Форма № Н-9.02

Міністерство освіти і науки України

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

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

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра
(освітньо-професійного ступеня)

на тему: **Розробка проєкту комп'ютерної мережі компанії "Стиль-Н"**

Виконав: студент IV курсу, групи КІ-412

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

_____ **Олександр ЦИГИПАЛО**
(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

Цигипало Олександру Михайловичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту комп'ютерної мережі компанії "Стиль-Н"**

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 _____ Олександр ЦИГИПАЛО
(підпис) (ім'я та прізвище)

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

АНОТАЦІЯ

Цигипало О М - Розробка проєкту комп’ютерної мережі компанії “Стиль-Н”: кваліфікаційна робота на здобуття освітньо-професійного ступеня фахового молодшого бакалавра, за спеціальністю 123 Комп’ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2026. -84с.

Тема даної роботи - “Розробка проекту комп'ютерної мережі компанії «Стиль-Н»

Мета даної роботи - спроектувати комп’ютерну мережу організації. При проектуванні ставляться вимоги забезпечення потрібної швидкості передачі інформації, спільного використання ресурсів, доступ до Інтернет.

Щоб спроектувати мережу приводиться опис організації, її план приміщень, і на основі нього, використовуючи знання про технології та топології передачі даних підбирається комутуюче обладнання та проводиться опис його налаштування. Також проводиться опис обґрунтування вибору програмного забезпечення та способи його налаштування.

Описано методику розрахунку вартості робіт та описано техніку безпеки при монтажі та налагодженні мережі.

ANNOTATION

Tsigipalo O M - Development of a computer network project for the company “Style-N”: qualification work for obtaining an educational and professional degree of a junior bachelor, in the specialty 123 Computer Engineering. Ternopil: VSP “TFK TNTU”, 2026. -84p.

The topic of this work is “Development of a computer network project for the company “Style-N”

The purpose of this work is to design a computer network for the organization. When designing, requirements are set for ensuring the required speed of information transfer, sharing of resources, and access to the Internet.

To design a network, a description of the organization, its premises plan are provided, and based on it, using knowledge of data transmission technologies and topologies, switching equipment is selected and its configuration is described. The justification for the choice of software and methods for its configuration is also described.

The methodology for calculating the cost of work is described and safety precautions during network installation and setup are described.

ЗМІСТ

ВСТУП.....8
1 ЗАГАЛЬНИЙ РОЗДІЛ.....9
1.1 Технічне завдання.....9
1.1.1 Найменування та область застосування.....9
1.1.2 Призначеннння розробки.....10
1.2.3 Вимоги до апаратного та програмного забезпечення.....11
1.2.4 Стадії та етапи розробки.....13
1.1.5 Вимоги до документації.....14
1.1.6 Техніко-економічні показники.....15
1.1.7 Порядок контролю та прийому.....16
2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ.....17
2.1 Опис задачі та характеристика підприємства.....17
2.2 Розробка та обґрунтування логічної та фізичної схем мережі.....19
2.3 Підбір обладнання для проектованої мережі.....27
2.4 Особливості монтажу мережі [14].....38
2.6 Тестування мережі.....41
2.7 Захист комп'ютерної мережі.....45
3 СПЕЦІАЛЬНИЙ РОЗДІЛ.....49
3.1 Налаштування маршрутизатора.....49
3.2 Інструкція з використання тестових наборів та тестових програм.....55
4 ЕКОНОМІЧНИЙ РОЗДІЛ.....59
4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР.....59
4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи 60
4.3 Розрахунок матеріальних витрат.....62

					2026.КВР.123.412.13.00.00 ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Цигипало О М			Розробка проєкту комп'ютерної мережі компанії "Стиль-Н" Пояснювальна записка	Літ.	Арк.	Аркушів
Перевір.		Пиж В С						
Реценз.						ВСП ТФК ТНТУ КІ-412 м. Тернопіль		
Н. Контр.								
Затверд.								

4.4 Розрахунок витрат на електроенергію.....64
4.5 Визначення транспортних затрат.....64
4.6 Розрахунок суми амортизаційних відрахувань.....65
4.7 Обчислення накладних витрат.....65
4.8 Складання кошторису витрат та визначення собівартості НДР.....66
4.9 Розрахунок ціни НДР.....67
4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень.....67
5.1 Вимоги безпечного виконання електромонтажних робіт при організації кабельних трас компанії “Стиль-Н”.....69
5.2 Оцінка та нормалізація рівнів шуму і вібрації на робочих місцях адміністраторів.....73
5.3 Аналіз пожежонебезпечних властивостей ізоляційних матеріалів та права керівника щодо контролю пожежної безпеки в компанії “Стиль-Н”.....76
ВИСНОВКИ.....81
ПЕРЕЛІК ПОСИЛАНЬ.....82

ВСТУП

Локальна обчислювальна мережа (ЛОМ) розглядається як фундамент сучасної ІТ-інфраструктури, що забезпечує інтеграцію комп'ютерних та периферійних систем у межах локалізованої території. На відміну від глобальних мереж, ЛОМ характеризується приватною формою власності, підвищеною пропускною здатністю та низьким коефіцієнтом бітових помилок, що критично важливо для корпоративного сектора.

Ключові вектори ефективності ЛОМ:

– Оптимізація ресурсів: Перехід від ізольованих робочих станцій до колективного використання серверних потужностей, дискових масивів (NAS) та мережевого друку.

– Централізація адміністрування: Можливість консолідованого управління безпекою, правами доступу та оновленням програмного забезпечення.

– Гетерогенність систем: Забезпечення сумісності між обладнанням різних вендорів та різними операційними системами в межах єдиного інформаційного простору.

– Комунікаційна швидкість: Усунення потреби у фізичних носіях даних, що радикально прискорює обробку великих обсягів інформації та мінімізує ризики її втрати.

Згідно зі стандартами IEEE 802, сучасні ЛОМ забезпечують універсальність і масштабованість, підтримуючи роботу сотень вузлів на відстані до кількох кілометрів. Використання технологій Ethernet та Wi-Fi дозволяє гнучко адаптувати топологію мережі під архітектурні особливості приміщень, забезпечуючи стабільно високу швидкість передачі даних (від 100 Мбіт/с до 10 Гбіт/с). Таким чином, ЛОМ виступає стратегічним інструментом для підвищення продуктивності праці та надійності зберігання корпоративних даних.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Кваліфікаційна робота присвячена розробці архітектури локальної обчислювальної мережі для компанії “Стиль-Н”. Основною метою виконання роботи є створення сучасної мережевої інфраструктури, яка забезпечить комплексну автоматизацію бізнес-процесів підприємства шляхом впровадження ієрархічної моделі інформаційних потоків та централізованих систем зберігання даних. Запропоноване рішення передбачає організацію єдиного інформаційного середовища, що дозволить підвищити ефективність обробки даних і спростити управління інформаційними ресурсами.

Реалізація даного проєкту дозволить об’єднати розрізнені технічні засоби підприємства в єдину цілісну інформаційну інфраструктуру. Такий підхід забезпечить можливість подальшого масштабування мережі, впровадження сучасних інформаційних технологій та підвищення загальної ефективності функціонування підприємства.

Проєктована мережева інфраструктура розглядається як інструмент для вирішення ключових стратегічних завдань підприємства, зокрема:

– Консолідація ресурсів. Передбачається інтеграція робочих станцій територіально або функціонально розподілених структурних підрозділів у єдиний логічний сегмент, що забезпечить централізований доступ до інформаційних ресурсів та підвищить ефективність їх використання.

– Оптимізація зовнішніх комунікацій. Планується організація спільного високошвидкісного доступу до глобальної мережі Інтернет для всіх вузлів системи, що дозволить покращити взаємодію із зовнішніми сервісами та інформаційними ресурсами.

– Сервісна інтеграція. Передбачається ефективне розгортання та експлуатація локальних і хмарних мережевих служб, необхідних для забезпечення функціонування підприємства та підтримки його інформаційної діяльності.

– Комунікаційна взаємодія. Створення надійного мережевого середовища для оперативного обміну даними між користувачами, що дозволить скоротити часові витрати на обробку корпоративної інформації та підвищити продуктивність роботи персоналу.

1.1.2 Призначеннння розробки

Проєктована комп'ютерна мережа розглядається як важливий стратегічний ресурс підприємства, який забезпечує ефективну взаємодію між усіма структурними підрозділами. Основною метою розробки є створення стабільного інформаційного середовища для колективної роботи користувачів, що ґрунтується на низці концептуальних вимог та технічних принципів організації мережевої інфраструктури. Такий підхід дозволяє підвищити продуктивність роботи персоналу та оптимізувати використання інформаційних ресурсів.

Впровадження локальної комп'ютерної мережі дозволить трансформувати розрізнені робочі місця підприємства у структуровану систему з високим рівнем керованості, надійності та економічної ефективності. Така інфраструктура створить основу для подальшого розвитку інформаційних технологій та масштабування мережевих ресурсів.

До ключових вимог, які враховуються під час проєктування мережі, належать:

– Оптимізація апаратних витрат. Передбачається консолідація мережевих ресурсів, зокрема використання спільних мережевих сховищ даних і високопродуктивних принтерів. Це дозволяє зменшити потребу в дублю-

ванні периферійного обладнання та скоротити капітальні витрати на його придбання.

– Раціоналізація програмного забезпечення. Планується впровадження мережевих версій програмних продуктів і використання групових ліцензій, що забезпечує централізоване управління програмним середовищем та зменшує витрати на встановлення окремих копій програмного забезпечення для кожного робочого місця.

– Централізація даних та підвищення безпеки. Організація єдиного сховища інформації на базі централізованого серверного ресурсу спрощує процедури резервного копіювання та відновлення даних. Крім того, це дозволяє реалізувати гнучку систему керування доступом користувачів, що сприяє підвищенню рівня інформаційної безпеки підприємства.

– Підвищення комунікаційної ефективності. Створення мережевого середовища для оперативного обміну файлами та повідомленнями між користувачами дозволяє зменшити затримки в обробці інформації та прискорити виконання внутрішніх бізнес-процесів.

– Уніфікація зовнішнього доступу. Передбачається використання спільного високошвидкісного шлюзу доступу до мережі Інтернет, що забезпечує стабільне підключення для всіх користувачів і водночас оптимізує витрати на експлуатацію мережі.

1.2.3 Вимоги до апаратного та програмного забезпечення

Оглядовий технічний аналіз специфікацій проєктованої мережі наведено з урахуванням вимог до пояснювальної записки. У тексті узагальнено основні параметри структурованої кабельної системи та архітектурні особливості мережевої інфраструктури з урахуванням сучасних стандартів побудови локальних мереж.

Технічні характеристики та архітектурні особливості СКС

Проєкт структурованої кабельної системи базується на міжнародному стандарті ISO/IEC 11801 (категорія 5e), що забезпечує надійну підтримку передачі даних на швидкостях 100/1000 Мбіт/с. Застосування пасивних компонентів відповідної категорії гарантує необхідну смугу пропускання для виконання сучасних корпоративних завдань, включаючи обмін файлами, роботу з мережевими сервісами та використання хмарних ресурсів. Крім того, така конфігурація дозволяє забезпечити сумісність із більшістю активного мережевого обладнання та спростити подальшу модернізацію інфраструктури.

Ключові параметри фізичного та апаратного рівнів:

– Організація робочих місць. Кожне робоче місце оснащується уніфікованим портом RJ-45 категорії 5e. Розташування мережевих вузлів визначається відповідно до план-схеми приміщень, що дозволяє оптимізувати довжину кабельних ліній та зменшити втрати сигналу. Такий підхід забезпечує впорядковану структуру кабельної підсистеми.

– Система ідентифікації. Реалізовано метод двостороннього унікального маркування кабелів і монтажних панелей. Це дає можливість швидко ідентифікувати з’єднання, спрощує технічне обслуговування та скорочує час пошуку несправностей у мережевій інфраструктурі.

– Апаратна стратегія. Для побудови мережі використовується стандартне мережеве обладнання з підтримкою функцій адміністрування. Основний акцент зроблено на високій ремонтопридатності, уніфікації компонентів та можливості оперативної заміни обладнання без зупинки роботи мережі.

– Програмне середовище та бездротові технології:

– Програмний стек. Мережева інфраструктура функціонує під управлінням операційних систем сімейства Microsoft Windows, що забезпечує високий рівень сумісності прикладного програмного забезпечення, централізоване адміністрування та спрощену інтеграцію користувачів у корпоративне середовище.

– Бездротовий сегмент. Точки доступу стандарту IEEE 802.11n інтегруються у загальну мережеву інфраструктуру. Для захисту бездротового каналу застосовуються протоколи автентифікації WPA та WPA2-PSK, що зменшує ризик несанкціонованого доступу та підвищує рівень інформаційної безпеки.

Логічний поділ мережі на робочі групи дозволяє оптимізувати мережевий трафік, підвищити ефективність використання пропускної здатності та забезпечити додатковий рівень ізоляції внутрішніх процесів підприємства. Такий підхід сприяє підвищенню стабільності роботи мережі та спрощує її подальше масштабування.

1.2.4 Стадії та етапи розробки

Створення мережевої інфраструктури — це послідовний життєвий цикл, який охоплює збір вихідних даних, розробку рішень, монтаж, пусконалагодження та подальше адміністрування з моніторингом. Така поетапна модель системно організовує впровадження мережі та гарантує її відповідність технічним вимогам підприємства.

Ключовим є етап аналізу вихідної інформації, де формуються базові параметри інфраструктури. На цій стадії бізнес-аналіз діяльності та структури організації дозволяє закласти необхідний резерв масштабованості. Паралельно аналізується стек програмного забезпечення для визначення вимог до пропускної здатності та затримок каналів зв'язку. Формування технічної архітектури передбачає вибір оптимальної топології, середовища передачі даних та складу активного обладнання. В межах інженерного проєктування СКС розраховується структура горизонтальних і вертикальних підсистем, трас та місць розташування телекомунікаційних шаф. На завершення аналізуються зовнішні комунікації для вибору оптимального провайдера, технології підключення до глобальних мереж та продуктивного маршрутизатора з функціями безпеки.

Системний підхід до збору цих даних мінімізує архітектурні помилки під час впровадження, забезпечує відповідність мережі перспективним потребам підприємства, підвищує її надійність і спрощує подальше адміністрування.

1.1.5 Вимоги до документації

Завершальним етапом інженерного циклу проєктування є формування повного пакету технічної документації, який визначає архітектуру майбутньої мережевої системи. Саме якісно підготовлений проєкт створює основу для переходу до стадії монтажу та подальшого ефективного супроводу локальної обчислювальної мережі. Наявність детальної документації дозволяє мінімізувати ризики під час реалізації, забезпечує узгодженість робіт і спрощує подальше адміністрування інфраструктури.

Після введення мережі в експлуатацію підготовлені документи переходять у категорію регламентних матеріалів. Вони використовуються як основа для системного адміністрування, забезпечують можливість оперативної локалізації несправностей і значно спрощують проведення технічного обслуговування. Крім того, така документація стає базою для подальшої модернізації та масштабування ІТ-інфраструктури підприємства, що підвищує її довгострокову ефективність.

До ключових складових проєктного рішення належать такі елементи:

– Логічна топологія. Вона визначає структуру взаємодії мережевих вузлів на логічному рівні. У межах цієї моделі описуються схеми адресації, формується IP-план, визначається сегментація мережевого трафіку за допомогою віртуальних локальних мереж, а також задаються маршрути передачі даних. При цьому логічна структура не залежить від фізичного розташування обладнання, що забезпечує гнучкість конфігурації мережі.

– Фізична топологія. Даний компонент деталізує просторове розміщення мережевого обладнання, комутаційних шаф, патч-панелей та

кабельних трас. Фізична схема відображає реальну прив’язку елементів структурованої кабельної системи до архітектурного плану об’єкта та враховує особливості приміщень, що дозволяє оптимізувати прокладання кабельних ліній і підвищити надійність інфраструктури.

1.1.6 Техніко-економічні показники

Реалізація проєкту ЛОМ базується на комплексному підході до розподілу ресурсів, що охоплює всі етапи — від аналізу до введення в експлуатацію. Структура витрат та часові обмеження визначають економічну доцільність та технічну ефективність впровадження.

Ключові статті витрат проєкту:

– Технічний аудит: Систематизація даних про наявну апаратну базу, оцінка стану та сумісності парку обчислювальної техніки.

– Інженерне проєктування: Формування повного пакету документації, що детермінує логічну та фізичну структуру мережі.

– Матеріальне забезпечення: Інвестиції в активне (комутатори, маршрутизатори) та пасивне (кабельні системи, шафи) обладнання, включаючи професійний монтаж.

– Програмна інтеграція: Ліцензування та конфігурація мережевих операційних систем, серверних ролей та клієнтського ПЗ.

– Валідація системи: Комплексне тестування пропускної здатності та відмовостійкості інфраструктури перед здачею в експлуатацію.

Ресурсний ліміт: Сумарна трудомісткість усіх процесів — включаючи проєктування, розгортання та фінальне налаштування — жорстко обмежена 100 нормо-годинами. Такий часовий регламент вимагає високої кваліфікації виконавців та чіткої координації етапів для дотримання встановлених термінів без втрати якості інфраструктури.

1.1.7 Порядок контролю та прийому

Фінальний етап розгортання мережі полягає у комплексній перевірці функціонування всіх вузлів інфраструктури. Валідація системи здійснюється за допомогою спеціалізованого діагностичного ПЗ та системних утиліт, що дозволяють об'єктивно оцінити стан мережевого середовища.

Регламент передачі об'єкта замовнику: Процес приймання стартує після офіційного повідомлення підрядника про завершення робіт. Замовник зобов'язаний сформувати приймальну комісію у термін до п'яти робочих днів. Комісія проводить всебічний аналіз функціональних характеристик мережі на відповідність технічному завданню.

Завершальним етапом є підписання акту здачі-приймання, що юридично підтверджує готовність IT-інфраструктури до промислової експлуатації.

Програма приймальних випробувань охоплює такі заходи:

– Фізичний рівень: Верифікація цілісності кабельних трас та перевірка відповідності маркування проєктній документації.

– Рівень мережевих налаштувань: Контроль коректності конфігурацій мережевих адаптерів, коректності розподілу IP-адрес, шлюзів та працездатності базових сервісів.

– Доступ до ресурсів: Тестування прав доступу, операцій читання/запису та цілісності даних у централізованих мережевих сховищах.

– Зовнішні комунікації: Перевірка стабільності та безпеки з’єднання з глобальною мережею.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис задачі та характеристика підприємства

Основною метою кваліфікаційної роботи є комплексна розробка, теоретичне обґрунтування та подальше практичне впровадження високопродуктивної локальної комп’ютерної мережі, яка покликана об’єднати всі наявні персональні комп'ютери та периферійне обладнання в єдиний, захищений інформаційний простір. Реалізація проєкту має забезпечити стабільний і швидкий обмін даними між підрозділами, централізоване зберігання критично важливої інформації, а також надати всім робочим станціям спільний, контрольований і безперебійний доступ до мережевих ресурсів, внутрішніх серверів та глобальної мережі Інтернет.

Специфіка фінансово-господарської діяльності досліджуваної організації полягає у високотехнологічному проєктуванні, розрахунку та подальшій експлуатації складних інженерних систем водопостачання, дренажу й меліорації. Крім основного інженерного напряму, компанія володіє та керує власним невеликим торговим майданчиком (магазином), де здійснюється роздрібна та гуртова реалізація спеціалізованої запірної, регулюючої та керуючої арматури для трубопроводів. Усі структурні підрозділи компанії, які підлягають автоматизації та безпосередній інтеграції в створювану локальну обчислювальну мережу, компактно й цілісно розміщені в межах першого поверху однієї адміністративної будівлі.

Приміщення офісу характеризується стандартною висотою стелі, яка від підлоги до плит перекриття становить 3,2 метра, а також комбінованим типом капітальних стін та міжкімнатних перегородок, зведених із сучасних піноблоків та міцної керамогранітної цегли. Зважаючи на ці архітектурно-конструктивні особливості будівлі, а також високі естетичні вимоги до інтер'єру робочих кабінетів, усі монтажні роботи з укладання кабельних ліній структурованої

кабельної системи (СКС) передбачено виконати виключно прихованим способом. Для організації централізованого підведення магістральних кабельних пучків до головної комутаційної шафи, яку заплановано встановити в окремому, ізольованому технічному приміщенні, буде облаштовано вертикальний і горизонтальний приховані канали з використанням захисного пластикового короба великого перерізу (розміром 100×100 мм або аналогічного залежно від загальної місткості кабельного масиву).

Важливою архітектурною та безпековою особливістю проєктування даної мережі є гостра потреба в логічному поділі єдиного фізичного адресного простору на кілька ізольованих віртуальних підмереж (технологія VLAN). Такий підхід дозволить суттєво підвищити загальний рівень інформаційної безпеки підприємства, надійно обмежити поширення шкідливого широкомовного трафіку в межах окремих сегментів, а також мінімізувати обчислювальне навантаження на комутаційне обладнання ядра мережі. Логічна сегментація на підмережі реалізується суворо на основі існуючої організаційної структури компанії, політик безпеки та типу мережевого трафіку для таких функціональних категорій:

- адміністративний апарат та вище керівництво;
- виробничий персонал профільних робочих груп;
- цифрові мультимедійні табло.

Безпосередні робочі місця кінцевих користувачів та мережеве обладнання будуть територіально й логічно розподілені по таких цільових локаціях, як кабінет керівника філії, фінансовий відділ (бухгалтерія), логістичний склад, а також просторі кабінети інженерів та проєктантів. Окремим специфічним елементом проектованої інфраструктури виступають сучасні мережеві смарт-телевізори, які інтегруються в загальну мережу і функціонують як інтерактивні інформаційні табло для оперативного відображення графіків, поточних технічних даних та іншого важливого корпоративного контенту.

2.2 Розробка та обґрунтування логічної та фізичної схем мережі

Топологія (конфігурація або структура) комп’ютерної мережі — це схема фізичного розміщення комп'ютерів та спосіб їхнього об'єднання за допомогою ліній зв'язку.

Цей термін переважно стосується локальних мереж (LAN), оскільки в них архітектуру зв'язків можна чітко відстежити.

Натомість у глобальних мережах (WAN) структура є прихованою від користувача та не має вирішального значення, адже дані щоразу можуть передаватися різними маршрутами.

Обраний тип топології безпосередньо впливає на:

- технічні вимоги до обладнання та тип кабелю;
- методи керування обміном даних;
- надійність, стабільність та можливості масштабування мережі.

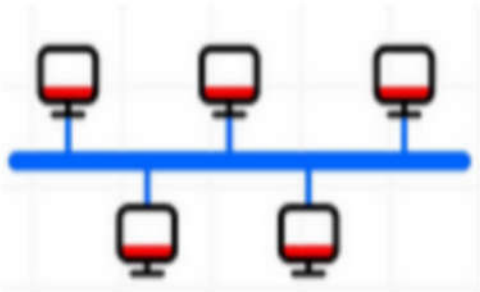


Рисунок 2.1 - Топологія типу “шина”

Виділяють три базові мережеві топології:

- Шина (bus): усі пристрої паралельно підключаються до єдиного спільного каналу зв'язку, через який дані від одного комп'ютера одночасно доступні всім іншим. Показана на рисунку 2.1

– Зірка (star): кожен периферійний комп'ютер з'єднаний з єдиним центральним вузлом через власну виділену лінію. Показана на рисунку 2.2

– Кільце (ring): пристрої об'єднані в замкнуте коло, де кожен комп'ютер приймає інформацію від попереднього і передає її наступному в ланцюжку. Показана на рисунку 2.3

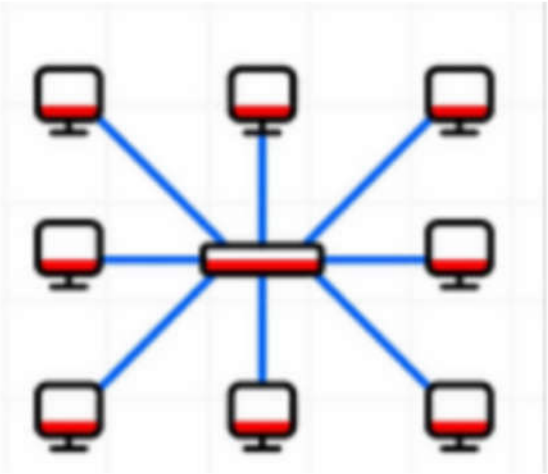


Рисунок 2.2 - Топологія типу “зірка”

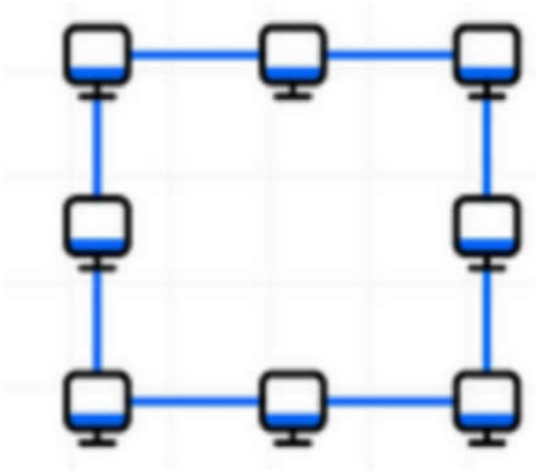


Рисунок 2.3 - Топологія типу “кільце”

Порівняльний аналіз та експлуатаційні характеристики базових топологій

На практиці часто застосовують комбінації базових конфігурацій, проте архітектура більшості сучасних мереж базується на трьох класичних типах. Розглянемо їхні інженерно-технічні особливості.

Топологія «Шина» (Common Bus)

Дана структура передбачає ідентичність мережевого обладнання та повну рівноправність усіх абонентів. Через використання єдиного каналу зв'язку вузли можуть передавати пакети даних лише по черзі. Одночасна передача призводить до накладання сигналів (колізії), тому в шині реалізовано режим напівдуплексного (half duplex) обміну.

Переваги:

– Висока надійність завдяки відсутності центрального комутаційного елемента.

– Простий алгоритм масштабування (підключення нових абонентів можливе без зупинки мережі).

– Мінімальні витрати кабельної інфраструктури.

– Економічна доступність обладнання стандартизованих архітектур (Ethernet, Arcnet).

Недоліки та обмеження:

– Складність апаратної частини мережевих адаптерів, на які покладено функцію вирішення колізій.

– Критична залежність від цілісності лінії: через особливості поширення електричного сигналу на кінцях шини обов'язкове встановлення термінаторів. Обрив кабелю або коротке замикання в будь-якій точці порушує узгодження лінії і повністю паралізує мережу.

– Складність локалізації несправностей та відмов обладнання через паралельне увімкнення адаптерів.

– Обмеження на сумарну довжину ліній через згасання сигналу (для розширення мережі використовують репітери, проте швидкість поширення сигналу обмежує їхню кількість).

Топологія «Зірка» (Star)

Характеризується наявністю чітко виділеного центрального вузла, через який проходить весь інформаційний обмін, що виключає можливість виникнення колізій завдяки централізованому керуванню.

Залежно від апаратної реалізації виділяють такі типи:

– Активна (справжня) зірка: у центрі розташований потужний комп'ютер (сервер), який повністю керує обміном даних.

– Пасивна зірка: у центрі встановлюється комутатор (світч або концентратор), що відновлює сигнали за принципом репітера. Фізично копіюючи схему зірки, логічно вона функціонує як шина, оскільки дані транслюються всім учасникам. Саме пасивна зірка є основою сучасних мереж Ethernet.

– Комбінована зірка: проміжний тип, де концентратор керує обміном, але безпосередньої участі в ньому не бере.

Переваги:

– Локалізація відмов: вихід з ладу периферійного абонента або обрив його кабелю не впливає на загальну працездатність системи.

– Спрощена архітектура кінцевого обладнання та стабільний рівень сигналу, що усуває потребу в зовнішніх термінаторах.

– Зручність адміністрування та моніторингу, оскільки всі точки підключення зосереджені в одному місці.

Недоліки:

– Низька відмовостійкість центрального вузла: його вихід з ладу повністю деактивує мережу.

– Підвищена витрата кабелю порівняно з іншими топологіями, що збільшує загальну вартість проєкту.

Топологія «Кільце» (Ring)

Передбачає послідовне з'єднання, за якого кожен комп'ютер зв'язаний лише з двома сусідніми. Важливою особливістю є те, що кожен абонент ретранс-

лює (відновлює) сигнал, виступаючи в ролі репітера, що мінімізує проблему згасання інформаційного сигналу на великих відстанях.

Право на передачу даних послідовно переходить по колу від одного комп'ютера до іншого за допомогою спеціальних маркерних методів керування.

Переваги:

– Найвища стійкість до перевантажень та здатність ефективно оперувати великими потоками інформації через відсутність колізій.

– Можливість побудови мереж великої протяжності (до десятків кілометрів).

– Відсутність потреби у зовнішніх термінаторах та центральному абоненті.

Недоліки:

– Низька відмовостійкість: вихід з ладу одного комп'ютера або обрив кабелю припиняє роботу всієї мережі. Для нівелювання цього недоліку часто прокладають другу (резервну) паралельну лінію, що також дозволяє подвоїти швидкість обміну за умови використання двоспрямованого трафіку.

– Підключення нового абонента потребує повної технологічної зупинки мережі.

Багаторівнева класифікація поняття мережевої топології

Окрім базових архітектур, часто використовується топологія «дерево» (tree), яка є ієрархічним поєднанням кількох пасивних або активних «зірок».

У контексті системного аналізу комп'ютерних мереж поняття «топологія» слід розглядати на чотирьох різних рівнях архітектури:

– Фізична топологія — реальна геометрична схема розташування комп'ютерів та прокладки кабельних ліній.

– Логічна топологія — структура внутрішніх зв'язків та фізичний характер поширення сигналів по мережі.

– Топологія керування обміном — алгоритм та черговість передачі права на захоплення мережевого ресурсу між абонентами.

– Інформаційна топологія — напрямок та архітектура потоків даних, що циркулюють у системі.

Саме характер цих зв'язків визначає підсумкові експлуатаційні параметри мережі: відмовостійкість, складність апаратної частини, метод керування доступом та лінійні масштаби проектованої системи.

Технологічні модифікації архітектури Ethernet та обґрунтування вибору середовища передавання

Ethernet — це базова архітектура комп'ютерних мереж, регламентована стандартом IEEE 802.3, що функціонує на основі логічної топології «шина» із розподіленим середовищем передавання та методом множинного доступу з контролем носія та виявленням колізій (CSMA/CD).

У процесі еволюції технології зафіксовано такі основні фізичні реалізації:

– 10Base5 — мережа на основі «товстого» коаксіального кабелю;

– 10Base2 — специфікація на базі «тонкого» коаксіального кабелю;

– 10Base-T — стандарт Ethernet зі швидкістю 10 Мбіт/с на базі витої пари;

– 10Broad36 — широкосмугова мережа на 75-Омному коаксіальному кабелі з частотним ущільненням каналів;

– 10Base-F — сімейство стандартів для оптичного волокна;

– 100Base-T (100Base-TX, 100Base-T4) — технологія Fast Ethernet зі швидкістю передавання до 100 Мбіт/с.

Маркування архітектур Ethernet здійснюється за уніфікованим принципом:

– Перший елемент вказує на номінальну швидкість передавання даних (Мбіт/с або Гбіт/с).

– Другий елемент визначає метод модуляції: Base — пряме немодульоване передавання (основна смуга частот), Broad — широкосмугове передавання із частотним розподілом каналів.

– Третій елемент детермінує тип середовища (T — вита пара, F — оптоволокно) або максимальну довжину сегмента кабелю в сотнях метрів.

Специфікація 10Base-T використовує дві неекрановані виті пари (UTP) категорії 3, 4 або 5, тоді як Fast Ethernet 100Base-T4 функціонує на базі чотирьох пар UTP категорії 5 або екранованої витої пари (STP). Функціонування вузла вимагає наявності двох пар провідників (окремо для прийому та передавання даних).

Сучасні стандарти передбачають інтеграцію чотирьох пар в один загальний кабель, що суттєво знижує витрати на монтаж і забезпечує модернізацію мережі до більш швидкісних стандартів без реструктуризації кабельної системи.

Основним деструктивним фактором архітектури на витій парі є централізована схема підключення: вихід з ладу кабельного центру (комутатора) призводить до повної деактивації мережевого сегмента. Попри це, середовище передавання на базі витої пари має суттєві експлуатаційні переваги:

– реалізація стійкої фізичної топології «зірка»;

– регламентована довжина кабельного променя до 100 метрів;

– індивідуальне підключення вузлів (пошкодження лінії ізолює лише один суб'єкт мережі);

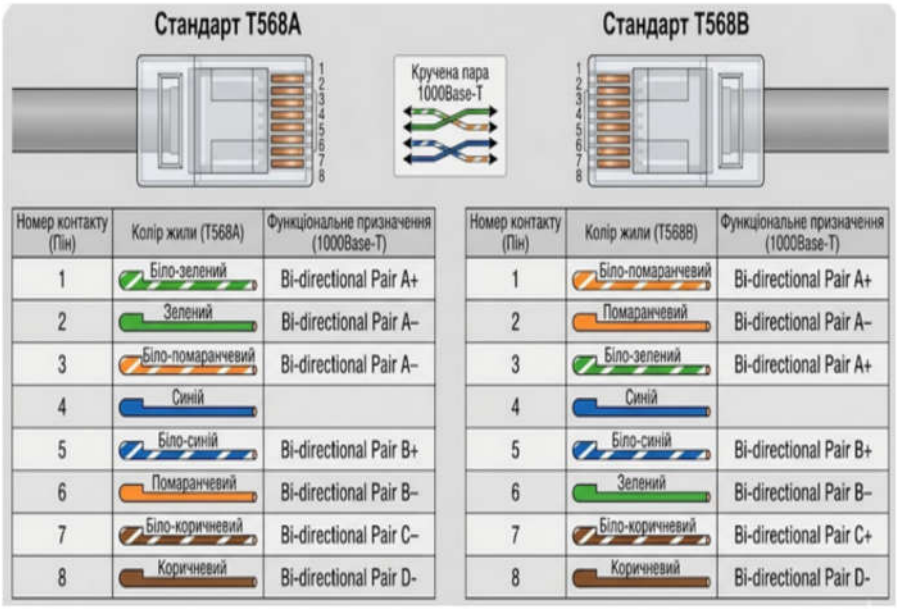
– підвищений рівень захисту від несанкціонованого перехоплення пакетів даних.

Сучасне проєктування локальних обчислювальних мереж майже повністю виключає використання коаксіального кабелю, який наразі застосовується виключно для низькошвидкісних міжпристроєвих з'єднань у монтажних шафах.

Пріоритетними середовищами є оптичне волокно та неекранована вита пара. Зокрема, гігабітний стандарт 1000Base-T орієнтований на кабельні системи крученої пари категорій 5e, 6 та 7.

Обґрунтування архітектурного рішення для проєкту об'єкта

Враховуючи геометричні параметри підприємства, щільність розташування робочих місць та вимоги до пропускної здатності, для реалізації проєкту обрано стандарт Ethernet 1000Base-T.



Номер контакту (Пін)	Колір жили (T568A)	Функціональне призначення (1000Base-T)
1	Біло-зелений	Bi-directional Pair A+
2	Зелений	Bi-directional Pair A–
3	Біло-помаранчевий	Bi-directional Pair A–
4	Синій	
5	Біло-синій	Bi-directional Pair B+
6	Помаранчевий	Bi-directional Pair B–
7	Біло-коричневий	Bi-directional Pair C–
8	Коричневий	Bi-directional Pair D-

Номер контакту (Пін)	Колір жили (T568B)	Функціональне призначення (1000Base-T)
1	Біло-помаранчевий	Bi-directional Pair A+
2	Помаранчевий	Bi-directional Pair A–
3	Біло-зелений	Bi-directional Pair A+
4	Синій	
5	Біло-синій	Bi-directional Pair B+
6	Зелений	Bi-directional Pair B–
7	Біло-коричневий	Bi-directional Pair C+
8	Коричневий	Bi-directional Pair D-

Рисунок 2.4 - Неекранована вита пара категорії 5e та правило її чергування коьорів

Фізичну структуру локальної мережі побудовано на основі неекранованої витої пари (UTP) категорії 5e., обтискання згідно стандарту показане на рисунку 2.4

Даний вибір зумовлений високими техніко-економічними показниками середовища передавання: кабель є економічно доступним, простим у прокладанні, діагностиці та технічному обслуговуванні. Застосування сучасного активного обладнання дозволяє гнучко керувати інфраструктурою.

Базовою архітектурною моделлю визначено топологію типу розширена зірка. Водночас, зважаючи на інтеграцію в структуру бездротових точок доступу (Wi-Fi), підсумкова топологія проєктуємої мережі класифікується як гібридна.

2.3 Підбір обладнання для проектованої мережі

Проєктована локальна обчислювальна мережа (ЛОМ) підприємства базується на поєднанні топологій «розширена зірка» та частково «комірчаста» (mesh), що класифікує підсумкову архітектуру як комбіновану (гібридну).

Таке рішення дозволяє забезпечити баланс між гнучкістю підключення периферійних пристроїв та відмовостійкістю магістральних каналів зв'язку.

Аналіз плану приміщень об'єкта та розрахунок робочих місць показали, що загальна кількість інформаційних розеток, які необхідно інтегрувати в єдиний інформаційний простір, становить менше 48 одиниць.Відповідно, для реалізації апаратної частини достатньо розгортання одного центрального комутатора на 48 портів. Обране обладнання належить до рівня L2+ (Layer 2 Plus) моделі OSI і додатково оснащене 2–4 магістральними аплінк-портами (Uplink/SFP), що створює необхідний технологічний резерв для подальшого масштабування мережі або підключення високошвидкісних сховищ даних (NAS). Для оптимізації мережевого трафіку, підвищення рівня безпеки та обмеження доменів колізій передбачено логічну сегментацію мережі за допомогою технології VLAN (Virtual Local Area Network) відповідно до стандарту IEEE 802.1Q. Центральний комутатор рівня L2+ забезпечує підтримку та тегування VLAN на фізичних портах.

При цьому функції конфігурування віртуальних мереж, маршрутизації міжсегментного трафіку (Inter-VLAN routing) та забезпечення доступу до глобальної мережі Інтернет покладено на головний прикордонний маршрутизатор (роутер).

У межах політики безпеки підприємства та оптимізації смуги пропускання запроєктовано розподіл пристроїв за такими ізольованими сегментами:

– Основний сегмент (робочі станції та сервери): для забезпечення внутрішнього документообігу та доступу до корпоративних ресурсів.

– Сегмент бездротового доступу (Wi-Fi): лінки від бездротових точок доступу підключаються до виділених портів комутатора, які ізольовані в окремий VLAN. Це мінімізує ризики несанкціонованого проникнення до внутрішньої інфраструктури з боку гостьових пристроїв.

– Сегмент мультимедійних пристроїв (Smart TV / телевізори): виділення телевізорів в окрему віртуальну мережу дозволяє ефективно керувати мультимедійним (мультикаст) трафіком та локалізувати широкомовні шторми.

Логічна конфігурація мережевих інтерфейсів, розподіл адресного простору та закріплення ідентифікаторів віртуальних мереж (VLAN ID) зведені та систематизовані у таблиці 2.1.

Таблиця 2.1 – Логічна адресація в мережі та відповідні Vlan-и на портах головного комутатора

Вузол мережі	Робоча група/ номер Vlan		Номер порта головного комутатора	Адреса підмережі/Маска
1	2		3	4
Робочі місця працівників	office	100	1-29, 33-35	100.100.10.0/24
Робочі місця бухгалтерії	buch	200	30-32	100.100.20.0/24
телевізори	tv	300	38-41	100.100.30.0/24
Точки доступу	wifi	400	42-45	100.100.40.0/24
сервери	office	100	47,48	100.100.10.0/24

Для реалізації фізичної та логічної структури мережі, а також забезпечення живлення периферійних пристроїв, як центральний комутатор ЛОМ обрано керований комутатор другого розширеного рівня TP-Link TL-SG3452P (JetStream L2+ Managed Switch).

З метою об’єктивного обґрунтування вибору головного комутаційного обладнання було проведено порівняльний аналіз обраної моделі TP-Link TL-SG3452P із ринковими аналогами у відповідному класі: Cisco Catalyst 1300-48P-4G та MikroTik CRS354-48P-4G+2S+RM.

Всі три пристрої є керованими комутаторами другого/третього (L2+/L3 Lite) рівня, мають 48 гігабітних LAN-портів та підтримують технологію живлення PoE+ (IEEE 802.3at/af). Порівняльні тактико-технічні та експлуатаційні характеристики наведено в таблиці 2.2. , а його вигляд на риснку 2.5. Вартість обраного комутатора 31 500 грн.

Дане апаратне рішення повністю задовольняє архітектурні вимоги проєкту завдяки наявності 48 портів RJ-45 зі швидкістю 10/100/1000 Мбіт/с та 4 незалежних гігабітних SFP-слотів для організації магістральних каналів зв'язку (Uplink).

Важливою інженерною перевагою обраної моделі є повна підтримка технології PoE/PoE+ (стандарти IEEE 802.3af/at) на всіх 48 портах із загальним енергетичним бюджетом 384 Вт. Це дозволяє реалізувати централізоване живлення бездротових точок доступу (`wifi_1`—`wifi_4`) безпосередньо через кабель «вита пара» (UTP Cat 5e), що суттєво знижує витрати на кабельну інфраструктуру та підвищує відмовостійкість системи.

Таблиця 2.2 – Порівняльна характеристика 48 портових комутаторів

Критерій порівняння	TP-Link TL-SG3452P	Cisco Catalyst 1300-48P-4G	MikroTik CRS354-48P-4G+2S+RM
1	2	3	4
Виробник (Бренд)	TP-Link (Китай)	Cisco (США)	MikroTik (Латвія)

Продовження таблиці 2.2

1	2	3	4
Рівень моделі OSI	L2+ (Layer 2 Plus)	L3 Lite / L2+	L3 / L2 (RouterOS / SwOS)
Кількість портів RJ-45	48 × 1 Гбіт/с	48 × 1 Гбіт/с	48 × 1 Гбіт/с
Магістральні порти (Uplink)	4 × 1 Гбіт/с SFP	4 × 1 Гбіт/с SFP	4 × 1 Гбіт/с SFP2 × 10 Гбіт/с SFP+
Комутаційна матриця	104 Гбіт/с	104 Гбіт/с	168 Гбіт/с
Швидкість форвардингу	77,4 Mpps	77,38 Mpps	125 Mpps
Бюджет потуж-ності PoE	384 Вт	370 Вт	750 Вт (гаряча заміна)
Тип охолодження	Активне (4 вентилятори)	Активне (внутрі-шні)	Активне (інтелектуа-льне)
Централізоване керування	Є (Omada SDN Cloud)	Є (Cisco Business Dashboard)	Частково (через CAPsMAN/The Dude)
Цінова категорія	Низька / Середня	Висока	Середня

Рисунок 2.5 – Зовнішній вигляд обраного головного комутатора

Для забезпечення надійного високошвидкісного підключення ЛОМ підприємства до глобальної мережі Інтернет, реалізації Inter-VLAN маршрутизації, налаштування серверів DHCP, NAT та контролю прав доступу (ACL), як пристрій запроєктовано маршрутизатор класу MikroTik CCR2004-16G-2S+PC.

Дана модель побудована на базі високоефективного 4-ядерного 64-бітного процесора Amazon Annapurna Labs Alpine AL32400 (архітектура ARM 64-bit) з тактовою частотою 1,2 ГГц та оснащена 4 ГБ оперативної пам'яті DDR4. Пристрій має 16 гігабітних LAN-портів, розділених на дві групи (кожна група підключена до окремого високошвидкісного чіпа комутації Marvell Amethyst), та 2 оптичні порти SFP+ 10 Гбіт/с для підключення високошвидкісних магістралей або каналів провайдера.

Конструктивною особливістю є масивний радіатор для пасивного охолодження, що забезпечує абсолютно безшумну роботу обладнання та підвищує його надійність через відсутність рухомих елементів.

З метою перевірки вибору проведено порівняльний аналіз технічних характеристик обраного пристрою з аналогами корпоративного класу від провідних виробників (дивися таблицю 2.3)

Таблиця 2.3. Порівняльний аналіз технічних характеристик маршрутизаторів

Критерій порівняння	MikroTik CCR2004-16G-2S+PC	Cisco Business C141M-4P	Ubiquiti UXG-Pro
1	2	3	4
Архітектура процесора	ARM 64-bit (4 ядра, 1.2 ГГц)	ARMv8 (4 ядра, 1.2 ГГц)	ARM Cortex-A57 (4 ядра, 1.7 ГГц)
Оперативна пам'ять (RAM)	4 ГБ DDR4	2 ГБ DDR4	2 ГБ DDR4

Продовження таблиці 2.3

1	2	3	4
Кількість портів RJ-45	16 × 1 Гбіт/с	4 × 1 Гбіт/с LAN, 1 × WAN	2 × 1 Гбіт/с (LAN/ WAN)
Магістральні порти (SFP+)	2 × 10 Гбіт/с	Відсутні	2 × 10 Гбіт/с (LAN/WAN)
Операційна система	RouterOS v7 (Licence L6)	Cisco IOS-XE	UniFi OS
Тип охолодження	Пасивне (безшу-мне)	Пасивне	Активне
Пропускна здатність (NAT/Firewall)	До 15-18 Гбіт/с	До 1.5 Гбіт/с	До 3.5 Гбіт/с (з IDS/IPS)
Орієнтовна ціна в Україні, грн	19 500 — 21 000	27 000 — 30 000	24 000 — 26 500

Результати порівняльного аналізу, наведені у таблиці 2.3, підтверджують раціональність використання моделі від MikroTik з огляду на такі фактори:

– Мережева ємність та інтерфейси: Маршрутизатор MikroTik CCR2004 суттєво перевершує аналоги за кількістю фізичних гігабітних портів (16 портів проти 5 у Cisco та 2 у Ubiquiti). Це дозволяє не лише під-ключити головний 48-портовий комутатор проєкту за допомогою опти-чного лінка 10 Гбіт/с через порт SFP+, а й безпосередньо підключити до маршрутизатора сервери підприємства (S_1, S_2), виділивши їх у макси-мально ізольовану зону.

– Продуктивність обчислень: Завдяки 4 ГБ оперативної пам'яті та операційній системі RouterOS v7 з ліцензією максимального 6-го рівня, пристрій демонструє швидкість обробки трафіку до 18 Гбіт/с. Це гарантує

повну відсутність затримок (bottleneck) при міжсегментній маршрутизації (Inter-VLAN) між офісною мережею, бухгалтерією та мультикаст-трафіком телевізорів.

– Надійність та експлуатація: Пасивна система охолодження усуває ризики відмови пристрою через заклинювання чи запилення кулерів. Пристрій може монтуватися як у стандартну 19-дюймову стійку (за допомогою комплектних кронштейнів), так і розміщуватися настільно.

– Економічний аспект: Пристрій є найдешевшим з-поміж представлених аналогів, пропонуючи при цьому функціонал операторського рівня без необхідності придбання додаткових ліцензій (на відміну від Cisco).

Таким чином, використання маршрутизатора MikroTik CCR2004-16G-2S+PC у парі з раніше обраним комутатором TP-Link забезпечує найвищу продуктивність, гнучкість налаштування та економічну ефективність у межах бюджету проєкту ЛОМ підприємства, зовнішній вигляд ораного маршрутизатора приведено на рисунку 2.6

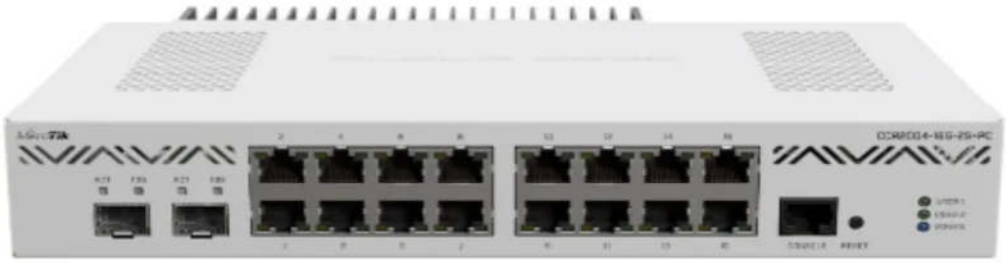


Рисунок 2.6 – Зовнішній вигляд обраного маршрутизатора Mikrotik CCR2004-16G-2S+PC

Для побудови бездротового сегмента локальної мережі (VLAN 400), забезпечення покриття Wi-Fi та підтримки мобільних робочих місць запроє-

ктовано використання дводіапазонних точок доступу MikroTik cAP XL ac (RbcAPGi-5acD2nD-XL).

Проведення порівняльного аналізу з аналогами інших виробників для даного класу обладнання є недоцільним, оскільки вибір пристроїв від MikroTik обумовлений жорсткими архітектурними вимогами щодо однорідності мережевого середовища.

Оскільки головним прикордонним пристроєм у проєкті визначено маршрутизатор серії CCR цього ж виробника, інтеграція точок доступу cAP XL ac дозволяє реалізувати апаратно-програмний комплекс централізованого керування CAPsMAN (Controlled Access Point system Manager).

Технологія CAPsMAN функціонує безпосередньо на базі операційної системи RouterOS маршрутизатора і забезпечує:

– створення єдиного бездротового простору (ESSID) з автоматичним розподілом частотних каналів;

– підтримку безшовного роумінгу (стандарти IEEE 802.11r/k/v) для мобільних абонентів без обриву мережевих сесій;

– централізований моніторинг стану радіоефіру та безпеки бездротового периметра.

Модель MikroTik cAP XL ac оснащена покращеною антеною з високим коефіцієнтом підсилення (5,5 дБі на частоті 2,4 ГГц та 6 дБі на 5 ГГц), підтримує стандарт 802.11ac Wave 2 (Wi-Fi 5) та має два гігабітних порти Ethernet. Живлення пристроїв здійснюється за технологією PoE (Passive PoE або 802.3af/at) безпосередньо від раніше обґрунтованого головного комутатора TP-Link TL-SG3452P через перший порт, тоді як другий порт може використовуватися для послідовного підключення (data pass-through) додаткового обладнання.

Конструктивне виконання пристрою передбачає непомітний стельовий або настінний монтаж, що дозволяє органічно інтегрувати його в інтер'єр приміщень підприємства.

Зовнішній вигляд і дизайн стельової точки доступу наведено на рисунку 2.7.

Рисунок 2.7 – Зовнішній вигляд точки доступу

Вибір серевера проведемо по https://artline.ua/uk/product/server-artline-business-t22v02.

Сервер Сервер ARTLINE Business T22v02 / AMD 6-core Ryzen 5 5500GT 3.6-4.4GHz / 32GB DDR4-3200 / 4 slots, maximum up to 128GB / 2x480GB SSD / 2x2TB / AMD B550 / Інтегрована / 400W 80+ Bronze / Tower / 1Gbit / Без ОС / 38міс. / T22v02

Сучасні підприємства і організації з IT-інфраструктурою обов'язково працюють під управлінням сервера. Його роль може виконувати як звичайний ПК із спеціалізованим ПО, так і ціла мережа пристроїв під обслуговуванням команди фахівців. Зупинка роботи сервера паралізує роботу всієї компанії, і тому вкрай важливо вибрати пристрій, який забезпечить стабільне виконання завдань з мінімальними витратами.

Компанія ARTLINE має багаторічний досвід в збірці, налаштуванні та обслуговуванні подібних пристроїв. Сервери ARTLINE Business стануть для вас надійним фундаментом у вирішенні офісних і виробничих завдань, вони

втілюють все, що Ви чекаєте від сервера: надійність, довговічність, продуктивність, економічність, простоту експлуатації, та, звичайно ж, вигідну ціну.

Ретельно підібрана конфігурація ARTLINE Business T22v02 включає в себе:

– Форм-фактор класичної вежі, який дозволить інтегрувати цю модель в будь-який, навіть невеликий офіс без додаткової покупки спеціалізованої серверної шафи. Оптимальний повітряний потік всередині корпусу забезпечить відмінне охолодження всіх компонентів даного сервера. Таким чином, T22v02 легко встановити, підключити і обслуговувати протягом усього терміну експлуатації.

– AMD Ryzen 5 5500GT з 8 ядрами, 16 потоками і частотою до 4.4 ГГц має кращу продуктивність багатозадачності в своєму класі.

– Материнську плату ASUS PRIME B550M-A формату micro-ATX з безліччю актуальних інтерфейсів, включаючи USB 3.1 Gen 2, M.2 (зі швидкістю передачі даних до 32 Гбіт/с і підключення сучасних SSD) і фірмовим комплексом захисних технологій 5X Protection III, який охоплює цілий ряд інженерних рішень, що служать для захисту від електричних перевантажень, корозії, електростатичних розрядів та інших неприємностей.

– ОЗУ з типом пам'яті DDR4, частотою 3200 МГц і об'ємом 32 ГБ.

– Два HDD об'ємом по 2 ТБ і два SSD-накопичувача по 480 ГБ для інсталяції ОС і необхідного для коректної роботи сервера ПО.

– Встановлений блок живлення Seasonic потужністю 400 Вт з сертифікатом 80+ Bronze, як один з найбільш надійних БЖ на ринку. Це гарантує безпроблемну роботу сервера довгі роки.

Купуючи сервер від компанії ARTLINE, Ви отримуєте професійно зібраний і надійний пристрій, забезпечений гарантійним пакетом Artline Premium з терміном ремонту в СЦ не більше 3-х днів, якісне технічне обслуговування безпосередньо від виробника.

Отже, ми обрали таке обладнання:

маршрутизатор — 1 шт — 16 700 грн - Mikrotik CCR2004-16G-2S+PC

комутатор головний - 1 шт — 31 500 грн - TP-Link TL-SG3452P

точка доступу — 4 шт — 3 500 грн - Mikrotik cAP XL ac (RbcAPGi-5acD2nD-XL)

сервер — 2 шт — 31 000 грн- ARTLINE Business R15v14+

2.4 Особливості монтажу мережі

Щоб кабель передавав дані без втрат, сигнал був якісним, а швидкість залишалася на належному рівні важливо правильно вибрати та прокласти кручену пару.

Вибір кручений пари

Насамперед, слід визначитися, де монтуватиметься кабель: у приміщенні або на вулиці. Внутрішні моделі оснащуються щільними оболонками з полівінілхлориду, часто вогнетривкими. Така ізоляція добре захищає провідники від перегинів, пилу та вологи. Однак вона не стійка до ультрафіолету та морозів, сильних механічних навантажень. Тому для вуличної прокладки варто вибирати спеціальну зовнішню кручену пару. Оболонка такого кабелю виготовляється із щільного поліетилену. Він забезпечує стійкість до перепадів температури, прямим сонячним променям та механічним ушкодженням.

Примітка: зовнішні кабелі зазвичай менш гнучкі, ніж внутрішні. Це важливо врахувати під час проведення монтажних робіт.

Окрім способу прокладання, при виборі варто орієнтуватися на матеріал провідників. їх роблять із сталі, алюмінію та міді. Також часто зустрічаються біметалічні варіанти - алюмінієві з мідним покриттям. Найкраще - мідний варіант. Він забезпечує якісніший сигнал, та до перегинів стійкіший.

Також важливо врахувати технічні характеристики, такі як категорію, кількість пар та екранування.

Категорія свідчить про максимальну швидкість передачі.

Що стосується типу екранування, то все залежить від умов монтажу. Якщо провід планується прокладати поруч із джерелами електромагнітного випромінювання (трансформаторами, електронікою), треба брати екранований кабель. Найпоширеніші - це FTP, із загальним для всіх пар екраном у вигляді фольги, і STP - з екраном у вигляді металевого обплетення. Але й інші варіанти. Екран захищає від радіочастотних перешкод.

Особливості монтажу крученого кабелю

Прокладання дроту у приміщенні. Ідеальний варіант - монтувати кабель усередині стіни, підлоги чи стелі. У цьому випадку його укладають у перекриттях, розміщуючи в гофрованих трубах або металорукавах. Головний плюс - провід добре захищений від зовнішніх впливів. Ще одна перевага — після ремонту кабелів не видно. У стіну, підлогу чи стелю можна укласти кабель, тільки якщо в приміщенні ще не зроблено ремонт.

У відремонтованому приміщенні можна прокласти кабель у спеціальному коробі. Найчастіше — пластиковому.

Він може кріпитися на стіну замість плінтуса і на стелю.

Фіксуються короби просто: на клей або шурупи. Перевага такого способу - легкий монтаж. Є варіанти, розраховані на різну кількість кабелів, що відрізняються діаметром. У такого способу прокладання є плюси:

– простота обслуговування та легкість розширення мережі: щоб відремонтувати провід, прокласти нову лінію, треба просто зняти кришку кабель- каналу;

– додатковий захист: короб береже провід від перегинів, вологи та пилу.

При прокладанні кабелю в каналі паралельно з електропроводкою варто поставити перегородку, яка розділить мережеву та силову частини. Це захистить від електромагнітного випромінювання.

Ще один метод внутрішнього монтажу - прокласти кабель по периметру приміщення та закріпити скобами. Однак тут більше мінусів, аніж плюсів. Недоліки способу - відсутність додаткового захисту дроту і порушення естетичності. Плюси - простота та невисока вартість прокладки.

При монтажі слід дотримуватися радіуса вигину, який виробник зазвичай вказує в характеристиках дроту. В іншому випадку ви ризикуєте поламати провідники.

Зазначимо, що найкраще підключати комп'ютери та мережеві пристрої за допомогою спеціальних сполучних шнурів на основі крученої пари — литих патч-кордів.

Це кабель, який обтиснутий конекторами з обох кінців. Однак якщо відстань між комутованими девайсами велика, довжини патчкорду може не вистачити.

З особливостей прокладки кабелю в даній мережі слід наголосити таке:

– всі робочі місця обладнанні розетками RJ45, котрі розміщені на стіні приміщення на висоті 30 см від підлоги (це показано на листі — фізична топологія),

– до розетки кабель монтується в стіні в штробах з підйомом понад стелею Армстронг, там він зібраний пучками та йде до ІТ відділу де він спускається в коробі 100х100 мм до комутаційної шафи та закінчується “забитим” в пач-панель,

– аналогічно проведені розетки для телевізорів, лише вонии знаходяться на висоті 1600 мм над підлогою,

– розетки точок доступу також проведені аналогічно, але вони знаходяться понад стелею Армстронг у вказаних місцях по схемі, котра зображена на листі — Фізична топологія. Там понад стелею варто забезпечити надлищок кабелю, скрученого в міні бухти, довжиною 3-5 метрів, для можливості радіопланування.

2.6 Тестування мережі

Тестування комп'ютерної мережі є завершальним етапом монтажу комп'ютерної мережі, а також необхідною умовою її прийняття в експлуатацію. Тестування дає можливість переконатися у якості роботи системи та нормальному функціонуванні всіх мережних додатків, а також гарантувати відповідність мережі існуючим нормативним документам. Об'єктивне тестування комп'ютерної мережі дозволяє усунути як дрібні, і серйозні недоліки у її роботі, заощадити на подальшому обслуговуванні комп'ютерних мереж хорошу суму.

Що таке тестування комп'ютерної мережі?

Отже, від якості тестування комп'ютерної мережі безпосередньо залежить її надійність та довговічність, тому до цього питання слід підходити вдумливо та докладно. Навпаки, якщо з тестуванням комп'ютерної мережі поспішити або зовсім пустити справу на самоплив, під загрозою опиниться вся інформаційна база підприємства.

Тестування комп'ютерних мереж реалізується як за допомогою спеціального тестового обладнання, так і з використанням комп'ютерного обладнання та програмного забезпечення. Процедура тестування включає наступні опорні пункти:

- детальне вивчення роботи мережі
- оцінка якості сигналів, що передаються
- виявлення «прихованих» дефектів
- визначення «вузьких місць» продуктивності серверів
- оцінка захищеності мережі від вторгнення внутрішніх та зовнішніх порушників
- внесення необхідних доповнень та коректив
- завершальне регулювання налаштувань обладнання
- усунення несправностей у роботі

Після завершення тестування пасивного та активного обладнання комп'ютерної мережі на неї складається документація " - процедура, покликана допомогти майбутнім користувачам мережі експлуатувати її вільно, раціонально і з максимально високими для роботи підприємства результатами.

Проблеми, що виникають у локальних мережах, можна умовно розділити на три основні групи: несправності на фізичному рівні, перевантаження в мережі і помилки в роботі мережевих протоколів. Несправності фізичного рівня обумовлені виходом з ладу будь-яких електричних або електронних мережевих пристроїв та компонентів. Перевантаження в мережі виникають, якщо той чи інший мережевий пристрій не справляється з обробкою запитів, що до нього надходять. Помилки в роботі мережних протоколів призводять до того, що мережні пристрої не можуть взаємодіяти один з одним через некоректне функціонування мережних драйверів або неможливість обробки мережею пакетів якогось протоколу (або декількох протоколів одночасно).

Несправності фізичного рівня можуть виникнути у мережному пристрої, середовищі передачі або в місці їх контакту. Вони найпростіше піддаються виявленню, оскільки мають постійний характер (природно, досі їх усунення). Локалізувати несправність можна зокрема за допомогою найпростіших тестерів для локальних мереж. Такі тестери перевіряють роботу каналу в один бік (від тестера до концентратора або мережної плати комп'ютера). Якщо дефект має місце в середовищі передачі, його можна виявити за допомогою кабельного тестера. Плаваючі помилки, зумовлені поганим контактом у з'єднувачах, діагностувати дещо складніше. Але навіть такі несправності можна виявити за допомогою кабельного тестера – достатньо бути уважним. До речі, хоч як це банально звучить, але хочеться нагадати, що найкращий спосіб профілактики утворення дефектів у середовищі передачі - використання якісних матеріалів та виконання професійного монтажу.

Зовсім інша справа - помилки внаслідок навантаження мережі та некоректної роботи мережевих протоколів. Такі помилки найважчі у виявленні,

оскільки найчастіше носять нерегулярний характер. Вони й більш підступні, оскільки можуть паралізувати роботу організації у невідповідний момент. Їх інструментальна діагностика виконується за допомогою досить дорогих приладів - мережевих тестерів та аналізаторів протоколів.

Мережеві тестери займають проміжне положення між кабельними тестерами та аналізаторами протоколів. Вони є незамінними для пошуку несправностей у мережах. Виробники випускають широку гаму таких приладів, що відрізняються набором контрольованих параметрів та сервісних функцій, здатністю працювати в тих чи інших мережах (наприклад, Ethernet та/або Token Ring), конструктивним виконанням та ціною. Ці прилади дозволяють вимірювати безліч різних параметрів, наприклад пікову та усереднену завантаженість, частку широкомовного трафіку, збої у роботі протоколів верхніх рівнів. У мережах Ethernet деякі з них здатні підраховувати кількість конфліктів (колізій), ідентифікувати адреси DLC-пакетів (з помилками CRC, коротких та довгих), відрізняти фрагменти від пакетів з помилками CRC та коротких пакетів.

Надзвичайно зручною та корисною є здатність деяких мережевих тестерів зберігати результати тестування для подальшої обробки. Зазвичай результати завантажуються потім у комп'ютер і обробляються відповідними програмами отримання аналітичної інформації (наприклад, піку максимального навантаження у мережі, кількості і типів помилок). Для отримання повної картини функціонування мережі дані можуть бути відсортовані за протоколами та помилками.

Деякі сучасні моделі мережевих тестерів можуть працювати як сервери Web, тому вони дозволяють як інтерфейс користувача використовувати звичайний браузер. Але найцікавішими пристроями є прилади, що поєднують функції портативного мережевого та кабельного тестера. Хоча їхня вартість і висока, вони поєднують у собі найкращі якості обох пристроїв і надзвичайно зручні в експлуатації.

Незважаючи на всі переваги, портативні мережеві тестери мають один недолік - вони не можуть перехоплювати і декодувати пакети. І якщо такі можливості необхідні, наприклад, для більш глибокого вивчення проблем функціонування мережних додатків, тоді вам варто звернути увагу на аналізатори протоколів. Фактично вони є комп'ютером з одним або кількома мережевими інтерфейсами, зі спеціалізованим програмним забезпеченням. Деякі з цих аналізаторів можуть розуміти дві сотні (!) різних протоколів. Кожен як мінімум здатний перехоплювати пакети та фільтрувати їх відповідно до заданих параметрів. Використовуючи відповідні фільтри, ви можете отримати масу різної інформації, що іноді виявляється просто незамінною. Надалі збережена інформація може бути оброблена для складання узагальненого зведення про пакети та отримання детального резюме про протоколи, що використовуються в них. Крім того, всі аналізатори фіксують час проходження пакета та показують мережеві та фізичні адреси його відправника та одержувача.

Аналізатори протоколів здатні навіть збирати дані роботи того чи іншого зазначеного користувачем рівня, причому вся необхідна інформація виявляється відразу перед очима користувача. Але щоб користуватися такими пристроями, адміністратор повинен мати високу кваліфікацію і досить добре розумітися на мережевих протоколах. В іншому випадку він або буде просто не в змозі впоратися з великим обсягом інформації (навіть фільтри не завжди допомагають), або може неправильно інтерпретувати дані аналізатора. Спроби ж внести виправлення на основі невірних висновків загрожують серйозною небезпекою виходу з ладу сегмента мережі. Тому аналізатори протоколів найчастіше використовуються як експертні системи і лише у тих випадках, коли всі інші засоби вичерпані.

Зазначимо, що портативні мережеві тестери хоча і вимагають певної кваліфікації, але в цілому простіше в освоєнні. Сьогодні, при мінімальній вазі та габаритах, вони мають потужність, достатню для діагностики більшості проблем у ЛОМ, особливо за підтримки функцій кабельного тестера.

2.7 Захист комп'ютерної мережі

Безпека комп'ютерної мережі являє собою комплекс організаційних, технічних, програмних та апаратних заходів, спрямованих на забезпечення захисту інформаційного середовища від несанкціонованого доступу, випадкового або навмисного втручання в роботу системи, а також від спроб модифікації, пошкодження чи знищення її компонентів. Захист мережевої інфраструктури підприємства є багаторівневим завданням, яке охоплює безпеку апаратного забезпечення, програмного середовища, каналів передавання даних та регламентацію дій користувачів і обслуговуючого персоналу. Надійна система захисту дозволяє забезпечити стабільність функціонування локальної мережі та мінімізувати ризики втрати або компрометації корпоративної інформації.

Сучасна концепція мережевої безпеки базується на принципі ешелонованого або багаторівневого захисту. Такий підхід передбачає використання декількох незалежних механізмів безпеки, що взаємодіють між собою. У результаті навіть у випадку компрометації одного із засобів захисту зловмисник не отримує повного доступу до внутрішніх ресурсів локальної обчислювальної мережі підприємства. Наприклад, викрадення облікових даних користувача не повинно автоматично призводити до порушення безпеки всієї мережевої інфраструктури.

Основою побудови системи захисту є процедура керування доступом до мережевих ресурсів, яка реалізується відповідно до архітектури AAA (Authentication, Authorization, Accounting). Першим етапом є аутентифікація, тобто перевірка автентичності користувача або іншого суб'єкта доступу шляхом підтвердження його ідентифікаційних даних. Залежно від рівня критичності інформаційних ресурсів можуть застосовуватися різні методи перевірки особи. Найпростішим варіантом є однофакторна аутентифікація, яка базується на використанні логіна та пароля. Більш надійним методом є двофакторна

аутентифікація, що поєднує пароль із додатковим засобом підтвердження, наприклад одноразовим кодом, апаратним токеном або смарт-карткою. Для систем із підвищеними вимогами безпеки використовується багатофакторна аутентифікація, яка додатково включає біометричні методи ідентифікації, зокрема відбитки пальців, сканування сітківки ока або розпізнавання обличчя.

Другим компонентом архітектури AAA є авторизація, яка визначає рівень доступу користувача до ресурсів системи відповідно до його службових обов'язків. Завдяки цьому кожен працівник отримує доступ лише до тих даних і сервісів, які необхідні для виконання його функцій. Третім компонентом є аудит або облік подій безпеки, який полягає у фіксації дій користувачів і системних процесів у журналах подій. Аналіз таких журналів дозволяє виявляти інциденти безпеки, проводити розслідування та контролювати роботу мережевої інфраструктури.

Проєктована система безпеки локальної мережі підприємства повинна забезпечувати ефективний захист від внутрішніх і зовнішніх загроз. Для цього реалізується постійний моніторинг мережевої активності, аналіз мережевого трафіку та виявлення аномальної поведінки, наприклад сканування портів, спроб несанкціонованого доступу або атак типу DDoS. Система повинна автоматично реагувати на виявлені загрози та блокувати потенційно небезпечну активність як із зовнішньої мережі Інтернет, так і з боку внутрішніх користувачів або заражених робочих станцій.

Важливою функцією системи захисту є забезпечення конфіденційності та цілісності даних. Це досягається за допомогою сучасних криптографічних методів шифрування інформаційних потоків, які унеможливлюють перехоплення або зміну службової інформації під час її передавання мережею. Додатково система повинна реалізовувати механізми диференціації доступу до ресурсів на основі рольових моделей керування доступом. У такій моделі права користувачів розподіляються відповідно до їх функціональних обов'язків, що дозволяє

ізолювати критичні сегменти мережі та обмежити доступ до конфіденційних даних.

Архітектура безпеки також повинна забезпечувати високу доступність та відмовостійкість мережевої інфраструктури. Це означає, що навіть у випадку виходу з ладу окремих вузлів або виникнення мережевих атак система повинна зберігати працездатність та забезпечувати безперервний доступ до основних сервісів. Особлива увага приділяється захисту від атак типу DoS і DDoS, які можуть спричинити перевантаження мережі та порушення роботи серверного обладнання.

Для практичної реалізації політики безпеки використовуються різноманітні програмно-апаратні засоби захисту. Одним із основних елементів є міжмережеві екрани або брандмауери, які виконують фільтрацію вхідного та вихідного мережевого трафіку на основі встановлених правил безпеки. Такі засоби можуть функціонувати як на рівні прикордонного маршрутизатора, так і безпосередньо на робочих станціях користувачів. Вони дозволяють блокувати несанкціоновані пакети, закривати вразливі порти та контролювати доступ до мережевих ресурсів.

Додатково використовуються системи виявлення та запобігання вторгненням IDS/IPS, які виконують глибокий аналіз вмісту пакетів і дозволяють виявляти сигнатури відомих атак або шкідливу активність у реальному часі. На відміну від звичайних брандмауерів, такі системи аналізують не лише заголовки пакетів, але й їх вміст, що значно підвищує рівень захисту мережі.

Важливим компонентом системи безпеки є антивірусний захист та засоби боротьби зі шкідливим програмним забезпеченням. Передбачається використання централізованої системи захисту кінцевих точок, яка забезпечує виявлення, локалізацію та видалення вірусів, троянських програм, мережевих хробаків і програм-вимагачів ще до моменту завдання шкоди корпоративним даним. Централізоване керування антивірусним захистом дозволяє оперативно

оновлювати бази сигнатур і контролювати стан безпеки всіх робочих станцій підприємства.

Для організації безпечного віддаленого доступу співробітників до корпоративної мережі використовуються технології VPN. Вони забезпечують створення захищених віртуальних тунелів поверх мережі Інтернет із використанням криптографічних протоколів IPsec, OpenVPN або WireGuard. Це дозволяє гарантувати конфіденційність, цілісність та автентичність переданих даних незалежно від місця розташування користувача. Завдяки впровадженню таких рішень працівники можуть безпечно працювати з корпоративними ресурсами під час відряджень або дистанційної роботи.

Таким чином, використання комплексного підходу до захисту комп'ютерної мережі дозволяє побудувати надійну, гнучку та стійку IT-інфраструктуру підприємства, яка відповідає сучасним вимогам інформаційної безпеки та забезпечує стабільне функціонування всіх мережевих сервісів.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Налаштування маршрутизатора

Для практичної реалізації розробленої схеми логічної сегментації, налаштування портів комутатора виконується через консольний порт (або протокол SSH) за допомогою командного рядка JetStream CLI. Скрипт містить ініціалізацію віртуальних мереж, призначення IP-адрес для керування (Management), конфігурацію абонентських портів (Access) та налаштування магістрального порту до маршрутизатора (Trunk). Далі приведемо скрипт налаштування комутатора:

1. Перехід до режиму привілейованого конфігурування

enable configure

Зміна системного імені пристрою

hostname Core-Switch-L2

2. Створення віртуальних локальних мереж (VLAN) згідно з Таблицею 2.1

vlan 100 name Office_and_Servers exit

vlan 200 name Accounting exit

vlan 300 name Smart_TV exit

vlan 400 name Wi-Fi_Network exit

3. Конфігурація портів для сегмента Офісного персоналу (VLAN 100)

Діапазон портів: 1-29 та 33-35 (Режим Access)

interface range gigabitEthernet 1/0/1-29, gigabitEthernet 1/0/33-35 switchport mode access switchport access vlan 100 description Office_Users exit

4. Конфігурація портів для сегмента Бухгалтерії (VLAN 200)

Діапазон портів: 30-32 (Режим Access)

interface range gigabitEthernet 1/0/30-32 switchport mode access switchport access vlan 200 description Accounting_Department exit

5. Конфігурація портів для сегмента Мультимедіа/Телевізорів (VLAN 300)

Діапазон портів: 38-41 (Режим Access)

interface range gigabitEthernet 1/0/38-41 switchport mode access switchport access vlan 300 description Multimedia_SmartTV exit

6. Конфігурація портів для бездротових точок доступу (VLAN 400)

Діапазон портів: 42-45. Оскільки MikroTik cAP XL ac підтримує роботу з тегованими VLAN безпосередньо через CAPsMAN, порти налаштовуються у гібридний/Trunk режим або чистий Access залежно від архітектури. Налаштуємо як Access підсистему з активацією PoE+.

interface range gigabitEthernet 1/0/42-45 switchport mode access switchport access vlan 400

Активація живлення PoE+ (увімкнено за замовчуванням, але прописуємо для верифікації)

poe administrative-status enable description Wi-Fi_APs_with_PoE exit

7. Конфігурація портів для Корпоративних серверів (VLAN 100)

Порти: 47 та 48 (Режим Access)

interface range gigabitEthernet 1/0/47-48 switchport mode access switchport access vlan 100 description Corporate_Servers exit

8. Налаштування інтерфейсу керування комутатором (Management IP)

Надаємо комутатору статичну IP-адресу в підмережі серверів/адміністрації для адміністрування

interface vlan 100 ip address 100.100.10.254 255.255.255.0 exit

Маршрут за замовчуванням у бік головного роутера (шлюз мережі)

ip route 0.0.0.0 0.0.0.0 100.100.10.1

9. Конфігурація магістрального порту (Trunk Uplink) до маршрутизатора MikroTik

Для цього використовуємо перший оптичний SFP порт комутатора (порт 49 / gigabitEthernet 1/0/49)

interface gigabitEthernet 1/0/49 switchport mode trunk

Дозволяємо проходження трафіку всіх створених віртуальних мереж

switchport trunk allowed vlan 100,200,300,400 description Uplink_to_MikroTik_CCR2004 exit

10. Збереження поточної конфігурації в енергонезалежну пам'ять (NVRAM)

end copy running-config startup-config

Для маршрутизатора MikroTik CCR2004-16G-2S+PC конфігурація виконується мовою скриптів RouterOS (v7).

Оскільки комутатор з'єднаний з роутером оптичним лінком (порт SFP+), маршрутизатор має прийняти цей тегований трафік, створити віртуальні інтерфейси (VLAN), підняти на них DHCP-сервери для автоматичної роздачі IP-адрес вузлам, налаштувати міжсерверну маршрутизацію та захистити мережу за допомогою файрвола (NAT).

Нижче наведено повний скрипт маршрутизатора.

2.8. Скрипт конфігурування маршрутизатора MikroTik CCR2004-16G-2S+PC

Налаштування маршрутизатора здійснюється через інтерфейс командного рядка RouterOS CLI. Скрипт реалізує технологію Router-on-a-Stick через оптичний інтерфейс sfp-sfpplus1, створює шлюзи для кожної підмережі згідно з таблицею 2.1, а також забезпечує безпеку та трансляцію адрес (NAT) для виходу в Інтернет.

1. Системні налаштування (Ім'я пристрою)

/system identity set name=Main-Router-CCR2004

2. Налаштування інтерфейсу Інтернет (WAN)

Припустимо, що кабель провайдера підключено до першого фізичного порту ether1

/interface set [find default-name=ether1] name=ether1-WAN comment="Internet Uplink"

3. Створення VLAN-інтерфейсів на магістральному оптичному порті sfp-sfpplus1 (Трунк до комутатора)

/interface vlan add interface=sfp-sfpplus1 name=vlan100-office vlan-id=100 comment="Office and Servers" add interface=sfp-sfpplus1 name=vlan200-acc vlan-id=200 comment="Accounting" add interface=sfp-sfpplus1 name=vlan300-tv vlan-id=300 comment="Smart TV" add interface=sfp-sfpplus1 name=vlan400-wifi vlan-id=400 comment="Wi-Fi Network"

4. Призначення IP-адрес (шлюзів за замовчуванням) на VLAN-інтерфейси згідно з Таблицею 2.1

/ip address add address=100.100.10.1/24 interface=vlan100-office comment="GW for Office & Servers" add address=100.100.20.1/24 interface=vlan200-acc comment="GW for Accounting" add address=100.100.30.1/24 interface=vlan300-tv comment="GW for Smart TV" add address=100.100.40.1/24 interface=vlan400-wifi comment="GW for Wi-Fi APs"

5. Конфігурація пулів IP-адрес для автоматичної роздачі (DHCP Pools)

Виключаємо статичні адреси серверів та комутатора з пулу VLAN 100

/ip dhcp-server pool add name=pool-office ranges=100.100.10.10-100.100.10.250 add name=pool-acc ranges=100.100.20.10-100.100.20.250 add name=pool-tv ranges=100.100.30.10-100.100.30.250 add name=pool-wifi ranges=100.100.40.10-100.100.40.250

6. Активація DHCP-серверів на відповідних VLAN-інтерфейсах

/ip dhcp-server add address-pool=pool-office interface=vlan100-office name=dhcp-office disabled=no add address-pool=pool-acc interface=vlan200-acc name=dhcp-acc disabled=no add address-pool=pool-tv interface=vlan300-tv name=dhcp-tv disabled=no add address-pool=pool-wifi interface=vlan400-wifi name=dhcp-wifi disabled=no

Налаштування параметрів мережі для DHCP (Шлюз та DNS)

/ip dhcp-server network add address=100.100.10.0/24 gateway=100.100.10.1 dns-server=100.100.10.1,8.8.8.8 add address=100.100.20.0/24

gateway=100.100.20.1 dns-server=100.100.20.1,8.8.8.8 add address=100.100.30.0/24 gateway=100.100.30.1 dns-server=100.100.30.1,1.1.1.1 add address=100.100.40.0/24 gateway=100.100.40.1 dns-server=100.100.40.1,1.1.1.1

7. Налаштування системного DNS-кешу

/ip dns set allow-remote-requests=yes servers=8.8.8.8,1.1.1.1

8. Налаштування безпеки та трансляції адрес (NAT / Маскарадинг для виходу в Інтернет)

/ip firewall nat add action=masquerade chain=srcnat out-interface=ether1-WAN comment="Internet Access for Local Network"

9. Налаштування базового міжмережевого екрана (Firewall Filter) для ізоляції VLAN

Забороняємо гостьовому Wi-Fi (VLAN 400) та телевізорам (VLAN 300) доступ до Бухгалтерії (VLAN 200) та Офісу (VLAN 100)

/ip firewall filter add action=drop chain=forward in-interface=vlan400-wifi out-interface=vlan100-office comment="Drop Wi-Fi to Office" add action=drop chain=forward in-interface=vlan400-wifi out-interface=vlan200-acc comment="Drop Wi-Fi to Accounting" add action=drop chain=forward in-interface=vlan300-tv out-interface=vlan100-office comment="Drop TV to Office" add action=drop chain=forward in-interface=vlan300-tv out-interface=vlan200-acc comment="Drop TV to Accounting"

Дозволяємо проходження вже встановлених та пов'язаних з'єднань (Ефективність фільтрації)

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

Для бездротової точки доступу MikroTik cAP XL ac скрипт конфігурації пишеться також для операційної системи RouterOS.

Оскільки в попередніх розділах ми обґрунтували використання технології централізованого керування CAPsMAN, конфігурація точки доступу розділяється на дві логічні частини:

На боці самої точки доступу (CAP): переведення її в режим керованого клієнта, щоб вона віддала свої радіоінтерфейси під контроль головного роутера.

На боці головного маршрутизатора CCR2004 (CAPsMAN-сервер): створення параметрів бездротової мережі (назва Wi-Fi, пароль, шифрування, прив'язка до VLAN 400).

Нижче наведено фінальний інженерний скрипт для кваліфікаційної роботи «Налаштування бездротової інфраструктури на базі технології CAPsMAN».

10. Скрипт конфігурування бездротової підсистеми

Частина 1. Локальна конфігурація точки доступу MikroTik cAP XL ac

Цей скрипт виконується безпосередньо на кожній із чотирьох точок доступу (wifi_1—wifi_4). Він очищує заводські налаштування, об'єднує фізичні порти в міст та активує режим підпорядкування CAPsMAN-серверу.

1. Очищення заводської конфігурації без створення дефолтних правил

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

[Після перезавантаження пристрою виконуються наступні команди]

2. Встановлення ідентифікатора точки доступу (наприклад, для першої точки)

/system identity set name=AP-WiFi-1

3. Створення мережевого мосту (Bridge) для об'єднання дротового інтерфейсу

/interface bridge add name=bridge-cap comment="Local Bridge for CAP"

4. Додавання фізичного порту ether1 (який підключено до комутатора TP-Link) у міст

/interface bridge port add bridge=bridge-cap interface=ether1

5. Активація режиму CAP (Controlled Access Point)

Точка доступу перенаправляє інтерфейси wlan1 (2.4GHz) та wlan2 (5GHz) на керування роутеру.

Пошук CAPsMAN-сервера здійснюється через створений міст.

/interface wireless cap set bridge=bridge-cap discovery-interfaces=bridge-cap enabled=yes interfaces=wlan1,wlan2

3.2 Інструкція з використання тестових наборів та тестових програм

Для діагностики мережі використовуються команди PING і TRACERT.

Команда ping - команда командного рядка, яка використовується для перевірки здатності даного комп'ютера “достукатися” вказаного цільового комп'ютера. Команда ping зазвичай використовується як простий спосіб перевірити, чи може комп'ютер здійснювати зв'язок через мережу з іншим комп'ютером або мережевим пристроєм.

Команда ping працює, відправляючи Інтернет-протокол керування повідомленнями (ICMP) Echo Request повідомлення на цільовий комп'ютер і очікування відповіді.

Основна функція цієї утиліти – перевірка наявності фізичного зв’язку між двома системами в мережі. Для обміну пакетами з віддаленою системою, використовується протокол ICMP. Віддалена система відсилає пакети назад, і таким чином, коло замикається. Команда PING видає інформацію про те, скільки часу виконувалась ця операція, а також повідомляє про помилки, якщо пакети не повернулись.

Команда ping доступна в командному рядку в операційних системах Windows 10, Windows 8, Windows 7, Windows Vista та Windows XP. Команда ping також доступна в старих версіях Windows, таких як Windows 98 та 95.

Синтаксис команди в операційних системах сімейства Windows має наступний вигляд:

ping [ключі] адреса (ім’я) вузла

Ключі:

– t – продовжує відправку запитів , доки робота не буде перервана командою Ctrl-C;

– a – дозволяє використовувати імена вузлів замість IP-адрес;

– n число – вказує кількість exo запитів для відправки ;

– l довжина – вказує довжину exo – запитів;

– f – забороняє фрагментування пакету, визначає, чи пристрій змінював розмір пакету;

– i час – встановлює час життя пакету (Time to Live -TTL) відправляємих пакетів;

– v тип – встановлює тип обслуговування (TOS)

– r число – відображає шляхи для заданого числа переприйомів;

– s число – відмічає час для вказаного числа переприйомів;

– j список вузлів – маршрутизація пакетів через вказані вузли. Послідовні вузли можуть бути розділені шлюзами;

– k список вузлів - маршрутизація пакетів через вказані вузли. Послідовні вузли не можуть бути розділені шлюзами.

– w час – встановлює час очікування відповіді в мілісекундах.

Команда TRACERT також використовує протокол ICMP для визначення всіх пристроїв, через які проходить пакет на шляху до вузла призначення.

За допомогою цієї команди, можна отримати досить обширну інформацію про те, як функціонує мережа.

Має наступний синтаксис :

tracert [ключі] ім’я вузла

Ключі :

– d – використовувати імена вузлів замість IP адрес;

– h максимальне число переприйомів – максимально допустиме число переприйомів для досягнення мети;

– j список вузлів - маршрутизація пакетів через вказані вузли. Послідовні вузли можуть бути розділені шлюзами. Вільний вибір шляху серед систем у вказаному списку;

– w час – встановлення часу очікування в мілісекундах.

Існує також команда IPCONFIG, яка використовується для отримання інформації про настройку TCP/IP сервера або робочої станції Windows NT.

Команда ifconfig в Unix та подібних системах використовується для налаштування та виведення параметрів мережевого інтерфейсу для мережі за допомогою TCP/IP. її можна використовувати, щоб призначити адресу мережевому інтерфейсу, налаштувати або переглянути інформацію про його конфігурацію.

Утиліта вважається застарілою, але все одно зустрічається в багатьох інструкціях для налаштування мережі. Ifconfig зручна: з простим синтаксисом і зрозумілим виведенням інформації.

Команда IPCONFIG виводить інформацію про всі мережеві карти, встановлені в системі і зв'язках PPP. В базову інформацію входять:

– IP-адреса;
– маска підмережі;
– шлюз по замовчуванню;
– сервери DNS;
– домен NT.

Якщо застосувати в даній команді ключ /all, то буде виведений список апаратних MAC-адрес пристроїв і інформацію по DHCP.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки проекту локальної комп'ютерної мережі компанії "Стиль-Н" 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	7
2	Розробка проекту мережі	Інженер	26
3	Монтаж пасивного обладнання	Лаборант	18
4	Налаштування активного комутаційного обладнання	Технік	10
5	Встановлення та на лаштування програмного забезпечення	Технік	10
6	Тестування мережі	Технік	4
Р а з о м		–	75

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.

Зосн.=145*33+130*18+120*24=10005,00 грн.

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

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

де Кдопл. – коефіцієнт додаткових виплат працівникам.

$$З_{дод.}= 10005,00 *0,15=1500,75 \text{ грн.}$$

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

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

$$В_{о.п.} = 10005,00 +1500,75=11505,75 \text{ грн.}$$

Крім того, слід визначити відрахування на заробітну плату:

єдиний соціальний внесок – 22 %.

Отже, сума відрахувань на соціальні заходи буде становити:

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

де ФОП – фонд оплати праці, грн.

$$В_{з.с.} =11505,75*0,22=4326,16 \text{ грн.}$$

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	145	33	4785,00	717,75	-	-
2	Технік	130	18	2340,00	351,00	-	-
3	Лаборант	120	24	2880,00	432,00	-	-
	Разом	-	75	10005,00	150,00	4326,16	15831,91

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 qi – кількість витраченого матеріалу і-го виду;

pi – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити:

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

$$З_{м.в.} = 155335{,}00 \text{ грн.}$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Факт. витрачено матеріалів	Ціна 1-ці, грн.	Загальна сума витрат, грн.
1	2	3	4	5	6
1	Кабель UTP Cat5e	м	750	24,0	18000,00
2	Роз'єми RJ-45	шт	200	2,12	424,00
3	Розетки RJ-45	шт	45	69,00	3107,00
4	Короб пластиковий 40*25*2м	шт	64	121,5	7776,00
5	Дюбель	шт	300	6,1	1830,00
6	Маршрутизатор Mikrotik CCR2004-16G-2S+PC	шт	1	16700,00	16700,00
7	Комутатор TP-Link TL-SG3452P	шт	1	31500,00	31500,00
8	Точка доступу Mikrotik cAP XLac (RbcAPGi-5acD2nD-XL)	шт	4	3500,00	14000,00
9	Сервер ARTLINE Business R15v14+	шт	2	31000,00	62000,00
	Р а з о м				155335,00

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 28 годин.

Зе=0,50*28*15,94=223,16 грн.

4.5 Визначення транспортних затрат

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

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

де ТВ – транспортні витрати.

$$T_В = 155335{,}00 * 0{,}08 = 12426{,}80 \text{ грн}$$

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:

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

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

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

НА – норма амортизації, %.

Для проектування даної комп'ютерної мережі використовується один

комп’ютер (вартість якого становить 32870 грн.), який працює 28 годин.

Тоді:

$$A = 32870*0,04*28/150=249,82 \text{ грн.}$$

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.

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

де НВ – накладні витрати.

$$H_В = 11505,75*0,5=5752,88 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 4.4.

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до заг. суми
1	2	3
Витрати на оплату праці	11505,75	8,06
Відрахування на соціальні заходи	4326,16	2,20
Матеріальні витрати	155335,00	79,13
Витрати на електроенергію	223,16	0,11
Транспортні витрати	12426,80	6,33

Продовження таблиці 4.4

1	2	3
Амортизаційні відрахування	249,82	0,13
Накладні витрати	5752,88	4,03
Собівартість	189819,6	100,00

Собівартість (СВ) НДР розрахуємо за формулою:

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

$$C_в = 189819{,}6 \text{ грн.}$$

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

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

де Ррен. – рівень рентабельності;

К – кількість замовлень, од.;

Ві.н. – вартість носія інформації, грн.;

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

Ц=189819,6*(1+0,26)*(1+0,2)= 287007,2 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 ($T_{ОК}$).

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

де КВ – затрати на проект;

Гп – грошовий потік за t–ий рік;

t – відповідний рік проекту;

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

ЧТВ = □189819,6 +159287,6/(1+0,1)+ 159287,6/(1+0,1)2=86630 (грн.)

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

Термін окупності визначається за формулою:

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

де ТПВ – період до повного відшкодування витрат, років;

НВ – невідшкодовані витрати на початок року, грн.;

ГПР – грошовий потік на початок року, грн.

ТОК=1+45012,6/159287,6=1,3

Таблиця 4.5 - Економічні показники НДР

№ п/п	Показник	Значення
1.	Собівартість, грн.	189819,6
2.	Плановий прибуток, грн.	97187,6
3.	Ціна, грн.	287007,2
4.	Чиста теперішня вартість, грн	86630,00
5.	Термін окупності, рік	1,3

В результаті аналізу економічних показників, розрахованих та зведених у таблицю 4.5, можна прийти до висновку, що при терміні окупності – 1,3 року проводити роботи по впровадженню даної мережі є доцільним та економічно вигідним.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

5.1 Вимоги безпечного виконання електромонтажних робіт при організації кабельних трас компанії “Стиль-Н”

Досвід експлуатації електроустановок показує, що для безпечної роботи поряд із засобами захисту необхідно так організувати експлуатацію, щоб була усунена можливість помилок з боку обслуговуючого персоналу.

При підготовці робочого місця з частковим або повним зняттям напруги технічні заходи проводять у такому порядку:

– Вимикають необхідні струмопровідні частини та проводять заходи, які виключають помилкову подачу напруги до місця проведення робіт.

– На вимкнутих комутаційних апаратах вивішують заборонні плакати: «Не вмикати — працюють люди!», «Не вмикати — робота на лінії!» та ін. В разі необхідності встановлюють огорожі навколо струмопровідних частин.

– До заземлюючого пристрою приєднують затискач переносного заземлення.

– Перевіряють, чи немає напруги на вимкнутій частині установки. Якщо її немає, то заземлюють цю частину до контура заземлення.

– Робоче місце огороджують переносними огорожами і вивішують попереджувальні і нагадувальні плакати: «Стій — висока напруга!», «Працювати тут!».

При підготовці робочого місця і в період роботи необхідно проводи ти такі організаційні заходи: 1) оформлення роботи нарядом або розпорядженням; 2) допуск до роботи; 3) нагляд під час роботи; 4) отримання певного порядку записів у журналі перерв у роботі, переходів на інше місце роботи, закінчення роботи. Проводячи електромонтажні роботи, електрик повинен дотримуватися вимог техніки безпеки.

Опір ізоляції вимірюють мегомметром, дотримуючись таких основ них правил техніки безпеки:

– Вимірювання можна проводити тільки тоді, коли вимкнені всі лінії, по яких подається напруга.

– Необхідно переконатися у відсутності людей, що працюють на тій частині електроустановки, до якої має бути під'єднаний манометр.

– Перед випробуванням кабелів напругою понад 1000 В їх слід роз рядити.

– Проводи, які приєднуються до мегомметра, повинні мати хорошу ізоляцію на відповідну напругу. Вимірювання переносними приладами і струмовимірювальними кліщами, згідно з вимогами ПТБ, повинні виконуватися двома особами. В період експлуатації ці вимірювання проводяться оперативним персоналом і роблять записи в журналі.

Вимірювання переносними приладами необхідно проводити в діелектричних рукавицях і калошах, або зі стояків на діелектричному килимку. На кабелях напругою понад 1000 В жили повинні бути рознесені одна від одної на відстань, не меншу ніж 250 мм. При вимірюванні кліщі тримають так, щоб прилад не торкався проводів вимірювальних транс форматорів. Приєднання і від'єднання приладів необхідно виконувати при знятій напрузі.

– Заміну плавких вставок запобіжників слід проводити при знятій напрузі. На групових щитах, де не можна зняти напругу, допускається заміна запобіжника під напругою, але при обов'язковому вимиканні навантаження. У цьому випадку треба обов'язково користуватися окулярами і діелектричними рукавицями або ізолюючими кліщами. Заміну плавких вставок з підлоги здійснює один електрик третього кваліфікаційного розряду, а якщо на висоті, — то два електрики, один з яких має кваліфікацію не нижче третього розряду. Електроінструмент і переносні електричні прилади повинні строго відповідати вимогам ПТБ. Робоча напруга

електроінструменту має бути не вище 220 В при роботі у приміщеннях без підвищеної безпеки і 36 В — в приміщеннях з підвищеною небезпекою і поза приміщеннями. В особливо небезпечних приміщеннях при використанні електроінструменту на 36 В потрібно використовувати захисні засоби або електроінструмент на напругу 12 В. Оболонки кабелів і проводів необхідно вводити в електроінструмент і міцно їх закріплювати для запобігання зламів і стирань. Корпус електроінструменту на напругу понад 36 В необхідно заземлювати під'єднуючи його до спеціального затискача на контурі заземлення, позначеному «З» або «Земля».

– Струмопровідні частини і заземлюючий контакт штепсельних з'єднань мають бути недоступні для доторкувань. Причому розетки і вилки, що використовуються на напругу 12 В і 36 В, повинні мати колір, який різко відрізняється від кольору штепсельних з'єднань напругою 127 і 220 В. Конструктивне виконання розеток має бути таким, щоб запобігти можливості помилкового вмикання на іншу напругу.

– Електроінструмент і переносні електричні світильники приєднують багатожильним гнучким проводом з ізоляцією за напругою не менше ніж 500 В. Стан ізоляції значною мірою визначає ступінь безпеки експлуатації електроустановок. Під впливом тепла, динамічних зусиль, комутаційних і атмосферних перенапруг ізоляція старіє, стає непридатною. Періодичний контроль ізоляції (вимірювання її опору) проводять у встановлені правилами строки і у випадку виявлення дефектів. Опір ізоляції частин електрообладнання, що не перебуває під напругою, вимірюють мегомметром. Опір ізоляції має бути не нижче 0,6 МОм, в установках до 1000 В; 1 МОм, — для електроінструменту з ізольованими ручками.

– Основними способами захисту від статичної електрики є заземлення металевих частин обладнання, які можуть електризуватися, застосовування струмопровідних покриттів, підлог, взуття. Це забезпечує

витікання генерованого заряду на заземлені частини. Використовують також зволоження навколишньої атмосфери, нейтралізатори, браслети.

– Під час монтування освітлювальних електроустановок слід дотримуватися наступних правил.

– Ремонтні роботи в діючих електромережах виконують, як правило, дві особи.

– При виконанні ремонтних робіт під напругою, роботу слід виконувати в діелектричних рукавицях, стоячи на гумовому килимку.

– На ручках комутаційних апаратів слід вивішувати попереджувальні плакати «Не вмикати, працюють люди!».

– Всі фази на вимкнутій частині ремонтної ділянки потрібно заземлювати і закорочувати.

– Отвори, гнізда, борозни можна пробивати тільки в захисних окулярах і рукавицях.

– Пробивати отвори і гнізда вручну дозволяється зубилами довжиною не менше 150 мм.

– Пробивати проходи і натягувати проводи поліспастом можна тільки з нерухомих риштувань та пересувних вишок. З підставних драбин ці роботи виконувати заборонено.

– Працювати на риштуваннях з додаткових підставок (ящиків, бочок і т. д.) не дозволяється. Залазити на риштування можна тільки по спеціально призначених для цього драбинах.

– Не можна працювати під закріпленим поліспастом, яким натягнуто проводи.

– Не можна працювати поблизу рухомих механізмів, останні необхідно надійно відгородити.

– Заборонено торкатися тимчасових проводок, необхідно стежити за тим, щоб вони не мали оголених проводів.

– Під час виконання електромонтажних робіт слід використовувати ручні переносні лампи на напругу до 36 В, а в особливо вологих місцях — на напругу 12 В.

– Торкатися до елементів електромережі, що перевіряються, не безпечно!

5.2 Оцінка та нормалізація рівнів шуму і вібрації на робочих місцях адміністраторів

Для вимірювання шуму використовують шумоміри з відповідними фільтрами і частотними аналізаторами (див.рис. 5.1)., які дозволяють виміряти рівні звукового тиску шуму в октавних смугах, а також за шкалою „А” визначити рівень звуку. Звичайний шумомір складається з мікрофона, підсилювача, фільтрів (корегуючих, октавних) та показуючого приладу.

Порядок контролю шуму регламентовано ДСН 3.3.6.037-99. Вимірювання шуму проводиться на постійних робочих місцях у приміщеннях, на території підприємств, у промислових спорудах та машинах (у кабінах, на пультах управління і т.п.). Результати вимірювань повинні характеризувати шумовий вплив за час робочої зміни (робочого дня).

Рисунок 5.1 - Прибор для контролю шуму – шумомір ШІ-01

При проведенні вимірювань мікрофон слід розташовувати на висоті 1,5 м над рівнем підлоги чи робочого майданчика (якщо робота виконується стоячи) чи на висоті і відстані 15 см від вуха людини, на яку діє шум (якщо робота виконується сидячи чи лежачи). Мікрофон повинен бути зорієнтований у напрямку максимального рівня шуму та віддалений не менш ніж на 0,5 м від оператора, який проводить вимірювання.

Тривалість вимірювання переривчастого шуму повинна відповідати часу повного робочого циклу з урахуванням сумарної тривалості перерв з рівнем фонового шуму. Для шуму, що коливається у часі, допускається загальна тривалість вимірювання 30 хвилин безперервно або вимірювання складається з трьох десятихвилинних циклів. Для імпульсного шуму тривалість вимірювання становить 30 хвилин.

Для вимірювання вібрацій широко використовуються електричні вібровимірювальні прилади, принцип дії котрих базується на перетворенні кінематичних параметрів коливного руху в електричні величини, які вимірюються та реєструються за допомогою електричних приладів (див.рис. 5.2).

Октава-101ВМ

ВВМ-201

Рисунок 5.2 - Віброметри

Основні елементи цих приладів - первинні вимірювальні перетворювачі, в якості яких використовують ємнісні, індукційні, п'єзоелектричні перетворювачі, які сприймають коливні зміщення, швидкість та прискорення.

Найчастіше використовуються п'єзоелектричні перетворювачі віброприскорення — акселерометри (див.рис. 5.3).

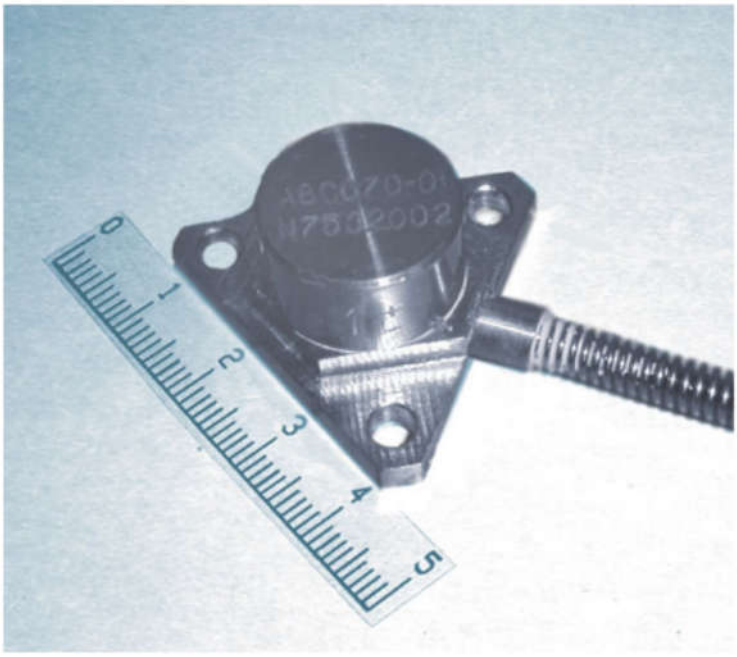


Рисунок 5.3 - Акселерометр АВС 070-01

Вібровимірювальними приладами з давачами можна вимірювати вібрації в багатьох точках. Їх перевага - дистанційність вимірювання параметрів вібрації, проста будова, відсутність інерційності.

Кількість вимірювань параметрів вібрації повинна бути не менше трьох для кожної октавної смуги частот. Вимірювальними параметрами вібрації є пікові аби середньоквадратичні значення віброзміщення, віброшвидкості або віброприскорення в октавних або 1/3-октавних смугах частот.

5.3 Аналіз пожежонебезпечних властивостей ізоляційних матеріалів та права керівника щодо контролю пожежної безпеки в компанії “Стиль-Н”

Горючість (спалимість) – це здатність речовини або матеріалу до горіння. За показником горючості всі речовини та матеріали поділяються на негорючі, важкогорючі та горючі.

Негорючі – речовини та матеріали не здатні до горіння на повітрі нормального складу. Це неорганічні матеріали, метали, гіпсові конструкції.

Важкогорючі – це речовини не здатні до займання в повітрі від джерела запалювання, однак після його вилучення не здатні до самостійного горіння. До них належать матеріали, які містять горючі та негорючі складові частини. Наприклад, асфальтобетон, фіброліт

Горючі – матеріали, які здатні до самозаймання, а також займання від джерела запалювання і самостійного горіння після його вилучення.

До них належать всі органічні матеріали. В свою чергу горючі матеріали поділяються на легкозаймисті, тобто такі, які займаються від джерела запалювання незначної енергії без попереднього нагрівання та важкозаймисті, які займаються від порівняно потужного джерела запалювання.

Температура спалаху – найнижча температура горючої речовини, при якій над її поверхнею утворюються пари або гази, здатні спалахнути від джерела запалювання, але швидкість їх утворення ще недостатня для стійкого горіння. За температурою спалаху розрізняють:

- легкозаймисті рідини (ЛЗР) – рідини, які мають температуру спалаху, що не перевищує 61°С у закритому тиглі (бензин, ацетон, етиловий спирт);
- горючі рідини (ГР) – рідини, які мають температуру спалаху понад 61°С. у відкритому тиглі (мінеральні мастила, мазут, формалін).

Займання – початок горіння під дією джерела запалювання. Температура

займання – найменша температура речовини, при якій вона виділяє горючі пари і гази з такою швидкістю, що після їх запалення виникає стійке горіння.

Температура спалахування – найнижча температура речовини, при якій вона виділяє горючі пари і гази з такою швидкістю, що після їх запалення виникає стійке горіння

Температура спалаху – найнижча температура речовини, при якій відбувається різке збільшення швидкості екзотермічних реакцій, що призводить до виникнення полум'янистого горіння. Температури спалаху та спалахування належать до показників пожежовибухонебезпечності лише рідин та твердих речовин.

Температура у вогнищі пожежі досягає 700-900°С. Особливістю пожеж, що розпочинаються у приміщенні з закритими дверима та вікнами, є порівняно повільний розвиток горіння протягом перших 30-40 хвилин через недостатню кількість повітря в зоні горіння.

На розвиток пожежі у приміщеннях та спорудах значно впливає здатність окремих будівельних елементів чинити опір впливу теплоти, тобто їх вогнестійкість.

Вогнестійкість – це здатність конструкцій, матеріалів затримувати поширення вогню, виражена в годинах. Усі будови і споруди за вогнестійкістю поділяються на 5 ступенів. Ступінь вогнестійкості залежить від вогнетривкості та займистості будівельних конструкцій, а також від межі поширення вогню по цих конструкціях.

У будівлях 1-го ступеню вогнестійкості всі конструктивні елементи неспалимі, з високою межею вогнестійкості (1,5-3 години).

2-го ступеню – також негорючі, але з меншою межею вогнестійкості (0,5-2,5 год.).

3-го ступеню – будови, які мають основні несучі конструкції негорючі, а ненесучі (міжповерхові й перекриття на горищі) – важкогорючі (0,25-2 год.).

4-го ступеню – будови, які мають всі конструкції важко спалимі (0,25-0,5

год.).

5-го ступеню – всі конструкції горючі.

Багато неорганічних матеріалів хоч і не горять, але мають порівняно невелику термічну стійкість. Наприклад, вапняки і мармур руйнуються при температурі 300-400°С, а шифер і азбоцементні вироби при температурі 300°С втрачають воду, стають крихкими, а при температурі 600°С при попаданні на них води – розтріскуються.

Межа вогнестійкості – це час (у годинах) від початку вогневого стандартного випробування зразків до виникнення одного з граничних станів елементів та конструкцій (втрата несучої та теплоізолюючої спроможності, щільності).

Межа поширення вогню – максимальний розмір пошкоджень, яким вважається обвуглення або вигорання матеріалу, що визначається візуально, а також оплавлюванням термопластичних матеріалів.

Обов’язки керівника, посадових осіб щодо організації та забезпечення пожежної безпеки на об’єкті.

Діяльність із забезпечення пожежної безпеки є складовою виробничої та іншої діяльності посадових осіб і працівників підприємств та об'єктів.

Керівник підприємства повинен визначити обов'язки посадових осіб щодо забезпечення пожежної безпеки, призначити відповідальних за пожежну безпеку окремих будівель, споруд, приміщень, дільниць, технологічного та інженерного устаткування, а також за утримання й експлуатацію засобів протипожежного захисту. Обов'язки щодо забезпечення пожежної безпеки, утримання та експлуатації засобів протипожежного захисту передбачаються у посадових інструкціях, обов'язках, положеннях про підрозділ.

На кожному об'єкті відповідним документом (наказом, інструкцією тощо) повинен бути встановлений протипожежний режим, який включає:

- порядок утримання шляхів евакуації;
- визначення спеціальних місць для куріння;
- порядок застосування відкритого вогню;

– порядок використання побутових нагрівальних приладів;

– порядок проведення тимчасових пожежонебезпечних робіт;

– правила проїзду та стоянки транспортних засобів;

– місця для зберігання і допустиму кількість сировини, напівфабрикатів та готової продукції, що можуть одночасно знаходитися у приміщеннях і на території;

– порядок прибирання горючого пилу й відходів, зберігання промасленого спецодягу та ганчір'я, очищення елементів вентиляційних систем від горючих відкладень;

– порядок відключення від мережі електроживлення обладнання та вентиляційних систем у разі пожежі;

– порядок огляду й зачинення приміщень після закінчення роботи;

– порядок проходження посадовими особами навчання й перевірки знань з питань пожежної безпеки, а також проведення з працівниками протипожежних інструктажів та занять з пожежно-технічного мінімуму з призначенням відповідальних за їх проведення;

– порядок організації експлуатації і обслуговування наявних засобів протипожежного захисту;

– порядок проведення планово-попереджувальних ремонтів та оглядів електроустановок, опалювального, вентиляційного, технологічного та іншого інженерного обладнання;

– порядок збирання членів пожежно-рятувального підрозділу добровільної пожежної охорони та посадових осіб, відповідальних за пожежну безпеку, у разі виникнення пожежі, виклику вночі, у вихідні й святкові дні;

– порядок дій у разі виникнення пожежі: порядок і способи оповіщення людей, виклику пожежно-рятувальних підрозділів, зупинки технологічного устаткування, вимкнення ліфтів, підйомників, вентиляційних установок,

– електроспоживачів, застосування засобів пожежогасіння; послідовність евакуації людей та матеріальних цінностей з урахуванням дотримання техніки безпеки. Працівники об'єкта мають бути ознайомлені з цими вимогами на інструктажах під час проходження пожежно-технічного мінімуму.

Під протипожежним режимом слід розуміти сукупність певних заходів і вимог пожежної безпеки, заздалегідь встановлених для об'єкта або окремого приміщення і підлягають обов'язковому виконанню всіма працюючими там особами.

Для кожного приміщення об'єкта мають бути розроблені та затверджені керівником об'єкта інструкції про заходи пожежної безпеки.

ВИСНОВКИ

В ході виконання кваліфікаційної роботи спроектовано комп’ютерну мережу компанії “Стиль-Н”. 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.

Кваліфікаційна робота містить повністю завершену логічну і фізичну топології мережі, таблицю IP-адресації та техніко-економічних показників які подано в графічній частині.

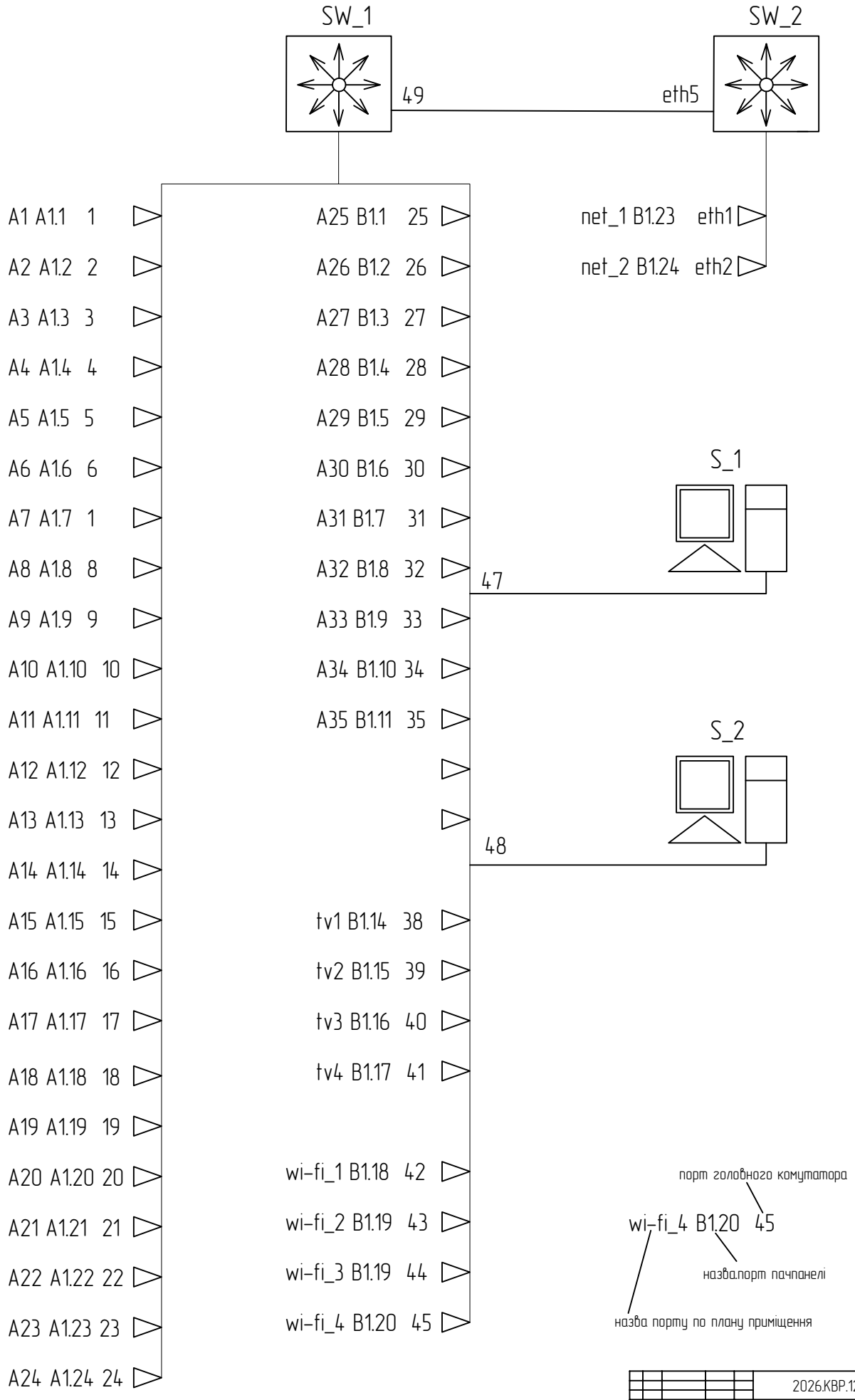
В економічному розділі розраховано собівартість мережі, її економічну ефективність, термін окупності та інші показники.

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

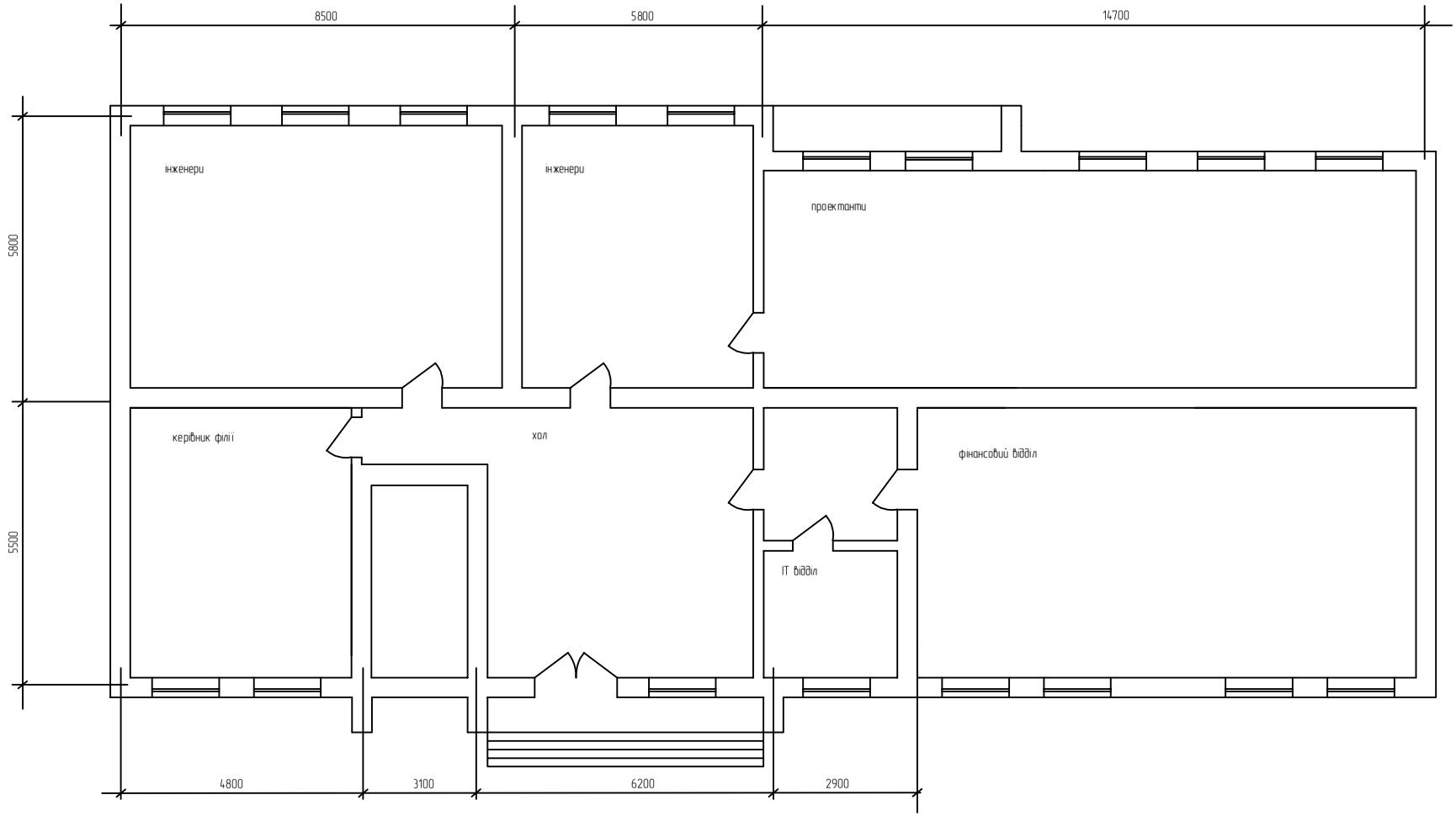
ПЕРЕЛІК ПОСИЛАНЬ

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. Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С., Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А. Комп’ютерні мережі: навчальний посібник. Київ: Компрінт, 2017. 821с.
4. Горбатий І.В., Бондарєв А.В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи. Львів: Львівська політехніка. 2016. 336с.
5. Додонов О. Г., Ланде Д. В., Путятін В. Г. Інформаційні потоки в глобальних комп’ютерних мережах.- К.: Наук, думка, 2009. - 295 с
6. Іртегов Д.В. Введення в мережні технології, К., 2014.
7. Комп'ютерні мережі. Принципи, технології, протоколи. Ювілейне видання. Оліфер В. Г.Оліфер Н. А.
8. Рамський Ю.С., Олексюк В.П., Балик А.В. Р21 Адміністрування комп’ютерних мереж і систем: Навч. пос. - Тернопіль: Навчальна книга – Богдан, 2010. - 196 с.
9. Шорошев В. В. Теоретичні і практичні аспекти організації і побудови архітектури захищених комп’ютерних систем. Монографія. - К.: ДУПСТ, 2011. - с.257.
10. Глобальні компютерні мережі URL:https://pidru4niki.com/74236/informatika/globalni_kompyuterni_merezhi (дата звернення: 18.04.2026).
11. Комутатори . URL:http://hotline.ua/computer/kommutatory/ . (дата звернення: 11.04.2026).
12. Мережеве устаткування компютерних мереж. URL: https://stud.com.ua/53330/informatika/merezheve_ustatkuvannya_programni_

komponenti_ upravlinnya_merezheyu (дата звернення: 11.05.2026).
13. Методи тестування та діагностики компютерних мереж. URL: file:///C:/Users/Downloads/metody-testirovaniya-i-diagnostirovaniya-kompyuternyh-setey.pdf (дата звернення: 3.05.2026).
14. Охорона праці – Москальова В.М. URL: http://studentbooks.com.ua/content/view/1327/76/ . (дата звернення: 3.05.2026).
15. Організація компютерних мереж. URL:http://nickshevtsov.blogspot. com/ 2017/10/blog-post.html (дата звернення: 22.04.2026).
16. Пожежна безпека на робочому місці. URL:https://ohoronapraci.kiev.ua/article/news/pozezna-bezpeka-na-robocomu-misci (дата звернення: 23.05.2026).
17. Як налаштувати UniFi AP без контролера https://wfshop.kiev.ua/kak-nastroit-unifi-ap-bez-kontrollera
18. Налаштування програмного VLAN у RouterOS на обладнанні Mikrotik URL: https://lanmarket.ua/ua/stats/bazovye-osnovy-nastroyki-vlan-v-routeros-na-oborudovanii-mikrotik-vlan-dlya-chaynikov-segmentatsiya/. Сайт lanmarket.ua (дата звернення: 19.05.2026).
19. Перевірка та тестування швидкості домашньої мережі. URL: https://www.agsat.com.ua/info/proverka-i-testirovanie-skorosti-domashney-seti/ (дата звернення: 19.05.2026).



					2026.КВР.123.412.13.00.00 /ІТ		
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі компанії "Стиль-Н" /Логічна Топологія	Літ.	Маса	Масшт.
Розроб.		Цигурда О.						
Керів		Лиж В. С.				Н		
Н.контр.		Язькіб А. В.				Аркуш 1	Аркушів 1	
Рецензія						ВСП ТФК ТНТУ КІ-412, м.Тернопіль		



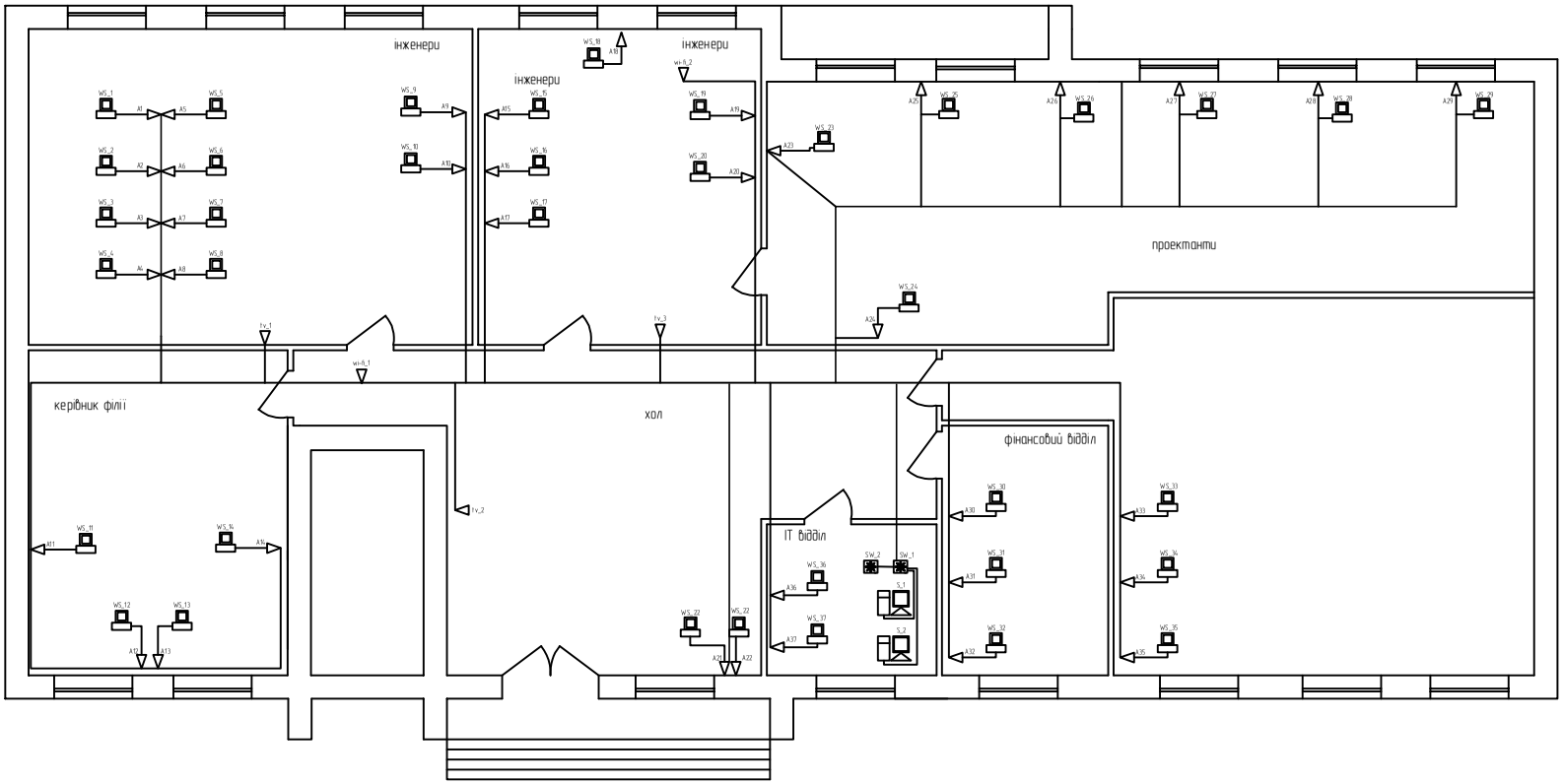
						2026.КВР.123.412.13.00.00 ПП	
Зм.	Арк.	№Докум.	Підпис	Дат.			
Розроб.		Шагіпадр О.			Розробка проекту комп'ютерної мережі компанії "Стиль-Н" План Приміщень	Літ.	Маса	Масшт.
Керів.		Пшк. В. С.						1:100
Н.контр.		Фазькіб. А. В.				Аркуш 1	Аркушів 1	
Рецензія						ВСП ТФК ТНТУ КІ-412, м.Тернопіль		
затв.								

ТАБЛИЦЯ ТЕХНІКО-ЕКОНОМІЧНИХ ПОКАЗНИКІВ							
№ п\п	параметр	одиниці виміру	значення	№ п\п	параметр	одиниці виміру	значення
1	технологія мережі	–	ethernet 1000	9	операційна система робочих станцій	–	windows 10
2	топологія мережі	–	гібридна	10	тип доступу до інтернет	–	вита пара
3	середовище передачі	–	Вита пара кат. 5Е	11	термін окупності	рік	1,3
4	кількість вузлів мережі	шт	45	12	плановий прибуток	грн	97187,6
5	марка головного комутатора	–	TP-Link TL-SG3452P	13	транспортні витрати	грн	12426,80
6	марка маршрутизатора	–	Mikrotik CCR2004-16G-2S+PC	14	собівартість	грн	189819,6
7	марка сервера	–	ARTLINE Business R15v14+	15	ціна	грн	287007,2
8	марка точки доступу	–	Mikrotik cAP XL ac (RbcAPGi-5acD2nD-XL)	16			

						2026.КВР.123.412.13.00.00 ТБ	
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі компанії "Стиль-Н" Таблиця техніко-економічних показників	Літ.	Маса	Масшт.
Розроб.		Шагидар О.						
Керів.		Пшк. В. С.				Н		
Нконтр.		Фазькіб. А. В.				Аркуш 1	Аркушів 1	
Рецензія						ВСП ТФК ТНТУ КІ-412, м.Тернопіль		
затв.								

ТАБЛИЦЯ IP-АДРЕСАЦІЇ В МЕРЕЖІ							
№ п.п	НАЗВА	IP-АДРЕСА ПІДМЕРЕЖІ	МЕТОД ОТРИМАННЯ АДРЕСИ	НАЗВА VLAN	НАЗВА МЕРЕЖЕВОЇ РОЗЕТКИ	МАСКА	РОБОЧА ГРУПА
1	WS_1-WS_29	10.100.10.0	DHCP	100	A_1-A_29	255.255.255.0	OFFICE
2	WS_30-WS_32	10.100.20.0	DHCP	200	A_30-A_32	255.255.255.0	BUCH
3	WS_33-WS_35	10.100.10.0	DHCP	100	A_33-A_35	255.255.255.0	OFFICE
4	tv_1-tv_4	10.100.30.0	DHCP	300	tv_1-tv_4	255.255.255.0	tv
5	wifi_1-wifi_4	10.100.40.0	DHCP	400	wifi_1-wifi_4	255.255.255.0	WIFI
6	S_1	10.100.10.150	STATIC	100		255.255.255.0	OFFICE
7	S_2	10.100.10.151	STATIC	100		255.255.255.0	OFFICE
8	SW_1	10.100.10.200	STATIC	100		255.255.255.0	OFFICE
9	SW_2	10.100.10.201	STATIC	100		255.255.255.0	OFFICE

						2026.КВР.123.412.13.00.00 ТА	
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі компанії "Стиль-Н" Таблиця IP адресації	Літ.	Маса	Масшт.
Розроб.		Цигипало О.				Н		
Керів.		Пшк. В. С.				Аркуш 1	Аркушів 1	
Нконтр.		Фазькіб. А. В.				ВСП ТФК ТНТУ КІ-412, м.Тернопіль		
Рецензія								
затв.								



						2026.КВР.123.412.13.00.00 ФТ	
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проєкту комп'ютерної мережі компанії "Стиль-Н" Фізична Топологія	Літ.	Маса	Масшт.
Розроб.		Цигипдло О.						1:100
Керів.		Пшк В. С.				Аркуш 1	Аркушів 1	
Нконтр.		Фазкіф А. В.				ВСП ТФК ТНТУ КІ-412, м.Тернопіль		
Рецензія								
затв.								