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 "ОптімаНет Сервіс"**

Виконав: студент IV курсу, групи КІ-412

Спеціальності 123 Комп'ютерна інженерія

(шифр і назва спеціальності)

_____ **Станіслав МУЗИКА**

(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

Музиці Станіславу Петровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту комп'ютерної мережі компанії "ОптімаНет Сервіс"**

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 _____ Станіслав МУЗИКА
(підпис) (ім'я та прізвище)

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

АНОТАЦІЯ

Музика С. П. - Розробка проєкту комп’ютерної мережі компанії “ОптімаНет Сервіс”: кваліфікаційна робота на здобуття освітньо-професійного ступеня фахового молодшого бакалавра, за спеціальністю 123 Комп’ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2026. -90с.

Дана кваліфікаційна робота присвячений розробці комплексної мережевої інфраструктури для компанії “ОптімаНет Сервіс”, що базується на інтеграції технічних, організаційних та економічних вимог підприємства. Робота має чітку послідовну структуру, яка розпочинається з формування детального технічного завдання, де визначаються ключові параметри продуктивності та функціональні можливості майбутньої системи. На основі цих вимог проведено аналіз архітектурних планів об'єкта, що дозволило обґрунтувати вибір топології, активного комутаційного обладнання та серверних потужностей з урахуванням необхідної пропускної здатності.

Особлива увага в проєкті приділена практичній реалізації, а саме конфігурації мережевих служб та впровадженню багаторівневої системи інформаційної безпеки, спрямованої на захист від зовнішніх загроз та несанкціонованого доступу. Економічний блок роботи містить детальний розрахунок капітальних інвестицій у апаратне та програмне забезпечення, що підтверджує фінансову доцільність запропонованих рішень. Завершальний етап дослідження охоплює регламентацію норм техніки безпеки та екологічної відповідності, забезпечуючи надійну та безпечну експлуатацію інфраструктури. Цілісність проєкту підкріплена пояснювальною запискою на аркушах формату А4 та відповідною графічною частиною формату А1.

ABSTRACT

Muzyka S. P. - Development of a computer network project for the company “OptimaNet Service”: qualification work for obtaining the educational and professional degree of a junior bachelor, in the specialty 123 Computer Engineering. Ternopil: VSP “TFK TNTU”, 2026. -90p.

This qualification work is devoted to the development of a comprehensive network infrastructure for the company “OptimaNet Service”, based on the integration of technical, organizational and economic requirements of the enterprise. The work has a clear sequential structure, which begins with the formation of a detailed technical task, which determines the key performance parameters and functional capabilities of the future system. Based on these requirements, an analysis of the architectural plans of the facility was carried out, which allowed to justify the choice of topology, active switching equipment and server capacities, taking into account the required bandwidth.

Particular attention in the project is paid to practical implementation, namely the configuration of network services and the implementation of a multi-level information security system aimed at protecting against external threats and unauthorized access. The economic block of work contains a detailed calculation of capital investments in hardware and software, which confirms the financial feasibility of the proposed solutions. The final stage of the study covers the regulation of safety standards and environmental compliance, ensuring reliable and safe operation of the infrastructure. The integrity of the project is supported by an explanatory note on A4 sheets and the corresponding graphic part of A1 format.

ЗМІСТ

ВСТУП

Сучасний етап розвитку цивілізації характеризується стрімкою конвергенцією обчислювальних систем і телекомунікаційних технологій. Процес інтеграції національних сегментів у глобальні мережеві структури привів до формування єдиного світового інформаційного простору.

Це не лише спростило транскордонний обмін даними, а й радикально підвищило ефективність експлуатації розподілених ресурсів у всіх сферах людської діяльності.

Зі зростанням аудиторії мережевих сервісів критично актуалізується потреба в інструментах структурованого зберігання, швидкого пошуку та безпечної обробки інформації.

Сучасні інформаційні мережі вирішують ці завдання, виступаючи універсальним засобом доступу до віддалених баз даних, програмних бібліотек та обчислювальних потужностей. Такий технологічний комплекс, що поєднує апаратні та програмні рішення, дозволяє оптимізувати роботу складних інформаційних систем через спільне використання спільних ресурсів.

У класифікації телекомунікаційних систем особливе місце посідають глобальні мережі (WAN), які об'єднують територіально розрізнені локальні мережі на базі уніфікованих протоколів та стандартів зв'язку. Історично кожна велика мережа (зокрема INTERNET, BITNET чи DECNET) створювалася для специфічних задач, проте їхня еволюція призвела до утворення масштабних розподілених структур.

Центральну роль у цій екосистемі відіграє Internet — найбільша глобальна мережа, архітектура якої базується на концепції інтеграції різнорідних систем.

Завдяки використанню стеку протоколів, що нівелюють різницю між фізичними середовищами передачі даних, забезпечується безперешкодна

взаємодія пристроїв з різними технічними характеристиками в планетарному масштабі.

Таким чином, Internet є складною сукупністю технічних засобів, стандартів та організаційних домовленостей, що забезпечують глобальну комунікацію та доступ до сучасних інформаційних сервісів.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Темою кваліфікаційної роботи є розроблення проєкту комп'ютерної мережі для компанії "ОптімаНет Сервіс". Основною метою створення такої мережевої інфраструктури є забезпечення ефективної взаємодії між усіма підрозділами підприємства, а також організація централізованого доступу до інформаційних ресурсів. Реалізація даного проєкту передбачає впровадження сучасних мережевих технологій, що дозволять підвищити продуктивність роботи персоналу та оптимізувати використання наявного обладнання.

Комп'ютерна мережа повинна забезпечувати об'єднання персональних комп'ютерів, які належать до різних структурних підрозділів організації, у єдину інформаційну систему. Це дозволить організувати централізований обмін даними між співробітниками та підвищити оперативність виконання службових завдань. Крім того, мережа має передбачати можливість спільного використання одного підключення до мережі Інтернет, що сприятиме зменшенню витрат на телекомунікаційні послуги та спростить адміністрування доступу.

Важливою вимогою до проєктованої мережі є підтримка служб локальної мережі та використання ресурсів глобальної мережі Інтернет у повсякденній діяльності компанії. Це включає доступ до мережевих сервісів, інформаційних ресурсів, а також можливість використання спільних програмних і апаратних засобів. Також одним із ключових завдань є організація недорогого та ефективного засобу обміну інформацією між працівниками, що дозволить забезпечити швидку передачу даних без значних фінансових витрат.

1.1.2 Призначенння розробки

Специфіка діяльності компанії “ОптімаНет Сервіс” у сегменті реалізації автозапчастин вимагає створення відмовостійкої мережевої інфраструктури для інтенсивної роботи з базами даних товарів, електронним документообігом та операційними комунікаціями.

Проєктована мережа виступає технологічним базисом для інтеграції підрозділів підприємства в єдиний інформаційний простір.

Ключові функціональні вектори:

– Оптимізація внутрішніх процесів: Впровадження системи електронного документообігу та забезпечення швидкого доступу до службових файлів суттєво прискорює обробку замовлень.

– Колективне використання ресурсів: Організація мережевого друку та спільного доступу до периферійного обладнання дозволяє знизити капітальні витрати та спростити адміністрування.

– Централізоване управління даними: Використання виділеного серверного обладнання гарантує цілісність, впорядкованість та доступність корпоративної інформації за умови гнучкого розмежування прав доступу.

– Зовнішня комунікація: Забезпечення стабільного високошвидкісного виходу до Internet є критичним для взаємодії з постачальниками, клієнтами та використання галузевих онлайн-сервісів.

Технічні вимоги до мережі передбачають пропускну здатність на рівні 1000 Мбіт/с (Gigabit Ethernet).

Це мінімізує затримки при роботі з великими масивами даних та забезпечує високу продуктивність праці персоналу, створюючи надійну основу для безперебійного функціонування бізнес-логіки підприємства.

1.1.3 Вимоги до апаратного та програмного забезпечення

Мережа, що проєктується в межах даної роботи, повинна будуватися із використанням сучасних програмних та апаратних засобів, які забезпечують надійність функціонування та можливість подальшого масштабування. При створенні мережевої інфраструктури необхідно застосовувати актуальні протоколи обміну даними, що гарантують сумісність обладнання та ефективну взаємодію між вузлами. Крім того, передбачається використання сучасних мережевих технологій і відповідної топології, які дозволять оптимально організувати передачу інформації та мінімізувати затримки. Проєктована мережа повинна бути логічно поділена на робочі групи, що забезпечить зручність адміністрування, розмежування доступу до ресурсів і підвищення рівня інформаційної безпеки. Передбачено, що швидкість передачі даних у мережі має становити 100/1000 Мбіт/с, що дозволить підтримувати як стандартні, так і високопродуктивні режими роботи.

Апаратне забезпечення мережі повинно відповідати вимогам доступності та практичності використання. Обладнання має бути загальновживаним і широко представленим на ринку, що спростить його придбання та обслуговування. Водночас воно повинно залишатися економічно доцільним, тобто відносно недорогим, без втрати необхідних технічних характеристик. Використовувані пристрої мають підтримувати задану швидкість передачі даних, а також забезпечувати можливість швидкої заміни або ремонту у випадку відмови. Додатково обладнання повинно мати засоби централізованого адміністрування, що дозволить ефективно контролювати роботу мережі та виконувати її налаштування.

Програмне забезпечення мережі являє собою сукупність операційних систем, встановлених на робочих станціях працівників підприємства. У межах даного проєкту передбачається використання операційної системи Windows 10, яка забезпечує підтримку сучасних мережевих протоколів, сумісність із прикладним програмним забезпеченням і зручні засоби адміністрування.

Використання єдиної операційної системи на всіх робочих місцях дозволить спростити технічну підтримку та забезпечити уніфіковану конфігурацію середовища користувачів.

Безпровідні точки доступу, що планується використовувати в мережі, повинні підтримувати сучасні механізми захисту бездротового з'єднання, зокрема протоколи WPA-PSK та WPA2-PSK. Також вони мають відповідати стандарту IEEE 802.11n, який забезпечує достатню швидкість передачі даних і стабільність роботи бездротового сегмента мережі. Застосування таких точок доступу дозволить організувати безпечний і надійний доступ мобільних пристроїв до мережевих ресурсів підприємства.

1.1.4 Стадії та етапи розробки

Ефективна розробка мережевої інфраструктури базується на комплексному аудиті поточної діяльності та стратегічних цілей підприємства. Специфіка бізнес-процесів організації безпосередньо детермінує архітектуру системи, визначаючи критичні обсяги трафіку та необхідний набір мережевих сервісів. При цьому архітектурні рішення повинні закладати потенціал для горизонтального та вертикального масштабування, враховуючи можливе зростання штату або впровадження нових інформаційних систем.

Ключові аспекти аналітичного етапу:

– Аудит існуючої бази: Дослідження стану наявного обладнання на предмет його продуктивності, сумісності та доцільності інтеграції з новим мережевим сегментом.

– Програмна сумісність: Аналіз прикладного ПЗ для формування вимог до надійності, захищеності та пропускної здатності каналів зв'язку.

– Вибір фізичної архітектури: Обґрунтування логічної топології, вибір середовища передачі даних (кабельна інфраструктура) та специфікація пасивного обладнання.

– Ієрархія комутації: Розрахунок кількості комутаторів доступу для формування робочих груп та визначення параметрів центрального комутатора (ядра мережі), що забезпечуватиме міжсегментну взаємодію.

– Маршрутизація та зовнішній шлюз: Оцінка потреб у маршрутизації трафіку та організація безпечного підключення до мережі Інтернет із застосуванням відповідного шлюзового обладнання.

1.1.5 Вимоги до документації

Фіналізація етапу проєктування полягає у створенні пакету технічних документів, які детермінують архітектуру мережі та слугують інструкцією для подальшого впровадження. Наявність повної документації гарантує точність монтажу та спрощує майбутнє обслуговування системи.

Тільки після верифікації та затвердження вказаної документації стає можливим перехід до фази фізичного монтажу. Такий підхід мінімізує ризик виникнення помилок у комутації та забезпечує відповідність створеної інфраструктури вимогам замовника.

Обов’язкові компоненти проєктного пакету:

– Логічна топологія: Схема, що відображає архітектуру мережі на рівні протоколів та адресації. Вона описує взаємодію між мережевими пристроями, розподіл IP-адрес, сегментацію (VLAN) та логічні зв'язки між серверами й робочими станціями.

– Фізична топологія: План реального розміщення обладнання в приміщеннях. Вона фіксує точне розташування комутаційних шаф, серверів, активних пристроїв та точок підключення користувачів відносно архітектурних особливостей будівлі.

– Схема маркування портів (виходів): Документація, що містить унікальні ідентифікатори кожної розетки та порту на патч-панелі. Це забезпечує швидку ідентифікацію ліній під час підключення кінцевого обладнання.

– План кабельних трас: Схема прокладання магістральних та горизонтальних кабельних каналів із зазначенням типів провідників, способів кріплення та маршрутів обходу інженерних перешкод.

1.1.6 Техніко-економічні показники

Проєктована інфраструктура розробляється як збалансоване рішення, що поєднує високу продуктивність із принципом економічної ефективності. Основним пріоритетом є створення надійного технологічного фундаменту, який підтримує актуальні галузеві стандарти та забезпечує тривалий життєвий цикл системи через механізми масштабування. Така структура дозволяє не лише впорядкувати інформаційні потоки підприємства, а й створити безпечне, кероване та продуктивне IT-середовище.

Ключові технічні параметри:

– Пропускна здатність: Використання стандарту Gigabit Ethernet (100/1000 Мбіт/с) дозволяє однаково ефективно опрацьовувати як стандартний офісний трафік, так і операції з ресурсомісткими базами даних.

– Масштабованість: Архітектура передбачає можливість нарощування кількості вузлів та сегментів без докорінної перебудови ядра мережі.

– Конвергенція середовищ: Поєднання стабільного провідного сегмента з бездротовою складовою (Wi-Fi) для забезпечення мобільності персоналу та гнучкого доступу до ресурсів.

– Зовнішні комунікації: Організація єдиного шлюзу для централізованого та безпечного виходу до глобальної мережі Інтернет.

Серверна інфраструктура: Для оптимізації бізнес-процесів у структурі мережі виділяються спеціалізовані серверні ролі:

– Бухгалтерський сервер: Призначений для централізованого зберігання та обробки фінансової звітності, баз даних і забезпечення високого рівня захисту конфіденційної інформації.

– WEB-сервер: Слугує платформою для внутрішніх корпоративних ресурсів або представництва компанії в мережі, що сприяє ефективній взаємодії з клієнтами та партнерами.

1.1.7 Порядок контролю та прийому

Завершальна стадія проєктування — здача в експлуатацію — є критичним етапом, що гарантує надійність та якість функціонування мережевої інфраструктури протягом усього життєвого циклу. Процес приймання базується на комплексній верифікації технічних параметрів та їх відповідності проєктній документації.

Ключові вимоги:

– Апаратна верифікація: Обов'язкова перевірка працездатності кожного мережевого вузла та контроль наявності цілісного маркування кабельної системи для забезпечення прозорості подальшого обслуговування.

– Інструментальний контроль: Діагностика функціональних характеристик мережі здійснюється за допомогою спеціалізованих сертифікаційних утиліт або програмних пакетів аналізу трафіку, що дозволяє виявити приховані дефекти монтажу чи конфігурації.

– Організаційне забезпечення: Після офіційного завершення робіт підрядником, замовник ініціює роботу спеціалізованої приймальної комісії. Комісія проводить всебічний аналіз представленої документації та фактичних результатів тестування.

Системний підхід до процедури приймання дозволяє мінімізувати експлуатаційні ризики, підтвердити відповідність мережі вимогам технічного завдання та зафіксувати готовність об'єкта до повноцінного функціонування у складі IT-інфраструктури підприємства.

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

Кваліфікаційна робота спрямована на створення цілісної мережевої екосистеми для компанії “ОптімаНет Сервіс”, що спеціалізується на дистрибуції автозапчастин та автохімії. Впровадження сучасної СКС (структурованої кабельної системи) розглядається як інструмент оптимізації повного циклу продажу: від автоматизованого підбору деталей до логістичного відстеження та SMS-інформування клієнтів. Ефективність бізнес-моделі безпосередньо залежить від швидкості доступу до централізованих баз даних та стабільності онлайн-комунікацій. Реалізація запропонованої схеми дозволить побудувати гнучку мережу, де кожен підрозділ має необхідну автономію, залишаючись частиною єдиного інформаційного середовища з високою пропускною здатністю та централізованим керуванням.

Функціональний розподіл та топологія розміщення

Для забезпечення високої продуктивності праці мережева інфраструктура сегментована відповідно до функціонального призначення підрозділів:

– Адміністративно-фінансовий сектор: Бухгалтерія комплектується трьома робочими станціями, виділеним сервером для фінансових баз даних та локальним комутаційним вузлом. Кабінети керівництва інтегровані в мережу для оперативного моніторингу та управління ресурсами.

– Комерційний блок: Два офіси менеджерів об'єднують десять ПК, що складають ядро відділу продажу. Виставковий зал обладнується чотирма терміналами для візуалізації асортименту та взаємодії з відвідувачами.

– Комунікаційні вузли: Конференц-зал отримує змішану інфраструктуру — п'ять ПК з провідним підключенням та точку бездротового доступу (Wi-Fi) для мобільності під час нарад.

– Ядро мережі (Технічний відділ): Тут концентрується центральне активне обладнання: магістральний комутатор, шлюзи доступу до Інтернет та основний серверний стек. Така централізація спрощує адміністрування, технічне обслуговування та забезпечує захист критичних вузлів системи.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЄКТУ

2.1 Розробка та обґрунтування логічної та фізичної схем мережі

Під топологією комп'ютерної мережі звичайно розуміється фізичне розташування комп'ютерів мережі друг щодо друга й спосіб з'єднання їхніми лініями зв'язку. Важливо відзначити, що поняття топології ставиться, насамперед, до локальних мереж, у яких структуру зв'язків можна легко простежити.

Топологія визначає вимоги до устаткування, тип використовуваного кабелю, можливі й найбільш зручні методи керування обміном, надійність роботи, можливості розширення мережі.

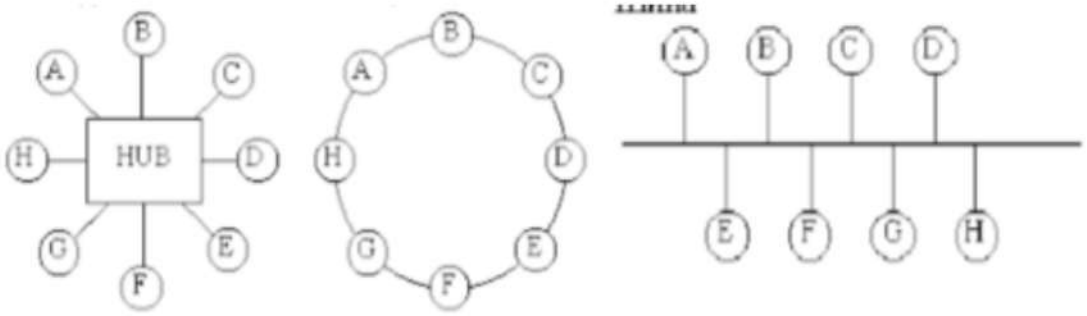


Рисунок 2.1 - Типи топологій комп'ютерних мереж

Існує три основних топології мережі (див рис. 2.1):

– Зірка (star): архітектурна схема, в якій усі периферійні робочі станції підключаються безпосередньо до єдиного центрального вузла, при цьому для кожного окремого пристрою виділяється власна незалежна лінія зв'язку.

– Кільце (ring): топологічна структура, де обмін даними організовано послідовно — кожен комп'ютер транслює інформацію виключно одному наступному вузлу в ланцюжку і приймає її лише від попереднього, утворюючи замкнене інформаційне коло.

– Шина (bus): мережева конфігурація, яка передбачає паралельне приєднання всіх робочих станцій до спільного каналу передачі даних, завдяки чому сигнали від будь-якого комп'ютера одночасно стають доступними для кожного пристрою в мережі.

Особливості мережевих топологій «Зірка» та «Кільце»

Топологія «Зірка» будується навколо чітко виділеного центру, до якого підключаються всі периферійні абоненти. Оскільки весь інформаційний обмін проходить через центральний вузол, на нього припадає максимальне навантаження з керування мережею, що вимагає використання значно потужнішого та складнішого обладнання порівняно з крайовими пристроями. Завдяки повній централізації керування в такій системі повністю виключаються колізії та конфлікти між абонентами.

Ця архітектура демонструє високу стійкість до локальних пошкоджень: вихід з ладу окремого комп'ютера або обрив його кабелю ізолює лише цей вузол, не впливаючи на роботу інших сегментів. Проте несправність центрального пристрою зупиняє функціонування всієї мережі, що вимагає впровадження спеціальних заходів із підвищення його надійності. На відміну від шини, кожна лінія зв'язку у «зірці» з’єднує лише двох абонентів (центр і периферію), зазвичай за допомогою двох однонаправлених ліній. Наявність лише одного приймача й передавача на канал спрощує апаратну частину, усуває потребу в термінаторах і полегшує стабілізацію рівнів сигналів. Суттєвим обмеженням «зірки» є ліміт портів центрального вузла (зазвичай 8–16). Якщо в цих межах масштабування є простим, то для подальшого розширення необхідно створювати ієрархічні структури, підключаючи додаткові комутатори замість периферійних клієнтів.

Топологія «Кільце» є найбільш вразливою до фізичних пошкоджень ліній зв'язку, через що в ній часто проєктують дві або більше паралельних ліній для резервування. Головна перевага такої схеми — ретрансляція сигналу кожним вузлом, що дозволяє збільшувати загальну протяжність мережі до десятків кілометрів, значно перевершуючи інші топології. Порівняно із

«зіркою», «кільце» потребує підведення двох кабелів до кожної робочої станції. Інколи архітектура реалізується на базі двох зустрічних кільцевих ліній: це дозволяє подвоїти пропускну здатність в ідеальних умовах, а у випадку аварії — зберегти працездатність системи на резервному каналі із меншою швидкістю.

Топологія «Шина» (Bus) Концепція «загальної шини» передбачає використання ідентичного мережевого обладнання та повну рівноправність усіх підключених абонентів. Оскільки фізичний канал передачі даних є єдиним для всієї системи, комп'ютери змушені транслювати інформацію суворо по черзі. Одночасне відправлення пакетів кількома вузлами призводить до їхнього спотворення через виникнення колізій. Через це в шині реалізовано напівдуплексний режим роботи (half duplex), де приймання та передача рознесені в часі.

Відсутність центрального керуючого елемента підвищує загальну живучість системи, адже вихід з ладу будь-якої робочої станції не порушує роботу інших. До переваг шини належать легкість масштабування без зупинки мережі та мінімальні витрати кабелю, хоча підключення кожного проміжного комп'ютера за допомогою двох кабелів може створювати незручності під час монтажу. Оскільки завдання вирішення конфліктів покладається на клієнтські пристрої, внутрішня архітектура мережевих адаптерів є досить складною, проте масове використання стандартів Ethernet та Arcnet дозволило утримати ринкову вартість такого обладнання на низькому рівні.

Вплив обладнання на логічну структуру та мережеві пристрої

Залежно від функціональних можливостей та алгоритмів роботи активного обладнання, одна й та сама фізична схема прокладання кабелю може трансформуватися у зовсім іншу логічну топологію.

– Комутатор (Світч): Цей пристрій призначений для об'єднання вузлів у межах одного або кількох сегментів на канальному (другому) рівні моделі OSI. На відміну від застарілих концентраторів (хабів), комутатор аналізує вхідний кадр і перенаправляє його виключно на порт отримува-

ча, що суттєво підвищує як безпеку даних, так і загальну пропускну здатність. Робота пристрою базується на динамічному веденні таблиці комутації (таблиці MAC-адрес), де фіксується відповідність фізичних адрес вузлів конкретним портам. Таким чином, комутатор організовує топологію логічної «зірки».

– Маршрутизатор (Роутер): Апаратний комплекс для забезпечення зв'язку між різними, логічно ізольованими мережами, що функціонує на мережевому (третьому) рівні моделі OSI. Для доставки пакетів він використовує глобальну топологію інтермережі та правила, задані адміністратором (таблиці маршрутизації). Роутер здатний виконувати трансляцію адрес (NAT), фільтрацію та сегментацію трафіку, а також шифрування каналів зв'язку. Ключовою відмінністю від комутаторів є те, що маршрутизатори не пропускають через себе широкомовний шторм (broadcast traffic), обмежуючи його дію лише межами одного домену, тоді як комутатори без додаткових налаштувань (VLAN) транслюють такі запити на всі порти.

– Мережеві мости (Bridges): Пристрої, що використовуються для об'єднання двох окремих сегментів мережі, які мають обмеження за своєю фізичною довжиною. Мости здійснюють передачу та фільтрацію трафіку між цими ділянками на основі MAC-адрес, а також можуть виконувати функції посилення, відновлення та конвертації електричних чи оптичних сигналів.

Порівняльний аналіз мережевих топологій

Топологія «Зірка» (Star Topology)

– Переваги: Високі показники швидкодії, оскільки загальна пропускна здатність лімітується виключно характеристиками центрального комутаційного пристрою. Процес масштабування (підключення нових робочих станцій) є максимально простим і швидким. Система має високу відмовостійкість: апаратний збій на одному з периферійних вузлів не порушує функціонування інших сегментів. Завдяки виділеним каналам зв'язку між

клієнтом і центром повністю нівелюється ризик виникнення колізій (зіткнення пакетів даних). Крім того, архітектура забезпечує зручність централізованого адміністрування та легкість локалізації лінійних пошкоджень.

– Недоліки: Підвищена вартість реалізації через необхідність придбання активного центрального обладнання та більшу витрату кабельної продукції порівняно з шинною архітектурою. Критичною точкою відмови є центральний вузол — його вихід з ладу повністю паралізує мережу. Кількість можливих підключень жорстко обмежена числом фізичних портів на комутаторі.

Топологія «Кільце» (Ring Topology)

– Переваги: Спрощений контроль процесу доставки пакетів безпосередній адресат за рахунок послідовного обходу вузлів. Реалізовано ефективний механізм циркуляції повідомлень, що дозволяє відправляти кілька інформаційних блоків один за одним. Схема спрощує моніторинг і виявлення некоректно функціонуючих точок. Загальна протяжність такої мережі може бути досить значною, оскільки кожен активний вузол фактично виконує функцію ретранслятора (повторювача) сигналу без залучення стороннього обладнання.

– Недоліки: Із розширенням клієнтської бази та зростанням кількості вузлів швидкість обміну даними пропорційно знижується, адже кожен пакет має транзитом пройти через усі проміжні станції. Надійність є низькою: одиничний обрив кабелю або вимкнення будь-якого ПК розриває кільце та зупиняє всю систему. Для інтеграції нового користувача необхідно тимчасово зупиняти роботу мережевого сегмента.

Топологія «Шина» (Bus Topology)

– Переваги: Інформаційні потоки транслюються в загальне середовище, стаючи одночасно доступними для кожного підключеного комп'ютера. Метод відрізняється низькою фінансовою вартістю розгортання, простотою монтажу та базових налаштувань. Робочі станції інтегруються

незалежно одна від одної, тобто підключення нового абонента не потребує призупинення мережевого обміну. Аварія на окремому клієнтському пристрої не впливає на життєздатність інших ліній.

– Недоліки: Низький рівень інформаційної безпеки, оскільки трафік на кожному комп'ютері може бути перехоплений з будь-якого іншого вузла сегмента. Швидкість передачі даних є порівняно низькою і суттєво деградує при збільшенні кількості активних абонентів. Будь-яке фізичне пошкодження магістрального кабелю або кінцевих роз'ємів (і навіть відсутність термінатора) повністю паралізує мережу, при цьому локалізувати точне місце дефекту без спеціальних приладів вкрай важко.

Коміркова топологія (Mesh Topology)

– Переваги: Максимальний рівень живучості — поодинокі чи навіть множинні розриви кабельних ліній не впливають на працездатність мережі завдяки динамічному перенаправленню трафіку альтернативними маршрутами. Цей підхід є суттєво економічнішим та ефективнішим порівняно з теоретичною повнозв’язною топологією, оскільки прямі фізичні канали прокладаються лише між тими вузлами, що здійснюють найбільш інтенсивний та регулярний обмін даними.

– Недоліки: Висока складність проектування та значні питомі витрати кабелю для організації надлишкових зв'язків.

Для проєктування мережі підприємства оптимальним є комбінований підхід. Базові робочі зони та кабінети реалізуються за топологією «зірка» задля забезпечення високої продуктивності та простоти обслуговування робочих місць. Для зв'язку між ключовими комутаційними вузлами та серверною (ядро мережі) застосовується коміркова (частково повнозв'язна) топологія, що гарантує абсолютну відмовостійкість і безперебійність бізнес-процесів у разі аварій на магістральних лініях.

При виборі конкретного типу кабельної продукції для побудови СКС підприємства аналізуються такі взаємопов'язані характеристики:

– Економічна доцільність: Оцінюється повна вартість придбання матеріалів, проведення монтажних робіт, встановлення кінцевого обладнання (конекторів, патч-панелей) та подальшого технічного обслуговування ліній.

– Пропускна здатність: Здатність кабелю забезпечувати необхідну швидкість передачі даних (наприклад, 1 Гбіт/с або 10 Гбіт/с) для підтримки сучасних корпоративних сервісів.

– Максимальна дальність трансляції: Гранична відстань, на якій фізичні властивості кабелю гарантують якісний і чіткий сигнал без згасання та без залучення проміжних підсилювачів чи повторювачів (репітерів).

– Захищеність та безпека: Рівень стійкості до зовнішніх електромагнітних завад (перешкодозахищеність завдяки екрануванню), а також ступінь захисту від потенційного несанкціонованого зняття інформації з лінії (наприклад, через індукційні наведення).

В інженерній практиці виділяють три основні класи кабелів.

1. Вита пара (Twisted Pair — TP)

Цей тип кабелю складається з ізольованих мідних провідників, які скручені попарно з певною кількістю витків на одиницю довжини для мінімізації взаємних наведень між парами. Вита пара розподіляється на два ключові підкласи:

– Неекранована (UTP): простіша у монтажі та найдешевша, використовується у звичайних умовах.

– Екранована (FTP/STP): оснащена загальним або індивідуальними екранами з фольги чи металевого обплетення, що забезпечує значно вищу стійкість до зовнішніх електромагнітних завад.

Вита пара є промисловим стандартом та найкращим вибором для побудови горизонтальних підсистем СКС у малих та середніх установах. Водночас мідні провідники мають високий коефіцієнт загасання сигналу та є чутливими до потужного наведення, через що максимальна довжина кабельного сегмента між двома активними пристроями (наприклад, від

комутатора до робочої станції) чітко обмежена стандартом і не повинна перевищувати 100 метрів.

2. Волоконно-оптичний кабель (Optical Fiber)

Волоконно-оптичні технології є найбільш прогресивним і швидкісним рішенням для сучасних телекомунікацій. Замість електричних імпульсів носієм інформації тут виступає світловий промінь, що генерується лазером або світлодіодом і проходить крізь надтонкі скляні чи пластикові волокна.

Оскільки світловий сигнал повністю байдужий до електромагнітних та радіочастотних полів, оптоволоконні лінії демонструють абсолютну завадостійкість. Це дозволяє організувати захищену від перехоплення, безпомилкову та надшвидкісну передачу даних на швидкостях до 40 Гбіт/с (і вище) на одному ініційованому каналі. Кількість інформаційних каналів, які можна ущільнити в одному кабелі, є колосальною.

Проте передача світла по одному скляному волокну є суворо односпрямованою (симплексний режим). Для того щоб забезпечити повноцінний двосторонній дуплексний обмін (одночасне приймання та передача), обладнання необхідно з’єднувати щонайменше двома оптичними волокнами. Саме тому у промисловому виробництві волоконно-оптичні кабелі завжди випускаються з парною кількістю внутрішніх жил. До основних недоліків оптики відносять високу вартість самого кабелю та інтерфейсних модулів, а також технологічну складність зварювання волокон і монтажу кінцевих роз'ємів, що вимагає залучення висококваліфікованих фахівців та спеціального дорогого інструментарію.

Радіохвилі активно використовуються як фізичне середовище передачі інформаційних сигналів у бездротових локальних обчислювальних мережах (WLAN), а також для організації каналів зв'язку між територіально рознесеними локальними мережами.

Для узагальнення та систематизації розглянутого матеріалу порівняльні характеристики різних типів ліній зв'язку, включаючи провідні та бездротові рішення, зведено в таблицю 2.1.

Таблиця 2.1 — Комплексні порівняльні характеристики фізичних середовищ передачі даних

Тип лінії зв'язку	Максимальна швидкість передачі	Гранична відстань сегмента	Стійкість до завад	Складність монтажу та вартість ліній
1	2	3	4	5
Неекранована вита пара (UTP)	100 Мбіт/с – 1 Гбіт/с	до 100 метрів	Низька / Середня	Низька складність, мінімальна вартість
Екранована вита пара (FTP/STP)	1 Гбіт/с – 10 Гбіт/с	до 100 метрів	Висока	Середня складність, помірна вартість
Коаксіальний кабель	до 10 Мбіт/с (без модуляції)	від 4 до 50 км (з модуляцією)	Висока	Середня складність, низька затребуваність
Волоконно-оптичний кабель	10 Гбіт/с – 40 Гбіт/с і вище	від декількох км до десятків км	Абсолютна (імунітет до ЕМЗ)	Висока складність (зварювання), висока вартість
Радіохвилі (Бездротове середовище)	від 2 Мбіт/с (базова) до сотень Мбіт/с	200–300 м (в приміщенні) / зона прямої видимості	Чутлива до перешкод та атмосфери	Дуже низька складність, швидке розгортання

На основі проведеного аналізу техніко-експлуатаційних характеристик, вибір неекранованої витої пари категорії 5e (Category 5e) є найбільш раціональним і збалансованим рішенням для побудови горизонтальної підсистеми СКС.

Даний тип кабелю повністю задовольняє вимогам стандарту Gigabit Ethernet (1000BASE-T), забезпечуючи пропускну здатність до 1000 Мбіт/с на відстані до 100 метрів, що є оптимальним для архітектури нашого підприємства.

Логічна архітектура та комутаційна структура мережі

Логічна побудова мережі базується на ієрархічній моделі та розподілі навантаження між пристроями доступу та магістральним вузлом. Апаратна частина структури складається з таких елементів:

– Рівень доступу (Access Layer): Формується за допомогою шести 16-портових некерованих комутаторів другого рівня (L2). До них безпосередньо підключаються кінцеві пристрої працівників (робочі станції, принтери). Оскільки ці комутатори є некерованими, вони виконують лише базову функцію просування кадрів на основі MAC-адрес у межах своїх локальних сегментів.

– Магістральний вузол / Рівень ядра (Core/Distribution Layer): Представлений головним комутатором 3-го рівня (L3 Switch). Саме на цей пристрій покладається вся інтелектуальна робота з керування мережею, маршрутизації між підмережами та забезпечення безпеки.

Кожен із шести некерованих комутаторів підключається окремим виділеним магістральним лінком (Uplink) до відповідного порту головного L3-комутатора.

Організація віртуальних мереж (VLAN) та ізоляція робочих груп

Попри використання некерованих комутаторів на рівні доступу, архітектура дозволяє створити ізольовані та незалежні робочі групи. Це досягається завдяки конфігуруванню віртуальних локальних мереж (VLAN) безпосередньо на портах головного L3-комутатора:

– Поділ за портами (Port-based VLAN): Кожен порт головного комутатора, до якого підключено певний 16-портовий комутатор, жорстко закріплюється за відповідним VLAN (наприклад, VLAN 10 — Бухгалтерія, VLAN 20 — Відділ продажів тощо). Таким чином, увесь широкомовний трафік від некерованого комутатора ізолюється в межах свого віртуального сегмента.

– Міжвекторна маршрутизація (Inter-VLAN Routing): Оскільки головний пристрій працює на 3-му рівні моделі OSI (мережевому), саме він виступає в ролі шлюзу за замовчуванням (Default Gateway) для кожного VLAN. Роутинг між різними робочими групами відбуватиметься виключно через цей комутатор за чітко визначеними правилами та списками контролю доступу (ACL), що суттєво підвищує безпеку даних.

Використання бездротового сегмента (Wi-Fi)

Для забезпечення мобільності персоналу та гостьового доступу до логічної структури інтегрується бездротова точка доступу (Access Point).

Лінк від точки доступу підключається до окремого фізичного порту головного L3-комутатора. Цей порт конфігурується у складі абсолютно ізольованого, окремого VLAN (наприклад, VLAN 90 — Wireless/Guest). Таке рішення дозволяє:

– Повністю відокремити бездротовий трафік від корпоративної дротової мережі.

– Захистити внутрішні ресурси та бази даних від потенційних загроз із боку мобільних пристроїв чи гостьових підключень.

– Застосувати окремі політики обмеження швидкості та фільтрації трафіку для бездротових клієнтів безпосередньо на головному комутаторі.

Все описане відображено в таблиці 2.2. та таблиці 2.3

Таблиця 2.2 – Логічна адресація в мережі

Позначення вузлів	Робоча група/ Кількість вузлів		Назва кабінету	Номер VLAN	Адреса підмережі/ Маска
1	2	3	4	5	6
WS_1—WS_2	MENEJ	2	Керівник та його заступник	20	192.168.20.0/24
WS_3—WS_7	MENEJ	5	менеджери	20	192.168.20.0/24
WS_8-WS_11, PR_1	MENEJ	4	менеджери	20	192.168.20.0/24
WS_12—WS_17	MENEJ	8	менеджер3	20	192.168.20.0/24
WS_18—WS_22, PR_2	MENEJ	5	конференц-зал	20	192.168.20.0/24
WS_23—WS_25, PR_3, S_2	BUCH	3	бухгалтерія	30	192.168.30.0/24
WS_26	MENEJ	1	охорона	20	192.168.20.0/24
S_1	MENEJ		Технічний відділ	20	192.168.20.0/24
Ap_1	MENEJ		Конференц приміщення	40	192.168.40.0/24

Таблиця 2.3 - Таблиця конфігурування VLAN

№ п/п	Познач. вузла	Номер порту	Тип порту	Назва мереж. пр-ю	Номер порту	Тип порту	Номер VLAN
1	2	3	4	5	6	7	8
2	SW_4	10	Провайдер інтернет				
3	SW_4	12	Access	S_1	-	Access	-

Продовження таблиці 2.3

1	2	3	4	5	6	7	8
4	SW_4	1	Access	SW_1	16	Access	20
5	SW_4	2	Access	SW_2	16	Access	20
6	SW_4	3	Access	SW_3	16	Access	20
7	SW_4	4	Access	SW_5	16	Access	20
8	SW_4	5	Access	SW_6	16	Access	20
9	SW_4	6	Access	SW_7	16	Access	30
	SW_4	10	Access	WS_26		Access	20
18	SW_4	12	Access	AP_1	WAN	Access	40

2.2 Обґрунтування вибору комунікаційного обладнання

Для кваліфікаційної роботи оберемо (керуючись таблиуею 2.4) MikroTik CRS326-24G-2S+RM — це класичний смарт-комутатор, який завдяки операційній системі RouterOS та апаратній підтримці (L3 Hardware Offloading) може виконувати базову маршрутизацію між VLAN на швидкості портів (Wire-speed), залишаючись дуже бюджетним рішенням.

Комутатор Mikrotik CRS326-24G-2S+RM є відмінним вибором для професіоналів, які шукають надійне мережеве рішення. З 24-ма гігабітними Ethernet-портами та двома високошвидкісними SFP+ слотами, цей пристрій забезпечує максимальну продуктивність для мережі будь-якого масштабу. Унікальна функція Dual boot дозволяє користувачам обрати між операційними системами SwOS і RouterOS, що забезпечує гнучкість у виборі оптимального програмного забезпечення згідно з потребами бізнесу.

Цей керований комутатор, (показаний на рисунку 2.3) розроблений для встановлення в стійку, виготовлений з високоякісного металу, що гарантує довговічність та надійність. Комутатор підтримує віддалене управління, що дозволяє з легкістю реалізовувати комплексні мережеві конфігурації без

фізичного втручання. Інноваційні комутаційні можливості включають управління переадресацією між портами, налаштування VLAN, активацію MAC-фільтрів та обмеження смуги пропускання. Також передбачена функція віддзеркалення трафіку та можливість зміни полів заголовків IP і MAC, що робить цей комутатор чудовим вибором для складних мережевих середовищ. З 16 Мб flash-пам’яті ви можете розраховувати на швидку обробку даних та ефективність обчислень.

Таблиця 2.4 - Таблиця втбору головного комутатора

Характеристика	MikroTik CRS326-24G-2S+RM	Cisco Catalyst 1000-24T-4X-L	Aruba Instant On 1960 24G (JL806A)
1	2	3	4
Клас пристрою	Smart / L3 Light	Enterprise / L3 Light	Smart / L3 Light
Кількість портів 1G RJ45	24	24	24
Порти 10G SFP+ (оптика)	2	4	2
Порти 10G RJ45 (мідь)	Відсутні	Відсутні	2
Пропускна здатність (Switching Capacity)	44 Гбіт/с	128 Гбіт/с	128 Гбіт/с
Швидкість пересилання пакетів	32.7 Mpps	95.23 Mpps	95.23 Mpps
Тип керування (OS)	RouterOS / SwOS (Dual Boot)	Cisco IOS (CLI, Web-UI)	Web-UI, Cloud (Instant On App)

Продовження таблиці 2.4

1	2	3	4
Функціонал L3 (Маршрутизація)	Статична/Динамічна (з HW Offloading на нових версіях)	Статична маршрутизація (до 16 маршрутів)	Статична маршрутизація (IPv4/ IPv6)
Охолодження	Пасивне (безвентиляторний, тихий)	Пасивне (безвентиляторний)	Активне (вбудовані вентилятори)
Ціновий сегмент	Бюджетний (найнижча ціна) орієнтовно 8000 грн	Преміум (всока ціна)	Середній

Рисунок 2.3 – Зовнішній вигляд комутатора MikroTik CRS326-24G-2S+RM

У комп’ютерній мережі необхідно використати шість шістнадцяти-портових комутаторів.

Для вибору комутатора складемо порівняльну таблицю 2.5 популярних комутаторів.

Таблиця 2.5 – Порівняльна характеристика шістнадцятипортових комутаторів, некерованих

Характеристика	Cisco CBS110-16T-EU	HPE Aruba 1430 16G (R8R47A)	D-Link DGS-1016D
1	2	3	4
SFP слоти (оптика)	Відсутні	Відсутні	Відсутні
Комутаційна матриця (Внутрішня швидкість)	32 Гбіт/с	32 Гбіт/с	32 Гбіт/с
Швидкість пересилання пакетів (Forwarding)	23.8 Mpps	23.8 Mpps	23.8 Mpps
Буфер пакетів	2 Мбіт	2 Мбіт	512 КБ (4.1 Мбіт загальний масив)
Таблиця MAC-адрес	8K	8K	8K
Охолодження	Пасивне (без вентиляторів)	Пасивне (без вентиляторів)	Пасивне (без вентиляторів)
Додаткові функції	QoS (802.1p), Loop detection (захист від петель), Cable diagnostics	QoS (802.1p), Jumbo Frames (9216 байт), автоматична пріоритезація	QoS (802.1p), Енергозбереження (802.3az)
Ціновий сегмент	Вище середнього	Вище середнього	Бюджетний / Доступний

Виходячи з таблиці 2.5, враховуючи співвідношення ціни до технічних характеристик пристрою для мережі вибрано комутатор Cisco CBS110-16T-EU, зовнішній вигляд якого зображено на рисунку 2.4.

Рисунок 2.4 – Зовнішній вигляд комутатора Cisco CBS110-16T-EU

Для забезпечення бездротового сегмента інфраструктури в проєкті передбачено використання сучасної точки доступу.

Попри велике різноманіття мережевого обладнання від різних світових виробників, для цієї мережі було обрано модель MikroTik cAP ac (RBcAPGi-5acD2nD), зовнішній вигляд якої представлено на рисунку 2.5.

Головним технічним критерієм на користь цього пристрою стала його повна сумісність із вибраним головним комутатором MikroTik.

Це дозволяє реалізувати централізоване керування всією бездротовою екосистемою за допомогою фірмової технології CAPsMAN (Controlled Access Point System Manager), інтегрувати Wi-Fi клієнтів в ізольовані віртуальні мережі (VLAN) та гнучко масштабувати покриття.

Орієнтовна ринкова вартість даної моделі становить 3600 грн, що робить її економічно вигідним рішенням для корпоративного сектору. Візуальне виконання пристрою наведено на рисунку 2.4.

Бездротова точка доступу cAP 2nD оснащена інтегрованим радіомодулем із підтримкою стандартів зв'язку IEEE 802.11b/g/n, що забезпечує стабільну роботу бездротового сегмента в класичному частотному діапазоні 2.4 ГГц. Конструктивне виконання пристрою передбачає подачу електроживлення виключно за технологією PoE (Power over Ethernet) через

стандартний мережевий кабель «вита пара», що спрощує монтаж і позбавляє від необхідності прокладання силових ліній до місця встановлення.

Рисунок 2.5 – Вигляд точки доступу MikroTik cAP

Дане апаратне рішення є ідеальним вибором для інтеграції у фірмову екосистему CAPsMAN — спеціалізовану технологію централізованого керування бездротовими точками доступу від компанії MikroTik. Функціонал контролера CAPsMAN може бути безкоштовно активований на будь-якому маршрутизаторі чи L3-комутаторі серії RouterBOARD, який виконує роль ядра мережі. Завдяки такому архітектурному підходу відпадає потреба у придбанні стороннього програмного забезпечення, розгортанні складних віртуальних машин або виділенні окремого персонального комп'ютера для адміністрування Wi-Fi мережі.

У комп’ютерній мережі передбачено використання серверного комп’ютера.

Сервер ARTLINE Business - це справжнє серце вашої IT інфраструктури. Він має збалансовану продуктивність і невелике споживання енергії, що дасть вам змогу з мінімальними витратами ефективно виконувати бізнес-завдання.

Конфігурації моделей ARTLINE Business створюються з максимальною спрямованістю на стабільну та безперебійну роботу.

Модель ARTLINE Business T17v23 втілила все, що ви чекаєте від сервера: надійність, довговічність, продуктивність, економічність, простоту використання та обслуговування. Зовнішній вигляд серверного ПК приведено на рисунку 2.6

Сервер побудований на базі материнської плати ASUS PRIME H670-PLUS D4. Компанія ASUS є лідером на ринку материнських плат протягом багатьох років, а це означає, що плата забезпечить гарантовано довгий термін служби сервера. Підтримує процесори Intel 12-го покоління. Включає: модуль регулятора напруги VRM Digi+ для стабільної та ефективної роботи процесора, технологію підвищення продуктивності оперативної пам'яті (ASUS OptiMem) і технологію для регулювання енергопостачання компонентів ПК (ASUS EPU).

Продуктивний процесорний чип дванадцятого покоління Intel Core i5-12400 володіє шістьма ядрами (12 потоків обробки) з частотою роботи 2.5 ГГц (4.4 ГГц у режимі Turbo) і вбудованою графікою Intel UHD 730, що дасть йому змогу чудово справлятися з поставленими завданнями.

У лінійці Business T17 встановлюється A-Brand пам'ять (Samsung, Hynix, Trancend, Kingston), що вже саме говорить про якість, гарантовану маркою відомого виробника.

Два встановлені швидкісні SSD накопичувачі на 500 ГБ кожен забезпечать швидке завантаження системних файлів ОС і всіх інших програм, а також надійне зберігання великої кількості необхідної інформації.

У сервері ARTLINE Business T17v23 використовується один із найкращих на сьогодні блоків живлення ASUS TUF потужністю 450 Вт із сертифікатом 80+ Bronze. Якість продуктів ASUS TUF перевірена часом і підтверджується тисячами систем, зібраних на їхній основі.

Професійна збірка сервера ARTLINE забезпечить оптимальний повітряний потік усередині корпусу, а отже, і чудове охолодження всіх компонентів.

Вартість 58 000 грн

За матеріалами https://rozetka.com.ua/ua/artline-t17v23/p396394248/

Рисунок 2.6 – Зовнішній вигляд ARTLINE Business T17v23

Зведемо все вибране нами обладнання в одну таблицю.

Таблиця 2.6 — Перелік обладнання мережі

№ п.п	назва	Кількість	ціна
1	2	3	4
1	комутатор Cisco CBS110-16T-EU	6	8600,00 грн.
2	комутатор MikroTik CRS326-24G-2S+RM	1	8000,00 грн.
3	точка доступу MikroTik cAP ac (RB	1	3600,00 грн.

Продовження таблиці 2.6

1	2	3	4
	cAPGi-5acD2nD)		
4	Сервер ARTLINE Business T17v23	1	58000,00 грн.
7	Комутаційна шафа	1	16860,00 грн.
8	Кабель мережевий	4	3 400,00 грн.
9	Короб 20х40х2000	45	69,00 грн.

2.3 Особливості монтажу мережі

На сьогодні найбільш затребуваним і масовим середовищем для транспортування інформаційних потоків у межах структурованих кабельних систем (СКС) залишаються кабельні вироби з мідними жилами. Водночас під час проектування та розгортання магістральних ліній першого й другого рівнів розробники все частіше віддають перевагу волоконно-оптичним технологіям, які спроможні забезпечити колосальну пропускну здатність і надвисокі швидкості обміну даними.

Рівень стабільності, швидкісні параметри та загальний життєвий цикл функціонування телекомунікаційної інфраструктури безпосередньо корелюють із тим, наскільки технологічно коректно під час монтажних робіт було здійснено протягування, фіксацію та кріплення кабельних трас. Базові та специфічні правила до організації прокладання й утримання провідникових ліній регламентуються чинними профільними стандартами індустрії СКС, серед яких ключовими є міжнародний регламент ISO/IEC IS 11801, а також відповідні національні нормативні акти (наприклад, ДСТУ чи ГОСТ Р 53246).

Одним із найкритичніших аспектів є забезпечення проходження кабельних маршрутів на безпечній відстані від будь-яких джерел потужного електромагнітного випромінювання. До цієї категорії традиційно відносять

магістральні лінії силової електропроводки, трансформаторні підстанції та вузли, великі промислові електродвигуни, генераторні установки, радіопередавальні пристрої та високопродуктивну копіювально-розмножувальну техніку. Взаємне географічне розташування слабкострумових мереж та силових інженерних вузлів має детально прораховуватися ще на стадії ескізного проектування.

Якщо ж в умовах реального об'єкта дотриматися нормативних просторових інтервалів неможливо, інженери застосовують захищені кабелі з додатковим екрануванням, а також ізолюючі металеві короби та екрановані кабель-канали. Для ефективного придушення індукованих наведень усі металеві кабельні лотки й траси, незалежно від наявності власного екрану у провідників, в обов'язковому порядку підлягають технологічному заземленню в процесі будівництва СКС.

Досить часто виникають ситуації, коли телекомунікаційні траси прокладаються паралельно з електричними кабелями живлення. У таких випадках критично важливо витримувати мінімальну дистанцію, величина якої безпосередньо залежить від робочої потужності силової лінії. Відповідно до положень галузевого стандарту EIA/TIA 569, встановлюються такі рамкові обмеження:

– Не менше 127 мм — для сусідства з лініями потужністю до 2 кВт;

– Не менше 305 мм — якщо потужність силової лінії перебуває в діапазоні від 2 до 5 кВт;

– Не менше 610 мм — для кабельних ліній, чия потужність перевищує 5 кВт.

У разі розміщення телекомунікаційного провідника всередині заземленого замкненого металевого лотка, зазначені нормативні відстані дозволяється зменшити вдвічі. Якщо ж і силовий, і слабкострумовий кабелі ізольовані один від одного у власних заземлених металевих кабель-каналах, вимоги до просторового рознесення знижуються у чотири рази від початкових. Також під час монтажу слід уникати безпосереднього наближення

кабельних ліній до трубопроводів, радіаторів центрального опалення та інших теплогенеруючих приладів.

Під час маніпуляцій із кабелем необхідно повністю виключити виникнення надлишкових механічних напруг, які з'являються внаслідок осьового скручування, надмірного натягу або занадто гострих кутів вигину. Гранично допустимий радіус вигину суворо регламентований правилами СКС, причому ці показники суттєво відрізняються залежно від призначення кабельного виробу: для магістральної підсистеми, горизонтальної розводки, або ж для гнучких комутаційних і апаратних шнурів (патч-кордів). Головне правило інсталятора говорить: якщо технічні специфікації від безпосереднього заводу-виробника кабелю містять жорсткіші вимоги до радіуса вигину, ніж загальні стандарти, пріоритет завжди віддається строгішим інструкціям виробника. Для запобігання перекручуванню та зламам провідників як під час монтажу, так і в період тривалої експлуатації, кабельні канали обладнуються спеціальними допоміжними аксесуарами та напрямними.

Будь-які тягові зусилля, що діють на кабель під час протягування, не повинні перевищувати паспортну межу сили натягу, інакше виникає ризик порушення внутрішньої геометрії кручених пар та розриву жил. Даний параметр є індивідуальним для кожного типу продукції, проте стандарт висуває фіксовану універсальну вимогу для всіх типів 4-парних кабелів на основі витої пари — максимальне зусилля натягу для них обмежене позначкою в 110 Н.

Невід'ємною вимогою технологічного процесу є формування технологічного запасу кабелю в телекомунікаційних приміщеннях (кросових та серверних). Для апаратних кімнат і магістральних вузлів стандарт рекомендує залишати технологічну петлю завдовжки не менше 3 метрів для кожного кабелю витої пари. Безпосередньо на робочих місцях користувачів, поблизу телекомунікаційних розеток RJ-45, також необхідно передбачити запас близько 30 см. Наявність такого резерву дозволяє проводити подальшу модернізацію чи перестановку обладнання без заміни всієї лінії, а також

суттєво полегшує проведення ремонтних робіт у разі випадкового обриву чи пошкодження розетки.

Під час укладання кабельних запасів перевагу слід віддавати U-подібним петлям або технологічним укладанням у вигляді «цифри 8» із великим радіусом заокруглення. Категорично не рекомендується скручувати виту пару в щільні круглі бухти малого діаметра, оскільки концентрований кабель у такій геометричній формі перетворюється на потужне вогнище взаємних електромагнітних наведень.

Для впорядкування, фіксації та формування кабельних пучків застосовують різноманітні монтажні хомути, бандажі та пластикові або текстильні стяжки. Вони використовуються не лише для утримання ліній усередині лотків, а й для відкритого прокладання пучків по стінах або монтажних стійках.

Нормативи вимагають, щоб після затягування пластикового хомута він зберігав мінімальну рухливість у поздовжньому та поперечному напрямках. Це дозволяє уникнути деформації, перетискання оболонки та внутрішньої структури витих пар.

Хоча при монтажі силових ліній чи традиційної телефонії для відкритої проводки часто застосовують скоби та будівельні степлери, вітчизняні стандарти категорично не рекомендують використовувати такий метод фіксації для телекомунікаційних кабелів комп'ютерних мереж через високий ризик прихованого пошкодження жил. Таким чином, суворе виконання технологічних інструкцій є головним критерієм якості побудови СКС.

У межах розробки нашої конкретної мережі всі кабельні траси будуть інтегровані прихованим способом — вони пройдуть під стелею, у просторі над конструкцією підвісної стелі.

Безпосередні спуски ліній до робочих місць співробітників та інженерного обладнання будуть виконані всередині технологічних пустот гіпсокартонних стін та перегородок.

2.4 Тестування мережі

Протягом кількох років більшість питань підвищення продуктивності та надійність мереж вирішувалося закупівлею нової техніки.

Не завжди подібне рішення було технічно та економічно обґрунтовано, але майже завжди воно дозволяло досягти бажаної мети - мережа починала працювати швидше та краще. За наявності 200% запасу пропускної спроможності практично всі "вузькі місця" можна легко "розширити", а купуючи тільки найдорожче обладнання лідерів мережевих технологій, ви можете з великим ступенем ймовірності убезпечити себе від "прихованих дефектів".

Сьогодні ситуація змінилася, та економічне обґрунтування проектів з модернізації мереж стає актуальним. Світовий досвід показує, що інвестиції у професіоналізм фахівців дають більшу віддачу, ніж інвестиції в "залізо", навіть дуже гарне. Необхідну пропускну здатність мережі чи її надійність не можна оцінити без детального аналізу її поточного стану. Це можна зробити тільки за допомогою діагностичних засобів та методів тестування комп'ютерних мереж.

Діагностичні засоби, призначені для комп'ютерних мереж, можна класифікувати за двом основним ознакам:

– засіб призначений для діагностики мережі або для тестування мережі;

– засіб призначений для реактивної діагностики або попереджувальної діагностики.

Під діагностикою мережі прийнято розуміти вимірювання характеристик роботи мережі у процесі її експлуатації (без зупинення роботи операторів).

Діагностикою мережі є, зокрема, вимір числа помилок передачі даних, ступеня завантаження (утилізації) ресурсів мережі чи часу реакції прикладного ПЗ, яку адміністратор мережі повинен здійснювати щоденно.

Діагностика буває двох типів: попереджувальна (proactive) та реактивна (reactive).

Випереджальна діагностика повинна проводитись у процесі експлуатації мережі щодня, основна ціль попереджувальної діагностики - запобігання збоям у роботи мережі. Реактивна діагностика виконується, коли в мережі вже стався збій і треба швидко локалізувати джерело та виявити причину.

Для того, щоб перевірити відповідність якості кабельної системи вимогам стандартів, визначити максимальну пропускну здатність мережі або оцінити час реакції прикладного програмного забезпечення (ПЗ) при зміни параметрів налаштування комутатора або операційної системи (ОС), то такі виміри можна зробити лише за відсутності в мережі працюючих користувачів. В цьому випадку правильно вживати термін "тестування" мережі.

Таким чином, тестування мережі – це процес активної дії на мережу з метою перевірки її працездатності та визначення потенційних можливостей щодо передачі мережевого трафіку.

Тестування можна умовно поділити на кілька видів в залежності від мети, заради якою воно проводиться. Це:

– тестування кабельної системи мережі на відповідність стандартам TIA/EIA TSB-67;

– стресове тестування конкретних мережевих пристроїв з метою перевірки стійкості їх роботи за різних рівнів навантажень та різних типах мережевого трафіку;

– тестування ПЗ, зокрема визначення його вимог до пропускної спроможності мережевих ресурсів (до характеристик каналу зв'язку, сервера та т. п.);

– стресове тестування мережі (конкретних мережевих конфігурацій) з метою виявлення "прихованих дефектів" в обладнанні та "вузьких місць" в архітектурі мережі, а також з метою визначення порогових значень трафіку, допустимих у даній мережі.

Тестування прикладного програмного забезпечення з метою визначення вимог до пропускної спроможності мережевих ресурсів проводять компанії-розробники ПЗ. Таке тестування здійснюється в рамках комплексної перевірки ПЗ перед випуском його на ринок і називається тестуванням на відповідність якості (Quality Assurance Test, QAT)

Стресове тестування мережевих пристроїв зазвичай проводиться незалежними спеціалізованими лабораторіями. Прикладами таких лабораторій є організації LANQuest та Data Communications. Найчастіше стресове тестування пристроїв проводиться з метою перевірки заявлених технічних характеристик та виявлення різноманітних дефектів.

Кошти, призначені для діагностики мереж, можна умовно розділити на дві категорії залежно від принципу їх роботи: засоби моніторингу та управління роботою мережі (далі засоби моніторингу — monitoring software) та аналізатори мережевих протоколів (далі аналізатори протоколів — analyzers). Принцип роботи засобів моніторингу заснований на взаємодії консолі оператора з так званими агентами, які, власне, займаються моніторингом та управлінням роботою пристроїв мережі.

Прикладами засобів моніторингу є програми Transcend компанії 3Com, Optivity компанії Bay Networks (нині Nortel), HP OpenView Net Metrix. Агенти можуть бути вбудовані в обладнання або завантажені програмним чином. Оскільки найпоширенішим протоколом спілкування консолі оператора та агентів є SNMP, такі агенти часто називають SNMP-агентами. SNMPагенти можуть виконувати різні функції в залежності від типу баз керуючої інформації (Management Information Base, MIB), які вони підтримують. Ці функції можуть включати управління конфігурацією пристрою, в яке агенти вбудовані (configuration management), управління контролем доступу до інформації (security management), аналіз продуктивності пристрою (perfomance management), вимірювання числа помилок при передачі даних (fault management) та інші. При реактивній діагностиці мережі за допомогою засобів моніторингу вимірювальним приладом є SNMP-агент самого пристрою, що

діагностується. Однак у разі збоїв показання SNMP-агента не можна вважати достовірними. Це особливо актуально, коли збої відбуваються у пристрої з встановленим SNMP-агентом. У таких випадках спостерігач повинен бути "незалежним" від діагностованого пристрою. SNMP-агент пристрою спостерігає за колізійним доменом мережі завжди тільки з однієї точки і, що особливо важливо для реактивної діагностики, не має змоги генерувати тестовий трафік. В результаті, якщо не все обладнання має вбудовані агенти, то частина помилок канального рівня в домені мережі може не фіксуватися. З погляду реактивної діагностики, т. е. можливості швидкої локалізації дефектів у мережі, застосування аналізаторів мережевих протоколів виявляється кращим. Вони є значно більш потужний засіб у порівнянні із засобами моніторингу мережі, оскільки позбавлені всіх перерахованих вище недоліків. Саме можливість ефективного проведення реактивної діагностики є сьогодні актуальним завданням для адміністраторів мереж. Принцип роботи аналізатора протоколів відрізняється від принципу роботи засобу моніторингу мережі. Аналізатор мережевих протоколів досліджує весь мережний трафік, що проходить повз нього.

Локальні мережі за своєю природою є широкомовними, тобто кожен кадр від будь-якої станції межах колізійного домену бачать все станції цього домену мережі. Підключаючи аналізатор до будь-якої точки колізійного домену мережі, ви будете бачити весь трафік у цьому домену. Аналізатори протоколів надають можливість збирати дані про роботу протоколів всіх рівнів мережі та, як правило, здатні проводити генерацію тестового трафіку в мережу. Маючи великий буфер для збору пакетів, аналізатори протоколів дозволяють швидко локалізувати причину збою в мережі: наприклад, виявити факт перевантаження конкретного сервера, безслідне зникнення пакетів транспортного рівня на несправних мережних платах, комутаторах та маршрутизаторах, IP-пакети з неправильною контрольною сумою, дублікати IPадрес багато іншого.

Аналізатори протоколів можна розділити на дві категорії: програмні та апаратні (або програмно-апаратні).

Програмний аналізатор – це програма, яка встановлюється на комп'ютер із звичайною мережевою платою. Аналізатор протоколів переводить мережну плату комп'ютера режим прийому всіх пакетів (promiscous mode).

Прикладами програмних аналізаторів протоколів є Observer та Distributed Observer компанії Network Instruments, NetXray компанії Network Associates, LANalyzer for Windows компанії Novell та багато інших. Використання всіляких методів тестування та діагностування комп'ютерних мереж дозволяє своєчасно виявити помилки в роботі мережі, що дозволить значно підвищити ефективність роботи комп'ютерних мереж, а також збільшити експлуатаційний строк.

2.5 Захист комп’ютерної мережі

Концепція та архітектура мережевої безпеки

Безпека мережі — це комплекс взаємопов'язаних організаційних, правових та програмно-апаратних заходів, спрямованих на захист інформаційного середовища від несанкціонованого доступу, випадкового або навмисного втручання в операційну діяльність, а також від спроб руйнування чи модифікації її компонентів. Захисту підлягають усі ключові активи підприємства: фізичне обладнання, системне та прикладне програмне забезпечення, конфіденційні дані та персонал.

Політика мережевої безпеки формується, затверджується та контролюється системним адміністратором або офіцером з кібербезпеки. Її першочергова мета — регулювання прав доступу до внутрішніх ресурсів, моніторинг активності та запобігання атакам типу «відмова в обслуговуванні» (DoS/DDoS).

Для ініціації сесії в державній, корпоративній або приватній мережі користувачу присвоюється індивідуальний ідентифікатор (ID/Username) та пароль, які визначають межі його повноважень згідно з матрицею доступу.

Рівні автентифікації користувачів

Захист будь-якого мережевого ресурсу починається з процедури перевірки справжності суб'єкта — автентифікації. Залежно від цінності інформації та вимог безпеки, застосовують різні класи захисту:

– Однофакторна автентифікація: найпростіший метод, що базується на перевірці лише одного знання (як-от класична пара: логін та пароль).

– Двофакторна автентифікація (2FA): потребує комбінації двох різних типів чинників. Крім знання пароля, користувач повинен володіти фізичним маркером безпеки — апаратним токеном, смарт-карткою, або мати доступ до мобільного телефона для отримання одноразового OTP-коду.

– Трифакторна автентифікація (3FA): до вищеперелічених умов додає унікальні біометричні параметри особи — відбитки пальців, геометрію обличчя (FaceID) або результати сканування сітківки ока.

Ключові функції комплексної системи безпеки

Сучасний кіберзахист підприємства не може будуватися на якомусь одному ізольованому рішенні. Це завжди багаторівнева ешелонована система, яка зберігає загальну працездатність та продовжує захищати корпоративні дані навіть у разі виходу з ладу окремих апаратних вузлів.

Впровадження такої системи забезпечує вирішення чотирьох стратегічних завдань:

– Нівелювання внутрішніх та зовнішніх загроз: Ефективний захист однаково якісно протидіє як зовнішнім хакерським атакам, так і внутрішнім інсайдерським загрозам чи помилкам персоналу. Система безперервно аналізує мережеву активність і миттєво реагує на будь-які аномалії.

– Гарантування конфіденційності під час віддаленої роботи: Завдяки захищеним каналам зв'язку співробітники компанії можуть безпечно під-

ключатися до робочого середовища з дому, відрядження чи будь-якої точки світу через публічну мережу Інтернет без ризику перехоплення даних.

– Диференційований контроль доступу: Адміністратор має можливість гнучко налаштовувати права доступу до файлових серверів та баз даних. Права делегуються на основі ідентифікатора користувача, його посадових обов'язків, часу доби чи навіть типу пристрою, з якого здійснюється вхід.

– Загальна стійкість та проактивність: Технологічні інструменти безпеки оновлюють бази знань у реальному часі, що дозволяє системі успішно блокувати не лише вже відомі типи уразливостей, а й протидіяти новим деструктивним вторгненням.

Базові інструменти та засоби мережевого захисту

Для реалізації безпекової політики в архітектуру локальної обчислювальної мережі інтегрують такі апаратні та програмні інструменти:

– Брандмауери (Міжмережеві екрани / Firewalls): Можуть бути реалізовані як на централізованому рівні (на межі між корпоративною мережею та Інтернетом), так і локально на кожному комп’ютері. Вони здійснюють глибоку фільтрацію вхідних та вихідних пакетів даних, блокуючи несанкціонований і шкідливий трафік згідно з набором встановлених правил.

– Антивірусні комплекси та системи IPS: Програмне забезпечення для моніторингу файлової системи та трафіку. Системи запобігання вторгненням (IPS) аналізують поведінку мережі, виявляють та нейтралізують віруси, мережеві хробаки, трояни та інші шкідливі програми на ранніх стадіях — до моменту завдання реальних збитків інфраструктурі.

– Засоби моніторингу та аналізу стану мережі: Спеціалізований інструментарій (сканери вразливостей, SIEM-системи), який допомагає адміністраторам відстежувати поточний стан ліній зв'язку, виявляти слабкі місця в конфігураціях та оперативно визначати вектори потенційних загроз.

– Захищений віддалений доступ (VPN): Організація безпечного віртуального тунелю між віддаленим клієнтом та ядром мережі. Використання стійких алгоритмів криптографічного шифрування гарантує цілісність та конфіденційність інформації, що передається, незалежно від типу використовуваного пристрою (ноутбук, планшет, смартфон).

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкція з інсталяції програмного забезпечення серверів та активного комутаційного обладнання

Налаштування маршрутизатора MikroTik CRS326-24G-2S+RM

Для того щоб комутатор MikroTik працював згідно з таблицями 2.2 та 2.3, необхідно налаштувати його як пристрій 3-го рівня (L3). Скрипт включає створення VLAN, призначення їх на фізичні порти в режимі Access, налаштування IP-адресації (шлюзів) та базову маршрутизацію.

Оскільки у нас використовуються некеровані комутатори доступу, ми налаштовуємо порти головного MikroTik як Access (мітка VLAN буде додаватися самим MikroTik при вході трафіку на порт).

Створення мосту з підтримкою фільтрації VLAN

/interface bridge add name=bridge1 vlan-filtering=yes

Додавання портів до мосту

Порти 1-5 та 7 (VLAN 20 - Менеджери та Охорона)

/interface bridge port add bridge=bridge1 interface=ether1 pvid=20 add bridge=bridge1 interface=ether2 pvid=20 add bridge=bridge1 interface=ether3 pvid=20 add bridge=bridge1 interface=ether4 pvid=20 add bridge=bridge1 interface=ether5 pvid=20 add bridge=bridge1 interface=ether7 pvid=20

Порт 6 (VLAN 30 - Бухгалтерія/Техвідділ згідно схеми)

add bridge=bridge1 interface=ether6 pvid=30

Порт 8 (VLAN 40 - Wi-Fi Точка доступу)

add bridge=bridge1 interface=ether8 pvid=40

Порт 12 (VLAN 20 або окремий - для Сервера S_1)

add bridge=bridge1 interface=ether12 pvid=20

Порт 10 залишаємо під провайдера (WAN) - не додаємо в міст

Налаштування VLAN в межах мосту

/interface bridge vlan add bridge=bridge1 tagged=bridge1 untagged=ether1,ether2,ether3,ether4,ether5,ether7,ether12 vlan-ids=20 add bridge=bridge1 tagged=bridge1 untagged=ether6 vlan-ids=30 add bridge=bridge1 tagged=bridge1 untagged=ether8 vlan-ids=40

Створення віртуальних інтерфейсів для призначення IP

/interface vlan add interface=bridge1 name=VLAN20_Menej vlan-id=20 add interface=bridge1 name=VLAN30_Buch vlan-id=30 add interface=bridge1 name=VLAN40_WiFi vlan-id=40

/ip address add address=192.168.20.1/24 interface=VLAN20_Menej network=192.168.20.0 add address=192.168.30.1/24 interface=VLAN30_Buch network=192.168.30.0 add address=192.168.40.1/24 interface=VLAN40_WiFi network=192.168.40.0

Налаштування порту провайдера (WAN) - приклад отримання IP автоматично

/ip dhcp-client add interface=ether10 disabled=no

Пули адрес

/ip pool add name=pool_VLAN20 ranges=192.168.20.10-192.168.20.250 add name=pool_VLAN30 ranges=192.168.30.10-192.168.30.250 add name=pool_VLAN40 ranges=192.168.40.10-192.168.40.250

Конфігурація серверів

/ip dhcp-server add address-pool=pool_VLAN20 interface=VLAN20_Menej name=server_v20 add address-pool=pool_VLAN30 interface=VLAN30_Buch name=server_v30 add address-pool=pool_VLAN40 interface=VLAN40_WiFi name=server_v40

/ip dhcp-server network add address=192.168.20.0/24 dns-server=8.8.8.8,1.1.1.1 gateway=192.168.20.1 add address=192.168.30.0/24 dns-server=8.8.8.8,1.1.1.1 gateway=192.168.30.1 add address=192.168.40.0/24 dns-server=8.8.8.8,1.1.1.1 gateway=192.168.40.1

/ip firewall nat add action=masquerade chain=srcnat out-interface=ether10

Базова ізоляція (заборона доступу з Wi-Fi до Бухгалтерії)

/ip firewall filter add action=drop chain=forward in-interface=VLAN40_WiFi out-interface=VLAN30_Buch

/interface bridge settings set allow-fast-path=yes

Перевірка та активація L3 HW Offloading (для версій RouterOS 7.x)

/interface bridge port set [find] hw=yes

3.2 Налаштування точки доступу

Для того щоб централізовано керувати точкою доступу з головного комутатора, ми використаємо технологію CAPsMAN.

Використання CAPsMAN — це великий плюс до лнгкості керування. Для додавання нової точки доступу не потрібно її налаштовувати вручну — достатньо просто підключити її до мережі зі скриптом CAP.

Нижче наведено два окремі скрипти: перший для CRS326 (контролер), другий для cAP ac (керований пристрій).

1. Скрипт для головного комутатора (CAPsMAN Controller)

Цей скрипт створює «мізки» бездротової мережі на комутаторі. Ми налаштовуємо дві мережі: основну (для персоналу) та окрему (для гостей/ конференц-залу) з прив'язкою до VLAN 40

1. Активація пакету CAPsMAN (у ROS v7 він вбудований у пакет wireless або wifi-qcom)

/caps-man manager set enabled=yes

2. Налаштування безпеки (пароль для Wi-Fi)

/caps-man security add authentication-types=wpa2-psk encryption=aes-ccm name=sec_corporate passphrase="ВашПарольТут"

3. Конфігурація каналів (Auto)

/caps-man configuration add country=ukraine datapath.bridge=bridge1 datapath.vlan-id=40 datapath.vlan-mode=use-tag mode=ap name=cfg_wifi_v40 security=sec_corporate ssid="Enterprise_WiFi"

4. Створення розкладу (Provisioning) - як автоматично налаштовувати точки, що підключаються

/caps-man provisioning add action=create-dynamic-enabled master-configuration=cfg_wifi_v40

2. Скрипт для точки доступу MikroTik cAP ac (CAP)

Цей скрипт повністю очищує точку доступу та переводить її в режим «керованого пристрою». Вона знайде комутатор і отримає всі налаштування автоматично.

Важливо: Перед запуском підключіться до точки доступу через Winbox (порт ether1).

1. Скидання конфігурації до абсолютно чистої (виконувати в терміналі)

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

Після перезавантаження.

2. Створення мосту для портів

/interface bridge add name=bridgeCAP

3. Додавання фізичних інтерфейсів до мосту

/interface bridge port add bridge=bridgeCAP interface=ether1 add bridge=bridgeCAP interface=ether2

4. Налаштування клієнта для отримання IP адреси (щоб точка бачила контролер)

/ip dhcp-client add interface=bridgeCAP disabled=no

5. Переведення радіоінтерфейсів у режим керування CAPsMAN

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

3.2 Початкове налаштування сервера Ubuntu 20.04

Після встановлення операційної системи необхідно виконати ряд важливих кроків у конфігурації в рамках базових налаштувань. Ці кроки

допомагають підвищити рівень безпеки та полегшити роботу з сервером і послужити надійною основою для наступних дій.

Крок 1 — Вхід з привілегіями root

Щоб увійти на сервер, вам потрібно знати публічну IP-адресу вашого сервера . Також вам потрібен пароль або, якщо ви встановили ключ SSH для аутентифікації, приватний ключ для облікового запису користувача root .

Якщо ви ще не підключилися до сервера, зробіть вхід в систему як користувач root , використовуючи наступну команду:

ssh root@your_server_ip

Зверніть увагу на автентичність хоста, якщо він з'явиться на екрані. Якщо ви використовуєте аутентифікацію за паролем, введіть пароль root для входу в систему. Якщо ви використовуєте ключ SSH із захистом за фразою-паролем, вам може бути запропоновано ввести фразу-пароль у перший раз під час використання ключа в кожному сеансі. Якщо ви перший раз виконуєте вхід на сервер за допомогою пароля, вам також можна запропонувати змінити пароль root .

Детальніше про root

root user — це користувач із правами адміністратора в середовищі Linux, який має дуже широкий набір привілеїв. Із-за такого широкого набору привілеїв облікового запису root *не рекомендується* використовувати її на регулярній основі. Це пов'язано з тим, що частина можливостей, отриманих за допомогою root , включає можливість внесення дуже руйнівних змін, навіть якщо це відбувається непередбачено.

У наступному кроці буде створено новий обліковий запис користувача з обмеженими привілеями для щоденного використання.

Крок 2 — Створення нового користувача.

Після входу в систему з правами root ми готові додати новий обліковий запис користувача. У майбутньому ми виконаємо вхід за допомогою цього нового облікового запису, а не з правами root .

adduser admin

Вам буде запропоновано відповісти на кілька питань, починаючи з пароля облікового запису.

Введіть надійний пароль і введіть за бажанням будь-яку додаткову інформацію. Це робити необов'язково, і можна натиснути ENTER в будь-якому полі, яке ви хочете пропустити.

Крок 3 — Надання адміністративних прав

Тепер у нас є новий обліковий запис користувача зі стандартними правами. Однак іноді може знадобитися виконання адміністративних завдань.

Щоб не здійснювати вихід із стандартного облікового запису та виконати вхід до системи з облікового запису root , ми налаштуємо так званого *суперкористувача* або додамо привілегії root для стандартного облікового запису. Це дозволить нашому звичайному користувачеві запускати команди з правами адміністратора, вказавши слово sudo перед кожною командою.

Щоб додати ці права для нового користувача, нам потрібно додати користувача в групу sudo . За замовчуванням в Ubuntu 20.04 користувачі, що входять до групи sudo , можуть використовувати команду sudo.

Використовуючи права root , запустіть цю команду, щоб додати нового користувача в групу sudo:

usermod -aG sudo admin

Тепер, коли ви ввійдете в систему зі стандартним користувачем, ви можете ввійти sudo перед командами для виконання дій з правами суперкористувача.

Крок 4 — Налаштування базового брандмауера

Сервери Ubuntu 20.04 можуть використовувати Brandmauer UFW для перевірки, щоб надати дозволи лише до певних служб. Ми можемо легко створити базовий брандмауер за допомогою додатків.

Рекомендовано використовувати тільки один брандмауер в один момент часу, щоб уникнути конфліктів, які можуть затруднити проведення відладки.

Додатки можуть зареєструвати свої профілі в UFW після встановлення. Ці профілі дозволяють UFW керувати цими додатками по імені. OpenSSH, служба, що дозволяє підключитися до нашого сервера зараз, має профіль, зареєстрований в UFW.

Щоб побачити це, можна ввести наступну команду:

ufw app list

Нам потрібно переконатися в тому, що брандмауер дозволяє підключення SSH, щоб ми могли зайти на сервер в наступний раз. Щоб відключити ці підключення, можна ввести наступне:

ufw allow OpenSSH

Після цього ми можемо активувати брандмауер за допомогою наступної команди:

ufw enable

Введіть YES, натисніть ENTER, щоб продовжити. Щоб побачити, що підключення SSH дозволено, введіть наступне:

ufw status

Оскільки брандмауер в даний час блокує всі підключення, крім SSH , якщо ви встановите і налаштуєте додаткові служби, потрібно змінити налаштування брандмауера, щоб дозволити вхідний трафік.

Крок 5 — Активація зовнішнього доступу для стандартного користувача.

Тепер, коли у нас є стандартний обліковий запис для щоденного використання, необхідно переконатися, що ми можемо ввести SSH безпосередньо в обліковий запис.

Процес налаштувань доступу SSH для нового користувача залежить від того, чи використовує обліковий запис із правами root пароль входу на сервер чи ключі SSH для автентифікації.

Якщо root використовує аутентифікацію за паролем:

Якщо ви заповнили вхід в обліковий запис root *за допомогою пароля* , тоді для SSH активована *аутентифікація* за паролем. Ви можете використовувати SSH для нового користувача, запустивши новий сеанс-термінал і використовуючи SSH з новим іменем:

ssh admin@your_server_ip

Після введення пароля для звичайного користувача можна виконати вхід. Якщо вам потрібно запустити команду з правами адміністратора, введіть sudo перед командою таким чином:

sudo command_to_run

Вам буде запропоновано використовувати пароль звичайного користувача під час використання sudo в перший раз для кожного сеансу (і періодично після цього).

Щоб підвищити рівень безпеки вашого сервера, ми обов’язково рекомендуємо встановити ключі SSH замість використання аутентифікації за паролем.

Якщо root використовує аутентифікацію за ключем SSH:

Якщо ви заповнили вхід в обліковий запис root *за допомогою ключів SSH* , тоді аутентифікація за паролем для SSH *відключена* . Вам потрібно додати копію локального відкритого ключа у файл ~/.ssh/authorized_keys нового користувача для успішного входу.

Якщо ваш відкритий ключ уже включено в кореневий ~/.ssh/authorized_keys файл на сервері, ми можемо скопіювати структуру цього файлу та каталоги для нашого нового користувача в існуючому сеансі.

Самий простий спосіб копіювання файлів з правами володіння та дозволами — скористатися командою rsync. Вона копіюватиме директорію .sshкористувача root , збереже дозволи та змінить файли власників, усе в одній команді. Обов'язково змініть виділені нижче частини відповідно до імені вашого стандартного користувача:

rsync --archive --chown=admin:admin ~/.ssh /home/admin

Тепер відкрийте новий сеанс-термінал на локальному комп’ютері та використовуйте SSH з новим іменем користувача:

ssh admin@your_server_ip

Ви повинні зайти в обліковий запис без використання пароля. Якщо вам потрібно запустити команду з правами адміністратора, введіть sudo перед командою таким чином:

sudo command_to_run

Тепер у вас є основа для вашого сервера. Ви можете перейти до установки програмного забезпечення, яка потрібна на вашому сервері.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки комп'ютерної мережі для компанії "ОптімаНет Сервіс" і прийняття рішення про її подальше впровадження в роботу.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

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

Таблиця 4.1 - Середній час виконання НДР та стадій технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	2	3	4
1	Розробка логічної та фізичної топологій мережі. Аналіз плану приміщення будівлі	Керівник проекту	14
2	Монтаж кабельних каналів	Технік	30
3	Монтаж активного та пасивного мережевого обладнання	Технік	10
4	Тестування мережі. Моніторинг основних параметрів (кільк. переданих та прийнятих пакетів та їх тип).	Інженер	18

Продовження таблиці 4.1

1	2	3	4
5	Налагодження мережі та створення технічної документації	Інженер	10
Разом		-	82

Сумарний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі складає 82 годин.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

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

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

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

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

Основна заробітна плата розраховується за формулою:

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

де Тс – тарифна ставка, грн.;

Кг – кількість відпрацьованих годин.

Отже, основна заробітна плата для:

- керівника проекту: Зосн1 = 14· 150 = 2100,00 грн.
- інженера: Зосн2 = 28 · 140 = 5600,00 грн.
- техніка: Зосн3 = 40 · 120 = 3360,00 грн.

Сумарна основна заробітна плата становить:

Зосн = 2100,00 + 5600,00 + 3360,00 = 11060,00 грн

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

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

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

Отже, додаткова заробітна плата по категоріях працівників становить:

1. керівника проекту: Здод1= 2100,00 · 0,15 = 315,00 грн.
2. інженера: Здод2= 5600,00 · 0,15 = 840,00 грн.
3. техніка: Здод3= 3360,00 · 0,15 = 504,00 грн.

Загальна додаткова заробітна плата становить:

Здод = 315,00 + 840,00 + 504,00 = 1659,00 грн.

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

$$Во.п.=Зосн.+Здод\ , \qquad (4.3)$$

Во.п = 11060,00 + 1659,00= 12719,00 грн

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

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

де ФОП – фонд оплати праці, грн.

$$В_{с.з.} = 12719,00 \cdot 0,22 = 2798,18 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія праці-вни-ків	Основна заробітна плата, грн.			Додатк. зароб. плата, грн.	Нарах ув. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Та-риф. Ставка, грн.	К-сть відпр. год.	Факт. нарах. з/пл., грн.			
1	Керівник проекту	150	14	2100,00	315,00	-	-
2	Інженер	140	28	600,00	840,00		
3	Технік	120	40	3360,00	504,00	-	-
Разом				11060,00	1659,00	2798,18	15517,18

Отже, загальні витрати на оплату праці становлять 15517,18 грн.

4.3 Розрахунок матеріальних витрат

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

$$МВі = qi \cdot pi \quad (4.5)$$

де qi – кількість витраченого матеріалу і-го виду;

pi – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$Зм.в. = \sum МВі \quad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. вим.	Факт. витрачено матеріалів	Ціна 1-ці, грн.	Загальна сума витрат, грн.
1	комутатор Cisco CBS110-16T-EU	шт	6	8600	51600
2	комутатор MikroTik CRS326-24G-2S+RM	шт	1	8000	8000
3	точка доступу MikroTik cAP ac (RBcAPGi-5acD2nD)	шт	1	3600	3600
4	Сервер ARTLINE Business T17v23 MikroTik	шт	1	58000	58000 грн.
5	Комутаційна шафа	шт	1	16860	16860
6	Кабель мережевий	шт	4	3400	13600
7	Короб 20х40х2000	шт	45	69	3105
11	конектор	шт	50	2,6	130
Разом					154895

Отже, загальна сума матеріальних витрат дорівнюють Зм.в = 154895,00 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$Зе=W \cdot T \cdot S, \quad (4.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 14 годин, споживана потужність - 0,5 кВт/год, вартість електроенергії 15,94 грн.

Тому:

$Зе = 0,5 \cdot 14 \cdot 15,94 = 111,58$ грн.

4.5 Визначення транспортних затрат

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

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

де Тв – транспортні витрати.

Отже,

$Тв = 154895,00 \cdot 0,08 = 12391,60$ грн.

4.6 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі ви-

робництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

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

Комп'ютери та оргтехніка належать до четвертої групи основних фондів.

Мінімально допустимі строки їх використання 2 роки.

Для визначення амортизаційних відрахувань застосовуємо формулу:

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

де А – амортизаційні відрахування за звітний період, грн.

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

НА – норма амортизації, %;

Т – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 14 год., балансова вартість ПК – 24000,00 грн., тому:

А = 24000,00 · 0,04 /150 · 14 = 89,60 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.

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

де Нв – накладні витрати.

Нв = 17501,34 · 0,5 = 8750,67 грн.

4.8 Складання кошторису витрат та визначення собівартості НДР.

Результати проведених вище розрахунків зведемо у таблиці 4.4.

Таблиця 4.4 – Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці	12719,00	8,82
Відрахування на соціальні заходи	2798,18	2,41
Матеріальні витрати	154895,00	78,02
Витрати на електроенергію	111,58	0,06
Транспортні витрати	12391,6	6,24
Амортизаційні відрахування	89,6	0,05
Накладні витрати	8750,672	4,41
Собівартість	191755,64	100

Собівартість (Св) НДР розрахуємо за формулою:

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

Отже, собівартість дорівнює

Св =91755,64 грн

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

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

де Св – собівартість виконання НДР;

Ррен. – рівень рентабельності,

ПДВ – ставка податку на додану вартість,

Ц = 191755,64· (1+0,3) · (1+0,2) = 299138,80 грн.

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

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

Для визначення ефективності продукту розраховують чисту теперішню вартість (ЧТВ) і термін окупності ($T_{ОК}$).

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

де K_B – затрати на проект;

$Г_n$ – грошовий потік за t–ий рік;

t – відповідний рік проекту;

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

$$ЧТВ = -191755,64 + 183213,16/(1+0,15) + 183213,16/(1+0,15)^2 =$$

$$= 106095,63 \text{ (грн.)}$$

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

Термін окупності визначається за формулою:

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

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

$H_{В}$ – невідшкодовані витрати на початок року, грн.;

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

$$T_{ОК}=1+32439,9/183213,16=1,2$$

Таблиця 4.5 - Економічні показники НДР

№ п/п	Показник	Значення
1.	Собівартість, грн.	191755,64
2.	Плановий прибуток, грн.	107383,16
3.	Ціна, грн.	299138,8
4.	Чиста теперішня вартість, грн	106095,65
5.	Термін окупності, рік	1,2

Загальна вартість розробленої комп'ютерної мережі становить 299138,8 грн. Термін окупності становить 1,2 роки.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

5.1 Розміщення та використання первинних засобів гасіння осередків пожежі на об'єктах компанії “ОптімаНет Сервіс”

Пункт написано за матеріалами: https://ors.nuczu.edu.ua/ images/PPPR/ 15.pdf

Первинний засіб пожежогасіння - технічний засіб, речовина, матеріал або їх комплекс, придатний до використовування людиною для локалізування і (або) ліквідування пожежі на її початковій стадії

До первинних засобів пожежогасіння належать вогнегасники, пожежні кран-комплекти, пожежний інвентар (покривала з негорючого теплоізолювального полотна або повсті, ящики з піском, бочки з водою, пожежні відра, совкові лопати) та переносний пожежний інструмент.

Пожежу в час її виникнення можливо погасити первинними засобами пожежогасіння, до яких відносяться вогнегасники, відра, багри, діжка з водою, ящики з піском, кошма (покривало з негорючого теплоізоляційного полотна, грубововняної тканини або повсті), ломи, лопати, сокири і т. ін.

Покривало (кошма) призначене для гасіння пожеж на початковому етапі, коли пожежа ще не набула великих розмірів та інтенсивність теплового випромінювання невелика. Гасіння пожежі відбувається шляхом накривання осередку пожежі. Працює принцип припинення горіння – ізоляція реагуючих речовин від зони горіння.

Кошма має один або декілька шарів однотипного матеріалу. Не повинна мати швів та зістрочуватись з окремих кусків. Виключення складають торцева обробка матеріалу та кріплення пристроїв для утримання руками.

Кошма повинна мати розмір не менш як 1×1 м. У місцях застосування та зберігання ЛЗР та ГР розміри покривал можуть бути збільшені до величин: 2×1,5 м, 2×2 м.

Покривало слід застосовувати для гасіння пожеж класів "A", "B", "D", (E).

Під час експлуатації покривала передбачається скручування його в рулон.

Під час гасіння пожежі можна виконувати наступні види робіт:

– гасіння осередку пожежі в початковій стадії розвитку пожежі;

– гасіння одежі, яка горить на потерпілому.

Гасіння пожеж невеликої площі повинно проводитись шляхом накривання полотнищем поверхні горючого матеріалу (рідини), ізолюючи її від доступу повітря.

При гасінні розливів легкозаймистих рідин (далі ЛЗР) або горючих рідин (далі ГР) повинно проводитись двома особами. Кошму заводять з навітряного боку. Накривання повинно проводитись одночасно. Необхідно вжити заходи щодо недопущення потрапляння повітря під кошму. Для цього ущільнюють прилягання кошми до ґрунту. За необхідності можна здійснювати прибивання кошми від краю до її середини. Покривало утримується не менш 20 секунд.

Бочки з водою встановлюються у виробничих, складських та інших приміщеннях, спорудах у разі відсутності внутрішнього протипожежного водогону та за наявності горючих матеріалів, а також на території об'єктів, у садибах індивідуальних жилих будинків, дачних будиночків тощо. Їх кількість у приміщеннях визначається з розрахунку установки однієї бочки на 250-300 м захищуваної площі.

Бочки для зберігання води з метою пожежогасіння відповідно повинні мати місткість не менше 0,2 $м^3$ і бути укомплектовані пожежним відром місткістю не менше 0.008 $м^3$.

Пожежні щити (стенди) (показані на рисуку 5.1 та рисунку 5.2) встановлюються на території об'єкта з розрахунку один щит (стенд) на площу 5000 $м^2$.

До комплекту засобів пожежогасіння, які розміщаються на ньому, слід включати: вогнегасники - 3 шт., ящик з піском - 1 шт., покривало з негорючого теплоізоляційного матеріалу або повсті розміром 2×2м - 1 шт., гаки - 3 шт., лопати - 2 шт., ломи - 2 шт., сокири - 2 шт.

Ящики для піску (див рис 5.3) повинні мати місткість 0,5; 1,0 або 3,0 м^3 та бути укомплектованими совковою лопатою.

Рисунок 5.1 – Пожежний щит відкритого типу з ящиком для піску

Вмістилища для піску, що є елементом конструкції пожежного стенду, повинні бути місткістю не менше 0.1 м^3. Конструкція ящика (вмістилища) повинна забезпечувати зручність діставання піску та виключати попадання опадів.

Рисунок 5.2 – Пожежний шит закритого типу

Керівним документом, який визначає порядок комплектування пожежних щитів первинними засобами пожежогасіння, є Правила пожежної безпеки в Україні, де в додатку № 3 викладено рекомендації щодо оснащення об'єктів первинними засобами пожежогасіння.

Рисунок 5.3 – Пожежний стенди стаціонарний з ящиком для піску закритого типу

Керівними документами, які визначають види та типи вогнегасників та порядок оснащення об'єктів, є:

– Типові норми належності вогнегасників, затверджені наказом МНС України від 2.04.2004 року № 151;

– Правила експлуатації вогнегасників, затверджені наказом МНС України від 2.04.2004 року № 152.

5.2 Організація вентиляції для дотримання норм виробничої санітарії та видалення надлишків тепла від обладнання

Для створення нормальних умов виробничої діяльності необхідно забезпечити не лише комфортні метеорологічні умови, а й необхідну чистоту повітря. Адже внаслідок виробничої діяльності у повітряне середовище приміщень можуть надходити різноманітні шкідливі речовини, що використовуються в технологічних процесах. Одним з ефективних засобів нормалізації повітря у приміщенні є вентиляція.

Вентиляція — повітрообмін, завдяки якому забруднене повітря виводиться з приміщення, а замість нього вводиться свіже зовнішнє або очищене повітря.

Під вентиляцією виробничих приміщень розуміють сукупність заходів та засобів, призначених для забезпечення на постійних робочих місцях та зонах обслуговування виробничих приміщень метеорологічних умов та чистоти повітряного середовища, що відповідають гігієнічним та технічним вимогам. Основне завдання вентиляції — створити оптимальний мікроклімат у приміщенні по температурі, швидкості руху повітря, його вологості, хімічній і мікробній чистоті, запиленості, що сприяє збереженню і зміцненню здоров’я і підвищенню працездатності людини. Гігієнічні вимоги до вентиляції зводяться до її достатності для конкретного приміщення, постійності протягом доби і рівномірності для всього приміщення.

Вентиляція класифікується за такими ознаками:

– за способом переміщення повітря (природна (організована та неорганізована), штучна (механічна) і суміщена (природна та штучна одночасно));

– за напрямком потоку повітря (припливна, витяжна, припливно-витяжна);

– за місцем дії (загальнообмінна, місцева, комбінована);

– за призначенням (робоча, аварійна).

Організована природна вентиляція називається аерацією. Для аерації в стінах будівлі роблять отвори для надходження зовнішнього повітря, а на даху чи у верхній частині будівлі встановлюють спеціальні пристрої (ліхтарі) для видалення відпрацьованого повітря.

Неорганізована природна вентиляція включає інфільтрацію — просочування повітря через нещільності у вікнах, дверях, перекриттях тощо та провітрювання, що здійснюється при відкриванні вікон та кватирок.

Припливна вентиляція передбачає подачу чистого повітря ззовні у приміщення. При витяжній вентиляції повітря вилучається з приміщення, а зовнішнє надходить через вікна, двері, нещільності будівельних конструкцій. Припливно-витяжна вентиляція поєднує першу і другу.

Загальнообмінна вентиляція підтримує нормальне повітряне середовище у всьому об’ємі робочої зони виробничого приміщення (цеху). За допомогою місцевої вентиляції шкідливі виділення вилучаються або розчиняються шляхом надходження чистого повітря безпосередньо у місцях їх утворення. Комбінована вентиляція поєднує загальнообмінну і місцеву.

Аварійну вентиляцію влаштовують у тих виробничих приміщеннях, в яких можуть статися аварії з виділенням значної кількості шкідливостей, а також коли при виході з ладу робочої вентиляції в повітрі можуть утворюватись небезпечні для життя працівників або вибухонебезпечні концентрації шкідливих речовин. Основним завданням розрахунку

вентиляційних систем є визначення кількості повітря ($м^3$/годину), необхідного для його надходження або вилучення з приміщення. Повітрообмін визначають розрахунковим шляхом за конкретними даними про кількість шкідливих виділень (теплоти, вологи, пари, газу, пилу).

Системи вентиляції мають бути пожежо- й вибухобезпечними, простими в облаштуванні, не переохолоджувати приміщення, не створювати надмірного шуму, бути надійними в експлуатації, економними. Крім паспорта на кожну вентиляційну установку складають журнал експлуатації, з внесенням технічних характеристик вентустановки. Усі вентиляційні пристрої (установки) підлягають планово-попереджувальному огляду і ремонту, а також періодичному технічному випробуванню відповідно до затверджених графіків.

Розрахунки повітрообміну для проектування вентиляційних систем та систематичний контроль за ефективною роботою вентустановок (підчас їх експлуатації) мають на меті забезпечення належного санітарно-гігієнічного стану у робочій зоні виробничого приміщення та попередження виникнення професійних захворювань серед працівників.

Джерело: редакція журналу «Охорона праці і пожежна безпека» за матеріалами Управління Держпраці у Миколаївській області

5.3 Класифікація приміщень компанії за ступенем небезпеки ураження електричним струмом та вибір відповідних захисних заходів

Відповідно до ПУЕ, приміщення за небезпекою електротравм поділяються на три категорії:

- без підвищеної небезпеки;
- з підвищеною небезпекою;
- особливо небезпечні.

Категорія приміщення визначається наявністю в приміщенні чинників підвищеної або особливої небезпеки електротравм. До чинників підвищеної небезпеки належать:

– температура в приміщенні, що впродовж доби перевищує 35°С;

– відносна вологість більше 75%, але менше повного насичення (100%);

– струмопровідна підлога – металева, бетонна, цегляна, земляна тощо;

– струмопровідний пил;

– можливість одночасного доторкання людини до неструмовідних частин електроустановки і до металоконструкцій, що мають контакт із землею.

До чинників особливої небезпеки електротравм належать:

– відносна вологість близька до насичення (до 100%);

– агресивне середовище, що пошкоджує ізоляцію.

Якщо в приміщенні відсутні чинники підвищеної і особливої небезпеки, то воно належить до приміщень без підвищеної небезпеки електротравм.

За наявності одного з чинників підвищеної небезпеки, приміщення належить до приміщень підвищеної небезпеки електротравм.

За наявності одночасно двох чинників підвищеної небезпеки або одного чинника особливої небезпеки, приміщення вважається особливо небезпечним.

Із наведеного видно, що класифікація приміщень за небезпекою електротравм враховує тільки особливості цих приміщень, стан їхнього середовища і не враховує електротехнічних параметрів електроустановок.

Категорія приміщень є одним з основних чинників, які визначають вимоги щодо виконання електроустановок, безпечної їх експлуатації, величини напруги, заземлення (занулення) електроустановок. Умови поза приміщеннями прирівнюються до особливо небезпечних.

Електротравми можуть бути наслідком технічних, організаційно-технічних, організаційних і організаційно-соціальних причин.

До технічних причин належать: недосконаліть конструкції електроустановки і засобів захисту, допущені недоліки при виготовленні, монтажі і ремонті електроустановки. Крім перерахованих, технічними причинами електротравм можуть бути несправності електроустановок, що виникають в процесі їх експлуатації, несправність захисних засобів, невідповідність будови електроустановок і захисних засобів умовам їх застосування, використання електрозахисних засобів із простроченою датою чергових випробувань.

До організаційно-технічних причин належать: невиконання вимог чинних нормативів щодо контролю параметрів та опосвідчення технічного стану електроустановок; помилки в знятті напруги з електроустановок при виконанні в них робіт без перевірки відсутності напруги на електроустановці, на якій працюють люди; відсутність огороджень або невідповідність конструкції і розміщення вимогам чинних нормативів та відсутність необхідних плакатів і попереджувальних та заборонних написів; помилки в установленні і знятті переносних заземлень, або їх відсутність.

До основних організаційних причин електротравм належать:

– відсутність (непризначення наказом) на підприємстві особи, відповідальної за електрогосподарство або невідповідність кваліфікації цієї особи чинним вимогам;

– недостатня укомплектованість електротехнічної служби працівниками відповідної кваліфікації;

– відсутність на підприємстві посадових інструкцій для електротехнічного персоналу та інструкцій із безпечного обслуговування та експлуатації електроустановок;

– недостатня підготовленість персоналу з питань електробезпеки, несвоєчасна перевірка знань, невідповідність групи з електробезпеки персоналу характеру робіт, що виконуються;

– недотримання вимог щодо безпечного виконання робіт в електроустановках за нарядами-допусками, розпорядженнями та в порядку поточної експлуатації;

– неефективний нагляд, відомчий і громадський контроль за дотриманням вимог безпеки при виконанні робіт в електроустановках та їх експлуатації.

До основних організаційно-соціальних причин електротравм належать: змушене виконання не за спеціальністю електронебезпечних робіт; негативне ставлення до виконуваної роботи, обумовлене соціальними чинниками; залучення працівників до понадурочних робіт; порушення виробничої дисципліни; залучення до роботи осіб віком до 18 років.

Безпосередніми причинами потрапляння людей під напругу є:

– дотик до неізольованих струмовідних частин електроустановок, які знаходяться під напругою, або до ізольованих за фактично пошкодженої ізоляції – 55%;

– дотик до неструмовідних частин електроустановок або до електрично зв’язаних з ними металоконструкцій, які опинилися під напругою в результаті пошкодження ізоляції – 23%;

– дія напруги кроку – 2,5%;

– ураження за виникнення електричної дуги – 1,2%;

– інші причини – менше 20%.

Виконання, розміщення, вибір, спосіб установки і клас ізоляції застосовуваних машин, апаратів та іншого електроустаткування проводять відповідно до вимог державних стандартів і правил експлуатації електроустановок відповідно до НПАОП 40.1-1.21-98 “Правила безпечної

експлуатації електроустановок споживачів”. Розглянемо загальні заходи захисту від дії електричного струму.

Застосування ізоляції. Ізоляція струмопровідних частин електроустановок, а в особливих випадках подвійна чи посилена, перешкоджає появі струму на металевих неструмопровідних частинах електроустаткування, протіканню на землю, а також забезпечує захист людини від впливу електричного струму під час випадкового дотику її до струмоведучих частин. Розрізняють наступні види ізоляції.

Робоча ізоляція – електрична ізоляція струмопровідних частин електроустановки, що забезпечує її нормальну роботу і захист від ураження електричним струмом.

Допоміжна ізоляція – ізоляція, передбачена як допоміжна до робочої ізоляції для захисту від ураження електричним струмом у випадку ушкодження робочої ізоляції.

Подвійна ізоляція – ізоляція, що складається з робочої і допоміжної ізоляції.

Посилена ізоляція – поліпшена робоча ізоляція, що забезпечує такий же ступінь захисту від ураження електричним струмом, як і подвійна ізоляція.

Від стану ізоляції, який згодом погіршується, залежить безпека експлуатації електроустановок і систем електропостачання. Стан ізоляції зменшується, знижується еластичність, тому з’являються тріщини, розриви та інш.

Причини погіршення ізоляції електроустановок і мереж:

– вплив низьких і, навпаки, високих температур повітря й устаткування;

– нагрів ізоляції від струмів, що протікають головним чином під час перевантаження і короткого замикання;

– механічні впливи ударного, вібраційного і розривного характеру;

– вплив хімічно активних речовин, підвищеної і зниженої вологості повітря.

Підтримання ізоляції електроустановок в належному стані, її опір вимірюють або періодично, або безперервно. Приймально-здавальні випробування ізоляції проводяться при уведенні в експлуатацію нових і відремонтованих електроустановок.

Контроль ізоляції періодичний проводять, зазвичай, на вимкненій електроустановці за допомогою мегометра, який дозволяє визначати опір ізоляції електроустановок під номінальною чи близькою до неї напругою, на відміну від виміру опору ізоляції за допомогою омметра, де напруга, під якою проводиться вимір опору ізоляції, складає одиниці вольт. У мегометра джерелом струму є індуктор, що обертається рукою.

Більш надійна подвійна ізоляція застосовується в електроустановках і електроприймачах, де тільки одна робоча ізоляція не може забезпечити безпеку людей від впливу електричного струму. Наприклад, у ручних електричних машинах ізоляція інтенсивно зношується через великі перевантаження, перегрів, удари, вібрації і забруднення. Тому в машинах I класу всі деталі, що знаходяться під напругою, мають робочу ізоляцію, а окремі деталі подвійну і посилену ізоляцію. У той же час ці машини повинні заземлюватися, а штепсельна вилка повинна мати контакт, що заземлює. У машинах II класу всі деталі, що знаходяться під напругою, мають подвійну чи посилену ізоляцію. У них немає пристрою для заземлення, тому що подвійна ізоляція забезпечує безпеку їх експлуатації. Машини II класу використовуються в побуті. Машини I класу в продаж не допускаються як такі, що потребують заземлення, без якого їхнє застосування небезпечне.

Розміщення струмопровідних частин на недоступній для дотику висоті. Електропроводку усередині приміщень з незахищеними ізольованими проводами прокладають на ізоляторах і роликах на висоті не менше 2 м від підлоги при напрузі вище 42 В. у приміщеннях без підвищеної небезпеки На

висоті не менше 2,5 м від рівня підлоги в приміщеннях з підвищеною небезпекою й особливо небезпечних при напрузі вище 42 В.

Відстань до вимикачів, розеток, щитків, світильників на стінах захищають від механічних впливів до висоти не менше 1,5 м від підлоги.

Внутрішні електропроводки усередині приміщень прокладають у трубах, коробах і гнучких металевих рукавах.

Захисні огородження і закриття струмопровідних частин

Захисні огородження і закриття струмопровідних частин у виробничих приміщеннях і електроприміщеннях виготовляють сітчастими чи дірчастими. У житлових і громадських будівлях, захисні огородження конструктивно виконують так, що зняти їх або відкрити можна лише за допомогою ключів чи інструментів.

Блокування. Електричні й механічні блокувальні пристрої застосовують в електроустановках, де небезпека дотику до струмоведучих частин велика. Також можливе проникнення сторонніх осіб на електроустановку, що знаходиться під високою напругою.

При електричному блокуванні ланцюг живлення високої напруги розривається, і електроустановка вимикається, коли відчиняються, наприклад, двері, або знімається захисний кожух чи відкривається панель випробувального стенда, на якому встановлюють нормально замкнуті електричні контакти при зачинених дверях і встановлених кожухах. Якщо електроустановка включається в мережу за допомогою магнітного пускача чи контактора, то доцільно ланцюг живлення обмотки керування магнітного пускача чи контактора підводити через блокувальні контакти.

Механічне блокування не дозволяє відкрити двері електроустановки, не вимкнувши рубильник чи пускач. При вимиканні рубильника механічне блокування замикального пристрою знімається.

Захисне вимкнення – швидкодіючий захист, що забезпечує автоматичне вимкнення електроустановки при виникненні в ній струму. Така небезпека виникає при:

– повному чи неповному замиканні фази на корпус електроустановки;

– випадковому дотику людини безпосередньо до струмопровідної частини;

– зниженні опору ізоляції мережі;

– несправності захисного заземлення чи занулення.

Пристрій захисного вимкнення (ПЗВ) складається з чутливого елемента – датчика, що сприймає сигнал, і виконавчого пристрою, що забезпечує, власне, вимкнення електроустановки від мережі при сигналі заданого рівня.

Такі пристрої захисного вимкнення повинні мати: високу чутливість, малий час спрацьовування, селективність вимкнення, здатність до самоконтролю справності, достатню надійність.

Вимкнення захисне електроустановок застосовують головним чином у мережах напругою до 1000 В, коли захисне заземлення чи занулення їх зробити важко чи неможливо, а також коли в процесі експлуатації існує висока ймовірність випадкового дотику до струмопровідних частин.

Захисне вимкнення ефективне в пересувних електроустановках, а також при експлуатації ручного електроінструмента. Стаціонарні електроустановки із захисним вимкненням використовують у районах з великим питомим опором землі.

Розпізнають кілька типів схем захисного вимкнення. Датчики, що сприймають сигнал, можуть бути чутливі до:

– напруги на корпусі щодо землі;

– струму замикання на землю;

– напруги нульової послідовності;

– струму нульової послідовності;

– напруги фази щодо землі;

– постійного чи змінного оперативного струму.

Чутлива до напруги на корпусі щодо землі схема, показана на рис.12.4 у вимкненому стані. При пробої фази 1 на корпус електроустановки реле РН, включене між корпусом і допоміжним заземлювачем, спрацьовує і розмикає нормально замкнені контакти реле РН, включені в ланцюг живлення відмикальної котушки (ОК) магнітного пускача. Котушка знеструмлюється і магнітний пускач відмикає електроустановку.

ВИСНОВКИ

В ході кваліфікаційної роботи спроектовано комп'ютерну мережу компанії "ОптімаНет Сервіс". 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.

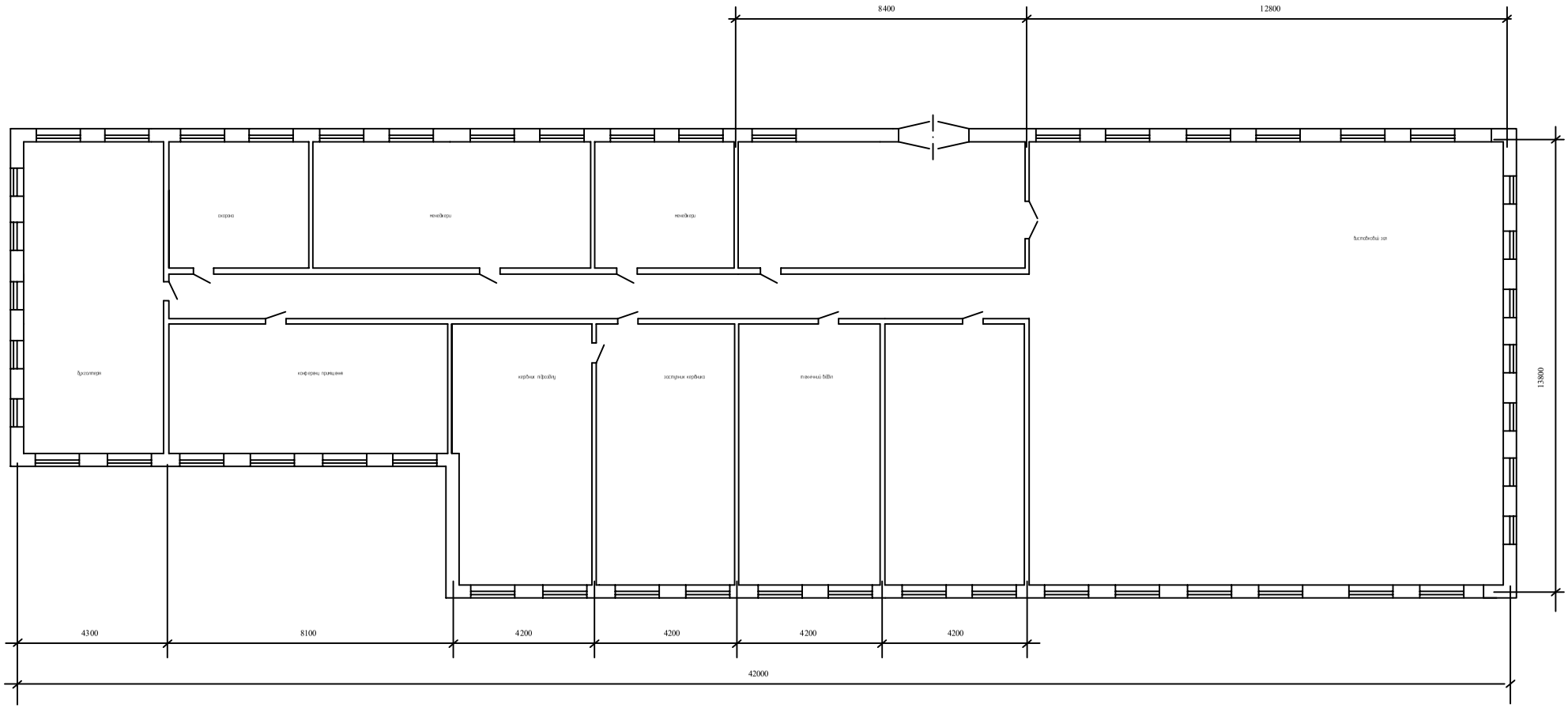
Останній розділ кваліфікаційної роботи описує питання охорони праці, та техніки безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

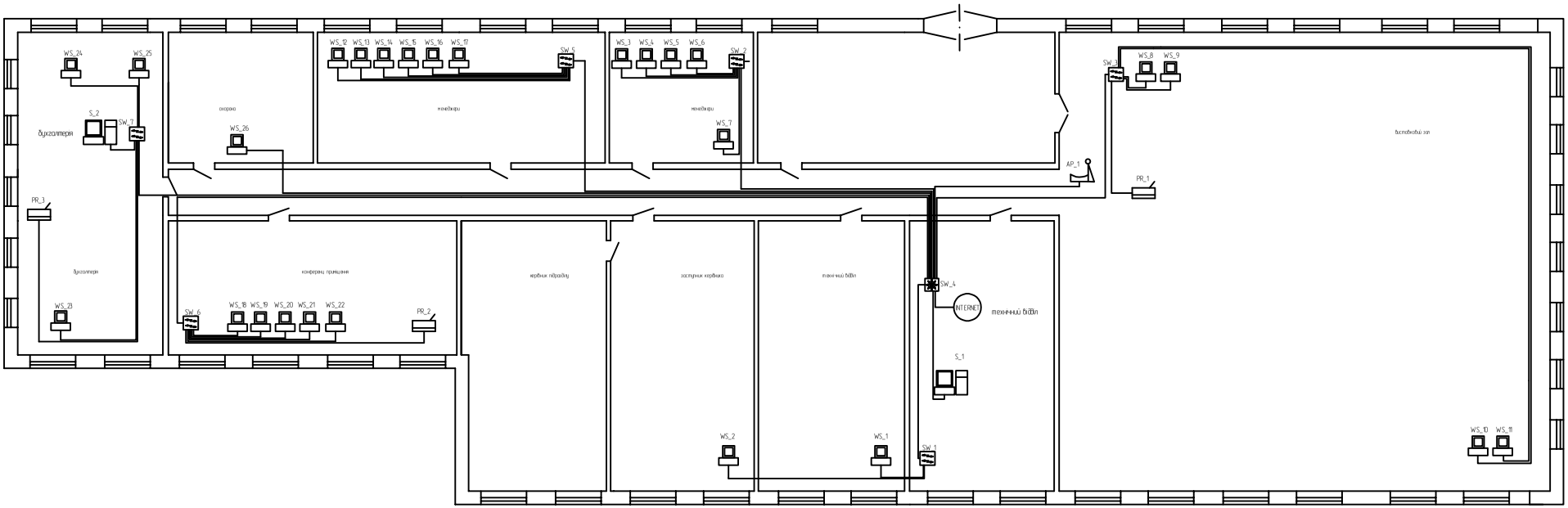
1. Антонов В.М. Сучасні комп'ютерні мережі. Підручник - К.: "МК-Прес", 2005. - 480 с.
2. Буров Є. Комп'ютерні мережі, 2-е видання. - БаК, 2004. - 584 с.: іл.
3. Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С., Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А. Комп’ютерні мережі: навчальний посібник. Київ: 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_program

ni_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).

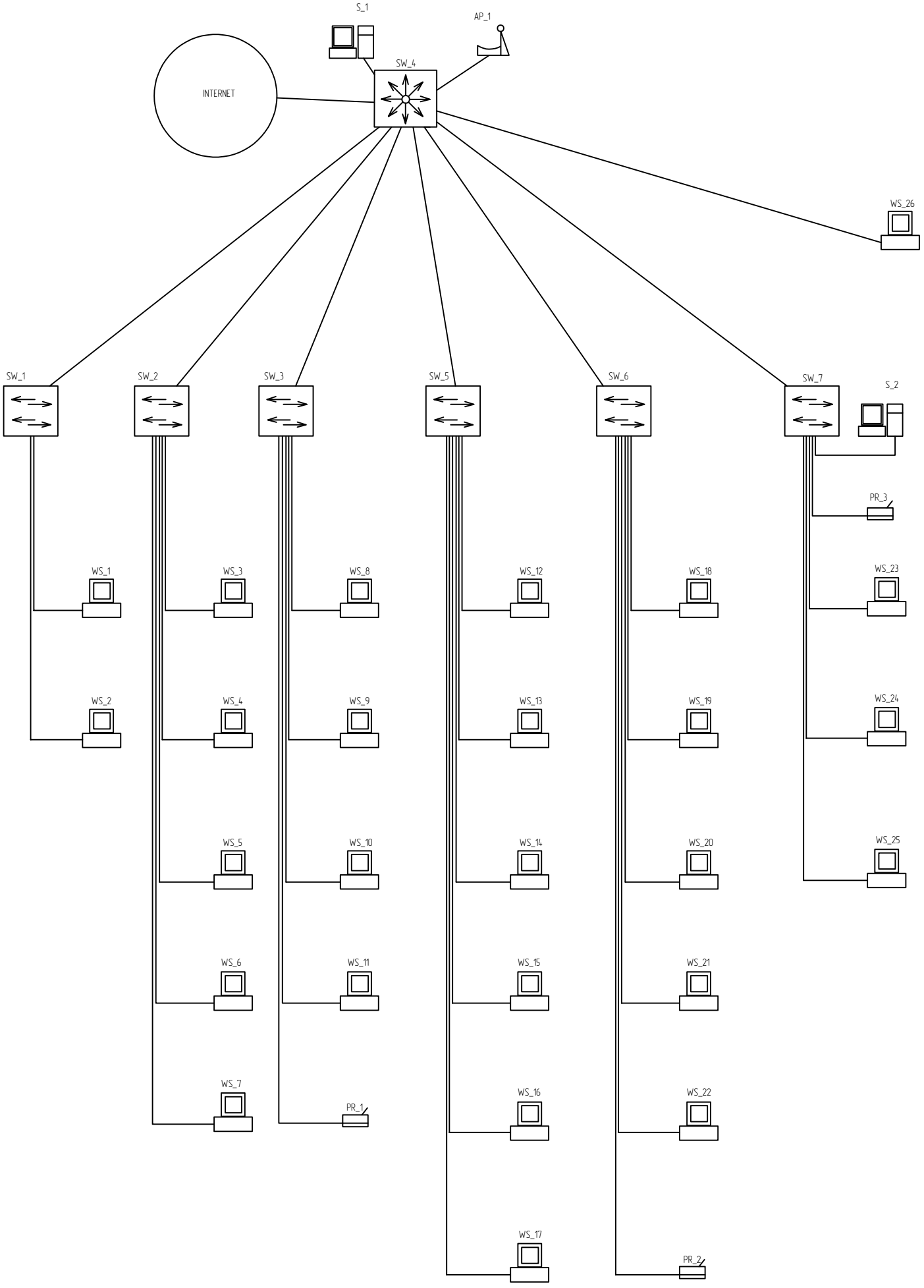
2026.КВР.123.412.09.00.00 ПП



						2026.КВР.123.412.09.00.00 ПП	
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі компанії "ОптімаНет Сервіс" План Приміщень	Літ.	Маса	Масшт.
Розроб.		Музицка С.П.						1:100
Керів.		Пшк. В. С.				Аркуш 1	Аркушів 1	
Нконтр.		Фазькіф А.В.				ВСП ТФК ТНТУ КІ-412, м.Тернопіль		
Рецензія								
затв.								



						2026.КВР.123.412.09.00.00 ФТ	
Зм.	Арк.	№Докум.	Підпис	Дат.		Розробка проекту комп'ютерної мережі компанії "ОптімаНет Сервіс" Фізична Топологія	Літ. / Маса / Масшт. 1:100
Розроб.		Музика С.П.					
Керів.		Пшк. В.С.					
Н.контр.		Фазикіб А.В.					Аркуш 1 / Аркушів 1
Рецензія							ВСП ТФК ТНТУ КІ-412, м.Тернопіль
затв.							



					2026.КВР.123.412.09.00.00 /ЛТ		
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі компанії "ОптімаНет Сервіс" Логічна Топологія	Літ.	Маса	Масшт.
Розроб.		Музика С.П.						
Керів		Лиж В.С.				Н		
Н.контр.		Язьків 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	МАСКА	РОБОЧА ГРУПА
1	WS_1	192.168.20.1	255.255.255.0	MENEJ
2	WS_2	192.168.20.2	255.255.255.0	MENEJ
3	WS_3	192.168.20.3	255.255.255.0	MENEJ
4	WS_4	192.168.20.4	255.255.255.0	MENEJ
5	WS_5	192.168.20.5	255.255.255.0	MENEJ
6	WS_6	192.168.20.6	255.255.255.0	MENEJ
7	WS_7	192.168.20.7	255.255.255.0	MENEJ
8	WS_8	192.168.20.8	255.255.255.0	MENEJ
9	WS_9	192.168.20.9	255.255.255.0	MENEJ
10	WS_10	192.168.20.10	255.255.255.0	MENEJ
11	WS_11	192.168.20.11	255.255.255.0	MENEJ
12	WS_12	192.168.20.12	255.255.255.0	MENEJ
13	WS_13	192.168.20.13	255.255.255.0	MENEJ
14	WS_14	192.168.21.14	255.255.255.0	MENEJ
15	WS_15	192.168.20.15	255.255.255.0	MENEJ
16	WS_16	192.168.20.16	255.255.255.0	MENEJ
17	WS_17	192.168.20.17	255.255.255.0	MENEJ
18	WS_18	192.168.20.18	255.255.255.0	MENEJ
19	WS_19	192.168.20.19	255.255.255.0	MENEJ
20	WS_20	192.168.20.20	255.255.255.0	MENEJ
21	WS_21	192.168.20.21	255.255.255.0	MENEJ
22	WS_22	192.168.20.22	255.255.255.0	MENEJ
23	WS_26	192.168.20.26	255.255.255.0	MENEJ
24	PR_1	192.168.20.50	255.255.255.0	MENEJ
25	PR_2	192.168.20.51	255.255.255.0	MENEJ
26	WS_23	192.168.30.1	255.255.255.0	BUCH
27	WS_24	192.168.30.2	255.255.255.0	BUCH
28	WS_25	192.168.30.3	255.255.255.0	BUCH
29	S2	192.168.30.100	255.255.255.0	BUCH
30	PR_3	192.168.30.50	255.255.255.0	BUCH
31	S1	192.168.20.100	255.255.255.0	MENEJ
32	SW_4	192.168.1.1	255.255.255.0	MENEJ
		призначається провайдером		
33	AP_1	192.168.20.1	255.255.255.0	MENEJ

					2026.КВР.123.412.09.00.01 ТА		
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі компанії "ОптімаНет Сервіс" Таблиця IP адресації	Літ.	Маса	Масшт.
Розроб.		Музика С.П.				Н		
Керів		Пиж В.С.				Аркуш 1	Аркушів 1	
Н.контр.		Язькіб А.В.				ВСП ТФК ТНТУ КІ-412, м.Тернопіль		
Рецензія								

ТАБЛИЦЯ ТЕХНІКО-ЕКОНОМІЧНИХ ПОКАЗНИКІВ							
№ п\п	параметр	одиниці виміру	значення	№ п\п	параметр	одиниці виміру	значення
1	технологія мережі	–	ethernet 1000	8	марка точки доступу	–	MikroTik cAP ac (RB
2	топологія мережі	–	гібридна	9	операційна система робочих станцій	–	windows 11
3	середовище передачі	–	Вита пара кат. 5Е	10	тип доступу до інтернет	–	вита пара
4	кількість вузлів мережі	шт	30	11	термін окупності	рік	1,2
5	марка головного комутатора	–	MikroTik CRS326-24G-2S+RM	12	плановий прибуток	грн	107383,16
6	марка 16-ти портового комутатора	–	Cisco CBS110-16T-EU	13	собівартість	грн	191755,64
7	марка сервера	–	ARTLINE Business T17v23	14	ціна	грн	299138,8