Форма № Н-9.02

Міністерство освіти і науки України

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

(повне найменування вищого навчального закладу)

Відділення інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра

(освітньо-професійного ступеня)

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

Виконав: студент IV курсу, групи КІ-412

Спеціальності 123 Комп'ютерна інженерія

(шифр і назва спеціальності)

_____ **Роман КУЗЬ**

(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

Кузь Роману Андрійовичу
(прізвище, ім'я, по батькові)

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

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 _____ Роман КУЗЬ
(підпис) (ім'я та прізвище)

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

АНОТАЦІЯ

Кузь Р А. Розробка проєкту комп’ютерної мережі ПП “ТехноХата”»: кваліфікаційна робота на здобуття освітньо-професійного ступеня фахового молодшого бакалавра, за спеціальністю 123 Комп’ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2026. -93с.

Основною метою роботи є проєктування та реалізація комп’ютерної мережі підприємства відповідно до поставлених технічних вимог, забезпечення необхідної швидкості передавання даних, організація спільного використання мережевих ресурсів, а також надання стабільного доступу до глобальної мережі Інтернет.

У кваліфікаційній роботі наведено систематизований опис структури підприємства, принципів організації передачі даних, особливостей інформаційних процесів та методів адміністративного керування мережею. Також подано характеристику мережевих вузлів, виконано обґрунтування вибору програмного забезпечення та розглянуто способи його налаштування і конфігурації.

У роботі проведено аналіз сучасного мережевого обладнання, яке використовується для побудови комп’ютерних мереж різного рівня складності. Виконано огляд основних мережевих топологій і технологій передачі даних, а також здійснено вибір оптимальних рішень для впровадження в мережеву інфраструктуру підприємства.

ABSTRACT

Kuz R A. Development of a computer network project for the enterprise “TechnoKata”: qualification work for obtaining the educational and professional degree of a junior bachelor, specialty 123 Computer Engineering. Ternopil: VSP “TFK TNTU”, 2026. -93p.

The main purpose of the work is to design and implement the enterprise’s computer network in accordance with the specified technical requirements, ensuring the required data transfer speed, organizing the sharing of network resources, and providing stable access to the global Internet.

The qualification work provides a systematic description of the enterprise’s structure, the principles of organizing data transfer, the features of information processes, and methods of administrative network management. The characteristics of network nodes are also presented, the justification for the choice of software is made, and the methods of its setup and configuration are considered.

The work analyzes modern network equipment used to build computer networks of various levels of complexity. A review of the main network topologies and data transmission technologies was carried out, and the optimal solutions were selected for implementation in the enterprise's network infrastructure.

ЗМІСТ

ВСТУП

Поява комп’ютерної техніки відкрила принципово нові можливості для накопичення, обробки та поширення інформації. Інформаційні ресурси завжди були тісно пов’язані зі способами їх зберігання та передавання, зокрема друкованими, звуковими або візуальними носіями. Розвиток сучасних цифрових технологій сприяв виникненню новітніх засобів подання інформації – гіпермедійних ресурсів, які поєднують текст, графіку, звук та відео в єдиному інформаційному середовищі. Саме ці технології стали основою стрімкого розвитку інформаційного суспільства та значного зростання обсягів обміну даними.

На сьогодні комп’ютери використовуються не лише для виконання складних математичних і числових обчислень, але й для створення текстових документів, графічних зображень, музичних композицій, відеофільмів та програмного забезпечення. За допомогою комп’ютерних систем здійснюється керування виробничими процесами, автоматизованими лініями, транспортними системами, а також космічними апаратами та іншими складними технічними комплексами. Це свідчить про те, що комп’ютер став універсальним засобом обробки інформації практично в усіх сферах людської діяльності.

Використання сучасного програмного забезпечення значно спрощує процес підготовки та редагування документів у порівнянні з традиційними методами роботи. Текстові редактори забезпечують можливість застосування різних типів шрифтів, автоматичного форматування, вставлення графічних елементів, нумерації сторінок, перевірки орфографії та виконання багатьох інших функцій. Додатковою перевагою комп’ютерних систем є наявність зручного інтерфейсу користувача, широких можливостей налаштування програмного середовища, довідкових систем та підтримки модифікації програмного забезпечення відповідно до потреб користувача.

Сучасні комп’ютерні технології також дозволяють створювати двовимірні та тривимірні моделі об’єктів, виконувати автоматизоване проєктування, розпізнавання тексту та графічних символів, переклад текстової інформації різними мовами, а також моделювати складні технічні та інформаційні процеси. Завдяки таким можливостям комп’ютерна техніка стала невід’ємною складовою сучасного суспільства та продовжує активно розвиватися.

Комп’ютерна мережа являє собою систему взаємопов’язаних комп’ютерів і мережевих пристроїв, що забезпечують розподілену обробку, передавання та зберігання інформації за допомогою каналів зв’язку. Основним призначенням комп’ютерних мереж є організація обміну даними між користувачами, забезпечення спільного доступу до ресурсів та підвищення ефективності роботи інформаційних систем.

Комп’ютерна мережа складається із сукупності територіально розташованих комп’ютерів та інших мережевих пристроїв, які можуть взаємодіяти між собою через середовище передавання даних. Для організації такої взаємодії використовуються різноманітні мережеві технології, протоколи та апаратні засоби, що забезпечують надійне та швидке передавання інформації між вузлами мережі.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Темою кваліфікаційної роботи є розробка проєкту комп'ютерної мережі для ПП «ТехноХата». Основною метою створення мережевої інфраструктури підприємства є забезпечення ефективної взаємодії між усіма структурними підрозділами компанії, підвищення швидкості обміну інформацією та організація стабільного доступу до мережевих ресурсів. Проєктована комп'ютерна мережа повинна відповідати сучасним вимогам щодо продуктивності, надійності та безпеки передавання даних.

Реалізація наступних вимог дозволить створити сучасну комп'ютерну мережу, яка забезпечить стабільну роботу підприємства, оптимізацію інформаційних процесів та підвищення ефективності функціонування всіх структурних підрозділів компанії.

До основних вимог підприємства щодо побудови комп'ютерної мережі можна віднести:

- об'єднання персональних комп'ютерів, які належать до різних структурних підрозділів підприємства, у єдине інформаційне середовище;
- забезпечення спільного використання високошвидкісного підключення до глобальної мережі Інтернет;
- організацію стабільного доступу користувачів до служб локальної мережі та ресурсів мережі Інтернет;
- створення надійного та безпечного засобу обміну інформацією між працівниками підприємства;
- забезпечення безперервної роботи мережевих сервісів та можливості подальшого масштабування мережевої інфраструктури;

- підвищення ефективності роботи працівників за рахунок централізованого доступу до мережевих ресурсів і спільного використання даних.

1.1.2 Призначеннння розробки

Комп'ютерна мережа, що розробляється для ПП «ТехноХата», призначена для забезпечення ефективної та безперервної роботи всіх працівників підприємства. Основним завданням мережевої інфраструктури є організація швидкого та надійного обміну інформацією між структурними підрозділами компанії, а також забезпечення стабільного доступу до мережевих ресурсів і сервісів.

ПП «ТехноХата» спеціалізується на виготовленні зовнішньої та внутрішньої реклами, виконуючи повний цикл робіт — від створення дизайнерського макету до виготовлення та монтажу готових виробів різного рівня складності на території України.

Мережа буде використовуватися переважно для організації документообігу, передавання службової інформації між відділами підприємства, роботи з мережевими ресурсами та забезпечення доступу до зовнішніх інформаційних сервісів через мережу Інтернет.

Однією з важливих вимог до мережевої інфраструктури є забезпечення належного рівня захисту інформації від несанкціонованого доступу. Для реалізації даної вимоги передбачається використання механізмів автентифікації користувачів, встановлення паролів доступу, а також розмежування прав доступу до службових ресурсів та конфіденційної інформації. Це дозволить підвищити рівень інформаційної безпеки як для внутрішніх користувачів мережі, так і при взаємодії із зовнішніми ресурсами мережі Internet.

Для централізованого зберігання інформації у мережі буде виділено окремий персональний комп’ютер, який виконуватиме функції файлового та FTP-сервера.

Використання такого рішення дозволить організувати централізоване зберігання даних, спростити обмін файлами між працівниками та забезпечити резервування важливої інформації.

Для забезпечення високої продуктивності та стабільності роботи мережі передбачається використання мережевого обладнання, яке підтримує швидкість передавання даних 100/1000 Мбіт/с. Це забезпечить достатню пропускну здатність мережі для роботи з великими обсягами інформації, графічними файлами та мережевими сервісами підприємства.

1.1.3 Вимоги до апаратного та програмного забезпечення

Апаратні та програмні засоби комп’ютерної мережі повинні відповідати ряду технічних, експлуатаційних та організаційних вимог, які забезпечать стабільну, безпечну та ефективну роботу мережевої інфраструктури підприємства.

При проєктуванні мережі необхідно враховувати особливості роботи структурних підрозділів, інтенсивність обміну даними, можливість масштабування та простоту обслуговування обладнання.

Проєктована комп’ютерна мережа буде поділена на окремі робочі групи відповідно до структури підприємства та функціональних обов’язків працівників.

Такий підхід дозволить оптимізувати мережевий трафік, підвищити рівень безпеки та забезпечити більш ефективне адміністрування мережевих ресурсів.

Швидкість передавання даних у локальній мережі повинна становити 100/1000 Мбіт/с, що забезпечить достатню пропускну здатність для роботи з документами, графічними матеріалами та іншими службовими файлами.

До основних вимог щодо апаратного забезпечення мережі належать:

- використання загальнодоступного та поширеного мережевого обладнання;
- невисока вартість обладнання та витратних матеріалів;
- підтримка швидкості передавання даних 100/1000 Мбіт/с;
- можливість швидкої заміни або ремонту мережевих компонентів;
- простота технічного обслуговування та адміністрування;
- забезпечення стабільної та безперервної роботи мережі.

Для організації безпровідного доступу до мережі передбачається використання точки доступу Wi-Fi, яка повинна відповідати сучасним вимогам безпеки та продуктивності.

У структурі комп'ютерної мережі передбачається використання декількох типів комутаторів.

Комутатори, які обслуговують окремі робочі групи, повинні бути некерованими, що дозволить знизити вартість мережевої інфраструктури та спростити її експлуатацію.

Головний комутатор мережі повинен бути керованим, оскільки він виконуватиме функції централізованого керування мережею, розподілу трафіку та забезпечення підключення основних сегментів мережі.

Для забезпечення централізованого зберігання даних та роботи служб підприємства у мережі передбачається використання серверного обладнання, а саме:

- файлового сервера для зберігання та спільного доступу до інформації;
- сервера бухгалтерського програмного забезпечення для підтримки роботи бухгалтерії та обробки фінансової документації.

1.1.4 Стадії та етапи розробки

Під час організації комп'ютерної мережі всі роботи доцільно поділити на кілька основних етапів, кожен із яких забезпечує правильне проєктування та подальшу стабільну роботу мережевої інфраструктури.

До основних етапів організації мережі належать:

- збір інформації;
- створення та затвердження проєктної документації;
- фізична реалізація комп'ютерної мережі;
- експлуатація та моніторинг мережі.

На етапі збору інформації необхідно визначити основні вимоги до майбутньої мережі та врахувати особливості роботи підприємства. При цьому потрібно встановити:

- тип організації та можливість її подальшого розвитку;
- наявність існуючих комп'ютерних мереж;
- вимоги керівництва та користувачів;
- програмне забезпечення, яке буде використовуватися;
- тип мережі, топологію, кабельну систему та мережеве обладнання;
- необхідність використання комутаторів, маршрутизаторів та іншого активного обладнання;
- тип підключення до мережі Internet;
- вимоги до захисту інформації та адміністрування мережі.

Усі отримані дані необхідно враховувати під час створення проєкту комп'ютерної мережі.

Для побудови сучасної та надійної мережевої інфраструктури доцільно використовувати стандарти структурованих кабельних систем (СКС), що забезпечують впорядкованість кабельного господарства та спрощують обслуговування мережі.

Також рекомендується застосовувати сертифіковане обладнання одного виробника та спеціалізовані тестові засоби для перевірки працездатності мережі після завершення монтажних робіт.

1.1.5 Вимоги до документації

У результаті проєктування комп'ютерної мережі необхідно підготувати комплект технічної документації, яка буде використовуватися під час монтажу, налаштування та подальшої експлуатації мережевої інфраструктури. Наявність правильно оформленої документації значно спрощує процес адміністрування мережі, проведення ремонтних робіт та модернізації обладнання.

До основної документації, що створюється під час проєктування мережі, належать:

- інженерний журнал;
- схема логічної топології мережі;
- схема фізичної топології мережі;
- матриця можливих проблем та способів їх усунення;
- маркування виходів кабельних ліній;
- маркування трас прокладання кабелю;
- опис кабельних трас та точок підключення;
- таблиця MAC-адрес та IP-адрес мережевих пристроїв.

1.1.6 Техніко-економічні показники

Розроблена комп'ютерна мережа повинна відповідати сучасним вимогам щодо продуктивності, надійності та економічної доцільності. Під час вибору мережевого обладнання необхідно враховувати не лише техні-

чні характеристики, але й вартість обладнання, можливість його подальшого обслуговування та масштабування мережевої інфраструктури.

До основних вимог, які ставляться до проєктованої мережі, належать:

- використання сучасного та надійного мережевого обладнання;
- забезпечення невисокої вартості реалізації мережі, зокрема використання комутаторів у ціновому діапазоні від 2000 до 5000 гривень;
- підтримка швидкості передавання даних 100/1000 Мбіт/с;
- можливість подальшого розширення та модернізації мережі;
- забезпечення стабільного доступу до глобальної мережі Internet;
- організація безпровідної мережі Wi-Fi для підключення мобільних та портативних пристроїв.

1.1.7 Порядок контролю та прийому

Під час приймання комп'ютерної мережі в експлуатацію необхідно виконати ряд перевірок та організаційних заходів, які забезпечать правильне функціонування мережевої інфраструктури.

Термін створення приймальної комісії не повинен перевищувати п'яти днів з моменту отримання замовником повідомлення про завершення робіт. Правильне виконання приймання мережі в експлуатацію забезпечує її стабільну та надійну роботу протягом усього терміну використання.

Основні вимоги та етапи приймання мережі:

- перевірка працездатності всіх мережевих вузлів та активного обладнання;
- перевірка правильності підключення кабельних ліній;
- маркування всіх кабелів та точок підключення відповідно до проєктної документації;
- тестування функціонування мережі за допомогою спеціалізованих прикладних утиліт і програмних пакетів;

- перевірка швидкості передавання даних та доступності мережевих ресурсів;
- контроль стабільності роботи мережевих служб та доступу до мережі Internet;
- підготовка комплекту технічної документації після завершення монтажних робіт;
- передача замовнику письмового повідомлення про завершення інсталяції мережі;
- створення спеціальної приймальної комісії для перевірки функціональних характеристик мережі;
- проведення комплексного тестування мережевої інфраструктури;
- оформлення та підписання акту введення мережі в експлуатацію після успішного завершення перевірки.

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

Метою даного кваліфікаційної роботи є розробка сучасної комп'ютерної мережі для ПП «ТехноХата», яка забезпечить об'єднання всіх персональних комп'ютерів підприємства в єдину інформаційну систему. Проєктована мережа повинна забезпечувати швидкий та надійний обмін інформацією між працівниками, централізоване зберігання даних, а також спільний доступ користувачів до мережевих ресурсів і глобальної мережі Internet.

ПП «ТехноХата» спеціалізується на виготовленні зовнішньої та внутрішньої рекламної продукції та виконує повний цикл робіт — від розробки дизайнерських макетів до виготовлення та монтажу рекламних конструкцій різної складності по всій території України. Основними напрямками діяльності підприємства є:

- інтер’єрне оформлення приміщень;
- виготовлення рекламних вивісок;
- монтаж дахових конструкцій;
- виробництво пілонів та стел;
- брендування транспортних засобів;
- широкоформатний друк рекламної продукції.

Для забезпечення ефективної роботи підприємства персональні комп’ютери та мережеве обладнання будуть розміщені у таких приміщеннях:

- кабінет керівника підрозділу;
- кабінет заступника керівника;
- відділ роботи з клієнтами;
- технічний відділ;
- конференц-зал;
- виробничі приміщення;
- інші службові приміщення підприємства.

Проєктована комп’ютерна мережа повинна забезпечувати стабільну роботу всіх структурних підрозділів підприємства, підтримувати високу швидкість передавання даних, можливість подальшого розширення мережевої інфраструктури та безпечний доступ до інформаційних ресурсів підприємства.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Розробка та обґрунтування логічної та фізичної схем мережі

З самого початку створення комп’ютерних мереж все обладнання розташовувалося за певними правилами і це розташування називалося топологіями.

Топологія комп'ютерної мережі відображає структуру зв'язків між її основними функціональними елементами. В залежності від компонентів, що розглядаються, розрізняють фізичну і логічну структури локальних мереж. Доповнюючи одна одну, фізична та логічна структури дають найповніше уявлення про комп'ютерну мережу.

Топологія мережі визначає не тільки фізичне розташування комп’ютерів, але, що набагато важливіше, характер зв’язків між ними, особливості поширення сигналів по мережі. Саме характер зв’язків визначає ступінь відмовостійкості мережі, необхідну складність мережної апаратури, найбільш підходящий метод керування обміном, можливі типи середовищ передачі (каналів зв’язку), припустимий розмір мережі (довжина ліній зв’язку й кількість абонентів), необхідність електричного узгодження й багато чого іншого.

Фізична топологія характеризує фізичне розташування комп'ютерів, кабелів й інших компонентів мережі. Комп'ютери, підключені до мережі, часто називають станціями, вузлами мережі або хостами.

Вибір фізичної топології істотно впливає на велику кількість характеристик мережі. Наприклад, існування резервних зв'язків підвищує надійність мережі та дозволяє організовувати, балансування завантаження окремих каналів. Простота приєднання нових вузлів, властива деяким топологіям, робить мережу легко розширюваною. Економічні міркування

часто призводять до вибору топологій, для яких характерна мінімальна сумарна довжина ліній зв'язку.

На даний час існує багато топологій мереж з яких найбільш поширеними є:

- топологія типу зірка
- шинна топологія
- топологія типу кільце
- деревовидна топологія.

Топологія типу зірка – концепція топології мереж у вигляді зірки прийшла з області великих ЕОМ, в якій головна машина получає і обробляє всю інформацію з периферійних пристроїв як активний вузол опрацювання даних.

Вся інформація між двома периферійними робочими місцями проходить через центральний вузол мережі. Схематичне зображення топології типу зірка зображено на рисунку 2.1.

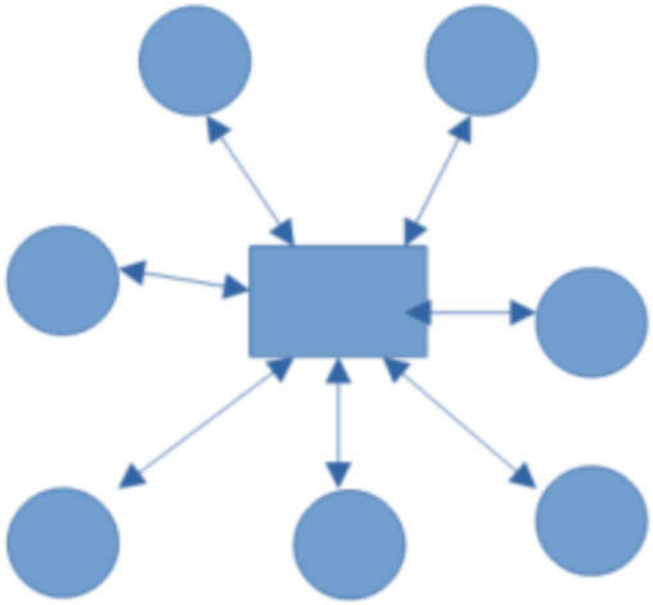


Рисунок 2.1 – Топологія типу «зірка»

Пропускна здатність мережі залежить від характеристик центрального вузла та забезпечується окремо для кожної робочої станції. У даній топології практично відсутні колізії даних, а кабельна система є відносно простою, оскільки кожна станція підключається окремим кабелем до центрального вузла.

Недоліком такої структури є значні витрати на прокладання кабельних ліній, особливо якщо центральний вузол розташований не в центрі мережі. Під час розширення мережі виникає необхідність прокладання нових кабельних маршрутів до кожного нового робочого місця.

Топологія типу «зірка» є однією з найшвидших серед існуючих топологій, оскільки обмін даними відбувається через центральний вузол по окремих лініях зв’язку.

Кількість конфліктів при передаванні інформації є мінімальною. У випадку виходу з ладу центрального вузла припиняється функціонування всієї мережі. Однією з переваг такої топології є можливість централізованого керування та підвищений рівень захисту інформації.

Кільцева топологія

У кільцевій топології всі робочі станції з’єднані між собою послідовно у вигляді замкненого кільця.

Кожна робоча станція має зв’язок із двома сусідніми вузлами, а остання станція з’єднується з першою. Схема кільцевої топології наведена на рисунку 2.2.

Передавання інформації у такій мережі здійснюється по замкненому колу. Кабельна система може бути складною та дорогою у випадку великої відстані між робочими станціями. Повідомлення циркулюють по мережі послідовно, а передавання інформації виконується після отримання відповідного дозволу на передавання.

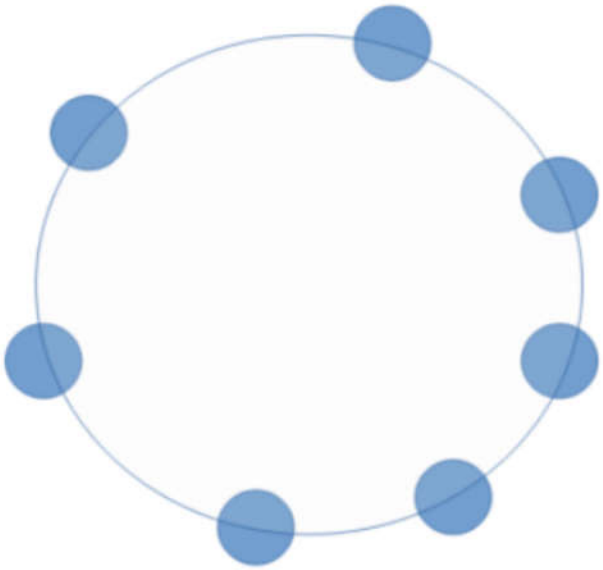


Рисунок 2.2 – Топологія типу «кільце»

Кільцева топологія забезпечує ефективне передавання даних та дозволяє швидко організувати широкомовну передачу повідомлень усім вузлам мережі.

Недоліком є збільшення часу передавання даних зі зростанням кількості робочих станцій у мережі.

Шинна топологія

У шинній топології середовище передавання даних реалізоване у вигляді єдиного комунікаційного каналу, до якого підключаються всі робочі станції. Усі вузли мережі мають можливість безпосередньо взаємодіяти між собою через спільний канал передавання даних.

Робочі станції можуть підключатися або відключатися від мережі без повного припинення її роботи.

Для реалізації шинної топології часто використовувався тонкий коаксіальний кабель типу Cheapernet. Однак підключення або відключення нових пристроїв потребувало фізичного розриву шини, що могло призвести до порушення передавання інформації.

Сучасні рішення дозволяють підключати робочі станції через спеціальні комутаційні розетки та штепсельні коробки. Одним із недоліків шинної топології є нижчий рівень інформаційної безпеки, оскільки доступ до мережевого середовища може бути отриманий у будь-який момент часу.

Деревовидна топологія

Деревовидна топологія формується шляхом поєднання декількох базових топологій. Основою такої структури є центральний вузол, від якого відходять окремі сегменти мережі. Даний тип топології використовується у випадках, коли застосування базових структур у чистому вигляді є неможливим.

Для підключення великої кількості робочих станцій використовуються активні концентратори або комутатори. Схематичне зображення деревовидної топології наведено на рисунку 2.3.

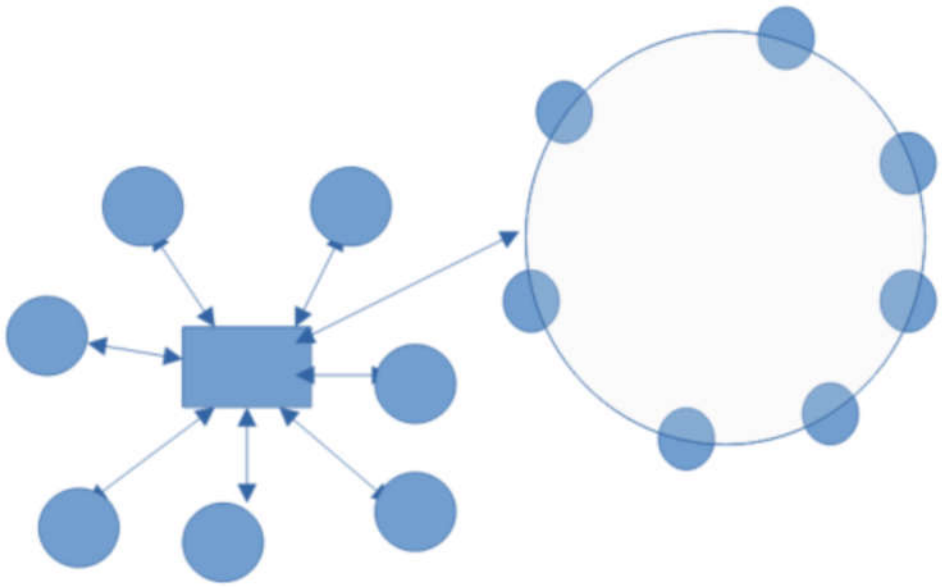


Рисунок 2.3 – Топологія типу «дерево»

Короткі характеристики основних топологій наведені у таблиці 2.1.

Таблиця 2.1 — Порівння мережевих топологій

Критерій порівняння	Топологія «Шина» (Bus)	Топологія «Кільце» (Ring)	Топологія «Зірка» (Star)	Гібридна «Розширена зірка»
1	2	3	4	5
Фізична структура	Усі вузли паралельно підключені до одного загального кабелю.	Вузли з'єднані послідовно в замкнутий контур.	Кожен пристрій підключений до центрального комутатора.	Ієрархічна структура з кількох зіркоподібних сегментів.
Витрати на кабельну продукцію	Мінімальні (одна центральна магістраль).	Середні (достатньо з'єднати суміжні вузли).	Високі (окремий провід до кожного термінала).	Максимальні (через велику протяжність та резервування).
Складність масштабування	Середня (потрібно подовжувати магістральний кабель).	Складно (потрібно розривати та зупиняти мережу).	Дуже просто (достатньо підключити кабель у вільний порт).	Просто (можна додавати цілі нові комутаційні блоки).
Стійкість до обриву кабелю	Критично низька (один обрив виводить з ладу всю	Низька (при одному обриві зв'язок втрачається,	Висока (пошкодження лінії ізолює лише одну робочу	Висока (аварія в одному сегменті не впливає на інші

Продовження таблиці 2.1

1	2	3	4	5
	мережу).	якщо немає дублювання	станцію).	підмережі).
Залежність від активного обладнання	Відсутня (мережа може працювати на пасивних елементах).	Висока (вихід з ладу однієї мережевої карти зупиняє кільце).	Абсолютна (вийде з ладу центральний комутатор — впаде вся мережа).	Залежність розподілена (критичним є лише комутатор ядра).
Метод доступу до середовища	Випадковий (CSMA/CD), висока ймовірність колізій.	Маркерний (Token Passing), колізії відсутні.	Централізована комутація (пакети йдуть адресно, без колізій).	Ієрархічна маршрутизація та комутація на різних рівнях.
Ефективність під високим навантаженням	Критично знижується (через постійні конфлікти пакетів).	Стабільна, але зростає час очікування маркера.	Дуже висока (обмежується лише шиною комутатора).	Максимальна (трафік локалізується всередині своїх сегментів).

З урахуванням масштабів підприємства та кількості робочих місць для проєктованої мережі обирається технологія Ethernet 1000Base-T. Для даного типу мережі найбільш доцільною є топологія типу «розширена зірка», у якій максимальна відстань між робочою станцією та комутатором

не перевищує 100 метрів. Оскільки в мережі також передбачається використання безпровідної точки доступу, загальний тип топології можна вважати гібридним.

Вибір кабельної підсистеми залежить від типу мережі та обраної топології. Необхідні характеристики кабелю задаються виробником та позначаються відповідним маркуванням на оболонці кабелю.

Для мережі Ethernet 1000Base-T передбачається використання кабелю типу «кручена пара» категорій 5, 5e, 6 або 7. Кабельна система локальної мережі побудована на основі неекранованої витої пари категорії 5e, схематичне зображення якої наведено на рисунку 2.4.

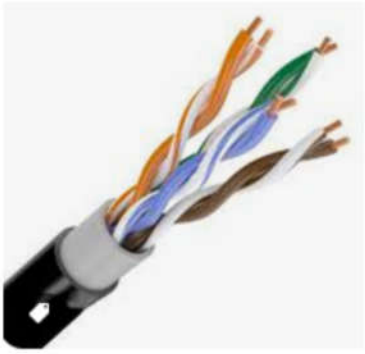


Рисунок 2.4 – Неекранована вита пара категорії 5e

Даний тип кабелю є недорогим та простим у прокладанні. Мережі на основі витої пари характеризуються простотою обслуговування, експлуатації та пошуку несправностей. Кабелі горизонтальної підсистеми повинні використовуватись разом із комутаційним обладнанням та патч-кордами відповідної або вищої категорії.

У мережі передбачено використання шести восьмипортових некерованих комутаторів, які підключаються до головного керованого комутатора. Така структура дозволяє створити окремі робочі групи, незалежні одна від одної.

Кожну робочу групу можна помістити у власний VLAN, що дозволить ізолювати мережевий трафік окремих сегментів. На сервері можливо реалізувати контроль доступу до мережі Internet за допомогою відповідного програмного забезпечення.

Безпровідна точка доступу також підключається до окремого VLAN, що дозволяє мінімізувати можливий негативний вплив безпровідного сегмента на роботу локальної мережі в цілому.

Усі описані параметри та характеристики мережі наведені у таблицях 2.2 та 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_13—WS_14	WG1	2	Керівник та помічник	90	192.168.9.0/24
WS_1-WS_12	WG2	7	Менеджери, відділ роботи з клієнтами	60	192.168.6.0/24
WS_16—WS_17, WS_21—WS_23	CONFER	5	конференц-зал	80	192.168.8.0/24
WS_18—WS_20	BUCH	3	бухгалтерія	100	192.168.10.0/24
WS_15	IP	1	Тенічний відділ	30	192.168.3.0/24
PR_2	BUCH	1	бухгалтерія	100	192.168.10.4/24
PR_1	CONFER	1	Конференц-зал	80	192.168.8.4/24

Продовження таблиці 2.3

1	2	3	4	5	6
S_1	IP		Тенічний відділ	30	192.168.3.100/24
S_2	BUCH		бухгалтерія	100	192.168.10.10/24
Ap_1	IP		конференц-зал	30	192.168.3.200/24

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
3	SW_2	3	Access	S_2	-	Access	-
4	SW_2	4	Access	SW_1	16	Access	30
5	SW_2	5	Access	SW_3	16	Access	30
6	SW_2	6	Access	SW_4	16	Access	30
10	PR_1			SW_6	7	Access	80
11	PR_2			SW_7	7	Access	100
18	SW_4	24	Access	AP_1	WAN	Access	30

2.3 Обґрунтування вибору комунікаційного обладнання

Для побудови локальної обчислювальної мережі приватного підприємства «ТехноХата» сформовано чіткі вимоги до апаратної складової. Архітектура мережі передбачає використання такого комплекту обладнання:

- Три недорогих шістнадцятипортових комутатори доступу для забезпечення зв'язку всередині локальних робочих груп (SW_1, SW_3, SW_4);
- Один центральний шістнадцятипортовий керований (інтелектуальний) комутатор рівня агрегації та ядра (SW_2);
- Одна бездротова точка доступу для покриття конференц-залу (AP_1);
- Два виділених серверних персональних комп'ютери для забезпечення збереження даних та роботи внутрішніх служб (S_1 та S_2).

Оскільки фізична та логічна структура мережі підприємства критично залежить від комутаційних вузлів, виникла інженерна необхідність у підборі оптимальних 16-портових моделей, здатних підтримувати гігабітну швидкість (10/100/1000 Мбіт/с) та технологію віртуальних мереж (802.1Q VLAN) для ізоляції трафіку робочих груп відповідно до розробленого плану адресації.

Вибір периферійних та центрального комутаторів було зосереджено серед трьох актуальних на ринку моделей телекомунікаційного обладнання класу Easy/Smart Managed. Їхня детальна порівняльна техніко-економічна характеристика наведена в таблиці 2.4. Аналіз параметрів, наведених у таблиці 2.4, показує, що моделі від D-Link та Cisco мають надлишкові для даного проєкту оптичні SFP-порти та підвищену вартість, що суттєво збільшує загальний кошторис пусконалагоджувальних робіт.

З огляду на специфіку схеми конфігурування ЛОМ ПП «ТехноХата», функціонал моделі TP-Link TL-SG1016DE є абсолютно достатнім, зовнішній вигляд якого зображено на рисунку 2.5.

Цей пристрій забезпечує повноцінну комутацію на швидкості 1 Гбіт/с, підтримує пріоритезацію трафіку (QoS), моніторинг портів, петлевий захист (Loop Prevention) та тегування VLAN 802.1Q. Пасивна система охолодження гарантує безшумну роботу обладнання в офісних приміщен-

них. Завдяки найкращому співвідношенню ціни та продуктивності, комутатор TP-Link TL-SG1016DE обрано як єдину уніфіковану апаратну платформу як для периферійних робочих груп, так і для центрального інтелектуального вузла агрегації підприємства.

Таблиця 2.4 - Таблиця характеристик шістнадцятипортових комутаторів

Технічний параметр	TP-Link TL-SG1016DE	D-Link DGS-1210-20	Cisco CBS220-16T-2G
1	2	3	4
Кількість портів RJ-45	16 × 10/100/1000 Мбіт/с	16 × 10/100/1000 Мбіт/с	16 × 10/100/1000 Мбіт/с
Додаткові Uplink-слоти	Відсутні	4 × 1 Гбіт/с SFP	2 × 1 Гбіт/с SFP
Тип керування (OSI)	L2 (Easy Smart)	L2 (Smart Managed)	L2 (Smart Managed)
Комутаційна матриця	32 Гбіт/с	40 Гбіт/с	36 Гбіт/с
Швидкість пересилання	23.8 Mpps	29.8 Mpps	26.78 Mpps
Підтримка 802.1Q VLAN	Так (до 32 VLAN)	Так (до 256 VLAN)	Так (до 256 VLAN)
Тип охолодження	Пасивне (безвентиляторне)	Пасивне (безвентиляторне)	Пасивне (безвентиляторне)
Орієнтовна вартість	~ 3 700 грн	~ 7 100 грн	~ 12 600 грн

Рисунок 2.5 – Зовнішній вигляд комутатора TP-Link TL-SG1016DE

Також у комп'ютерній мережі потрібен керований комутатор.

Центральний комутатор мережі (SW_2) є критично важливим елементом інфраструктури ПП «ТехноХата», оскільки він здійснює агрегацію всього внутрішнього трафіку, забезпечує взаємодію між периферійними комутаторами робочих груп та відкриває доступ до серверного обладнання (S_2) і маршрутизатора.

До апаратної платформи ядра висуваються підвищені вимоги: наявність 16 або більше гігабітних портів, підтримка розширеного функціоналу другого та третього рівнів (L2+ / L3 Static Routing) для забезпечення маршрутизації між ізольованими віртуальними мережами без залучення ресурсів центрального роутера, а також висока швидкість обробки пакетів.

З метою вибору головного комутатора було проаналізовано три моделі керованого обладнання корпоративного класу.

Зведені технічні характеристики пристроїв представлені в таблиці 2.5. Зіставлення параметрів таблиці 2.5 показує що збалансованим та технічно виправданим рішенням для ПП «ТехноХата» є керований комутатор TP-Link TL-SG3428X.,зовнішній вигляд якого зображено на рисунку 2.6.

Таблиця 2.5 – Порівняльна характеристика керованих комутаторів

Технічний параметр	TP-Link TL-SG3428X	Cisco CBS350-24T-4G	Mikrotik CRS326-24G-2S+RM
1	2	3	4
Кількість портів Downlink	24 × 1000 Мбіт/с RJ-45	24 × 1000 Мбіт/с RJ-45	24 × 1000 Мбіт/с RJ-45
Високошвидкісні Uplink-порти	4 × 10 Гбіт/с SFP+	4 × 1 Гбіт/с SFP	2 × 10 Гбіт/с SFP+
Рівень керування (OSI)	L2+ (JetStream Managed)	L3 (Fully Managed)	L2/L3 (Dual Boot RouterOS)
Комутаційна матриця	128 Гбіт/с	56 Гбіт/с	88 Гбіт/с
Швидкість пересилання пакетів	95.23 Mpps	41.66 Mpps	65.4 Mpps
Таблиця MAC-адрес	16 K	16 K	16 K
Функції третього рівня (L3)	Статична маршрутизація, DHCP Relay	Статична маршрутизація, Policy-Based Routing	Статична маршрутизація, HW-offloaded routing
Орієнтовна вартість	~ 9 400 грн	~ 16 500 грн	~ 7 300 грн

Рисунок 2.6 – Зовнішній вигляд _TP-Link TL-SG3428X

Для реалізації бездротового сегмента мережі ПП «ТехноХата», зокрема для покриття зони конференц-залу, де згідно з розробленою топологією розгортається точка доступу AP_1, оптимальним вибором є дводіапазонна гігабітна точка доступу TP-Link EAP610. Зовнішній вигляд TP-Link EAP610 показано на рисунку 2.7

По-перше, пристрій підтримує сучасний стандарт бездротового зв'язку Wi-Fi 6 (802.11ax), що забезпечує сумарну швидкість передачі даних у двох діапазонах до 1775 Мбіт/с.

Це гарантує стабільну роботу великої кількості одночасно підключених мобільних пристроїв та ноутбуків у конференц-залі (VLAN 80) без затримок та втрати пакетів.

По-друге, модель обладнана гігабітним Ethernet-портом із підтримкою технології PoE (Power over Ethernet) за стандартом 802.3at/af. Це дозволяє подавати живлення на пристрій безпосередньо через мережевий кабель витої пари від комутатора, усуваючи необхідність монтажу окремих силових розеток під стелею чи на стіні конференц-залу.

По-третє, і це є ключовим фактором, TP-Link EAP610 повністю інтегрується в раніше обрану екосистему централізованого управління Omada SDN.

Це дозволяє адміністратору гнучко налаштовувати бездротову мережу, ізолювати гостьовий трафік пацієнтів чи клієнтів від корпоративних

ресурсів за допомогою віртуальних мереж (Multi-SSID з прив'язкою до VLAN 30 та VLAN 80), а також безперешкодно масштабувати бездротове покриття в майбутньому.

Таким чином, за сукупністю технічних параметрів, сумісності з інфраструктурою та цінової доступності для підприємства, кращим інженерним рішенням для вузла AP_1 є точка доступу TP-Link EAP610.

Рисунок 2.7 – Зовнішній вигляд TP-Link EAP610

У комп’ютерній мережі передбачено використання серверного комп’ютера, призначення якого бути сервером для документів.

Сервер ARTLINE Business R17v24

Сервер ARTLINE Business – справжнє серце вашої IT інфраструктури. Він має збалансовану продуктивність і невелике споживання енергії, що дозволить вам з мінімальними витратами ефективно виконувати бізнес-завдання. ARTLINE Business R17v24 втілив усе, що Ви чекаєте від сервера: надійність, довговічність, продуктивність, економічність, простоту використання та обслуговування.

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

Сервер ARTLINE Business R17v24 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 материнська плата ASUS забезпечить гарантовано тривалий термін служби сервера ARTLINE. Плата підтримує процесори Intel 12 покоління.

З особливостей: оптимізована система живлення, повноцінне охолодження та утиліта Fan Xpert 2+, технологія OptiMem для стабільної роботи модулів пам'яті, сучасні інтерфейси: три слоти PCIe 4.0, три слоти M.2, 2.5G Ethernet (контролер Realtek) та порти USB 3.2 Type-C.

У даній збірці за продуктивність відповідає процесор Intel Core i5-12400 12-го покоління мікроархітектури Alder Lake, який належить до сімейства високопродуктивних процесорів. Intel Core i5-12400 виробляється за стандартом 7-нм техпроцесу, має 6 ядер, які працюють у 12 потоків зі штатною тактовою частотою 2.5 ГГц, 4.4 ГГц у режимі Turbo Boost.

Оперативна пам'ять DDR4 на 16 ГБ з ефективною робочою частотою 2666 МГц забезпечить швидку та стабільну роботу сервера. Є можливість апгрейду у майбутньому до 128 ГБ.

Два встановлені SSD накопичувачі об'ємом 500 ГБ кожен забезпечать швидке завантаження системних файлів та всіх інших програм, а два жорсткі диски, кожен з яких має 2 ТБ вільного місця – надійне зберігання дуже великої кількості необхідної інформації.

У сервері ARTLINE Business R17v24 використовується надійний блок живлення потужністю 450 Вт із сертифікатом 80+ Bronze.

Професійне складання сервера ARTLINE та наявність двох 80 мм вентиляторів забезпечать оптимальний повітряний потік усередині корпусу з формфактором 2U, а значить і відмінне охолодження всіх компонентів.

Зведена таблиця 2.8 обладнання, яке я підібрав:

Таблиця 2.8 -Зведена таблиця обладнання мережі.

№ п\п	Тип обладнання	Марка	кількість	ціна
1	2	3	4	5
1	Некерований комутатор	TP-Link TL-SG1016DE	3	3700 грн
2	Керований комутатор	TP-Link TL-SG3428X	1	9400 грн
3	Точка доступу	TP-Link EAP610	1	2800 грн
4	сервер	ARTLINE Business R17v24	2	72900 грн

2.4 Особливості монтажу мережі

Розглянемо основні особливості монтажу неекранованої витої пари UTP категорії 5е.

Довжина кабелю. Максимальна довжина горизонтальної кабельної лінії становить 90 метрів. Для підключення робочих станцій, використання патч-кордів та перемичок у телекомунікаційних шафах допускається додатково до 10 метрів кабелю.

Допустиме розтягувальне зусилля. Максимально допустиме навантаження для чотирипарного кабелю становить 50 Н. Надмірне натягування під час монтажу може спричинити деформацію кабелю та погіршення його електричних характеристик. У випадку серйозного пошкодження кабель необхідно замінити.

Мінімальний радіус вигину. Радіус вигину кабелю повинен бути не менше 8 діаметрів під час монтажу та не менше 4 діаметрів під час експлуатації. Недотримання цих вимог може призвести до деформації провідників

та погіршення параметрів передачі даних. Найчастіше порушення виникають у місцях встановлення інформаційних розеток та в монтажних шафах. Кабель необхідно прокладати плавно, без різких перегинів та сильного стискання.

Монтаж при низьких температурах. Мінімально допустима температура монтажу кабелю становить 0 °С. Якщо роботи виконуються при нижчій температурі, кабель необхідно попередньо витримати у теплому приміщенні при температурі понад 10 °С не менше 24 годин. На робочий майданчик рекомендується виносити лише необхідну кількість кабелю. Надмірно туге намотування на котушки може викликати пошкодження оболонки кабелю.

Надмірне навантаження та скручування. Під час монтажу необхідно уникати надмірного натягу та перекручування кабелю, оскільки це може спричинити його деформацію або розрив оболонки. Рекомендована відстань між точками кріплення кабелю становить 120–150 см. Також слід дотримуватись мінімальної відстані 15 см між кабелем та джерелами електромагнітних перешкод, такими як силові кабелі або люмінесцентні лампи.

Монтаж інформаційних розеток та комутаційних панелей. Монтаж повинен виконуватись відповідно до інструкцій виробника із використанням спеціалізованого інструменту. Інформаційні розетки мають кольорове маркування відповідно до схем T568A або T568B. Під час монтажу необхідно використовувати однакову схему розведення пар на всіх ділянках мережі. Максимальна довжина розкрученої ділянки витої пари під час підключення не повинна перевищувати 1,5 см, оскільки це може погіршити параметри передачі даних.

Будь-який компонент нижчої категорії автоматично знижує характеристики всієї кабельної лінії. Для екранованого кабелю необхідно додатково виконувати правильне заземлення екрану відповідно до рекомендацій виробника. При горизонтальному прокладанні мідного

кабелю не допускається виконання зрощень або створення укорочених ділянок кабельної лінії.

Тестування кабельної системи. Після завершення монтажу рекомендується провести тестування кабельних ліній та налаштувати параметр NVP відповідно до фактичної довжини кабелю. Це дозволяє підвищити точність вимірювань та перевірити відповідність кабельної системи встановленим стандартам.

У даному проєкті комп'ютерна мережа буде прокладатися над підвісною стелею із подальшим опусканням кабельних ліній у пластикових коробах до робочих місць користувачів.

2.5 Обґрунтування вибору операційних систем та програмного забезпечення для серверів та робочих станцій в мережі

Для організації роботи комп'ютерної мережі в даній кваліфікаційній роботі було обрано операційну систему Windows 10. Вибір даної операційної системи обумовлений її широким розповсюдженням, стабільністю роботи та підтримкою сучасних мережевих технологій.

Операційна система Windows 10 має зручний графічний інтерфейс, що значно спрощує роботу користувачів та адміністрування мережі. Вона підтримує всі основні мережеві протоколи, служби спільного доступу до файлів і принтерів, а також забезпечує стабільну роботу в локальних та бездротових мережах.

Важливою перевагою даної операційної системи є її сумісність із сучасним апаратним забезпеченням, мережевими пристроями та прикладним програмним забезпеченням, яке використовується на підприємстві. Windows 10 підтримує автоматичне встановлення драйверів, засоби захисту інформації, віддалене адміністрування та регулярне оновлення системи безпеки.

Ще однією перевагою є підтримка технологій VLAN, VPN, Wi-Fi та засобів централізованого керування користувачами й мережевими ресурсами. Це дозволяє забезпечити стабільну роботу комп'ютерної мережі та високий рівень інформаційної безпеки.

Крім цього, операційна система має невисокі вимоги до апаратних ресурсів у порівнянні з новішими версіями, що дозволяє ефективно використовувати наявні персональні комп'ютери підприємства без необхідності значної модернізації обладнання.

Таким чином, використання Windows 10 у даній кваліфікаційій роботі є доцільним рішенням, оскільки дана операційна система забезпечує стабільність роботи, підтримку сучасних мережевих технологій, простоту адміністрування та сумісність із програмним і апаратним забезпеченням підприємства.

В якості серверної операційної системи у кваліфікаційній роботі було обрано Ubuntu 24.04 LTS. Вибір цієї операційної системи обумовлений її високою стабільністю, надійністю та широкими можливостями для організації серверної інфраструктури комп'ютерної мережі.

Операційна система Ubuntu 24.04 LTS є сучасною серверною платформою на базі Linux, яка підтримує велику кількість мережевих служб та серверного програмного забезпечення. Вона широко використовується для побудови файлових серверів, вебсерверів, FTP-серверів, серверів баз даних та систем централізованого адміністрування.

Однією з головних переваг даної операційної системи є її безкоштовне розповсюдження та відкритий програмний код. Це дозволяє зменшити витрати на ліцензійне програмне забезпечення та забезпечує можливість гнучкого налаштування серверного середовища відповідно до потреб підприємства.

Ubuntu 24.04 LTS характеризується високим рівнем інформаційної безпеки, стабільною роботою під великим навантаженням та підтримкою

сучасних мережевих технологій. Операційна система підтримує роботу служб DHCP, DNS, FTP, Samba, VPN, VLAN, а також засоби віддаленого адміністрування через SSH.

Важливою перевагою є невисокі системні вимоги та ефективне використання апаратних ресурсів сервера. Це дозволяє забезпечити стабільну роботу серверного обладнання навіть при значній кількості одночасних підключень користувачів.

Крім цього, Ubuntu 24.04 LTS має тривалий термін офіційної підтримки (LTS), регулярні оновлення безпеки та велику кількість технічної документації. Це спрощує адміністрування системи, підвищує надійність роботи мережі та забезпечує можливість подальшого розвитку серверної інфраструктури.

Таким чином, використання Ubuntu 24.04 LTS у кваліфікаційній роботі є доцільним рішенням, оскільки дана операційна система забезпечує високу продуктивність, стабільність, безпеку та підтримку сучасних мережевих сервісів.

2.6 Тестування мережі

Тестувати комп’ютерні мережі можна за допомогою різних методів та тестів. Одним з поширених варіантів є тест на проникнення, що являє собою метод оцінювання захищеності комп'ютерної системи чи мережі шляхом часткового моделювання дій зовнішніх зловмисників з проникнення у неї (які не мають авторизованих засобів доступу до системи) і внутрішніх зловмисників (які мають певний рівень санкціонованого доступу). Цей процес включає активний аналіз системи з виявлення будь-якої потенційної вразливості, що може виникати внаслідок неправильної конфігурації системи, відомих і невідомих дефектів апаратних засобів та програмного забезпечення, чи оперативне відставання в процедурних чи техні-

чних контрзаходах. Цей аналіз проводиться з позиції потенційного нападника і може включати активне використання вразливостей.

Проблеми безпеки, що були виявлені в ході тесту на проникнення, представляються власнику системи. Ефективний тест на проникнення поєднає цю інформацію з точною оцінкою потенційного впливу на організацію і окреслить межі технічних і процедурних контрзаходів для зменшення ризиків.

Тест на проникнення є корисним з кількох причин:

- визначення можливості певного набору атак;
- виявлення вразливостей вищого ризику, які є результатом комбінації вразливостей меншого ризику, що використовуються в певній послідовності;
- виявлення вразливостей, які може бути важко або неможливо знайти за допомогою автоматизованої мережі або застосування програмного забезпечення із сканування вразливостей;
- оцінювання величини потенційного впливу успішних атак на бізнес;
- тестування здатності захисників мережі успішно виявляти і реагувати на атаки;
- надання доказів на підтримку збільшення інвестицій у персонал і технології безпеки.

Тести на проникнення є складовою частиною повного аудиту безпеки.

Основне завдання тесту на проникнення - ідентифікація максимально можливого числа вразливостей інформаційної системи (ІС) за обмежений час при певних умовах і стані ІС. При проведенні тесту на проникнення вирішуються завдання:

- оцінка поточного стану системи захисту інформації ІС;
- виявлення вразливостей інформаційної системи;

- використання виявлених вразливостей для отримання несанкціонованого доступу чи здійснення несанкціонованого впливу на інформацію для демонстрації наявності вразливостей і існування високоймовірної загрози інформаційної системи;
- вироблення рекомендацій щодо підвищення ефективності захисту інформації в ІС.

В якості об'єкта дослідження може бути вибраний як зовнішній периметр мережі, так і окремо запущений сервіс або хост.

Вибирається режим тестування на основі рівня початкових знань виконавця про тестованої системі (Black Box або White Box) і рівня інформованості замовника про випробування (режим Black Hat або White Hat).

При виборі рівня Black Box виконавцю відомий лише діапазон зовнішніх IP-адрес. Даний підхід максимально наближений до дій хакера, дані про тестованому об'єкті будуть збиратися за допомогою відкритих джерел, соціальної інженерії і т.д. У режимі White Box доступна виконавцю інформація значно ширше. У цій ситуації фахівцям може бути надано документація, вихідні коди, структура мережі, а також повний доступ до об'єкту.

У режимі Black Hat про проведення робіт знають тільки керівники служби ІБ. У такому випадку вдається перевірити рівень оперативної готовності до атак мережевих адміністраторів та адміністраторів ІБ.

У режимі White Hat виконавці працюють в постійному контакті зі службою ІБ замовника, ІТ-фахівці замовника не перешкоджають виконанню необхідних тестів. і основне завдання зводиться до виявлення можливих вразливостей і оцінки ризику проникнення в систему.

Відносні переваги цих підходів обговорюються. Тестування методом чорної коробки імітує атаку того, хто не знайомий з системою. Тестування методом білої коробки моделює, що може статися під час «внутрішньої

роботи», або після «витоку» конфіденційної інформації, коли зловмисник має доступ до вихідного коду, мережних схем, і, можливо, навіть деякі паролі.

Тест на проникнення повинен проводитися на будь-якій комп'ютерній системі, яка буде розгорнута у ворожому середовищі, зокрема, на будь-якому інтернет-сайті, перш ніж він буде діяти. Це забезпечує рівень практичної гарантії того, що зловмисник не зможе проникнути в систему.

Звіт, що надається Замовнику за результатами проведення тесту на проникнення, містить детальний опис проведених робіт, всі виявлені вразливості системи і способи їх реалізації. Також звіт містить конкретні рекомендації щодо усунення даних вразливостей.

Рекомендується щорічно проводити тест на проникнення з метою виявлення нових вразливостей і для підтвердження реалізації рекомендацій, виданих в попередніх тестах. Тест на вторгнення може бути початковим етапом аудиту інформаційної безпеки компанії, на підставі якого можливі розробка політики інформаційної безпеки та впровадження систем захисту IT-ресурсів компанії.

Крім того, тест на проникнення проводиться в рамках аудиту інформаційної системи на відповідність стандарту захисту інформації PCI DSS в індустрії платіжних карт. Тестування на проникнення методом чорної коробки корисне в тих випадках, коли тестувальник бере на себе роль зовнішнього хакера і намагається проникнути в систему без достатніх знань про неї.

Тестування на проникнення може бути безцінним методом для програми інформаційної безпеки будь-якої організації. Тестування на проникнення методом білої коробки часто робиться, як повністю автоматизований недорогий процес. Тестування на проникнення методом чорної коробки є трудомісткою діяльністю і вимагає спеціальних знань, щоб мінімізувати ризик для цільових систем. Як мінімум, це може уповільнити час відгуку

мережі організації через сканування мережі та її вразливостей. Крім того, існує можливість, що система може бути пошкоджена чи виведена з ладу в процесі тестування на проникнення. Хоча цей ризик знижується за рахунок використання досвідчених тестувальників, він ніколи не може бути повністю усунутий.

OSSTMM (Open Source Security Methodology Manual) являє собою рецензовану методологію проведення тестів безпеки. OSSTMM випадки тестів діляться на п'ять каналів, які в сукупності тестують: управління інформацією та даними, рівні безпекової обізнаності персоналу, рівні управління шахрайством та соціальною інженерією, комп'ютерні та телекомунікаційні мережі, бездротові пристрої, мобільні пристрої, контроль безпеки фізичного доступу, фізичні місця розташування, такі як будівлі, периметри і військові бази.

OSSTMM зосереджується на технічних деталях: які саме елементи повинні бути перевірені, що робити до, під час і після тесту безпеки, як виміряти результат. OSSTMM також відомий своїми правилами ведення “бойових дій” (англ. Rules of Engagement), які визначають для тестувальника і клієнта, як тест повинен правильно протікати, починаючи з заперечення помилкових повідомлень від тестувальників, закінчуючи тим як клієнт може очікувати на отримання звіту. Нові тести для кращої міжнародної практики, закони, правила і етичні проблеми регулярно додаються та оновлюються.

NIST (National Institute of Standards and Technology) обговорює тестування на проникнення у документі SP800-115. Методологія NIST є менш вичерпною ніж OSSTMM, проте вона є кращою для прийняття регулюючими органами. З цієї причини NIST посилається на OSSTMM.

Роботи по тесту на проникнення включають в себе ряд послідовних етапів:

- Аналіз відкритих джерел
- Інструментальне сканування
- Аналіз / оцінка виявлених вразливостей і вироблення рекомендацій
- Підготовка звіту

2.7 Захист комп’ютерної мережі

Безпека мережі — заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу. Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів. Мережева безпека включає в себе дозвіл на доступ до даних в мережі, який надається адміністратором мережі. Користувачі вибирають або їм призначаються ID і пароль або інші перевірки автентичності інформації, що дозволяє їм здійснити доступ до інформації і програм у рамках своїх повноважень. Мережева безпека охоплює різні комп'ютерні мережі, як державні, так і приватні, які використовуються в повсякденних робочих місцях для здійснення угод і зв'язків між підприємствами, державними установами та приватними особами. Мережі можуть бути приватними, такими як всередині компанії або відкритими, для публічного доступу. Мережева безпека бере участь в організаціях, підприємствах та інших типів закладів. Найбільш поширений і простий спосіб захисту мережевих ресурсів є присвоєння їм унікального імені та відповідного паролю.

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

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

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

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

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

Система безпеки мережі:

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

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

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

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

Засоби захисту комп'ютерних мереж:

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

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

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

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

Даний пункт написано за матеріалами: «Організація комп'ютерної безпеки та захисту інформації» https://lektsii.org/3-135530.html

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкція по установці Ubuntu 24.04 LTS сервер

Для установки Ubuntu 24.04 LTS Сервера качаємо образ на сторінці офіційного сайту, записуємо скачаний образ дистрибутива на USB і завантажується з нього.

У першому вікні, вибираємо мову установки.(див. рис. 3.1)

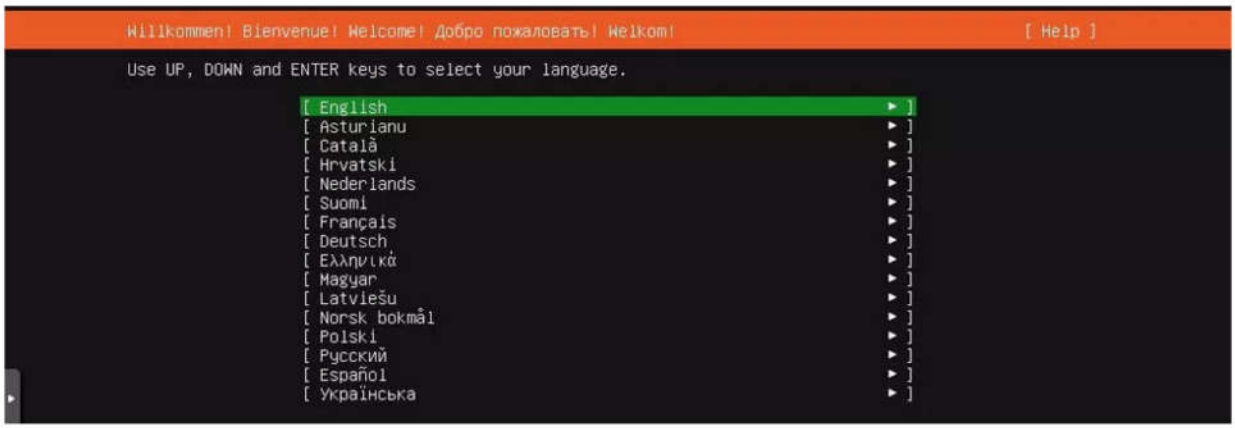


Рисунок 3.1 — Початкове вікно інсталятора. Вибір мови

На наступному етапі буде запропоновано використовувати дійсний інсталятор, або оновити його. Оновлення відбувається у фоновому режимі і займає не більше 10 секунд, поновіть його (див. рис. 3.2):

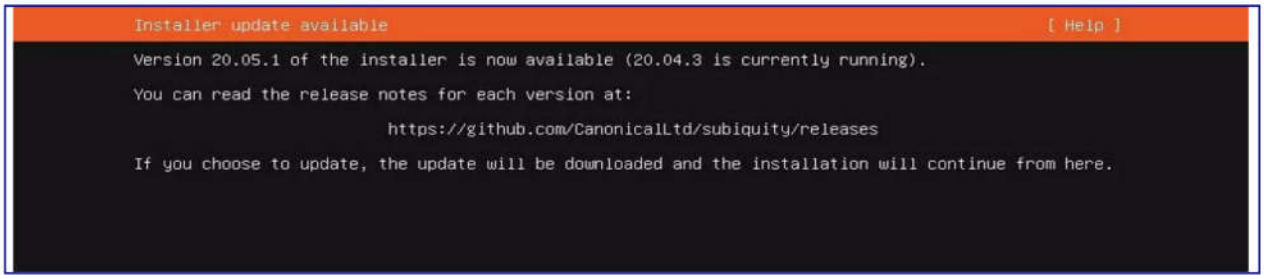


Рисунок 3.2 — оновлення інсталятора

Виберіть розкладку клавіатури.

Вибираємо мову розкладки:

Налаштуйте мережу. За замовчуванням, отримання IP адреси налаштоване по DHCP. У нашому прикладі ми будемо використовувати статичний IP адрес . Використовуючи інтуїтивно зрозумілу навігацію, заповніть необхідні поля(див. рис. 3.3)

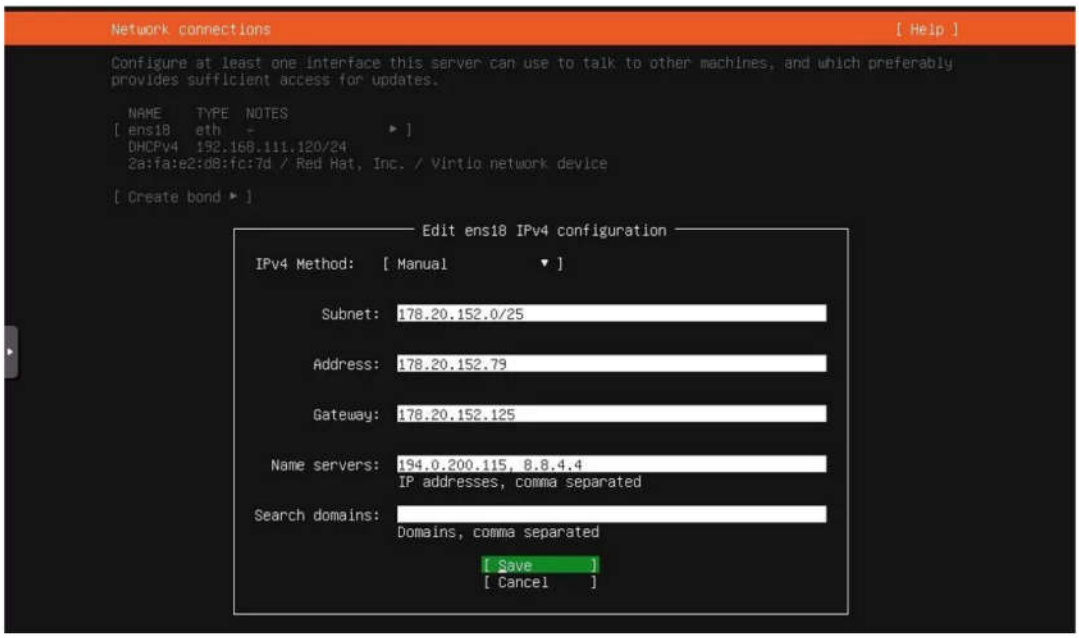


Рисунок 3.3 — Налаштування IP адресації

Якщо доступ в інтернет у вас здійснюється через proxy-сервер, вкажіть його:Вказівка проксі-сервера Далі, установник запропонуємо вам найближче дзеркало (Mirror), виходячи з вашого регіонального розташування. Залиште запропоноване за замовчуванням, або вкажіть свій.

На цьому етапі буде запропоновано розмітити дисковий простір. Вибравши «Use an entire disk» установник сам розмітить диски в автоматичному режимі. Залежно від завдань, ви можете виконати розбивку розділів на власний розсуд, вибравши «Custom storage layout».

Наступний приклад для наочності, виносити розділ boot окремо немає необхідності, ви можете все віддати під корінь «/», що буде рівнозначно «Use an entire disk».

Ви можете зробити окремим розділом boot або swap, вибрати формат файлової системи.

Так само є можливість створення LVM розділів. Меню інтуїтивно зрозуміле (див. рис. 3.4):

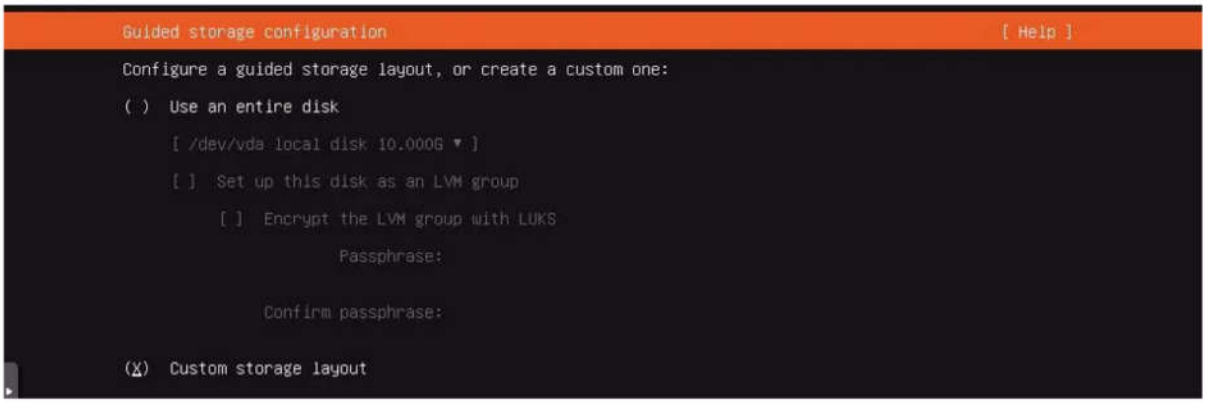


Рисунок 3.4 — Розбиття дискового простору

Вкажіть ім'я сервера і призначені для користувача дані для доступу до сервера.

Ви можете вибрати будь-якого користувача крім «root» і «admin», які зарезервовані системою.

Так само придумайте складний пароль, він повинен бути не менше 10 символів, включати в себе малі і великі символи латинського алфавіту, а так само цифри і спецсимволи.

Установка призначених для користувача даних

Відзначте установку OpenSSH Server, для можливості віддаленого підключення до нього, і натисніть «Done»:

Перед вами з'явиться довгий список того що можна встановити «з коробки».

Дуже цікавий етап, тут доступна і інтеграція з Kubernetes 1.18, etcd, інтеграція з Google Cloud, Postgresql10, Prometheus і багато чого іншого.

Вибирати компоненти для установки потрібно усвідомлено, за умови, що вам це дійсно необхідно для задач.

По закінченню установки, внизу інтерактивної консолі з'явиться «Reboot».

Вийміть носій з монтажником і виконайте перезавантаження сервера.

Первісне перезавантаження займе більш тривалий час, ніж це буде в подальшому.

Будуть ініційовані служби snapd, виконається ініціалізація пристроїв cloud-init та інше.

Все залежить від того, яким чином встановлюється Ubuntu, на гіпервізора, або baremetall. По закінченню ви побачите вікно аутентифікації в систему. Так само, сервер буде доступний по ssh.

Налаштування сервера

При підключенні, встановіть мінімальний набір утиліт, які знадобляться для роботи:

root @ dedicated: ~ # apt-get update

root @ dedicated: ~ # apt-get install atop wget ntp vim net-tools -y

Підключення до сервера по ssh

Перше, на що варто звернути увагу, це те, що в Ubuntu користувач root відключений від аутентифікації.

Це виконано з точки зору безпеки.

Підключення до сервера відбувається по імені користувача, який вказаний при установці:

admt @ freehost: ~ $ ssh user@178.20.152.78

user@178.20.152.78's password:

Щоб потрапити в режим суперкористувача, введіть наступну команду, яка проситиме пароль користувача user і перемкне в суперкористувача:

user @ dedicated: ~ # sudo su

[Sudo] password for user: **********

root @ dedicated: / home / user #

Якщо з якихось причин ви хочете дозволити доступ користувача root при підключенні по ssh, то змініть для нього пароль:

root @ dedicated: ~ # passwd root

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

root @ dedicated: ~ #

Потім в конфігураційному файлі / etc / ssh / sshd_config розкоментуйте рядок PermitRootLogin вказавши значення yes:

PermitRootLogin yes

Однак, з метою безпеки сервера, доступ за логіном root краще не надавати.

Налаштування мережевих інтерфейсів

Починаючи з Ubuntu 18.04 налаштування мережевих інтерфейсів відбувається не в звичному каталозі / etc / network / interfaces як це реалізовано в Debian-подібних дистрибутивах, а в каталозі / etc / netplan /. Після установки ОС, в ньому буде згенеровано конфігураційний файл 00-installer-config.yaml

Якщо конфігураційний файл з якоїсь причини порожній, згенеруйте го:

root @ dedicated: ~ # netplan generate

Для прикладу, виконаємо з ним деякі операції. Перейменуємо його у більш зручний вид:

root @ dedicated: ~ # mv /etc/netplan/00-installer-config.yaml /etc/ netplan/01-netcfg.yaml

Застосувати налаштування:

root @ dedicated: ~ # netplan apply

Конфігураційний файл має наступний вигляд:

файл конфігурацій

Він має формат Html і чутливий регістру. При конфігурації файлів даного формату табуляція неприпустима. Тільки парна послідовність пробілів і структура успадкування директив, інакше, ви отримаєте синтаксичну помилку.

У нашому прикладі, мережевий інтерфейс має назву eth0, але при інсталяції Ubuntu він мав назву enp0s8. Перейменувати в конфіг мережевий інтерфейс недостатньо. Так само слід правити завантажувач grub:

root @ dedicated: ~ # mcedit / etc / default / grub

знайдіть і відредагуйте значення:

GRUB_CMDLINE_LINUX = "net.ifnames = 0 biosdevname = 0"

root @ dedicated: ~ # grub-mkconfig -o /boot/grub/grub.cfg

root @ dedicated: ~ # reboot

Видалення непотрібних компонентів

root @ dedicated: ~ # echo 'datasource_list: [None]' | sudo -s tee /etc/ cloud/cloud.cfg.d/90_dpkg.cfg

root @ dedicated: ~ # apt-get purge cloud-init -y

root @ dedicated: ~ # rm -rf / etc / cloud /

root @ dedicated: ~ # rm -rf / var / lib / cloud /

Пакетний менеджер snap

Давайте так само, командою lsblk відобразимо наші носії пам'яті:

Відображення дискових пристроїв

Починаючи з версії 16.04, Ubuntu все наполегливіше намагається просунути менеджер управління пакетами snap. Наведемо коротке пояснення з офіційного сайту розробників:

«Snap пакети Ubuntu містять саму програму, а також всі її залежності. Це має кілька переваг перед звичайними deb або rpm пакетами, обробними залежності. А головне, з них - розробник може бути впевнений що немає ніяких регрессий через зміни версій бібліотек в системі »

Snap це зручна річ, і ми рекомендуємо з ним ознайомитися, документація Ubuntu досить інформативна як на російськомовних, так і на англомовних ресурсах.

Відобразимо список встановлених пакетів, які встановилися при інсталяції:

root @ dedicated: ~ # snap list

Якщо нам щось не потрібно, видалимо:

root @ dedicated: ~ # snap remove lxd

root @ dedicated: ~ # snap remove core18

Додати пакет можна наступним чином:

root @ dedicated: ~ # snap install docker

Оновити всі пакети:root @ dedicated: ~ # snap refresh

Оновити певний пакет:

root @ dedicated: ~ # snap refresh docker

Подивитися список доступних пакетів:

root @ dedicated: ~ # snap changes

Замість snap можете використовувати пакетний менеджер apt. Якщо у вас snapd не встановлено, встановити його можна в такий спосіб:

root @ dedicated: ~ # apt install snapd

Підключення swap розділу і настройка кешування

Для початку переконайтеся, що він не підключений:

root @ dedicated: ~ # swapon —show

Якщо список порожній, створіть файл підкачки, наприклад 2Gb. Змініть права, і активуйте його. Порядок команд наступний:

root @ dedicated: ~ # fallocate -l 2G / swapfile

root @ dedicated: ~ # sudo chmod 600 / swapfile

root @ dedicated: ~ # mkswap / swapfile

root @ dedicated: ~ # swapon / swapfile

Перевірка результату:

root @ dedicated: ~ # swapon -show

root @ dedicated: ~ # free -h

Налаштуємо swappiness. Параметр vm.swappiness за замовчуванням має значення 60, і контролює відсоток вільної пам'яті. Він контролює значення, після якого почнеться активний скидання даних в swap. Значення «60» означає наступне: 100-60 = 40%. Іншими словами, при завантаженні ОЗУ більш ніж 40%, дані почнуть кешedfnbcz в swap. Не існує оптимального значення, він обумовлений тільки конфігурацією вашого сервера. Якщо ОЗУ досить, це значення можна зменшити наступними командами:

root @ dedicated: ~ # sysctl vm.swappiness = 10

В кінці файлу /etc/sysctl.conf додайте наступний рядок:

vm.swappiness = 10

Налаштуйте кешування. Змініть параметр vfs_cache_pressure, що відповідає за швидкість видалення індексів з кеша. За замовчуванням це значення дорівнює 100. Так як звернення до індексів задоволене часте, це значення ви можете зменшити:

root @ dedicated: ~ # sysctl vm.vfs_cache_pressure = 50

В кінці файлу /etc/sysctl.conf додайте наступний рядок:

vm.vfs_cache_pressure = 50

Опціонально, не буде зайвим видалити підтримку IPv6. Навіть якщо ви цей протокол не використовуєте, деяке програмне забезпечення все одно його прослуховує і іноді трапляються збої в його роботі:

root @ dedicated: ~ # sh -c 'echo 1> / proc / sys / net / ipv6 / conf / all / disable_ipv6'

В кінці файлу /etc/sysctl.conf додайте наступний рядок, в залежності від інтерфейсів:

Відключення на всіх інтерфейсах

net.ipv6.conf.all.disable_ipv6 = 1

Відключення на певному інтерфейсі

net.ipv6.conf.eth0.disable_ipv6 = 1

3.2 Організація міжмережевого екранування на базі підсистеми Netfilter

У даному розділі досліджуються базові принципи та практичні аспекти конфігурування правил фільтрації пакетів для забезпечення безпеки серверної інфраструктури підприємства. При розгортанні політик безпеки особливу увагу слід приділяти коректності синтаксису, оскільки помилково застосоване обмежувальне правило може призвести до повної втрати віддаленого адміністративного доступу до операційної системи, що є критичним фактором при управлінні серверами у хмарних середовищах або ізольованих серверних кімнатах.

Для забезпечення термінологічної точності в межах наукового дослідження необхідно розмежувати поняття архітектури екранування. Безпосередньо вбудований у ядро операційної системи Linux міжмережевий екран називається Netfilter, тоді як утиліта iptables є лише високорівневим інтерфейсом (інструментом командного рядка) для управління та формування таблиць правил цієї підсистеми. На системному рівні комплекс Netfilter дозволяє реалізувати широкий спектр завдань захисту інформації. До них належать санкціонування або блокування вхідного та вихідного трафіку на основі аналізу номерів транспортних портів, мережевих протоколів (IPv4,

IPv6, TCP, UDP), а також ідентифікації джерела або призначення за унікальними апаратними MAC-адресами, індивідуальними IP-адресами чи цілими магістральними підмережами.

Основою архітектури Netfilter є три базові вбудовані ланцюжки перевірки пакетів: ланцюжок INPUT обробляє трафік, адресований безпосередньо серверу, OUTPUT відповідає за пакети, згенеровані самим сервером, а FORWARD здійснює транзитне пересилання даних через мережеві інтерфейси пристрою. Перегляд поточної конфігурації міжмережевого екрана з відображенням цифрових значень адрес і портів здійснюється за допомогою такої команди:

iptables -L -n

Для повної деінсталяції всіх існуючих правил та очищення таблиць фільтрації застосовується оператор скидання:

iptables -F

Зміна глобальної політики за замовчуванням визначає базову поведінку системи для пакетів, які не підпали під жодне з явних правил. В інженерній практиці використовується або концепція повної довіри (ACCEPT), або концепція максимального захисту (DROP), яка блокує весь невідомий трафік:

iptables -P INPUT DROP

iptables -P INPUT ACCEPT

Блокування доступу до сервера з боку конкретного мережевого вузла, цілої підмережі або за певним доменним ім'ям реалізується через додавання (ключ -A) заборонного правила із вказівкою цільової дії DROP:

iptables -A INPUT -s 123.45.67.89 -j DROP

iptables -A INPUT -s 123.45.0.0/16 -j DROP

iptables -A INPUT -s example.com -j DROP

Аналогічним чином здійснюється обмеження вихідної активності сервера шляхом аналізу адреси призначення за допомогою ключа -d у ланцюжку OUTPUT:

iptables -A OUTPUT -d 123.45.67.89 -j DROP

Синтаксис утиліти дозволяє застосовувати логічне заперечення у вигляді знака оклику, що є ефективним інструментом для створення правил виключення, коли доступ забороняється всім пристроям, окрім одного довіреного хоста управління:

iptables -A INPUT ! -s 123.45.67.89 -j DROP

Процедура видалення раніше створених правил (ключ -D) може виконуватися як за їхнім порядковим індексом у відповідному ланцюжку, так і на основі повної відповідності опису виконуваної дії:

iptables -D INPUT 1

iptables -D INPUT -s 123.45.67.89 -j DROP

Для точкового контролю сервісів використовується опція -p, яка визначає протокол транспортного або мережевого рівня (наприклад, TCP, UDP, ICMP), у поєднанні з селекторами портів відправника (--sport) або одержувача (--dport). Зазначений механізм дозволяє відкривати доступ лише до конкретних мережевих служб, наприклад, вебсервера:

iptables -A INPUT -p tcp --sport 80 -j ACCEPT

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

На відміну від ключа -A, який записує правило в кінець черги, оператор -I дозволяє інсталювати правило на початок ланцюжка або інтегрувати його у чітко визначену позицію, що має пріоритетне значення при обробці пакетів ядром:

iptables -I INPUT -p tcp --dport 22 -j ACCEPT

iptables -I INPUT 3 -p tcp --dport 443 -j ACCEPT

Оскільки конфігурація Netfilter за замовчуванням зберігається виключно в оперативній пам'яті, після перезавантаження операційної системи всі

налаштування анулюються. Для забезпечення персистентності (постійності) правил виконується процедура експорту поточної конфігурації у текстовий файл конфігурації, з якого згодом можна провести імпорт параметрів:

```
iptables-save > /etc/iptables.rules
iptables-restore < /etc/iptables.rules
```

Для автоматизації процесу відновлення політик захисту при ініціалізації мережевих інтерфейсів операційної системи Debian, у системній директорії передтопологічного підняття мережі створюється виконуваний сценарій оболонки командного процесора з призначенням відповідних прав доступу:

```
# Створення сценарію автоматичного завантаження правил
echo '#!/bin/sh' > /etc/network/if-pre-up.d/iptables
echo 'iptables-restore < /etc/iptables.rules' >> /etc/network/if-pre-up.d/iptables
echo 'exit 0' >> /etc/network/if-pre-up.d/iptables
# Надання файлу прав на виконання
chmod +x /etc/network/if-pre-up.d/iptables
```

Описаний комплекс заходів дозволяє організувати стійкий та автономний контур безпеки серверного обладнання підприємства, мінімізуючи ризики несанкціонованого доступу до корпоративних даних з боку зовнішніх мереж.

3.3 Налаштування комутатора

Скрипт конфігурування головного комутатора ядра та агрегації (SW_2). Комутатор SW_2 агрегує трафік від усіх робочих груп та здійснює внутрішню маршрутизацію між віртуальними мережами. Відповідно до твоєї таблиці конфігурування портів:

- Порт 3: виділений під сервер S_2 (Бухгалтерія, VLAN 100).
- Порти 4, 5, 6: підключення периферійних комутаторів SW_1, SW_3, SW_4 (Режим Access, VLAN 30).

```
# Вхід у режим суперкористувача та конфігурування
enable
configure terminal

# Налаштування ідентифікатора пристрою
hostname Switch-Core-SW2

# Створення віртуальних локальних мереж (VLAN) згідно з планом адресації
vlan 30
 name Tech_Dept_and_Mgmt
vlan 60
 name Managers_VLAN
vlan 80
 name Conf_Hall_VLAN
vlan 90
 name Director_VLAN
vlan 100
 name Accounting_VLAN
exit

# КОНФІГУРУВАННЯ ФІЗИЧНИХ ІНТЕРФЕЙСІВ (Згідно з наданою таблицею портів)

# Порт 3: Підключення сервера S_2 (Бухгалтерія)
interface gigabitethernet 1/0/3
```

```
 description Connection_to_Server_S2
 switchport mode access
 switchport access vlan 100
 spanning-tree portfast
no shutdown

# Порт 4: Магістральний лінк на комутатор доступу SW_1
interface gigabitethernet 1/0/4
 description Link_to_Switch_SW1_Port16
 switchport mode access
 switchport access vlan 30
no shutdown

# Порт 5: Магістральний лінк на комутатор доступу SW_3
interface gigabitethernet 1/0/5
 description Link_to_Switch_SW3_Port16
 switchport mode access
 switchport access vlan 30
no shutdown

# Порт 6: Магістральний лінк на комутатор доступу SW_4 (через який підключена AP_1)
interface gigabitethernet 1/0/6
 description Link_to_Switch_SW4_Port16
 switchport mode access
 switchport access vlan 30
no shutdown
```

АКТИВАЦІЯ ІНТЕРФЕЙСІВ ТРЕТЬОГО РІВНЯ (L3) ДЛЯ МІЖ-VLAN МАРШРУТИЗАЦІЇ

Налаштування IP-адрес як шлюзів за замовчуванням (Default Gateways) для підмереж

```
interface vlan 30
 ip address 192.168.3.1 255.255.255.0
 description Gateway_Tech_Dept

interface vlan 60
 ip address 192.168.6.1 255.255.255.0
 description Gateway_Managers

interface vlan 80
 ip address 192.168.8.1 255.255.255.0
 description Gateway_Conf_Hall

interface vlan 90
 ip address 192.168.9.1 255.255.255.0
 description Gateway_Director

interface vlan 100
 ip address 192.168.10.1 255.255.255.0
 description Gateway_Accounting

# Увімкнення глобальної маршрутизації IPv4 між інтерфейсами
ip routing
```

Створення статичного маршруту за замовчуванням на граничний роутер підприємства

(Припускаємо, що IP-адреса LAN-інтерфейсу роутера — 192.168.3.254)

ip route 0.0.0.0 0.0.0.0 192.168.3.254

ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ТА БЕЗПЕКИ

Глобальна активація протоколу швидкого розгортання дерева дерева (RSTP)

spanning-tree mode rstp

Збереження поточної конфігурації в енергонезалежну пам'ять (NVRAM)

end

write memory

Скрипт конфігурування бездротової точки доступу (AP_1)

Точка доступу TP-Link EAP610 фізично підключена до 24-го порту комутатора SW_4. Згідно з твоєю схемою логічної адресації, сама точка доступу знаходиться в керуючому VLAN 30 (IP: 192.168.3.200), але повинна транслювати бездротову мережу для конференц-залу (VLAN 80).

Сценарій для первинного налаштування через консольний інтерфейс CLI (SSH-сесія):

Вхід у командний інтерфейс пристрою

enable

configure terminal

Системне маркування точки доступу

hostname AP-Conference-Hall1

```
# Налаштування статичного IP-інтерфейсу управління у VLAN 30
interface management
 vlan 30
 ip address 192.168.3.200 255.255.255.0
 gateway 192.168.3.1
 dns 8.8.8.8
exit

# Конфігурування корпоративної бездротової мережі для персоналу (Діапазон 5 ГГц)
wlan 1
 ssid "TechKhata_Staff"
 band 5g
 security wpa3-sae
 wpa-pre-shared-key "SecureStaffKey2026"
 # Трафік персоналу залишається у керуючому / технічному сегменті
 vlan-id 30
 channel-width 80mhz
 tx-power max
no shutdown

# Конфігурування бездротової мережі для конференц-зал (Діапазон 2.4 ГГц / 5 ГГц гібрид)
wlan 2
 ssid "TechKhata_Conf_Hall"
 band dual
 security wpa2-psk
 wpa-pre-shared-key "WelcomeConf2026"
```

```
 # Тегування гостьового та загального трафіку конференц-залу у VLAN 80
 vlan-id 80
 # Увімкнення ізоляції клієнтів всередині Wi-Fi (захист користувачів один від одного)
 client-isolation enable
 no shutdown

# Налаштування безшовного роумінгу (стандарти 802.11k/v/r) для мобільних пристроїв
 roaming fast-transition enable
 roaming k-v-assist enable

# Вказівка адреси центрального контролера Omada SDN для переходу в режим централізованого управління
 # (У ролі контролера виступає сервер S_2, що має IP 192.168.10.10)
 omada-controller inform-url http://192.168.10.10:8043/inform

# Збереження конфігурації та примусове перезавантаження для застосування параметрів
 save
 reboot
```

3.4 Інструкція з використання тестових наборів та тестових програм

Для діагностики мережі використовуються команди PING і TRACERT.

Якщо є підозра, що відсутній зв’язок з деяким вузлом мережі, то команда PING (Packet Internet Groper)– перша, до якої необхідно звернутись. З допомогою цієї команди, можна перевірити правильність встановлення TCP/IP-з’єднання на локальному (віддаленому) комп’ютері.

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

Синтаксис команди в операційних системах сімейства Windows має наступний вигляд:

ping [ключі] адреса (ім’я) вузла

Ключі:

- t – продовжує відправку запитів , доки робота не буде перервана командою Ctrl-C;
- a – дозволяє використовувати імена вузлів замість IP-адрес;
- n число – вказує кількість exo запитів для відправки ;
- l довжина – вказує довжину exo – запитів;
- f – забороняє фрагментування пакету, визначає, чи пристрій змінював розмір пакету;
- i час – встановлює час життя пакету (Time to Live -TTL) відправляємих пакетів;
- v тип – встановлює тип обслуговування (TOS)
- r число – відображає шляхи для заданого числа переприйомів;
- s число – відмічає час для вказаного числа переприйомів;
- j список вузлів – маршрутизація пакетів через вказані вузли. Послідовні вузли можуть бути розділені шлюзами;

- k список вузлів - маршрутизація пакетів через вказані вузли. Послідовні вузли не можуть бути розділені шлюзами.
- w час – встановлює час очікування відповіді в мілісекундах.

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

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

Має наступний синтаксис :

tracert [ключі] ім’я вузла

Ключі :

- d – використовувати імена вузлів замість IP адрес;
- h максимальне число переприйомів – максимально допустиме число переприйомів для досягнення мети;
- j список вузлів - маршрутизація пакетів через вказані вузли. Послідовні вузли можуть бути розділені шлюзами. Вільний вибір шляху серед систем у вказаному списку;
- w час – встановлення часу очікування в мілісекундах.

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

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

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

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

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки комп'ютерної мережі для ПП "ТехноХата" 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	15
2	Монтаж кабельних каналів	Технік	15
3	Монтаж активного та пасивного мережевого обладнання	Технік	10
4	Тестування мережі. Моніторинг основних параметрів	Інженер	15

Продовження таблиці 4.1

1	2	3	4
5	Налагодження мережі та створення технічної документації	Інженер	5
Разом		-	70

Сумарний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі складає 70 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:

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

де T_c – тарифна ставка, грн.;

$K_г$ – кількість відпрацьованих годин.

Отже, основна заробітна плата для:

- керівника проекту: $З_{осн1} = 15 \cdot 150 = 2250{,}00$ *грн.*
- інженера: $З_{осн2} = 25 \cdot 120 = 3000{,}00$ *грн.*
- техніка: $З_{осн3} = 30 \cdot 100 = 3000{,}00$ *грн.*

Сумарна основна заробітна плата становить:

$$З_{осн} = 2250{,}00 + 3000{,}00 + 3000{,}00 = 8250{,}00 \text{ грн}$$

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

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

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

Отже, додаткова заробітна плата по категоріях працівників становить:

- керівника проекту: $З_{дод1} = 2250 \cdot 0{,}15 = 337{,}5$ *грн.*
- інженера: $З_{дод2} = 3000 \cdot 0{,}15 = 450{,}00$ *грн.*
- техніка: $З_{дод3} = 3000 \cdot 0{,}15 = 450{,}00$ *грн.*

Загальна додаткова заробітна плата становить:

$$З_{дод} = 337{,}5 + 450{,}00 + 450{,}00 = 1237{,}5 \text{ грн.}$$

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

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

$$В_{о.п} = 8250{,}00 + 1237{,}5 = 9487{,}5 \text{ грн}$$

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.

$B_{с.з.} = 9487,5 \cdot 0,322 = 2087,25$ *грн.*

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додатк. зароб. плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тариф. Ставка, грн.	К-сть відпр. год.	Факт. нарах. з/пл., грн.			
1	2	3	4	5	6	7	8
1	Керівник проекту	150	15	2250,00	337,5	-	-
2	Інженер	120	25	3000,00	450,00		
3	Технік	100	30	3000,00	450,00	-	-
Разом				2375,00	1237,50	2087,25	11574,75

Отже, загальні витрати на оплату праці становлять 11574,75 грн.

4.3 Розрахунок матеріальних витрат

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

$$M_{Bi} = q_i \cdot p_i \qquad (4.5)$$

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{Bi} \qquad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. вим.	к-сть	Ціна 1-ці, грн.	Загальна сума витрат, грн.
1	TP-Link TL-SG1016DE	шт	3	3700,00	11100,00
2	TP-Link TL-SG3428X	шт	1	9400,00	9400,00
3	TP-Link EAP610	шт	1	2800,00	2800,00
4	ARTLINE Business R17v24-2	шт	1	72900,00	72900,00
5	Комутаційна шафа	шт	1	7800,00	7800,00
6	Кабель мережевий	шт	5	5400,00	27000,00
7	Короб 20х40х2000	шт	60	120,00	7200,00
8	Конектор	шт	70	25,00	1750,00
Разом					139950,00

Отже, загальна сума матеріальних витрат дорівнюють

$$З_{м.в} = 139950{,}00\ грн.$$

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

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

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

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

Тому:

$З_е = 0{,}5 \cdot 25 \cdot 15{,}94 = 199{,}25\ грн.$

4.5 Визначення транспортних затрат

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

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

де $Т_в$ – транспортні витрати.

Отже,

$Т_в = 139950{,}00 \cdot 0{,}08 = 11196{,}00 грн.$

4.6 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення.

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

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

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

Мінімально допустимі строки їх використання 2 роки.

Для визначення амортизаційних відрахувань застосовуємо формулу:

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

де A – амортизаційні відрахування за звітний період, грн.

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

$Н_А$ – норма амортизації, %;

T – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 25 год., балансова вартість ПК – 33000 грн., тому:

$A = 33000 \cdot 0,04 / 150 \cdot 25 = 220,00$ *грн*

4.7 Обчислення накладних витрат

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

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

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

де $Н_в$ – накладні витрати.

$Н_в = 9487,5 \cdot 0,5 = 4743,75$ *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	9487,5	7,47
Відрахування на соціальні заходи	2087,25	2,04
Матеріальні витрати	139950,00	80,10
Витрати на електроенергію	199,25	0,11
Транспортні витрати	11196,00	6,41
Амортизаційні відрахування	220,00	0,13
Накладні витрати	4743,75	3,74
Собівартість	167883,75	100

Собівартість (Св) НДР розрахуємо за формулою:

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

Отже, собівартість дорівнює

$$C_в = 167883,75 \text{ грн}$$

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

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

де $C_в$ – собівартість виконання НДР;

$Р_{рен.}$ – рівень рентабельності,

$ПДВ$ – ставка податку на додану вартість,

$Ц = 167883,75 \cdot (1+0,3) \cdot (1+0,2) = 261898,65$ 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), можна визначити за формулою 4.13 та термін окупності ($Т_{ОК}$), який можна визначити за формулою 4.14.

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

де $К_В$ – затрати на проект;

$Г_п$ – грошовий потік за t – ий рік;

^{t} – відповідний рік проекту;

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

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

$$ЧТВ = -167883,75 + 159514,9/(1+0,15) + 159514,9/(1+0,15)^2 = 91441,03$$

Термін окупності визначається за формулою:

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

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.

$$T_{ОК} = 1 + 29175,15/159514,9 = 1,2$$

Всі дані розрахунків внесемо в зведену таблицю 4.5 техніко-економічних показників.

Таблиця 4.5 - Техніко-економічні показники розробки мережі

№ п/п	Показник	Значення
1.	Собівартість, грн.	167883,75
2.	Плановий прибуток, грн.	94014,9
3.	Ціна, грн.	261898,65
4.	Чиста теперішня вартість, грн.	91441,03
5.	Термін окупності, рік	1,2

Загальна вартість розробленої комп’ютерної мережі становить 261898,65 грн. Термін окупності становить 1,2 роки.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

1. Організація державного та відомчого пожежного нагляду за об'єктами ІТ-інфраструктури ПП “ТехноХата”

Згідно з Кодексом цивільного захисту України (далі — Кодекс) діяльність із забезпечення пожежної безпеки є складовою виробничої та іншої діяльності посадових осіб і працівників підприємств, установ та організацій. Забезпечення пожежної безпеки суб’єкта господарювання покладається на власників та керівників таких суб’єктів господарювання.

Виробничі, житлові, інші будівлі та споруди, обладнання, транспортні засоби, що вводяться в дію чи експлуатацію після завершення будівництва, реконструкції або технічного переоснащення, а також технологічні процеси та продукція мають відповідати вимогам нормативно-правових актів з пожежної безпеки.

Центральний орган виконавчої влади, який здійснює державний нагляд у сфері техногенної та пожежної безпеки, уповноважений організовувати та здійснювати державний нагляд (контроль) щодо виконання вимог законів та інших нормативно-правових актів з питань техногенної та пожежної безпеки, цивільного захисту.

У суб’єктів господарювання приватної форми власності органи державного нагляду в сфері цивільного захисту контролюють виконання заходів щодо захисту населення та працівників на випадок надзвичайної ситуації, а також вирішення питань техногенної та пожежної безпеки, що стосуються прав та інтересів інших юридичних осіб і громадян.

Центральний орган виконавчої влади, яки й здійснює державний нагляд у сфері техногенної та пожежної безпеки, здійснює державний нагляд (контроль) шляхом проведення планових та позапланових перевірок відповідно до Закону України «Про основні засади державного нагляду

(контролю) у сфері господарської діяльності» від 5 квітня 2007 р. № 877-V (далі — Закон № 877).

Перевірки проводяться з метою здійснення контролю за додержанням суб'єктами господарювання вимог законодавства з питань цивільного захисту, техногенної та пожежної безпеки, виявлення порушень і запобігання виникненню надзвичайних ситуацій, захисту життя та здоров'я людей.

Вимоги законодавства щодо здійснення заходів держнагляду Законом України «Про тимчасові особливості здійснення заходів державного нагляду (контролю) у сфері господарської діяльності» від 7 грудня 2017 р. № 2246-VIII (далі — Закон № 2246) встановлено до 31 грудня 2018 року мораторій на проведення органами державного нагляду (контролю) планових заходів зі здійснення державного нагляду (контролю) у сфері господарської діяльності.

До 31 грудня 2018 року позапланові заходи державного нагляду (контролю) здійснюються органами державного нагляду (контролю) в таких випадках:

- за письмовою заявою суб'єкта господарювання до відповідного органу державного нагляду (контролю) про здійснення заходу державного нагляду (контролю) за його бажанням;
- за рішенням суду;
- у разі настання аварії, смерті потерпілого внаслідок нещасного випадку, що було пов'язано з діяльністю суб'єкта господарювання;
- у разі наст ання події, що має значний негативний вплив відповідно до критеріїв, затверджених Кабінетом Міністрів України, на права, законні інтереси, життя та здоров'я людини, захист навколи-

шнього природного середовища та забезпечення безпеки держави;

- для перевірки виконання суб’єктом господарювання приписів, розпоряджень або інших розпорядчих документів щодо усунення порушень вимог законодавства, виданих за результатами проведення попереднього заходу органом державного нагляду (контролю).

2. Вимоги електробезпеки до телекомунікаційних стійок та організація захисного заземлення апаратури

Згідно з ПУЕ в електроустановках використовують такі системи заходів:

- захисне заземлення;
- занулення;
- ізоляція струмопровідних частин;
- захисне вимикання;
- малі напруги;
- недоступність до неізольованих провідників та ін..

Ці засоби захисту не є універсальними , тому для створення безпечних умов праці необхідно застосовувати не один, а кілька засобів одночасно.

Захисне заземлення – це зумисне електричне з’єднання з землею металевих не струмопровідних частин, які можуть опинитись під напругою внаслідок пошкодження електричної ізоляції

Захисне заземлення – це захист людини від ураження струмом, якщо вона доторкнулася до металевих конструкцій електрообладнання, яке опинилося під напругою.

Захисна функція полягає в тому, що сила струму, що буде проходити по тілу людини буде безпечної величини тому, що опір заземлення дуже малий порівняно з опором людини.

Отже, для виконання захисної ролі заземлюючі пристрої повинні мати дуже малий опір. Відповідно до ПУЕ допустимий опір заземлюючих пристроїв має бути не більший за 4 Ом.

Захисне заземлення обов'язково влаштовують у електроустановках при напрузі:

- 380В і більше при змінному струмі;
- 440В і більше при постійному струмі;
- 42В перемінного і 110В постійного струму в зовнішніх установках, особливо небезпечних та в умовах з підвищеною небезпекою;
- незалежно від значення напруги у всіх вибухонебезпечних приміщеннях.

Залежно від розміщення заземлювачів відносно електрообладнання заземлюючі пристрої бувають виносні і контурні, природні і штучні.

Для штучних заземлювачів використовують сталеві труби Ф від 3 до 5см з товщиною стінок 3-5мм і довжиною від 2,5 до 3м; сталеві стержні Ф 10-12мм і довжиною до 10м; кутикову сталь 40х40мм довжиною від 2,5 до 5м і т. ін..

На кожний заземлюючий пристрій складається паспорт, який включає схему заземлення, технічні дані, результати перевірки стану, характер проведених ремонтних робіт і т. ін..

Технічний стан визначається шляхом зовнішнього огляду видимої частини та вимірюванням опору, який не повинен перевищувати допустиме значення. Планове вимірювання опору виконують перед початком його експлуатації, а потім один раз на рік та після кожного капітального

ремонту. Наземну частину оглядають один раз на шість місяців, а у вологих і особливо небезпечних умовах – один раз на три місяці.

Небезпеку ураження струмом можна ліквідувати шляхом швидкого відключення пошкодженої електроустановки. Для цього влаштовують занулення.

Занулення – це зумисне з'єднання металевих частин електроустановки, які зазвичай не перебувають під напругою з нульовим захисним провідником.

Це є основний засіб захисту людей від ураження струмом в установках напругою до 1000В. Захист полягає у тому, що при пробиванні ізоляції виникає коротке замикання, яке швидко вимикає пошкоджене електрообладнання від електричної мережі.

Головною умовою безпеки при експлуатації електроустановок є надійна ізоляція струмопровідних частин шаром діалектрика, який забезпечує їх надійність.

Опір ізоляції згідно з ПУЕ нормується і має досягати не менше 0,5МОм.

Матеріал ізоляції має відповідати умовам оточуючого середовища, бути стійким до агресивного середовища, вологи, нагрівання та механічного впливу, старіння і т. ін..

Стан ізоляції електричних установок відповідно до ПУЕ визначають шляхом періодичних оглядів та вимірюванням електричного опору.

Заземлення і занулення не завжди гарантує безпеку людей від ураження струмом. Для захисту використовують захисне відключення.

Захисне відключення – це швидкодіючий захист, який забезпечує автоматичне відключення електроустановки при виникненні в ній небезпеки ураження людини струмом. Цей вид захисту спрацьовує за 0,1 – 0,05с, а занулення 0,2с і більше.

При такому нетривалому проходженні струму через тіло людини безпечним є навіть струм 500 – 650мА.

Захисне вимикання може застосовуватись як основний вид захисту, або разом з заземленням і зануленням.

Захисне вимикання окремо чи сукупно з іншими засобами захисту виконує такі функції:

- захист при замиканні на землю або корпус обладнання;
- захист при появі небезпечних струмів витікання;
- захист при переході вищої напруги на сторону нижчої;
- автоматичний контроль кола захисного заземлення і занулення.

Для захисту персоналу, що обслуговує електроустановки, використовують спеціальні захисні засоби. Ці засоби умовно поділяються на ізолюючі, огороджуючи і запобігаючи. Ізолюючі в свою чергу поділяються на основні і допоміжні.

Для обслуговування електроустановок і мереж допускаються особи, не молодше 18 років, що пройшли медичний огляд та отримали кваліфікаційну групу з техніки безпеки. Для установок понад 1000В – IV групу, а для установок до 1000В III кваліфікаційну групу.

Існує цілий список застережень, чому не можна використовувати занулення.

Заборонено використовувати нульовий провід двопровідної системи в якості захисного (наприклад, використовуючи перемичку між нульовою і заземлюючою клемами в розетці).

По-перше, такі жили не завжди відрізняються кольором ізоляції, тому існує велика ймовірність переплутати фазний і нульовий провід, внаслідок чого на корпус електроприладу потрапляє фазна напруга.

По-друге, якщо нульовий провід в розетці відгорить (відпаде, відламається), через перемичку на корпус приладу знову ж таки потрапляє фазна напруга.

Наостанок слід зазначити, що в обох випадках йдеться про захист тільки побутових приладів. Якщо відбудеться контакт з оголеним фазним поводом стаціонарної проводки, це призведе до ураження струмом незалежно від того, застосовується в будинку занулення чи заземлення. Крім того, в багатьох випадках пошкодження ізоляції не призводить до короткого замикання, але на корпусі з'являється напруга достатня для того, щоб завдати шкоди здоров'ю користувача. Тому для повного захисту поряд з автоматичними вимикачами (плавкими запобіжниками) слід використовувати пристрої захисного відключення (диференційні реле або диференційні автомати).

3. Методи і засоби захисту персоналу ПП "ТехноХата" від негативного впливу фізичних негативних факторів

На багатьох заводах і фабриках виробництво пов'язане з постійним впливом на працівників несприятливих умов. Шкідливі та небезпечні виробничі фактори нерозривно пов'язані між собою. ВПФ — це ті фактори, які в результаті свого тривалого або короткочасного впливу на людину призводять до погіршення стану його здоров'я або до травми. На виробництвах з такими умовами праці різні нещасні випадки відбуваються досить часто.

ВПФ — це фактори, які, діючи на працівника, знижують його працездатність або призводять до різних захворювань, їх часто ще називають професійними хворобами. Варто зазначити, що межа між цими двома групами факторів досить умовна. При деяких умовах шкідливі виробничі фактори можуть стати небезпечними. Наприклад, підвищена вологість відноситься до несприятливих умов праці, вона може викликати різні

захворювання дихальної системи. Якщо людині доводиться в таких умовах працювати з електричним струмом, то це стає вже занадто небезпечно, а не просто шкідливо.

Класифікація шкідливих виробничих факторів

Всі фактори на будь-якому підприємстві можуть мати різне походження. Часто можна стикатися з несприятливими умовами праці, які виникають з вини керівництва. Це питання потребує особливої уваги з боку перевіряючих органів. Хочеться сподіватися, що велика частина небезпечних факторів має природне походження, і людині просто необхідно вжити всі заходи, щоб їх вплив був мінімальним. Всі шкідливі виробничі фактори ГОСТ поділяє на наступні групи:

- Фізичні.
- Хімічні.
- Біологічні.
- Психофізіологічні, до яких можна віднести важкі та напружені умови праці.

Можна відзначити, що немає чіткої межі між шкідливими та небезпечними факторами, вона завжди умовна і в будь-який момент може бути зруйнована.

Джерела шкідливих хімічних факторів

На виробництві завжди є технологічні процеси, обладнання, які є джерелом виділення ВПФ.

Фізичні фактори

На багатьох виробництвах просто неможливо уникнути впливу деяких факторів. Серед них особливе місце займають:

- Температура, висока вологість і випромінювання.
- Електромагнітні поля.
- Лазерне і ультразвукове випромінювання.
- Вібрація.

- Сильний шум.
- Освітлення, яке може бути як занадто інтенсивним, так і недостатнім, що однаково шкідливо для зору.
- Вплив пилу і аерозолів.
- Заряджений повітря.
- Працюючі частини обладнання.

Кожен фактор окремо начебто і не становить особливої небезпеки для здоров'я людини при короткочасному впливі. Але часто працівник перебуває тривалий час у їх оточенні, та ще відразу декількох, тому їх вплив стає цілком відчутним.

Шум і його вплив на людину

На підприємствах, де в цехах стоять верстати та інше обладнання, без шуму, як правило, не обходиться. Постійно працює техніка видає гучні звуки, які можуть змінювати свою інтенсивність. Якщо людина змушений регулярно зазнавати такого впливу, то це негативно позначиться на його здоров'ї. Від сильного шуму починає боліти голова, підвищується тиск, знижується гострота слуху. Зрештою, від таких умов знижується працездатність, з'являється втома, знижується увага, а це вже може призвести до нещасного випадку. Керівники на подібних підприємствах повинні подбати про своїх працівників, щоб постаратися хоч трохи зменшити негативний вплив шуму на організм. Для цього можна використовувати:

Глушники шуму.

Індивідуальні засоби захисту, наприклад навушники, беруші, шоломи.

Виробляти звукоізоляцію галасливих місць з допомогою використання захисних кожухів, обладнання кабінок.

Оздоблення приміщень звукопоглинаючими матеріалами.

Вплив вібрації та її усунення

Вібрація входить в перелік шкідливих виробничих факторів. Її можна класифікувати по декількох категоріях:

За способом передачі: загальна і локальна.

По своєму напрямку: вертикальна і горизонтальна.

По часу дії: тимчасова і постійна.

В результаті постійного впливу даного фактора починає страждати не тільки нервова система, а й опорно-рухова, і система аналізаторів. Робітники, які змушені працювати в таких умовах, часто скаржаться на головні болі, запаморочення, заколисування.

Для захисту від неї можна запропонувати наступні заходи:

Заміна обладнання на більш технологічне.

Використання м’яких покриттів на вібруючих частинах приладів або устаткування.

Установка агрегатів на грунтовний фундамент.

Хімічні фактори

Речовини з цієї групи можна розрізняти за наступним категоріям:

За своїм впливом на організм людини шкідливі та небезпечні виробничі фактори хімічної природи поділяються на:

- Токсичні. Діють негативно на весь організм, наприклад чадний газ, ртуть, свинець.
- Дратівливі. Такі речовини, як ацетон, хлор, оксиди азоту викликають подразнення слизових оболонок.
- Канцерогенні. Оксиди хрому, берилій зі своїми з’єднаннями можуть призводити до розвитку ракових клітин.
- Викликаючі алергічні реакції.
- Мутагенні. Провокують зміни на рівні ДНК клітини.

- Ті що впливають на репродуктивну функцію.

За способом надходження в організм:

- Через дихальну систему.
- Через ШКТ.
- Через шкіру та слизові оболонки.
- Фактори трудового процесу

До психофізіологічних факторів можна віднести тягар умов праці і його напруженість. Коли мова йде про важку працю, то мається на увазі:

- Велике навантаження на опорно-рухову, серцево-судинну, дихальну системи.
- Величина статичного навантаження.
- Число однакових рухів.
- Величина вантажів, які доводиться піднімати.
- Поза робітника під час виконання процесу.

Під напруженістю роботи мається на увазі навантаження на нервову систему, органи почуттів (більше аналізатори). Сюди можна віднести тривалу розумову роботу, монотонність виконуваних процесів, емоційні перевантаження. Все це шкідливі виробничі фактори, які, якщо розібратися, практично кожен з нас на своєму робочому місці відчуває в тій чи іншій мірі.

Часто буває так, що всі вжиті заходи не можуть забезпечити повністю безпечні умови праці, в цих випадках без застосування ЗІЗ просто не обійтися. Серед них можна виділити наступні категорії, які найбільш поширені у використанні:

Від вібрації можуть бути: рукавиці, надолонники, рукавички. Так як такий захист може знижувати ефективність праці за незручності роботи, то треба передбачати додаткові перерви.

Навушники від шуму. Але вони можуть знижувати здатність людини орієнтуватися в просторі, провокувати головні болі через здавлювання.

Респіратори і протигази. Тривалий час працювати в них дуже складно і незручно, тому слід шукати альтернативні засоби захисту.

Можна зробити висновок про те, що засоби індивідуального захисту, з одного боку, зменшують вплив шкідливих факторів, а з іншого — можуть створювати іншу небезпеку для здоров’я працівника.

Заходи безпеки. Вони спрямовані, насамперед, на те, щоб шкідливі виробничі фактори не надавали свого небезпечного впливу на людину. З цією метою на будь-якому підприємстві в обов’язковому порядку повинен проводитись інструктаж з безпеки. Дата проведення, зміст фіксуються у спеціальному журналі за підписом усіх інструктируемих і того, хто провів цей інструктаж.

ВИСНОВКИ

В ході роботи над кваліфікаційною роботою спроектовано комп'ютерну мережу ПП "ТехноХата". 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.

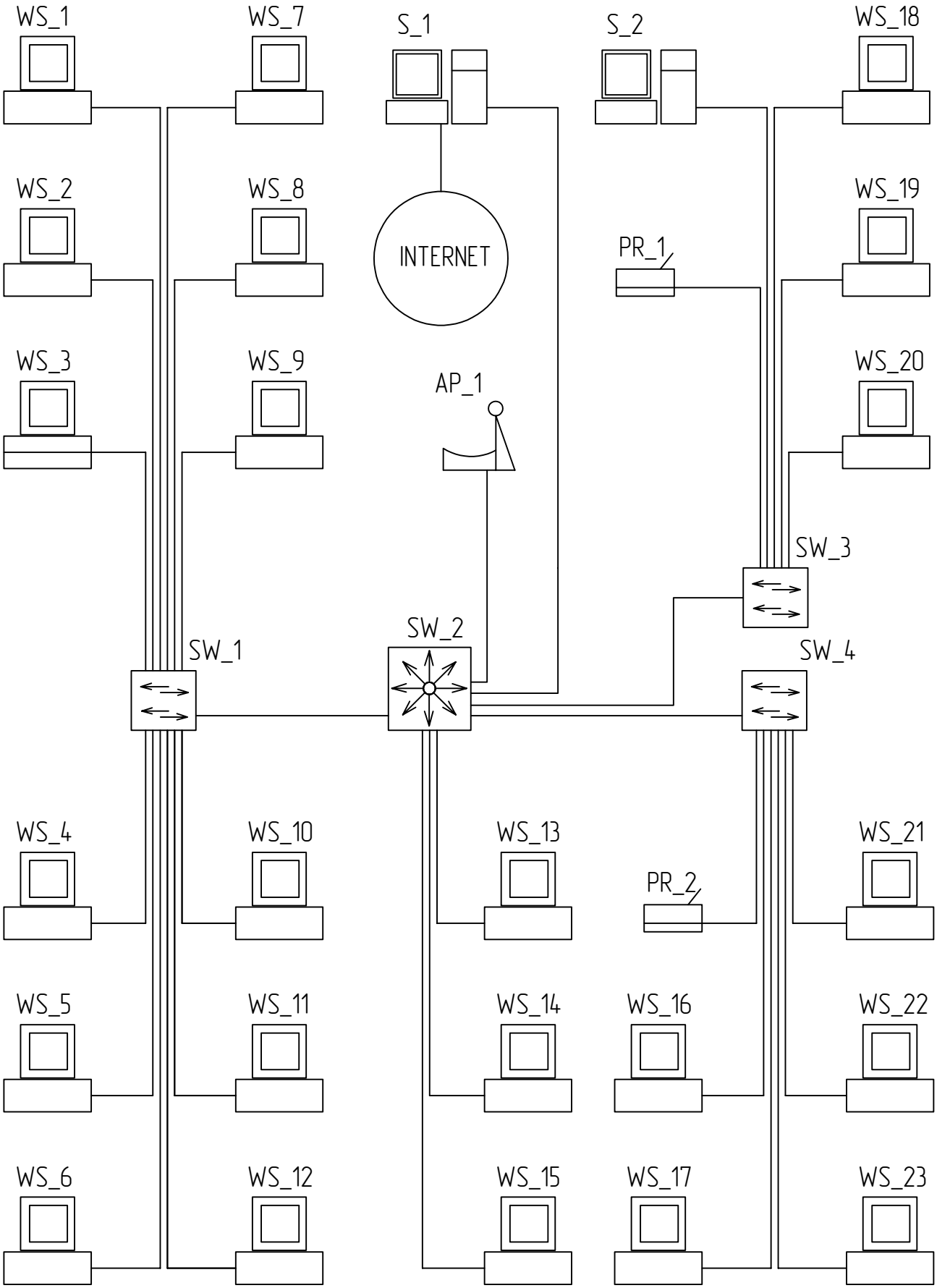
Останній розділ кваліфікаційної роботи описує питання охорони праці, та техніки безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Райський Ю.С., Олексюк В.П., Балик А.В. Адміністрування комп'ютерних мереж і систем: Навч. пос. Тернопіль: Навчальна книга Богдан. 2010. 196 с.
2. Городецька, О. С. Г70 Комп’ютерні мережі : навчальний посібник / О. С. Городецька, В. А. Гикавий, О. В. Онищук. Вінниця : ВНТУ, 2017. 129 с.
3. Усатенко, Каченюк, Терехова. Выполнение электрических схем по ЕСКД: Справочник. М.: Издательство стандартов, 1989. 325с.
4. Тхір І.Л., Юзьків А.В., Калушка В.П. Посібник користувача ПК. Тернопіль: Технічний коледж ТДТУ, 2005. : іл.
5. Чирва Ю.О., Баб'як О.С. Безпека життєдіяльності Навчальний псібник.-К.: Атаса, 2001.-304 с.
6. Комп’ютерні мережі URL: https://comp-net.at.ua/index/topologija_komp_39_juternikh_merezh/0-6 (дата звернення:4.04.2026).
7. Побудова та адміністрування INTRANET-мереж URL:https://ami.lnu.edu.ua/wp-content/uploads/2018/01/Intranet1.pdf (дата звернення:4.05.2026).
8. Побудова та адміністрування INTRANET-мереж URL: https://trigada.ucoz.com/publ/prokladka_vitoj_pary/1-1-0-229 (дата звернення:14.05.2026).
9. Тестування та діагностика локальних мереж. URL:https://skomplekt.com/tools/134446.html/ (дата звернення:24.05.2026).
10. Як налаштувати точку доступу URL: https://ntools.com.ua/ information/ faq/kak-nastroit-tochku-dostupa-ubiquiti- unifi-ap (дата звернення: 18.05.2026).

11. Домашнє файлосховище на базі FreeNAS URL: https://3dnews.ru/619273 (дата звернення:14.04.2026).
12. Монтаж кабеля витої пари URL: https://e-server.com.ua/sovety/123-pravilnyj-montazh-kabelya-vitoj-pary (дата звернення:23.05.2026).

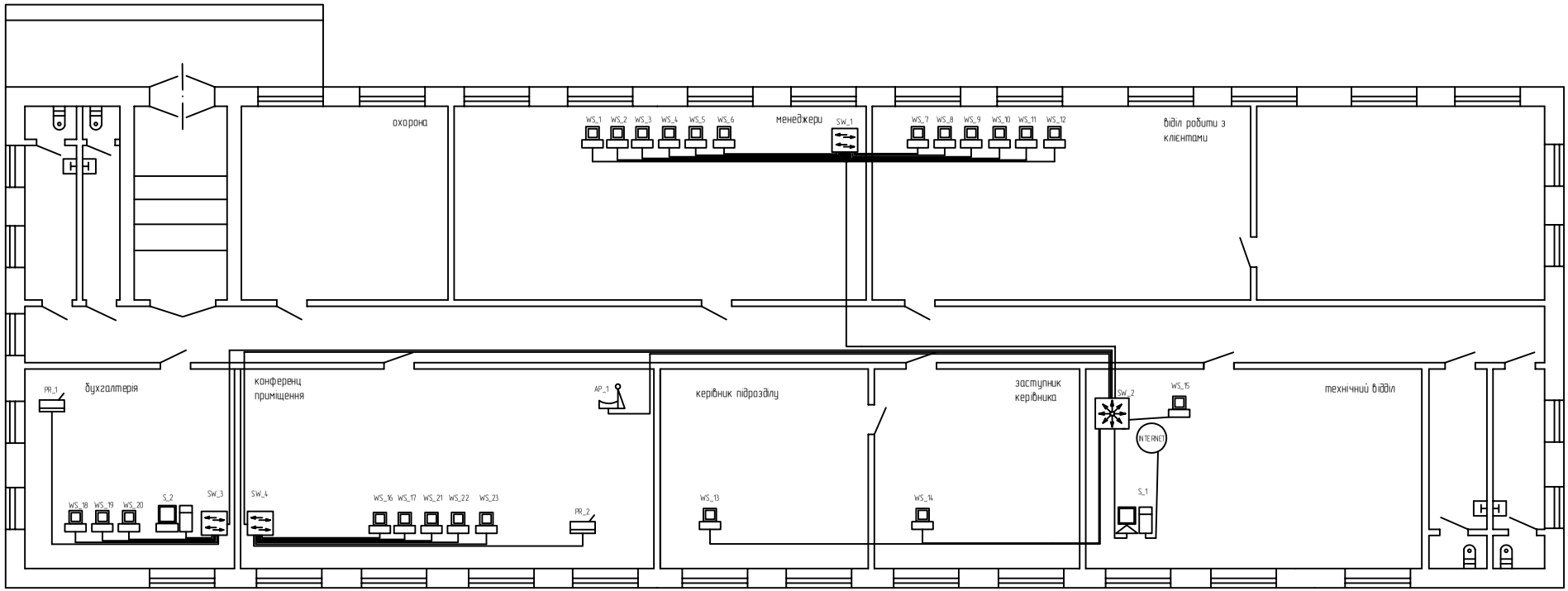
2026.КВР.123.412.05.0000 /ЛТ



					2026.КВР.123.412.05.00.00 /ЛТ		
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі ПП "ТехноХата" /Логічна топологія	Літ.	Маса	Масшт.
Розроб.		Кузь Р. А.						1:100
Керів.		Луж. В. С.				Н		
Н.контр.		Язькіб 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\Vlan
1	WS_1	192.168.6.1	255.255.255.0	WG2\60
2	WS_2	192.168.6.2	255.255.255.0	WG2\60
3	WS_3	192.168.6.3	255.255.255.0	WG2\60
4	WS_4	192.168.6.4	255.255.255.0	WG2\60
5	WS_5	192.168.6.5	255.255.255.0	WG2\60
6	WS_6	192.168.6.6	255.255.255.0	WG2\60
7	WS_7	192.168.6.7	255.255.255.0	WG2\60
8	WS_8	192.168.6.8	255.255.255.0	WG2\60
9	WS_9	192.168.6.9	255.255.255.0	WG2\60
10	WS_10	192.168.6.10	255.255.255.0	WG2\60
11	WS_11	192.168.6.11	255.255.255.0	WG2\60
12	WS_12	192.168.6.12	255.255.255.0	WG2\60
13	WS_13	192.168.9.1	255.255.255.0	WG1\90
14	WS_14	192.168.9.2	255.255.255.0	WG1\90
15	WS_15	192.168.3.1	255.255.255.0	IP\30
16	WS_16	192.168.8.1	255.255.255.0	WG4\60
17	WS_17	192.168.8.2	255.255.255.0	CONFER\80
18	WS_18	192.168.100.1	255.255.255.0	buch\100
19	WS_19	192.168.100.2	255.255.255.0	buch\100
20	WS_20	192.168.100.3	255.255.255.0	buch\100
21	PR_1	192.168.100.101	255.255.255.0	buch\100
22	WS_24	192.168.8.4	255.255.255.0	CONFER\80
23	WS_25	192.168.8.5	255.255.255.0	CONFER\80
24	WS_21	192.168.8.3	255.255.255.0	CONFER\80
25	WS_22	192.168.8.4	255.255.255.0	CONFER\80
26	WS_23	192.168.8.5	255.255.255.0	CONFER\80
27	S2	192.168.100.100	255.255.255.0	buch\100
28	S1	192.168.3.100	255.255.255.0	IP\30
		призначається провайдером		
29	SW_2	192.168.3.101	255.255.255.0	IP\30
30	AP_1	192.168.3.200	255.255.255.0	IP\30

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	–	TP-Link EAP610
2	топологія мережі	–	гібридна	9	операційна система робочих станцій	–	windows 10\11
3	середовище передачі	–	Вита пара кат. 5E	10	тип доступу до інтернет	–	вита пара
4	кількість вузлів мережі	шт	26	11	термін окупності	рік	1,2
5	марка головного комутатора	–	TP-Link TL-SG3428X	12	плановий прибуток	грн	94014,9
6	марка не керованого комутатора	–	TP-Link TL-SG1016DE	13	собівартість	грн	167883,75
7	марка сервера	–	ARTLINE Business R17v24	14	ціна	грн	261898,65



						2026.КВР.123.412.05.00.00 ФТ	
Зм.	Арк.	№Докум.	Підпис	Дат.			
Розроб.		Кизь Р.А.			Розробка проекту комп'ютерної мережі ПП "ТехноХата" Фізична топологія	Літ.	Маса	Масшт.
Керів.		Пцж В.С.						1:100
Нконтр.		Фазькіб А.В.				Аркуш 1	Аркушів 1	
Рецензія						ВСП ТФК ТНТУ, КІ 412, м.Тернопіль		
затв.								

2026.КВР.123412.05.00.00 ПП

Зм.	Кіл.	Уч.	№ док.	Підпис	Дата		
Розроб.			Князь Р.А.				
Керів.			Пик В.І.				
Н.контр.			Шакіб А.В.				
Реценз.							
затв.							

2026.КВР.123412.05.00.00 ПП

Розробка проекту комп'ютерної мережі ПП "ТехноХолод"

План Приміщень

Літ.	Маса	Масшт.
Н		1:100

Аркуш 1 Аркушів 1

ВСП ТФК ТНТУ, КІ-142, м.Тернопіль