– надзвичайні ситуації техногенного характеру: транспортні аварії (катастрофи), пожежі неспровоковані вибухи чи їх загроза, аварії з викидом (загрозою викиду) небезпечних хімічних, радіоактивних, біологічних речовин, раптове зруйнування споруд та будівель, аварії на інженерних мережах і спорудах життєзабезпечення, гідродинамічні аварії на греблях, дамбах тощо;

– надзвичайні ситуації природного характеру: небезпечні геологічні, метеорологічні, гідрологічні морські та прісноводні явища, деградація ґрунтів чи надр, природні пожежі, зміна стану повітряного басейну, інфекційна захворюваність людей, сільськогосподарських тварин, масове ураження сільськогосподарських рослин хворобами чи шкідниками, зміна стану водних ресурсів та біосфери тощо;

– надзвичайні ситуації соціально-політичного характеру, пов'язані з протиправними діями терористичного і антиконституційного спрямування: здійснення або реальна загроза терористичного акту (збройний напад, захоплення і затримання важливих об'єктів, ядерних установок і матеріалів, систем зв'язку та телекомунікацій, напад чи замах на екіпаж повітряного чи морського судна), викрадення (спроба викрадення) чи знищення суден, захоплення, встановлення вибухових пристроїв у громадських місцях, зникнення (крадіжка) зброї, виявлення застарілих боєприпасів тощо;

– надзвичайні ситуації воєнного характеру, пов’язані з наслідками застосування зброї масового ураження або звичайних засобів ураження, під час яких виникають вторинні фактори ураження населення внаслідок зруйнування атомних і гідроелектричних станцій, складів і сховищ радіоактивних і токсичних речовин та відходів, нафтопродуктів, вибухівки, сильнодіючих отруйних речовин, токсичних відходів, транспортних та інженерних комунікацій тощо.

Крім того, необхідно знати, що, відповідно до територіального поширення, обсягів заподіяних або очікуваних економічних збитків кількості людей, які загинули, за класифікаційними ознаками визначаються чотири рівні надзвичайних ситуацій:

– надзвичайна ситуація загальнодержавного рівня — це надзвичайна ситуація, яка розвивається на території двох та більше областей (Автономної Республіки Крим, міст Києва та Севастополя) або загрожує транскордонним перенесенням, а також у разі, коли для її ліквідації необхідні матеріали і технічні ресурси в обсягах, що перевищують власні можливості окремої області (Автономної Республіки Крим, міст Києва та Севастополя), але не менше одного відсотка обсягу видатків відповідного бюджету;

– надзвичайна ситуація регіонального рівня — це надзвичайна ситуація, яка розвивається на території двох або більше адміністративних районів (міст обласного значення) — Автономної Республіки Крим, областей, міст Києва та Севастополя, або загрожує перенесенням на територію суміжної області України а також у разі, коли для її ліквідації необхідні матеріальні і технічні ресурси в обсягах, що перевищують власні можливості окремого району, але не менше одного відсотка обсягу видатків відповідного бюджету;

– надзвичайна ситуація місцевого рівня — це надзвичайна ситуація, яка виходить за межі потенційно небезпечного об’єкта, загрожує поширенням самої ситуації або її вторинних наслідків на довкілля, сусідні населені пункти, інженерні споруди, а також у разі, коли для її ліквідації необхідні

матеріальні і технічні ресурси в обсягах, що перевищують власні можливості потенційно небезпечного об’єкта, але не менш одного відсотка обсягу видатків відповідного бюджету. До місцевого рівня також належать всі надзвичайні ситуації, які виникають на об’єктах житлово-комунальної сфери та інших, що не входять до затверджених переліків потенційно небезпечних об’єктів;

– надзвичайна ситуація об’єктного рівня — це надзвичайна ситуація, яка розгортається на території об’єкта або на самому об’єкті і наслідки якої не виходять за межі об’єкта або його санітарно-захисної зони.

Подальша класифікація як природних, так і техногенних надзвичайних ситуацій може бути проведена за такими ознаками: загальна причина виникнення, вид прояву, сфера, наслідки, терміни та масштаб прояву.

Зростання масштабів господарської діяльності і кількості великих промислових комплексів, концентрація на них агрегатів і установок великої і надвеликої потужності, використання у виробництві потенційно небезпечних речовин у великих кількостях — все це збільшує вірогідність виникнення техногенних аварій. Надзвичайні ситуації техногенного походження містять у собі загрозу для людини, економіки і природного середовища або здатні створити її внаслідок ймовірного вибуху, пожежі, затоплення або забруднення (зараження) навколишнього середовища.

Надзвичайні ситуації виникають, як правило, на потенційно техногенно небезпечних виробництвах. До них належать насамперед хімічно небезпечні об’єкти, радіаційно небезпечні об’єкти, вибухо та пожежонебезпечні об’єкти, а також гідродинамічно небезпечні об’єкти. В останні роки значно зросла також небезпека від аварій і катастроф на транспорті.

Надзвичайні ситуації техногенного характеру прийнято класифікувати за такими основними ознаками:

– за масштабами наслідків (об’єктового, місцевого, регіонального і загальнодержавного рівнів);

– за галузевою ознакою (у сільському господарстві; у лісовому господарстві; на заповідній території (об’єкти особливого природоохоронного значення); у водоймах; на матеріальних об’єктах — об’єктах інфраструктури, промисловості, транспорту, житлово-комунального господарства та населення (персонал підприємств та установ, мешканці житлових будинків, пасажири транспортних засобів тощо).

Аварії техногенного характеру класифікуються також з урахуванням критеріїв розміру заподіяних чи очікуваних економічних збитків.

Розглянемо більш детально надзвичайні ситуації техногенного характеру.

Транспортні аварії (катастрофи)

Щорічно в Україні транспортом загального користування перевозиться понад 900 млн т вантажів (у тому числі велика кількість небезпечних), і понад 3 млрд пасажирів. На частку залізничного транспорту припадає близько 60 % вантажних перевезень, автомобільного — 26 %, річкового і морського — 14 %.

Оскільки транспортом перевозяться і потенційно небезпечні вантажі (вибухонебезпечні, пожежонебезпечні, хімічні та інші речовини — 15 % від загального обсягу вантажів), небезпека життя і здоров’я людей збільшується. Скоротилося оновлення основних фондів всіх видів транспорту. Рівень зношення транспортних засобів становить понад 50 %, а на деяких підприємствах і значно більше, велика кількість транспортних засобів підлягає списанню.

Найбільша кількість надзвичайних ситуацій, особливо із загибеллю людей, припадає на транспорт, що свідчить про високу потенційну небезпечність транспорту як галузі господарства. У 1998 році сталося 109 аварій та надзвичайних подій на транспорті, внаслідок яких загинуло 64 та постраждало 80 осіб.

Усі підприємства, установи та організації повинні забезпечувати безпеку праці та дбати про здоров'я своїх працівників. До обов'язків робо-

тодавця входить розробка комплексних заходів з охорони праці, які б гарантували безпечні та здорові умови праці на робочому місці.

Здійснення контролю за додержанням законодавства про працю підприємствами, установами, організаціями та фізичними особами, які використовують найману працю покладено на Державну службу України з питань праці.

Також зазначена Служба здійснює державний нагляд за додержанням законодавства про працю та зайнятість населення центральними органами виконавчої влади; здійснює контроль за правильністю застосування роботодавцями списків на пільгове пенсійне забезпечення, готує пропозиції щодо вдосконалення таких списків; здійснює контроль за якістю проведення атестації робочих місць за умовами праці; здійснює державний контроль за додержанням вимог законодавства про працю, зайнятість населення в частині дотримання прав громадян під час прийому на роботу та працівників під час звільнення з роботи; використання праці іноземців та осіб без громадянства; наймання працівників для подальшого виконання ними роботи в Україні в іншого роботодавця; дотримання прав і гарантій стосовно працевлаштування громадян, які мають додаткові гарантії у сприянні працевлаштуванню; провадження діяльності з надання послуг з посередництва та працевлаштування; здійснює контроль за дотриманням вимог законодавства про рекламу щодо реклами про вакансії (прийом на роботу); здійснює державний контроль за додержанням підприємствами, установами та організаціями, у тому числі підприємствами, організаціями громадських об’єднань осіб з інвалідністю, фізичними особами, які використовують найману працю, законодавства про зайнятість та працевлаштування осіб з інвалідністю у частині виконання нормативу робочих місць, призначених для працевлаштування осіб з інвалідністю; здійснює контроль за своєчасністю та об’єктивністю розслідування нещасних випадків на виробництві, їх документальним оформленням і веденням обліку, виконанням заходів з усунення причин нещасних випадків; здійснює державний нагляд (контроль) у сфері гігієни пра-

ці, у тому числі нагляд (контроль) за факторами виробничого середовища та виробничих операцій, наявність яких може шкодити здоров'ю працівників; виконанням заходів щодо запобігання виникненню професійних захворювань; дотриманням вимог санітарних норм та правил; своєчасним здійсненням профілактичних заходів, спрямованих на попередження шкідливої дії факторів виробничого середовища і трудового процесу, збереження здоров'я працівників; наявністю обов'язкових медичних оглядів працівників; здійснює державний нагляд (контроль) за додержанням законодавства у сфері охорони праці, зокрема в частині безпечного ведення робіт, гігієни праці, промислової безпеки, безпеки робіт у сфері поводження з вибуховими матеріалами промислового призначення, у тому числі з питань забезпечення працівників спеціальним одягом, спеціальним взуттям та іншими засобами індивідуального та колективного захисту; монтажу, ремонту, реконструкції, налагодження і безпечної експлуатації машин, механізмів, устаткування, транспортних та інших засобів виробництва і машин, механізмів, устаткування підвищеної небезпеки; безпеки робіт у сфері поводження з вибуховими матеріалами промислового призначення, проведення робіт з утилізації звичайних видів боєприпасів, ракетного палива та вибухових матеріалів військового призначення; виробництва, зберігання, використання отруйних речовин у виробничих процесах, у тому числі продуктів біотехнологій та інших біологічних агентів; організації проведення навчання (в тому числі спеціального) і перевірки знань з питань охорони праці; навчання працівників у сфері поводження з вибуховими матеріалами промислового призначення та перевірки їх знань; здійснює дозиметричний контроль робочих місць та доз опромінення працівників; забезпечує складення санітарно-гігієнічних характеристик умов праці для подальшого визначення зв'язку захворювання з умовами праці та інше.

Також кожен працівник має право на пільги і компенсації за важкі та шкідливі умови праці (відповідно до вимог статті 7 Закону України "Про охорону праці"):

– працівники, зайняті на роботах з важкими та шкідливими умовами праці, безоплатно забезпечуються лікувально-профілактичним харчуванням, молоком або рівноцінними харчовими продуктами, газованою солоною водою, мають право на оплачувані перерви санітарно-оздоровчого призначення, скорочення тривалості робочого часу, додаткову оплачувану відпустку, пільгову пенсію, оплату праці у підвищеному розмірі та інші пільги і компенсації, що надаються в порядку, визначеному законодавством;

– у разі роз'їзного характеру роботи працівникові виплачується грошова компенсація на придбання лікувально-профілактичного харчування, молока або рівноцінних йому харчових продуктів на умовах, передбачених колективним договором.

Роботодавець може за свої кошти додатково встановлювати за колективним договором (угодою, трудовим договором) працівникові пільги і компенсації, не передбачені законодавством.

Протягом дії укладеного з працівником трудового договору роботодавець повинен, не пізніше як за 2 місяці, письмово інформувати працівника про зміни виробничих умов та розмірів пільг і компенсацій, з урахуванням тих, що надаються йому додатково.

Примітка: Написання даного розділу проводилося з використанням матеріалів інтернет сайтів.

ВИСНОВКИ

В ході роботи над кваліфікаційною роботою спроектовано комп’ютерну мережу ПП “СТО сорок”. Зроблено аналітичний огляд літератури та існуючих рішень, та на його основі спроектовано логічну та фізичну топологію мережі. Вибрано пасивне та активне комутаційне обладнання, сервер, точку доступу та програмне забезпечення.

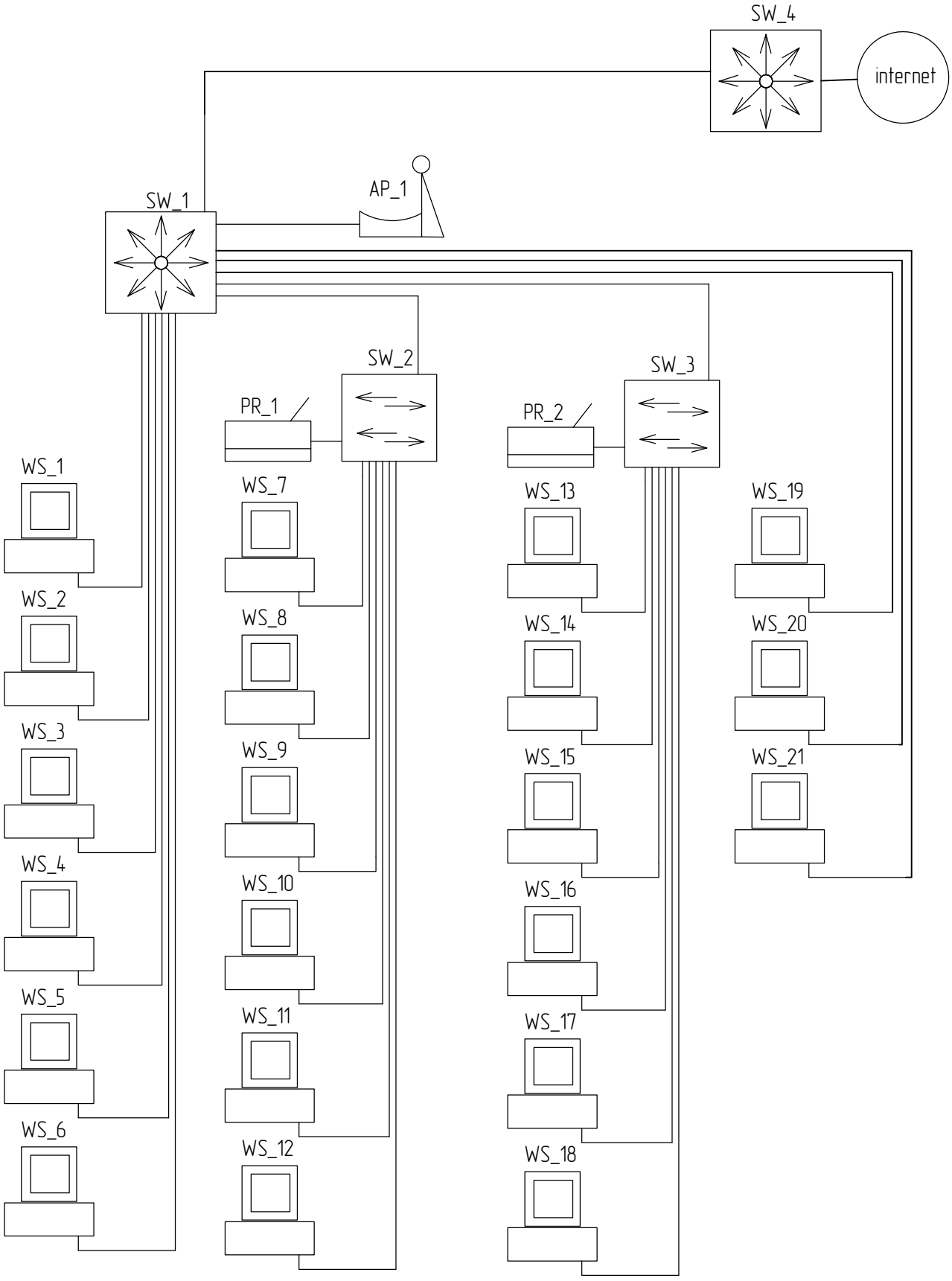
Робота містить створену логічну і фізичну топології мережі, таблицю IP-адресації та техніко-економічних показників .

В економічному розділі розраховано собівартість мережі, її економічну ефективність, термін окупності та інші показники.

Останній розділ кваліфікаційної роботи описує питання охорони праці, та техніки безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Антонов В.М. Сучасні комп'ютерні мережі. Підручник — К.: "МК-Прес", 2005. — 480 с.
2. Буров Є. Комп'ютерні мережі, 2-е видання. - БаК, 2004. – 584 с.: іл.
3. Додонов О. Г., Ланде Д. В., Путятін В. Г. Інформаційні потоки в глобальних комп’ютерних мережах. — К.: Наук, думка, 2009. — 295 с
4. Іртегов Д.В. Введення в мережні технології, К., 2014.
5. Шорошев В. В. Теоретичні і практичні аспекти організації і побудови архітектури захищених комп’ютерних систем. Монографія. - К.: ДУПСТ, 2011. - с.257.
6. Журавська І. М. Проектування та монтаж локальних комп’ютерних мереж : [навчальний посібник] / І. М. Журавська. – Миколаїв : Видавництво ЧДУ ім. Петра Могили, 2016. – 396 с.
7. Business Products. URL:: http://www.trendnet.com/products/business/category/switches. (дата звернення: 18.04.2026.)
8. Комутатори URL: http://hotline.ua/computer/kommutatory/ (дата звернення: 11.05.2024.)Москальова В.М. Охорона праці URL: http://studentbooks.com.ua/content/view/1327/76/ (дата звернення: 11.04.2026.)
9. Діагностика локальних мереж URL: http://ukrefs.com.Ua/print:paqe.1.170653-Diaqnostika-lokal-nyh-seteiy.html (дата звернення: 18.04.2026.)
10. Cisco RV345P-K9-G5 URL: https://brain.com.ua/ukr/Fayervol Cisco RV345P-K9-G5-p293786.html (дата звернення: 19.04.2026.)
11. Монтаж СКС URL: https://lib.chmnu.edu.ua/pdf/posibnuku/356/12.pdf (дата звернення: 20.04.2026.)
12. Налаштування точки доступу без контролера URL: https://lantorq.com/article/rabota-i-nastroyka-unifi-ap-bez-kontrollera/ (дата звернення: 22.04.2026.)

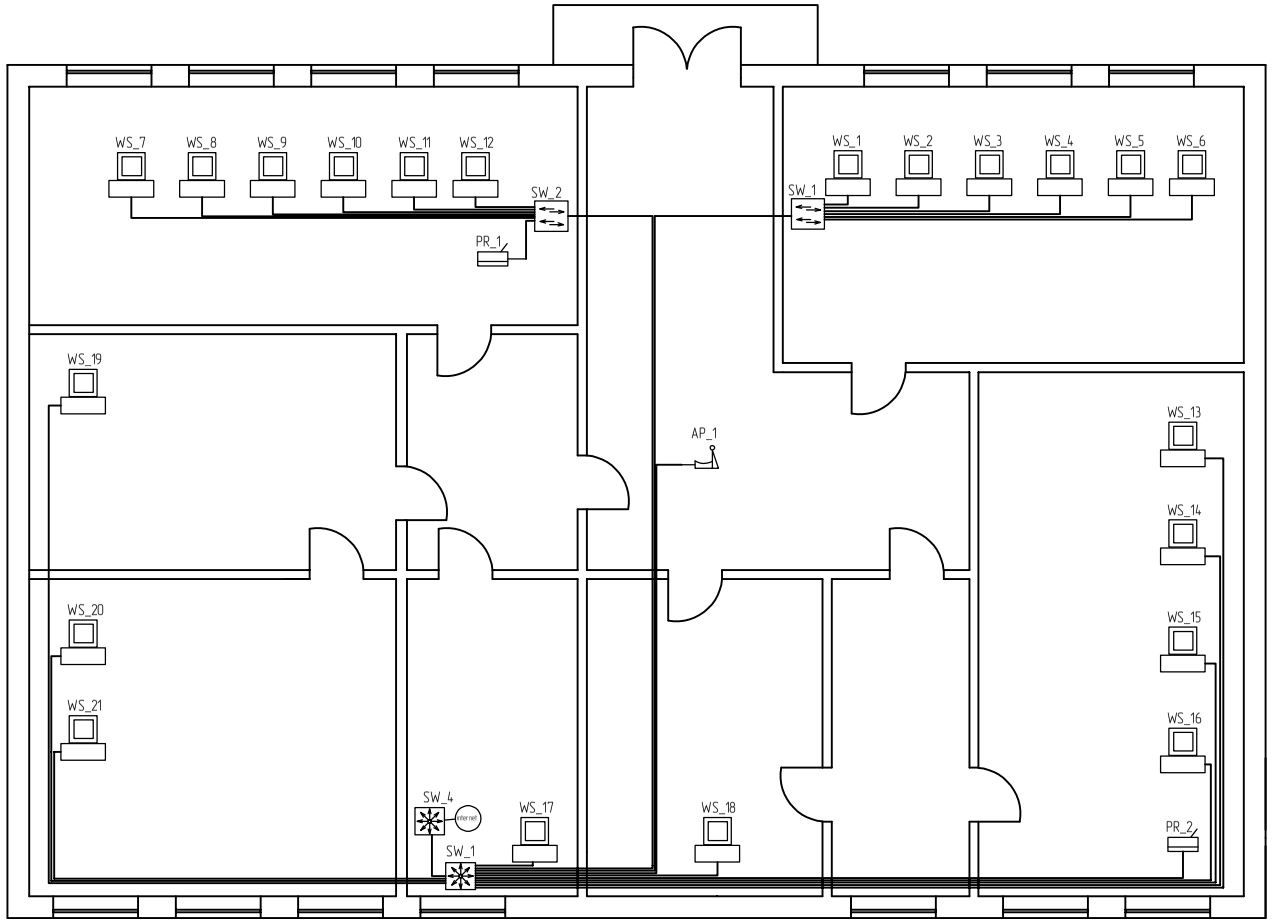


						2026.КВР.123.412.14.00.00 /ІТ	
Зм	Арк	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі ПП "СТО сорок" Логічна топологія	Літ.	Маса	Масшт.
Розроб.		Цяпцяпа А І						
Керів		Пиж В С						
Н.контр.		Язькіб А В				Аркуш 1	Аркушів 1	
Рецензія						ВСП ТФК ТНТУ КІ-412, м.Тернопіль		

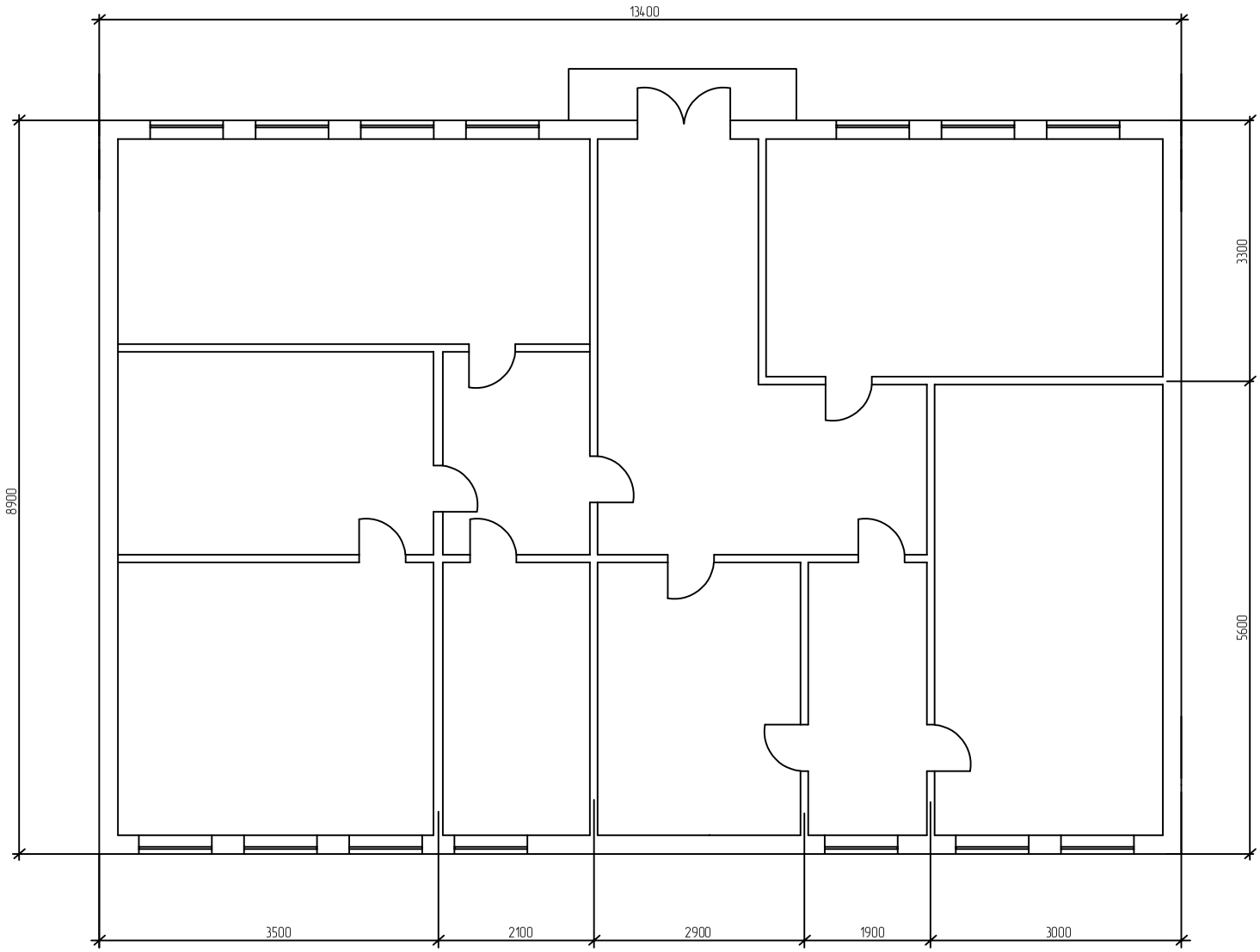
ТАБЛИЦЯ IP-АДРЕСАЦІЇ В МЕРЕЖІ					
№ П.П	НАЗВА	IP-АДРЕСА	МАСКА	РОБОЧА ГРУПА	НОМЕР VLAN
1	WS_1	192.168.100.1	255.255.255.0	work100	100
2	WS_2	192.168.100.2	255.255.255.0	work100	100
3	WS_3	192.168.100.3	255.255.255.0	work100	100
4	WS_4	192.168.100.4	255.255.255.0	work100	100
5	WS_5	192.168.100.5	255.255.255.0	work100	100
6	WS_6	192.168.101.1	255.255.255.0	work101	101
7	WS_7	192.168.101.2	255.255.255.0	work101	101
8	WS_8	192.168.101.2	255.255.255.0	work101	101
9	WS_9	192.168.101.3	255.255.255.0	work101	101
10	WS_10	192.168.101.4	255.255.255.0	work101	101
11	WS_11	192.168.101.5	255.255.255.0	work101	101
12	WS_12	192.168.101.6	255.255.255.0	work101	101
13	WS_13	192.168.102.1	255.255.255.0	work102	102
14	WS_14	192.168.102.2	255.255.255.0	work102	102
15	WS_15	192.168.102.2	255.255.255.0	work102	102
16	WS_16	192.168.102.3	255.255.255.0	work102	102
17	WS_17	192.168.102.4	255.255.255.0	work102	102
18	WS_18	192.168.103.5	255.255.255.0	work103	103
19	WS_19	192.168.103.1	255.255.255.0	work103	103
20	WS_20	192.168.103.2	255.255.255.0	work103	103
21	WS_21	192.168.102.2	255.255.255.0	work103	10
22	SW_1	192.168.101.6	255.255.255.0	work103	10
	SW_1	призначається провайдером			
23	AP_1	192.168.200.100	255.255.255.0	IP	200
21	PR_1	192.168.10.160	255.255.255.0	work	10
22	PR_2	192.168.10.161	255.255.255.0	work	10

ТАБЛИЦЯ ТЕХНІКО-ЕКОНОМІЧНИХ ПОКАЗНИКІВ

№ п\п	параметр	одинмці вимірювань	значення	№ п\п	параметр	одинмці вимірювань	значення
1	технологія мережі	–	ethernet 1000	8	марка точки доступу	–	MikroTik cAP ac (RBcAPGi-5acD2n) EBA63 AX3000
2	топологія мережі	–	гібридна	9	операційна система робочих станцій	–	windows 10\11
3	середовище передачі	–	Вита пара кат. 5E	10	тип доступу до інтернет	–	вита пара
4	кількість вузлів мережі	шт	21	11	термін окупності	рік	1,5
5	марка головного комутатора	–	Cisco CBS250-16T-2G	12	плановий прибуток	грн	30756,7
6	марка 16-ти портового комутатора	–	TP-Link TL-SG1016D	13	собівартість	грн	60071,8
7	маршрутизатор	–	MikroTik hEX S	14	ціна	грн	90828,5



						2026.КВР.123.412.14.00.00 ФТ	
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі ПП "СТО сорок" Фізична топологія	Літ.	Маса	Масшт.
Розроб.		Цапута А. І.						1:100
Керів.		Лих В. С.				Аркуш 1	Аркушів 1	
Н.контр.		Юзьків А. В.				ВСП ТФК ТНТУ КІ-412, м.Тернопіль		
Рецензія								
затв.								



						2026.КВР.123.412.14.00.00 ПП	
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі ПП "СТО сорок" План приміщень	Літ.	Маса	Масшт.
Розроб.		Цапутра А. І.						1:100
Керів.		Пих В. С.				Аркуш 1	Аркушів 1	
Н.контр.		Юзьків А. В.				ВСП ТФК ТНТУ КІ-412, м.Тернопіль		
Рецензія								
затв.								