Міністерство освіти і науки України

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

Відділення телекомунікацій та електронних систем
(назва відділення)

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

бакалавра
(освітній ступінь)

на тему: **Розробка проєкту комп'ютерної мережі компанії «Авто-ком»**

Виконав: студент VI курсу, групи КІб-602

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

_____ Андрій АВДИКОВИЧ
(ім'я та прізвище)

Керівник Василь ПИЖ
(ім'я та прізвище)

Рецензент _____
(ім'я та прізвище)

Тернопіль – 2025

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

Відділення телекомунікацій та електронних систем
Циклова комісія комп'ютерної інженерії
Освітній ступінь бакалавр
Освітньо-професійна програма: Комп'ютерна інженерія
Спеціальність: 123 Комп'ютерна інженерія
Галузь знань: 12 Інформаційні технології

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"06" травня 2025 року

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

Авдиковичу Андрію Михайловичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи **Розробка проєкту комп'ютерної мережі компанії «Авто-ком»**

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

затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університетут імені Івана Пулюя» від 05.05.2025 р №4/9-217.

2. Строк подання студентом роботи: 20 червня 2025 року.

3. Вихідні дані до роботи: плани приміщень, завдання на проектування, стандарти побудови СКС, документація на мережеве обладнання і сервери

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

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): План приміщень. Логічна топологія. Фізична топологія. Таблиця IP-адрес. Таблиця техніко-економічних показників. Модель мережі

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Оксана РЕДЬКВА заст. директора з НВР		
Безпека життєдіяльності, основи охорони праці	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	06.05	
2	Збір і узагальнення інформації	19.05	
3	Написання першого розділу	23.05	
4	Розробка технічного та робочого проекту	28.05	
5	Написання спеціального розділу	3.06	
6	Розрахунок економічної частини	5.06	
7	Написання розділу охорони праці	7.06	
8	Виконання графічної частини	12.06	
9	Оформлення проекту	16.06	
10	Погодження нормоконтролю	18.06	
11	Попередній захист роботи	20.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 06 травня 2025 року

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

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

АНОТАЦІЯ

У даній кваліфікаційній роботі представлено процес розробки комп’ютерної мережі для компанії «Авто-ком». Метою проєкту є проєктування корпоративної мережі, що включає виконання наступних етапів:

- формування технічного завдання на проєктування (розглянуто в розділі 1);
- аналіз плану приміщень підприємства, вибір оптимальної топології мережі, підбір мережевого комутаційного обладнання та серверного забезпечення (висвітлено в розділі 2);
- конфігурування комутаційного обладнання та серверів, а також вибір і опис засобів захисту мережі від шкідливого програмного забезпечення та несанкціонованого доступу (висвітлено в розділі 3);
- розрахунок вартості впровадження мережевої інфраструктури (розглянуто в розділі 4);
- опис вимог з техніки безпеки та екологічних норм, що мають дотримуватись під час проєктування та експлуатації мережі (наведено в розділі 5).

Робота супроводжується пояснювальними матеріалами, таблицями та ілюстративними матеріалами. Загальна структура проєкту включає дві частини: пояснювальну записку обсягом ___ аркушів формату А4 та графічну частину обсягом ___ аркушів формату А1.

ABSTRACT

This qualification work presents the process of developing a computer network for the company "Avto-kom". The purpose of the project is to design a corporate network, which includes the following stages:

- formation of technical specifications for the design (discussed in section 1);
- analysis of the plan of the enterprise premises, selection of the optimal network topology, selection of network switching equipment and server software (covered in section 2);
- configuration of switching equipment and servers, as well as selection and description of network protection tools against malicious software and unauthorized access (covered in section 3);
- calculation of the cost of implementing network infrastructure (discussed in section 4);
- description of safety requirements and environmental standards that must be observed during network design and operation (given in section 5).

The work is accompanied by explanatory materials, tables and illustrative materials.

The general structure of the project includes two parts: an explanatory note of ___ sheets of A4 format and a graphic part of ___ sheets of A1 format.

ЗМІСТ

					2025.КРБ.123.602.01.00.00 ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Авдиковіч А М			"Розробка проєкту комп'ютерної мережі компанії "АВто-ком"» Пояснювальна записка	Літ.	Арк. 5 / Аркушів
Перевір.		Пиж В С					
Реценз.						ВСП ТФК ТНТУ КІ-602	
Н. Контр.							
Затверд.							

ВСТУП

Основною функцією будь-якої комп’ютерної мережі є забезпечення доступу користувачів до інформаційних і обчислювальних ресурсів. З технічної точки зору комп’ютерна мережа розглядається як сукупність взаємопов’язаних пристроїв, зокрема серверів і клієнтських станцій. Сервер — це високопродуктивний комп’ютер, який виконує функції обслуговування запитів користувачів, надає їм доступ до файлів, баз даних, додатків або мережевих сервісів. Робоча станція — це персональний комп’ютер, підключений до локальної або глобальної мережі, через який користувач взаємодіє з інформаційною інфраструктурою.

Розвиток комп’ютерних технологій зумовив революційні зміни у способах зберігання, передачі та обробки інформації. Традиційні способи поширення інформації, пов’язані з друкованими, аудіо- або візуальними носіями, доповнилися сучасними цифровими форматами. Гіпермедійні системи поєднують текст, зображення, звук і відео в інтегроване інформаційне середовище, яке є динамічним та інтерактивним. Такі мультимедійні засоби стали базою для створення нових форм контенту — навчальних курсів, інформаційних порталів, віртуальних презентацій тощо.

Сучасні комп’ютери виконують широкий спектр завдань: від елементарних арифметичних операцій до складного моделювання фізичних процесів. За допомогою комп’ютерів створюються поліграфічні матеріали, цифрові зображення, відеопродукція, музичні композиції, а також здійснюється керування виробничими процесами, транспортними системами та науковими дослідженнями. Крім того, комп’ютери застосовуються в оборонній промисловості, телекомунікаціях, охороні здоров’я, освіті, фінансах та багатьох інших сферах.

Однією з ключових переваг сучасних комп’ютерних систем є зручність користування завдяки розвиненим інтерфейсам, які можуть адаптуватися під індивідуальні потреби користувача. Гнучка архітектура програмного забезпечення дозволяє розширювати функціональність системи шляхом встановлення додаткових модулів або оновлень. Наявність вбудованих довідкових систем, інтерактивних підказок та підтримки користувача значно полегшує роботу з технікою.

До функціональних можливостей комп’ютерів також належить створення дво- та тривимірних моделей, які можуть бути як статичними, так і анімованими. Такі моделі широко застосовуються у проєктуванні, будівництві, медицині, кіноіндустрії та ігровій сфері. Комп’ютери здатні розпізнавати символи та мову, автоматично перекладати текстові повідомлення між різними мовами, формувати аналітичні звіти та виявляти закономірності в великих обсягах даних.

Усе це зробило комп’ютери універсальним засобом для роботи з інформацією, що забезпечує ефективну підтримку прийняття рішень у різних галузях діяльності. З розвитком штучного інтелекту та машинного навчання функціональність комп’ютерних систем продовжує зростати. Перспективи застосування комп’ютерних мереж та інтелектуальних систем залишаються надзвичайно широкими як у комерційному, так і в науковому середовищі. У результаті, комп’ютерна техніка посідає ключове місце в інфраструктурі сучасного суспільства та має стратегічне значення для його подальшого розвитку.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Темою кваліфікаційної роботи є проєктування комп’ютерної мережі для компанії «Авто-ком».

В рамках проєктування враховано основні вимоги підприємства, зокрема:

- необхідність інтеграції персональних комп’ютерів, розміщених у різних структурних підрозділах організації, в єдину мережеву інфраструктуру;
- забезпечення спільного доступу до високошвидкісного підключення до мережі Інтернет;
- використання служб і сервісів як локальної мережі, так і глобальної мережі Інтернет у щоденній діяльності компанії;
- впровадження економічно ефективного засобу обміну інформацією між користувачами;
- забезпечення безпеки мережі та захисту даних від несанкціонованого доступу та загроз;
- організація централізованого моніторингу і управління мережевими пристроями для покращення ефективності і зниження витрат на обслуговування;
- оптимізація використання мережевих ресурсів з метою підвищення продуктивності та мінімізації витрат на інфраструктуру.

1.1.2 Призначенння розробки

Проєктована комп'ютерна мережа призначена для забезпечення ефективної роботи працівників компанії «Авто-ком». Підприємство орієнтоване на організацію відпочинку, що дозволяє людям ознайомлюватися з історією, культурою, традиціями та природою України. Мережа, що проектується, повинна забезпечити швидкий доступ до файлів, службової інформації та інших ресурсів, що використовуються на підприємстві, а також забезпечити безперешкодний вихід до Інтернету.

Мережа буде використовуватись для обміну документами та іншою інформацією між структурними підрозділами компанії, для підключення до Інтернету, а також для організації мережевого друку. Для зберігання і доступу до інформації в мережі буде використовуватися FTP-сервер, що буде розміщений у комутаційній шафі.

Швидкість передачі даних у мережі становитиме 1000 Мбіт/с, що забезпечить високу продуктивність і ефективність обміну інформацією. Мережа повинна мати надійний і стабільний доступ до Інтернету для виконання необхідних операцій і забезпечення зовнішніх комунікацій.

1.1.3 Вимоги до апаратного та програмного забезпечення

Проєктована комп'ютерна мережа буде організована за принципом поділу на робочі групи, з максимальною швидкістю передачі даних 100/1000 Мбіт/с. Апаратне забезпечення мережі буде складатися з загальнодоступних і економічно ефективних компонентів, що підтримують заявлену швидкість і дозволяють швидко здійснювати заміну або ремонт у разі потреби. Такі пристрої також повинні мати можливість для централізованого адміністрування, що спрощує процес управління мережею.

Програмне забезпечення мережі включає операційні системи, встановлені на комп’ютерах працівників підприємства. У даному випадку використовується сукупність операційних систем Windows 7/10, які забезпечують стабільну та безпечну роботу на кожному робочому місці.

Безпровідні точки доступу повинні підтримувати протоколи безпеки WPA-PSK, WPA2-PSK і відповідати стандарту 802.11n, що забезпечить високий рівень захисту та надійний зв’язок у межах підприємства. Для покращення швидкості передачі даних та стабільності з’єднання безпровідні точки доступу будуть налаштовані на оптимальні канали. Крім того, для підвищення ефективності мережі планується впровадження системи моніторингу та управління для вчасного виявлення та усунення можливих неполадок. Також у планах — реалізація автоматичного оновлення програмного забезпечення, що забезпечить підтримку мережі на актуальному рівні безпеки. Це дозволить значно знизити ризик виникнення уразливостей через застарілі версії програм.

1.1.4 Стадії та етапи розробки

При проектуванні комп’ютерної мережі необхідно вирішити низку ключових питань:

- Який тип організації планується, чи передбачене її розширення в майбутньому?
- Чи існує вже діюча комп’ютерна мережа, яку необхідно модернізувати або інтегрувати?
- Яке програмне забезпечення буде використовуватись у мережі для забезпечення її функціональності?
- Визначити тип мережі, топологію, а також провідники та інше обладнання першого рівня, необхідне для побудови основної інфраструктури.
- Визначити кількість комутаторів, необхідних для підключення

робочих груп, з урахуванням потреб у пропускній здатності та резервуванні.

- Оцінити потребу у головних і проміжних комунікаційних вузлах для забезпечення ефективного маршрутизування та управління трафіком.
- Визначити необхідність встановлення маршрутизаторів для управління трафіком між різними мережевими сегментами та зовнішніми ресурсами.
- Визначитися з підключенням до глобальної мережі Інтернет, обираючи відповідного провайдера та вид з'єднання для забезпечення стабільного доступу.

Процес організації мережі можна поділити на наступні етапи:

- Збір інформації – на цьому етапі проводиться вивчення потреб організації, аналіз існуючої інфраструктури та визначення вимог до нової мережі.
- Створення і затвердження проекту – розробляється детальний проєкт мережі, який включає вибір топології, необхідного обладнання, програмного забезпечення, а також визначення маршрутизації та безпеки. Після розробки проекту він затверджується керівництвом.
- Фізична реалізація мережі – на цьому етапі проводиться монтаж та налаштування всього необхідного обладнання, встановлення програмного забезпечення, прокладка кабелів, налаштування комутаторів і маршрутизаторів.
- Експлуатація та моніторинг мережі – після завершення налаштування мережі проводиться тестування її працездатності, а також організовується постійний моніторинг для виявлення та усунення можливих неполадок, оновлення програмного забезпечення та забезпечення безпеки.

Кожен етап розробки мережі є важливим для створення стабільної та ефективної інфраструктури, що забезпечить успішну роботу організації.

1.1.5 Вимоги до документації

Опишимо вимоги до документування мережі:

- Повна документація мережі повинна включати всі етапи проєктування та реалізації, з детальним описом кожного компонента та його функцій.
- Топологія мережі має бути зафіксована в схемах, що чітко відображають взаємозв'язки між всіма пристроями та вузлами.
- В документації повинна бути вказана конфігурація мережевого обладнання, з деталями про налаштування комутаторів, маршрутизаторів та серверів.
- Всі параметри з'єднань, такі як типи кабелів, швидкість передачі даних, а також використовувані протоколи, повинні бути зафіксовані в окремому документі.
- Схеми фізичної та логічної мережі повинні бути документовані з урахуванням можливих змін та оновлень.
- Інформація про безпеку повинна включати деталі про впроваджені механізми захисту, включаючи конфігурації брандмауерів, систем виявлення вторгнень та криптографічні протоколи.
- Інструкції з адміністрування мережі повинні бути доступні для IT-персоналу та включати налаштування сервісів, моніторинг мережі та процедури з усунення неполадок.
- У документації слід описати план резервування та відновлення мережі на випадок аварійних ситуацій або технічних збоїв.
- Всі мережеві політики та регламенти повинні бути чітко прописані, включаючи правила доступу, використання ресурсів і політики безпеки.
- Історія змін в мережі повинна бути задокументована, щоб мати мож-

ливість відслідковувати будь-які зміни в інфраструктурі та конфігурації мережі.

Ці вимоги допоможуть забезпечити надійне і безпечне функціонування мережі, а також дозволять швидко виявляти й усувати можливі проблеми.

1.1.6 Техніко-економічні показники

Проєктована мережа повинна відповідати наступним вимогам:

- бути актуальною за технічними характеристиками, економічно доцільною та мати можливість подальшого масштабування;
- забезпечувати швидкість передачі даних на рівні 100/1000 Мбіт/с;
- включати стабільне підключення до глобальної мережі Інтернет;
- на всі етапи реалізації — від розробки до тестування — передбачається виділення 30–40 людино-годин;
- мережа повинна включати бездротовий сегмент для забезпечення мобільності користувачів та зручності доступу.

1.1.7 Порядок контролю та прийому

Під час приймання комп’ютерної мережі необхідно виконати наступні дії:

- здійснити перевірку працездатності всіх мережевих вузлів;
- переконатися в наявності маркування на всіх кабельних з’єднаннях відповідно до проєктної документації;
- провести тестування функціонування мережі із застосуванням прикладного програмного забезпечення або спеціалізованих утиліт, які забезпечують повноцінну діагностику.

Процедура введення мережі в експлуатацію є критично важливою, оскільки вона визначає стабільність і надійність її подальшої роботи. Після

отримання офіційного повідомлення від виконавця про завершення робіт, замовник зобов'язаний ініціювати створення приймальної комісії для проведення повного функціонального контролю.

Комісія має бути призначена не пізніше ніж через п'ять календарних днів з моменту отримання відповідного повідомлення. За результатами перевірки, у разі відповідності мережі всім вимогам, оформлюється акт приймання в експлуатацію.

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

Мета проектування - створення комп'ютерної мережі підприємства, котра повинна:

- об'єднати всі ПК працівників,
- забезпечити можливість обміну інформацією та зберігання даних,
- забезпечити всім робочим станціям спільний доступ до мережевих ресурсів та Інтернет.

Персональні комп'ютери будуть розміщуватись у таких приміщеннях:

- фінансовий відділ — розміщено мережевий принтер, два ПК, сервер даних, комутуюче обладнання;
- регіональні керівники — чотири ПК в кабінеті, мережевий принтер
- IT відділ — все обладнання для створення мережі (центральний комутатор , доступ до інтернету, сервер FTP)
- робочий зал менеджерів - десять ПК, три мережеві принтери, комутатор;

Крім того варто зазаначити, що мережа буде мати вихід в інтернет, має один мережевий накопичувач, дві точки доступу доступу.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Розробка та обґрунтування логічної та фізичної схем мережі

На сучасному етапі розвитку комп'ютерних мереж існує велика кількість варіантів їх топологічної організації, серед яких найпоширенішими є: топологія зірка, шинна топологія, кільцева топологія, деревовидна топологія та гібридна топологія. Кожна з них має свої особливості побудови, переваги та обмеження, що визначають сферу її застосування.

Незважаючи на різноманіття існуючих рішень, більшість мережевих архітектур базується на трьох основних типах топологій — шинній, зіркоподібній та кільцевій. Вибір конкретної структури залежить від вимог до надійності, масштабованості, вартості впровадження, а також технічних умов експлуатації.

Порівнюючи ключові характеристики зазначених топологій, зокрема такі параметри, як складність реалізації, стійкість до відмов, простота діагностики несправностей та ефективність обміну даними, можна зробити висновок про доцільність застосування топології типу «зірка» в більшості практичних випадків. Детальний аналіз переваг та недоліків представлений у таблиц2.1.

Таблиця 2.1 - Характеристики топологій

Характеристика	"Зірка"	"Кільце"	"Шина"	Гібридна топологія
1	2	3	4	5
Переваги	Легкість додавання/видалення при	Усі пристрої мають рівний доступ до мере	Мінімальна кількість кабелю. Легкість роз	Гнучкість та масштабованість.

Продовження таблиці 2.1

1	2	3	4	5
	строїв. Відмова одного пристрою не впливає на інші. Зручне виявлення несправностей.	жі. Відносно проста реалізація для невеликих мереж.	ширення приєднанням нових пристроїв до шини.	Можливість використання переваг різних топологій.
Недоліки	Залежність від центрального пристрою (одинична точка відмови). Висока вартість кабелю для великих мереж.	Відмова одного пристрою може зупинити всю мережу. Складність додавання/видалення пристроїв. Труднощі з виявленням несправностей.	Відмова центрального кабелю призводить до відмови всієї мережі. Низька продуктивність при великому трафіку. Складнощі з виявленням несправностей.	Складність проектування та управління. Вища вартість реалізації.
Надійність	Висока	Низька	Дуже низька	потенційно висока.
Масштабованість	Висока.	Низька.	Обмежена.	Висока.

Процес вибору топології мережі є досить складним і залежить від багатьох чинників, що визначають її ефективність та доцільність використання у конкретних умовах. Остаточне рішення щодо вибору певної топології приймається лише після ретельного аналізу вимог до продуктивності, надійності, вартості впровадження, а також специфіки експлуатаційного середовища.

З огляду на викладені раніше технічні характеристики різних топологій, найоптимальнішим варіантом вважається топологія типу «зірка». Вона отримала широке розповсюдження завдяки своїй гнучкості, високому рівню надійності, простоті конфігурування та обслуговування, а також прийнятному рівню витрат при побудові мережі на основі кабелів типу «вита пара».Однією з основних переваг топології «зірка» є те, що у разі виходу з ладу окремого вузла мережі загальна працездатність системи не порушується. Єдиною критичною точкою є комутатор, і лише його відмова призводить до повного зупинення роботи локальної мережі. Така архітектура дозволяє ефективно локалізувати і усувати несправності, що суттєво підвищує стабільність функціонування мережної інфраструктури.Хоча реалізація мережі за топологією типу «зірка» потребує більших початкових інвестицій, зокрема через вартість активного мережевого обладнання (комутаторів, маршрутизаторів), ці витрати повністю виправдовуються в контексті забезпечення надійного і високошвидкісного з’єднання між усіма пристроями локальної мережі. У корпоративних середовищах це рішення є найбільш раціональним.

Серед численних мережевих технологій, що базуються на архітектурі Ethernet, особливу увагу заслуговує стандарт Gigabit Ethernet. Його впровадження стало можливим завдяки значному зниженню вартості компонентів і підвищенню вимог до пропускної здатності внаслідок активного використання таких сервісів, як потокове відео, відеоконференції, а також передача графічних та мультимедійних файлів високої роздільної здатності.

Gigabit Ethernet є логічним продовженням попередніх стандартів Ethernet і Fast Ethernet. Він зберігає основні принципи побудови мереж, вклю-

чаючи формат кадру, метод доступу до середовища CSMA/CD (множинний доступ з контролем колізій), а також підтримку як напівдуплексного, так і повнодуплексного режимів. Його зворотна сумісність із попередніми версіями забезпечує простоту інтеграції у вже існуючу інфраструктуру.

Стандарт 1000BASE-T передбачає використання всіх чотирьох пар витої пари (на відміну від 100BASE-TX, де задіяні лише дві пари), при цьому кожна пара передає дані зі швидкістю до 250 Мбіт/с, забезпечуючи сумарну пропускну здатність до 1000 Мбіт/с. Потоки даних здійснюються одночасно в обох напрямках, що дозволяє реалізувати повнодуплексний режим передачі на кожній парі.

Реалізація такого режиму вимагала впровадження спеціальних механізмів, здатних ефективно протидіяти електромагнітним перешкодам і наведенню сигналів. З цією метою було застосовано метод скремблювання сигналу, а також інтегровано інтелектуальні модулі розпізнавання та відновлення даних на приймальній стороні.

Кодування в 1000BASE-T виконується за допомогою п’ятирівневого імпульсно-амплітудного методу PAM-5, що дозволяє оптимізувати швидкість передачі без значного збільшення частоти сигналу. Крім того, були підвищені вимоги до якості кабельної системи. Для забезпечення стабільної роботи було рекомендовано використання неекранованої витої пари категорії не нижче 5e, яка відповідає сучасним вимогам щодо мінімізації наведень, втрат сигналу, затримок та фазових спотворень.

Порядок обтискання провідників у кабелі типу «вита пара» наведений на рисунку 2.1, який ілюструє стандартну схему підключення згідно з прийнятими нормами. З урахуванням вищенаведеного можна зробити висновок, що технологія Gigabit Ethernet є перспективною і найбільш прийнятною для використання як у корпоративному, так і в домашньому середовищі.

RJ-45 разводка (TIA/EIA-568-B T568B)

Контакт	Пара	Провод	Цвет
1	2	1	бело-оранжевый
2	2	2	оранжевый
3	3	1	бело-зелёный
4	1	2	синий
5	1	1	бело-синий
6	3	2	зелёный
7	4	1	бело-коричневый
8	4	2	коричневый

Рисунок 2.1 — Позначення обтискання кабелю

Після визначення фізичної топології мережі, вибору відповідної технології передачі даних та типу кабельної інфраструктури, наступним етапом проєктування є формування логічної структури мережі. На цьому етапі важливо описати принципи побудови логічних сегментів, методи маршрутизації та ізоляції трафіку між різними підсистемами.

У запропонованій мережевій архітектурі передбачається використання декількох некерованих комутаторів із вісьмома або шістнадцятьма портами, які будуть розміщені безпосередньо в робочих приміщеннях. Ці пристрої слугуватимуть для підключення кінцевих пристроїв користувачів. Від кожного з них прокладено лінії зв’язку до центрального комутатора, який є керованим і виконує функції агрегації трафіку.

Завдяки такій схемі побудови з’являється можливість формувати логічні сегменти — робочі групи, що функціонують незалежно одна від одної. Для ізоляції трафіку та підвищення рівня безпеки кожну робочу групу доцільно виділити в окрему віртуальну локальну мережу (VLAN). Це дозволяє уникнути перехресного трафіку між групами, мінімізуючи ризик конфліктів, витоків даних і підвищуючи продуктивність кожного сегмента.

На рівні керованого комутатора буде налаштовано доступ VLAN-груп до зовнішньої мережі — Інтернету, за допомогою відповідного маршрутизатора, який виконує функції міжмережевої маршрутизації та забезпечує фільтрацію трафіку згідно з політиками безпеки. Крім того, до центрального комутатора буде підключено точки доступу бездротової мережі. З метою ізоляції безпровідного трафіку та забезпечення додаткового рівня захисту, кожну точку доступу буде включено в окремий VLAN. Це дозволить відокремити бездротовий сегмент від дротового, зменшити потенційний негативний вплив безпровідних пристроїв на загальну стабільність та безпеку мережі, а також забезпечити ефективне управління трафіком.

Усі технічні характеристики побудови логічної структури мережі та параметри конфігурації VLAN наведені у таблицях 2.2 та 2.3, що відображають логіку сегментації, зв’язків і маршрутизації в мережевій інфраструктурі.

Таблиця 2.2 – Логічна адресація в мережі

Позначення вузлів	Робоча група/ Кількість вузлів		Назва кабінету	Номер VLAN	Адреса підмережі/ Маска
1	2	3	4	5	6
WS_1—WS_10, PR_1-PR_3	office	13	Робочий зал менеджерів	100	192.168.100.0/24
WS_11—WS_14, PR_4	office	5	Регіональні керівники	100	192.168.100.0/24
WS_16-WS_17, PR_5	office	5	Фінансовий відділ	100	192.168.100.0/24
WS_15	іт	3	Відділ іт	120	192.168.120.0/24
Ap_1, Ap_1	wi-fi	2	приміщення	150	192.168.150.0/24

Таблиця 2.3 - Таблиця конфігурування VLAN

№ п/п	Познач. вузла	Номер порту	Тип порту	Назва ме-реж. пр-ю	Номер порту	Тип порту	Номер VLAN
1	2	3	4	5	6	7	8
2	SW_3	1	Провайдер інтернет				
3	SW_5	7	Access	S_1	-	Access	100
4	SW_3	2	Access	SW_1	16	Access	100
5	SW_3	3	Access	SW_2	8	Access	100
6	SW_3	4	Access	SW_4	8	Access	100
7	PR_1			SW_1	13	Access	100
8	PR_2			SW_1	14	Access	100
9	PR_3			SW_1	15	Access	100
10	PR_4			SW_3	7	Access	100
11	PR_5			SW_4	7	Access	100
12	S1			SW_3	9	Access	100
13	SW_4	19		AP_1	WAN	Access	120
14	SW_4	20		AP_1	WAN	Access	120

2.2 Обґрунтування вибору комунікаційного обладнання

Компанія «Авто-ком» є представником торговельного сектору, що обумовлює специфіку її бізнес-процесів і вимоги до інформаційної інфраструктури. Ефективна взаємодія з клієнтами, постачальниками та партнерами є ключовим чинником успішного функціонування підприємства.

Основний профіль компанії — торгівля, що вимагає стабільного і продуктивного функціонування внутрішньої комп'ютерної мережі для забезпечення обліку, логістики, звітності та підтримки клієнтських запитів.

Для побудови локальної мережі в офісі компанії «Авто-ком» доцільно використати три недорогі шістнадцятипортові комутатори, які забезпечуватимуть підключення кінцевих пристроїв у різних зонах офісного приміщення. Такий підхід дозволяє забезпечити гнучку конфігурацію мережі з мінімальними фінансовими витратами, що особливо актуально для малих та середніх підприємств.

Щоб обрати найбільш оптимальну модель комутатора за співвідношенням «ціна/якість/функціональність», необхідно провести порівняльний аналіз кількох популярних моделей на ринку. Для цього буде складено аналітичну таблицю, у якій наведено технічні характеристики, функціональні можливості, рівень підтримки протоколів, енергоспоживання, а також вартість моделей, що розглядаються. Такий підхід дозволить обґрунтовано прийняти рішення щодо закупівлі мережевого обладнання, враховуючи як технічні параметри, так і економічну доцільність.

Порівняльна таблиця комутаторів 2.4 наведена нижче та слугує основою для подальшого вибору обладнання, яке найкраще відповідає потребам компанії «Авто-ком».

Таблиця 2.4 – Порівняльна характеристика шістнадцятипортових комутаторів

Характеристика	Zyxel GS1100-16 (GS1100-16-EU0103F)	D-Link DGS-1016D	Digitus DN-80115
1	2	3	4
Тип комутатора	Некерований	Некерований	Некерований
Кількість портів 10/100/1000Base-T	16 x (RJ-45)	16 x	16 x

Продовження таблиці 2.4

1	2	3	4
Комутаційна здатність	32 Гбіт/с	32 Гбіт/с	32 Гбіт/с
Швидкість пересилання пакетів	23.8 Мбіт/с	23.8 Мбіт/с	23.8 Мбіт/с
Розмір таблиці MAC-адрес	8K записів	8K записів	8K записів
Охолодження	Пасивне (без вентилятора)	Пасивне (без вентилятора)	Пасивне (без вентилятора)
Ціна, грн	3000	3500	5300

Виходячи з таблиці 2.4, враховуючи співвідношення ціни до технічних характеристик пристрою для мережі вибрано комутатор Zyxel GS1100-16, зовнішній вигляд якого зображено на рисунку 2.2.

Короткі технічні характеристики комутатора:

- Швидкість LAN портів 1 Гбіт/с
- Додатково Можливість монтажу у стійку
- Тип Некерований
- Тип портів 16 x Gigabit Ethernet (10/100/1000 Мбіт/с)
- Матеріал корпусу Метал
- Пропускна здатність, Гбіт/с
- Форм-фактор Настільний/Стійковий
- Країна-виробник Тайвань

Рисунок 2.2 – Зовнішній вигляд комутатора Zyxel GS1100-16

У структурі комп’ютерної мережі компанії також передбачається наявність центрального (або головного) комутатора, який виконуватиме функції основного вузла агрегації трафіку від усіх периферійних комутаторів. Саме цей пристрій забезпечуватиме зв’язок між різними сегментами мережі, VLAN-групами, а також матиме підключення до маршрутизатора для виходу в Інтернет.

Оскільки головний комутатор є критично важливим елементом інфраструктури, до його вибору необхідно підходити з урахуванням підвищених вимог до функціональності, продуктивності та надійності.

Серед основних параметрів, на які слід звернути увагу при виборі: кількість портів, наявність підтримки VLAN, можливість керування (управління через веб-інтерфейс, CLI або SNMP), пропускна здатність комутаційної матриці, наявність QoS, підтримка протоколів безпеки та тип живлення.

Для обґрунтування вибору головного комутатора проведено попередній аналіз трьох актуальних моделей, доступних на ринку. Основні технічні характеристики цих пристроїв зведені в таблицю 2.5.

Наведене порівняння дозволяє оцінити сильні та слабкі сторони кожної моделі та вибрати той варіант, який найкраще відповідає потребам мережевої інфраструктури компанії.

Таблиця 2.5 – Порівняльна характеристика керованих комутаторів

Характеристика	MikroTik CRS328-24P-4S+RM	TP-Link TL-SG3428MP	Ubiquiti USW-24-PoE
1	2	3	4
Кількість портів RJ45	24 x Gigabit Ethernet (PoE-out)	24 x Gigabit Ethernet (PoE+)	24 x Gigabit Ethernet (16 PoE+ / 8 без PoE)
Кількість портів SFP/ SFP+	4 x SFP+ (10Gbps)	4 x Gigabit SFP	2 x 1G SFP
Загальний PoE бюджет	450 Вт (до 30 Вт на порт)	384 Вт (до 30 Вт на порт)	95 Вт (до 32 Вт на порт)
Комутаційна здатність	128 Гбіт/с	56 Гбіт/с	52 Гбіт/с
Швидкість пересилання пакетів	95.2 Mpps	41.66 Mpps	38.69 Mpps
Рівень управління	L2/L3 (RouterOS) / L2 (SwitchOS) (Dual Boot)	L2+ (статична маршрутизація)	L2
Орієнтовна ціна грн	17000	14000	17000

В якості головного комутатора використаємо MikroTik CRS328-24P-4S+RM

Зовнішній вигляд комутатора MikroTik CRS328-24P-4S+RM можна показано на рисунку 2.3

Найбільш гнучкий варіант завдяки Dual Boot (RouterOS/SwitchOS), що дозволяє використовувати його як повноцінний маршрутизатор або просто комутатор. Має найбільший PoE бюджет та SFP+ порти для 10 Гбіт/с аплінків. Підходить для тих, хто потребує розширеної функціональності маршрутизації та гнучкості. маршрутизатор, комутатор, все в одному: Ethernet, Fiber або 4G (з додатковим USB-модемом) шлюз з'єднання з Інтернетом Маршрутизатор RouterOS / брандмауер / VPN з пасивним охолодженням до двадцяти п'яти гігабітних портів (1xSFP та 24xRJ45)

Рисунок 2.3 – Зовнішній вигляд комутатора MikroTik CRS328-24P-4S+RM

У структурі комп'ютерної мережі передбачено використання безпровідної точки доступу для забезпечення підключення мобільних пристроїв та організації сегменту Wi-Fi. Враховуючи зростаючі потреби користувачів у бездротовому доступі до мережевих ресурсів, наявність надійного й продуктивного точки доступу є важливою складовою сучасної мережевої інфраструктури.

На ринку представлено широкий асортимент бездротових точок доступу від різних виробників, що відрізняються за функціональністю, підтримуваними стандартами, дальністю дії та ціною. Для даного проєкту було обрано модель MikroTik cAP AC RBcAPGi-5acD2nD, яка поєднує хороше спів-

відношення ціни та технічних можливостей. Даний пристрій підтримує одночасну роботу в двох частотних діапазонах (2.4 ГГц і 5 ГГц), що дозволяє забезпечити стабільне покриття та високу швидкість передачі даних у бездротовому сегменті мережі.

Ключовим аргументом на користь вибору саме цієї моделі є її повна сумісність з керованим комутатором, що використовується у мережі. MikroTik cAP AC підтримує централізоване управління, створення кількох SSID, VLAN-ізоляцію трафіку, а також має вбудовані функції контролю доступу, що дозволяє реалізувати керовану безпровідну інфраструктуру.

Ціна даної точки доступу становить орієнтовно 3600 грн, що є прийнятним рівнем інвестицій для малого чи середнього офісу. Зовнішній вигляд пристрою зображено на рисунку 2.4.

Використання MikroTik cAP AC забезпечить не лише високу якість покриття, але й інтегрованість бездротового сегмента з основною мережею, що важливо з точки зору безпеки та централізованого адміністрування.

Рисунок 2.4 – Вигляд точки доступу MikroTik cAP AC

У проектованій комп’ютерній мережі передбачено встановлення окремого серверного комп’ютера, який буде розміщено у приміщенні бухгалтерії та виконуватиме функції централізованого сервера для обробки та зберігання фінансових і облікових даних.

Такий підхід дозволяє забезпечити надійне функціонування бухгалтерського програмного забезпечення, організувати централізований доступ до даних, а також підвищити рівень інформаційної безпеки.

У якості серверного обладнання для реалізації даної задачі обрано модель Lenovo ThinkSystem ST50 V2, яка характеризується низьким енергоспоживанням при збереженні високих показників продуктивності.

Завдяки сучасному процесору, можливості масштабування оперативної пам’яті та підтримці надійних накопичувачів, цей сервер є ефективним рішенням для потреб малого або середнього офісу.

Модель Lenovo ThinkSystem ST50 V2 відповідає основним вимогам до серверного обладнання: забезпечує стабільну роботу під навантаженням, підтримує тривалу безперервну експлуатацію, має ергономічний корпус та просту конструкцію для обслуговування.

Крім того, він відзначається довговічністю, високим рівнем енергоефективності та широкими можливостями для подальшого оновлення компонентів, що робить його доцільним вибором для корпоративного сегмента.

Універсальність і технічні характеристики цього серверного рішення дають змогу ефективно виконувати завдання з обробки бухгалтерських операцій, зберігання резервних копій даних, а також роботи в середовищі одночасного доступу декількох користувачів. Зовнішній вигляд сервера наведено на рисунку 2.5.

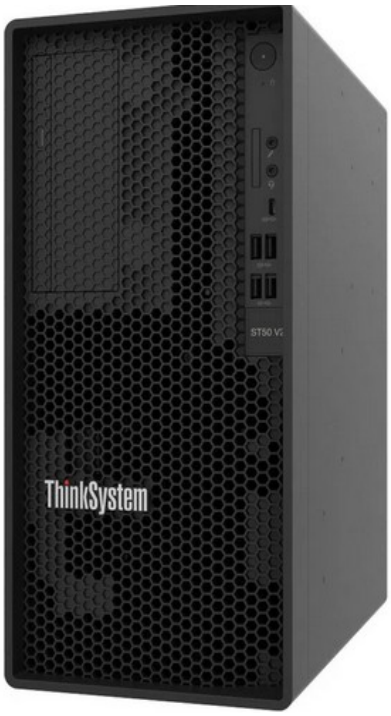


Рисунок 2.5 – Зовнішній вигляд Lenovo ThinkSystem ST50 V2

Технічні характеристики сервера:

- Процесор
- Модель CPU Intel Xeon E-2324G
- Кількість ядер 4
- Кількість потоків 4
- Номінальна частота, ГГц 3.1
- Максимальна частота, ГГц 4.6
- Кеш L3, МБ 8
- Потужність, Вт 65
- Оперативна пам'ять
- Тип ОЗУ DDR4 3200 МГц
- Об'єм ОЗУ, ГБ 8
- Максимально ОЗУ 128 ГБ
- Кількість слотів 4 / вільних - 3
- Постійна пам'ять Відсіки для дисків 2 х 3,5-дюймові NHS з підтри-

мкою жорстких дисків та твердотільних накопичувачів 1 x 2.5-inch NHS з підтримкою SSD 1 x NVMe M.2 M.2 SSD

- Підтримка HBA/RAID Підтримка програмного RAID-матриці Intel® VROC, Підтримує додаткові апаратні RAID-конфігурації
- Контролер зберігання 5350-8i
- Відеокарта Модель GPU nVidia Quadro T1000
- Мережі та комунікації LAN RJ-45, шт.
- Форм-фактор Tower (1S)
- Гарантія 3 роки

Зведемо все вибране нами обладнання в таблицю 2.6.

Таблиця 2.6 — Перелік обладнання мережі

№ п.п	назва	Кількість	ціна
1	2	3	4
1	комутатор Zyxel GS1100-16	3	3000,00 грн.
3	комутатор MikroTik CRS328-24P-4S+RM	1	17000,00 грн.
4	точка доступу MikroTik cAP AC RBcAPGi-5acD2nD	2	2 600,00 грн.
5	Сервер Lenovo ThinkSystem ST50 V2	2	40 000,00 грн.

2.3 Особливості монтажу мережі

Опишу вимоги до монтажу кабельних трас у структурованих кабельних системах (СКС)

1. Вибір середовища передачі даних

Найбільш розповсюдженим середовищем передачі даних у СКС є кабелі з мідними провідниками. Водночас у магістральних каналах першого та другого рівнів все частіше застосовують оптичні кабелі, що забезпечують високу швидкість передавання даних.

2. Вимоги до прокладання кабелів

Коректне прокладання та надійне закріплення кабелів під час монтажу визначає стабільність, швидкодію та довговічність роботи мережі. Загальні стандарти монтажу регламентуються документами ISO/IEC IS 11801 та ГОСТ Р 53246.

3. Уникнення електромагнітних завад

Прокладка кабельних трас повинна здійснюватися на відстані від джерел електромагнітних завад: силових ліній, трансформаторного обладнання, електродвигунів, радіопередавачів тощо. Якщо дотриматися мінімальної відстані неможливо, слід використовувати екрановані кабелі або заземлені металеві канали.

4. Вимоги до заземлення

Усі металеві кабельні конструкції мають бути надійно заземлені. Це стосується як екранованих, так і неекранованих кабелів. Заземлення знижує вплив завад на телекомунікаційні сигнали.

5. Мінімальні відстані при паралельному прокладанні з силовими кабелями

Згідно зі стандартом EIA/TIA 569:

- До 2 кВт — 127 мм,
- 2–5 кВт — 305 мм,
- Понад 5 кВт — 610 мм.
- Якщо телекомунікаційні кабелі розміщено в заземленому каналі, ці відстані зменшуються у 2 рази, а при спільному прокладанні силових

та інформаційних кабелів у заземленому каналі — в 4 рази.

6. Відстань до теплових джерел

Не рекомендується прокладати кабелі біля радіаторів, труб та інших джерел тепла.

7. Механічні навантаження та вигини

При монтажі слід уникати натягу, скручування чи різких вигинів кабелів. Мінімальний радіус вигину визначається окремо для магістральних, горизонтальних та комутаційних ліній і повинен відповідати жорсткішим вимогам: або стандарту, або виробника.

8. Захист від перегину та натягу

Кабельні траси мають бути оснащені пристроями, що запобігають перегину і перекрученню. Максимально допустиме навантаження, наприклад для кабелів на основі витої пари — 110 Н.

9. Резерв довжини кабелю

На кожному кінці лінії обов’язково залишаються запаси:

- У телекомунікаційних приміщеннях — не менше 3 м,
- Біля розеток RJ-45 — щонайменше 30 см.
- Резерви укладають у вигляді «вісімки» або U-подібних петель з великим радіусом.

10. Кріплення кабелів

Для фіксації використовують хомути, стяжки та бандажі. Вони повинні забезпечувати невеликий люфт кабелю після монтажу. Застосування степлерів і скоб для кріплення телекомунікаційних кабелів заборонено.

11. Дотримання стандартів — запорука якості

Точне виконання вимог щодо прокладання кабелів безпосередньо впливає на якість та стабільність функціонування всієї СКС.

12. Особливості монтажу в приміщеннях

Кабелі будуть прокладені понад підвісною стелею, спуски – у внутрішніх каналах гіпсокартонних конструкцій, що забезпечує естетику та безпечність траси.

2.4 Тестування мережі

Тестувати комп’ютерні мережі можна за допомогою різних методів та тестів.

Lan-тестер [13] - це прилад, призначений для перевірки цілісності телекомунікаційних мереж. Зазвичай такий пристрій складається з основної частини і знімною (найчастіше однією, але існують моделі, в яких передбачено кілька знімних частин). Lan-тестер дозволяє «продзвонювати» комп'ютерні мережі, телефонні комунікації, обтиснуті конектори. Мережевий тестер сильно полегшує роботу і заощаджує час фахівців-кабельників. Адже їх робота полягає не тільки в прокладанні комунікацій, але і в налагодженні всієї системи. Візуально практично неможливо визначити якість обтискача коннектора, а для того, щоб його продзвонити за допомогою тестера, знадобиться багато часу і помічник. Протяжка кручений пари не завжди буває в межах однієї кімнати, дуже часто кінці одного кабелю виявляються в різних сторонах будівлі і на різних поверхах, і «прозвонка» мультиметром в такому разі стане архіскладною і незручною. Ось тут нам і стане в нагоді допомогу такого приладу як Lan-тестер. Для «прозвонки» обжимаємо коннектори на обох кінцях кручений пари. Вставляємо один кінець в роз'єм основної частини тестера, а другий - в роз'єм знімною частини. Після цього включаємо прилад і запускаємо його в режим перевірки. Завдяки світлодіодним індикації, Lan-тестер дозволяє визначити не тільки наявність обривів проводів кручений пари і короткого замикання, а й виявити переплутані жили. Дуже часто новачки нехтують перевіркою обтиску конекторів.

Починають «продзвонювати» тільки в тому випадку, якщо комп'ютерна мережа не запрацювала.

Однак таку перевірку необхідно проводити при кожному обтиску конектора, щоб переконатися в правильності і цілісності з'єднання всіх контактів роз'єму, а не тільки тих, які використовуються в даний момент комп'ютерною мережею. В іншому випадку ви не зможете попередити майбутні помилки і збої в системі. Існує величезний вибір мережевих тестерів, як аматорських, так і професійних. У двох словах хотілося б описати переваги професійних приладів. Такі пристрої можуть тестувати не тільки кручені пари, а й телефонні коаксіальні кабелі.

Професійний лан-тестер (кабельний) крім стандартної перевірки, описаної вище, може вимірювати довжину, видавати тонові сигнали, а також сигналізувати про наявність активних жив.

Такі прилади мають повноцінні дисплеї, на яких відображається вся необхідна інформація про стан кабелю. І найголовніше, ці пристрої мають велику кількість віддалених модулів.

Наприклад, при протяганні кабелів через кабельгони «мережевики» часто стикаються з проблемою ідентифікації «свого» кабелю. Картина приблизно така: з щитової стирчать кінці 10-15 кручених пар, і просто неможливо зрозуміти, яка з них «твоя».

«Продзвонювання» аматорським тестером може затягнутися на тривалий час, особливо якщо другий кінець знаходиться в іншому краю будівлі.

У такій ситуації допоможуть виносні модулі професійного приладу. Ви можете одягнути на кожен кінець по модулю, а самі на другому кінці кабелю за допомогою основного блоку тестера обчислити необхідний вам провід.

Підбивши підсумок, скажімо, що Lan-тестер просто необхідний людям, які часто займаються протяжкою крученої пари для організації мережевих з'єднань комп'ютерної техніки.

Тестер кабельний RX-1000 UTP, BNC, USB для витої пари, коаксіалу, телефону, USB, зображений на рисунку 2.6.

Опис тестера RX-1000: Прилад для тестування витої пари, телефонного, USB і коаксіального кабелю. Застосовується для тестування ліній з конекторами типу RJ-45, RJ-11, USB, BNC Складається з активної і пасивної частини Має вбудований BNC термінатор 25/50 Ом, індикацію прямого або кросового з'єднання, індикацію зарядки батареї живлення Максимальна довжина досліджуваного 90 метрів кабелю

Рисунок 2.6 – Кабельний тестер. Зовнішній вигляд

2.5 Захист комп’ютерної мережі

Існує два підходи до проблеми забезпечення безпеки комп'ютерних систем і мереж: фрагментарний та комплексний.

Фрагментарний підхід спрямований на протидію чітко визначеним загрозам у заданих умовах. Як приклади реалізації такого підходу можна навести окремі засоби керування доступом, автономні засоби шифрування, спеціалізовані антивірусні програми тощо. Перевагою такого підходу є висока вибірковість до конкретної загрози. Суттєвим недоліком даного підходу є відсутність єдиного захищеного середовища обробки інформації.

Фрагментарні заходи захисту інформації забезпечують захист конкретних об'єктів КС лише від конкретної загрози. Навіть невелика видозміна загрози призводить до втрати ефективності захисту. *

Комплексний підхід орієнтований на створення захищеного середовища обробки інформації в КС, що об'єднує в єдиний комплекс різнорідні заходи протидії загрозам. Організація захищеного середовища обробки інформації дозволяє гарантувати певний рівень безпеки КС, що є безсумнівною перевагою комплексного підходу. До недоліків цього підходу належать: обмеження на свободу дій користувачів КС, чутливість до помилок встановлення та налаштування засобів захисту, складність керування. Комплексний підхід застосовують для захисту КС великих організацій або невеликих КС, що виконують відповідальні завдання або обробляють особливо важливу інформацію. Порушення безпеки інформації' в КС великих організацій може завдати величезних матеріальних збитків як самим організаціям, так і їхнім клієнтам. Тому такі організації змушені приділяти особливу увагу гарантіям безпеки та реалізовувати комплексний захист. Комплексного підходу дотримуються більшість державних і великих комерційних підприємств та установ. Цей підхід знайшов своє відображення в різних стандартах. ~

Комплексний підхід до проблеми забезпечення безпеки ґрунтується на розробленій для конкретної КС політиці безпеки. Політика безпеки регламентує ефективну роботу засобів захисту КС. Вона охоплює всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях. Надійна система безпеки мережі не може бути створена без ефективної політики мережевої безпеки. Для захисту інтересів суб'єктів інформаційних відносин необхідно поєднувати заходи наступних рівнів: ~

- законодавчого (стандарти, закони, нормативні акти тощо); *
- адміністративно-організаційного (дії загального характеру, що вживаються керівництвом організації, та конкретні заходи безпеки, що стосуються людей); ~

- програмно-технічного (конкретні технічні заходи).

Заходи законодавчого рівня дуже важливі для забезпечення інформаційної безпеки. До цього рівня можна віднести весь комплекс заходів, спрямованих на створення та підтримання в суспільстві негативного (у тому числі карального) ставлення до порушень та порушників інформаційної безпеки. Більшість людей не вчиняють протиправних дій тому, що це засуджується та/або карається суспільством, і тому, що так чинити не прийнято. v

Заходи адміністративно-організаційного рівня. Адміністрація організації повинна усвідомлювати необхідність підтримання режиму безпеки та виділення на ці цілі відповідних ресурсів. Основою заходів захисту адміністративно-організаційного рівня є політика безпеки та комплекс організаційно-технічних заходів. Під політикою безпеки розуміється сукупність документованих управлінських рішень, спрямованих на захист інформації та асоційованих з нею ресурсів організації. До комплексу організаційних заходів належать заходи безпеки, що реалізуються людьми. Можна виділити наступні групи організаційних заходів:

- управління персоналом;
- фізичний захист;
- підтримання працездатності;
- реагування на порушення режиму безпеки;
- планування відновлювальних робіт.

Для кожної групи в організації повинен існувати набір регламентів, що визначають дії персоналу. Для підтримання режиму інформаційної безпеки особливо важливі заходи програмно-технічного рівня, оскільки основна загроза комп'ютерним системам походить від них самих: збої обладнання, помилки програмного забезпечення, промахи користувачів, адміністраторів тощо. *

Заходи та засоби програмно-технічного рівня. У рамках сучасних інформаційних систем повинні бути доступні, щонайменше, наступні механізми безпеки:

- ідентифікація та перевірка автентичності користувачів;
- керування доступом;
- протоколювання та аудит;
- криптографія;
- екранування;
- забезпечення високої доступності.

Необхідність застосування стандартів. Інформаційні системи міністерств і відомств майже завжди побудовані на основі програмних і апаратних продуктів різних виробників. Річ у тім, що на даний момент немає жодної компанії-розробника, яка надала б споживачеві повний перелік засобів (від апаратних до програмних) для побудови сучасної ІС. Щоб забезпечити в різнорідній ІС надійний захист інформації, потрібні фахівці високої кваліфікації, які будуть відповідати за безпеку кожного компонента ІС: правильно їх налаштовувати, постійно відстежувати зміни, що відбуваються, контролювати роботу користувачів. Очевидно, що чим різнорідніша інформаційна система, тим складніше забезпечити її безпеку. Велика кількість в корпоративних мережах і системах пристроїв захисту, міжмережевих екранів, шлюзів і VPN, а також зростаючий попит на доступ до корпоративних даних з боку співробітників, партнерів і замовників призводять до створення складного середовища захисту, важкого для керування, а іноді й несумісного.

Стандарти утворюють понятійний базис, на якому будуються всі роботи із забезпечення інформаційної безпеки та визначають критерії керування безпекою. Стандарти є необхідною базою, що забезпечує сумісність продуктів різних виробників, що надзвичайно важливо при створенні систем мережевої безпеки в гетерогенних середовищах. Комплексний підхід до вирішення проблеми забезпечення безпеки, раціональне поєднання законодавчих, адміністративно-організаційних та програмно-технічних заходів і обов'язкове дотримання промислових, національних та міжнародних стандартів є тим фундаментом, на якому будується вся система захисту корпоративних мереж.

За матеріалами https://ua.kursoviks.com.ua/metodychni_vkazivky/article_post/801-lektsiya-21-na-temu-problemi-bezpeki-korporativnikh-informatsiynikh-sistem-z-kursu-zakhist-ta-bezpeka-informatsiynikh-resursiv-nudpsu

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

У рамках реалізації запропонованої мережевої інфраструктури на робочих станціях співробітників буде встановлено операційні системи сімейства Microsoft Windows, що забезпечує сумісність з основним програмним забезпеченням, зокрема офісними додатками, бухгалтерськими програмами та системами електронного документообігу. Проте, оскільки інсталяція та налаштування клієнтських операційних систем не є предметом безпосереднього аналізу в даному проекті, ці аспекти розглядатися не будуть.

Слід зазначити, що в архітектурі мережі не передбачено використання класичних апаратних серверів з інстальованими серверними операційними системами (такими як Windows Server чи Linux Server). Це обумовлено специфікою задач, які покладаються на мережеву інфраструктуру, а також орієнтацією на мінімізацію витрат за рахунок спрощеної моделі керування.

У наступному розділі буде розглянуто базове налаштування керованого комутатора, що відіграє центральну роль в управлінні потоками даних у мережі. Слід підкреслити, що такі пристрої функціонують на вбудованих операційних системах, розроблених на основі Linux, які мають гнучкі можливості конфігурування, масштабованість і високу стабільність у роботі.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкція з інсталяції програмного забезпечення серверів та активного комутаційного обладнання

Налаштування маршрутизатора MikroTik CRS125 24G-1S-IN

називаємо роутер

```
system identity set name=router-sw4
```

Позначимо фізичні порти по тим мережам, яким вони належать. Позначимо маркуванням lan фізичні порти, які будуть належати мережі підприємства, а маркуванням wifi фізичні порти, які будуть належати мережі (класу С).

```
interface ethernet set [ find default-name=ether1 ] name=ether1-wan
interface ethernet set [ find default-name=ether2 ] name=ether2-lan
interface ethernet set [ find default-name=ether3 ] name=ether3-lan
interface ethernet set [ find default-name=ether4 ] name=ether4-lan
interface ethernet set [ find default-name=ether5 ] name=ether5-lan
interface ethernet set [ find default-name=ether6 ] name=ether6-lan
interface ethernet set [ find default-name=ether7 ] name=ether7-lan
interface ethernet set [ find default-name=ether8 ] name=ether8-lan
interface ethernet set [ find default-name=ether9 ] name=ether9-lan
interface ethernet set [ find default-name=ether10 ] name=ether10-lan
interface ethernet set [ find default-name=ether11 ] name=ether11-lan
interface ethernet set [ find default-name=ether12 ] name=ether12-lan
interface ethernet set [ find default-name=ether13 ] name=ether13-lan
interface ethernet set [ find default-name=ether14 ] name=ether14-lan
interface ethernet set [ find default-name=ether15 ] name=ether15-lan
interface ethernet set [ find default-name=ether16 ] name=ether16-lan
interface ethernet set [ find default-name=ether17 ] name=ether17-lan
interface ethernet set [ find default-name=ether18 ] name=ether18-lan
interface ethernet set [ find default-name=ether19 ] name=ether19-lan
interface ethernet set [ find default-name=ether20 ] name=ether20-lan
interface ethernet set [ find default-name=ether21 ] name=ether21-lan
interface ethernet set [ find default-name=ether22 ] name=ether22-lan
interface ethernet set [ find default-name=ether23 ] name=ether23-lan
```

```
interface ethernet set [ find default-name=ether24 ] name=ether24-lan
interface ethernet set [ find default-name=sfp-sfpplus1 ] disabled=yes
interface ethernet set [ find default-name=sfp-sfpplus2 ] disabled=yes
```

Створимо віртуальні інтерфейси у вкладці bridge, для об'єднання LAN портів.

```
interface bridge add name=br1-lan
interface bridge add name=br100-lan
interface bridge add name=br110-lan
interface bridge add name=br120-lan
```

Призначаємо LAN порти маршрутизатора віртуальним інтерфейсам (bridge) відповідно до таблиці 2.4.

```
interface bridge port add bridge=br100-lan interface=ether2-lan
interface bridge port add bridge=br100-lan interface=ether3-lan
interface bridge port add bridge=br100-lan interface=ether4-lan
interface bridge port add bridge=br100-lan interface=ether5-lan
interface bridge port add bridge=br100-lan interface=ether6-lan
interface bridge port add bridge=br100-lan interface=ether7-lan
interface bridge port add bridge=br100-lan interface=ether8-lan
interface bridge port add bridge=br100-lan interface=ether9-lan

interface bridge port add bridge=br120-lan interface=ether10-lan
interface bridge port add bridge=br120-lan interface=ether11-lan
interface bridge port add bridge=br120-lan interface=ether12-lan
interface bridge port add bridge=br120-lan interface=ether13-lan
interface bridge port add bridge=br120-lan interface=ether14-lan

interface bridge port add bridge=br120-lan interface=ether15-lan
interface bridge port add bridge=br120-lan interface=ether16-lan
interface bridge port add bridge=br120-lan interface=ether17-lan

interface bridge port add bridge=br120-lan interface=ether18-lan
interface bridge port add bridge=br120-lan interface=ether19-lan
interface bridge port add bridge=br120-lan interface=ether20-lan

interface bridge port add bridge=br110-lan interface=ether21-lan

interface bridge port add bridge=br1-lan interface=ether22-lan
interface bridge port add bridge=br1-lan interface=ether23-lan
```

```
interface bridge port add bridge=br1-lan interface=ether24-lan
```

Призначаємо мережі віртуальним інтерфейсам

```
ip address add address=192.168.100.1/24 interface=br100-lan network=192.168.100.0
ip address add address=192.168.110.1/24 interface=br110-lan network=192.168.110.0
ip address add address=192.168.120.1/24 interface=br120-lan network=192.168.12.0
ip address add address=192.168.1.1/24 interface=br1-lan network=192.168.1.0

ip address add address=62.64.2.0/0 interface=ether1-wan network=62.64.2.0
```

Налаштуємо пул адрес мережі wi-fi, налаштуємо dhcp

```
ip pool add name=pool-wifi ranges=192.168.120.50-192.168.120.220

ip dhcp-server add address-pool=pool-wifi disabled=no interface=br2-wifi name=dhcp-wifi

ip dhcp-server network add address=192.168.120.0/24 dns-server=8.8.8.8,8.8.4.4 domain=wifi.local gateway=192.168.120.1
```

Включимо NAT, щоб пристрої, що знаходяться в мережах мали вихід в інтернет.

```
ip firewall nat add action=masquerade chain=srcnat out-interface=ether1-wan src-address=192.168.0.0/24
ip firewall nat add action=masquerade chain=srcnat out-interface=ether1-wan src-address=192.168.1.0/24
```

Ізолюємо підмережі, щоб пристрої з мережі 192.168.100.0/24 не бачили і не використовували пристрої, що знаходяться в мережі 192.168.120.0/24.

```
ip firewall filter add action=drop chain=forward disabled=yes dst-address=192.168.100.0/24 in-interface=br1-lan
```

3.2 Налаштування точки доступу

Основний акцент – налаштування контролера CAPsMAN v2 на пристрої MikroTik для керування точками доступу. Цей інструмент надає зручність керування точками доступу з одного централізованого інтерфейсу, дозволяючи визначати канали, їх ширину, SSID, параметри безпеки, централізоване керування пристроями, а також автентифікацію на основі сертифікатів та багато інших функцій. CAPsMAN v2 був введений у стандартний комплект RouterOS, починаючи з версії 6.37 і несумісний з першою версією. Для роботи з ним потрібний рівень ліцензії 4 або вище.

Необхідно врахувати один важливий момент: якщо точки доступу налаштовані на отримання параметрів від контролера і з якихось причин контролер стає недоступним, всі точки доступу зупиняють роботу до моменту, коли CAPsMAN знову буде онлайн.

Налаштування CAPsMAN

Зробимо підключення до роутера та перевіримо поточні налаштування:

У розділі General-Bridge включені порти ehter2-4. Порт ether1 спрямований на підключення до Інтернету. Також налаштовані IP-адресу, DNS та NAT.

Канали (див.рис. 3.1)

Сформуємо перший канал із частотою 2412, пропускною здатністю 20Mhz та стандартами G та N

Таким же чином налаштуємо шостий та одинадцятий канали

Доступ до даних Сформулюємо директиву для інтеграції інтерфейсів підключених точок доступу до загального мосту General-Bridge.

Local Forwarding – якщо опція не активована, то трафік від клієнтської AP буде надсилатися через контролер. Для мереж із великою кількістю точок

доступу (5-10 і більше) та багатьма підключеними клієнтами рекомендується активувати цю опцію для оптимізації роботи мережі.

Client to Client Forwarding – цей параметр дозволяє клієнтам точки доступу взаємодіяти між собою безпосередньо.

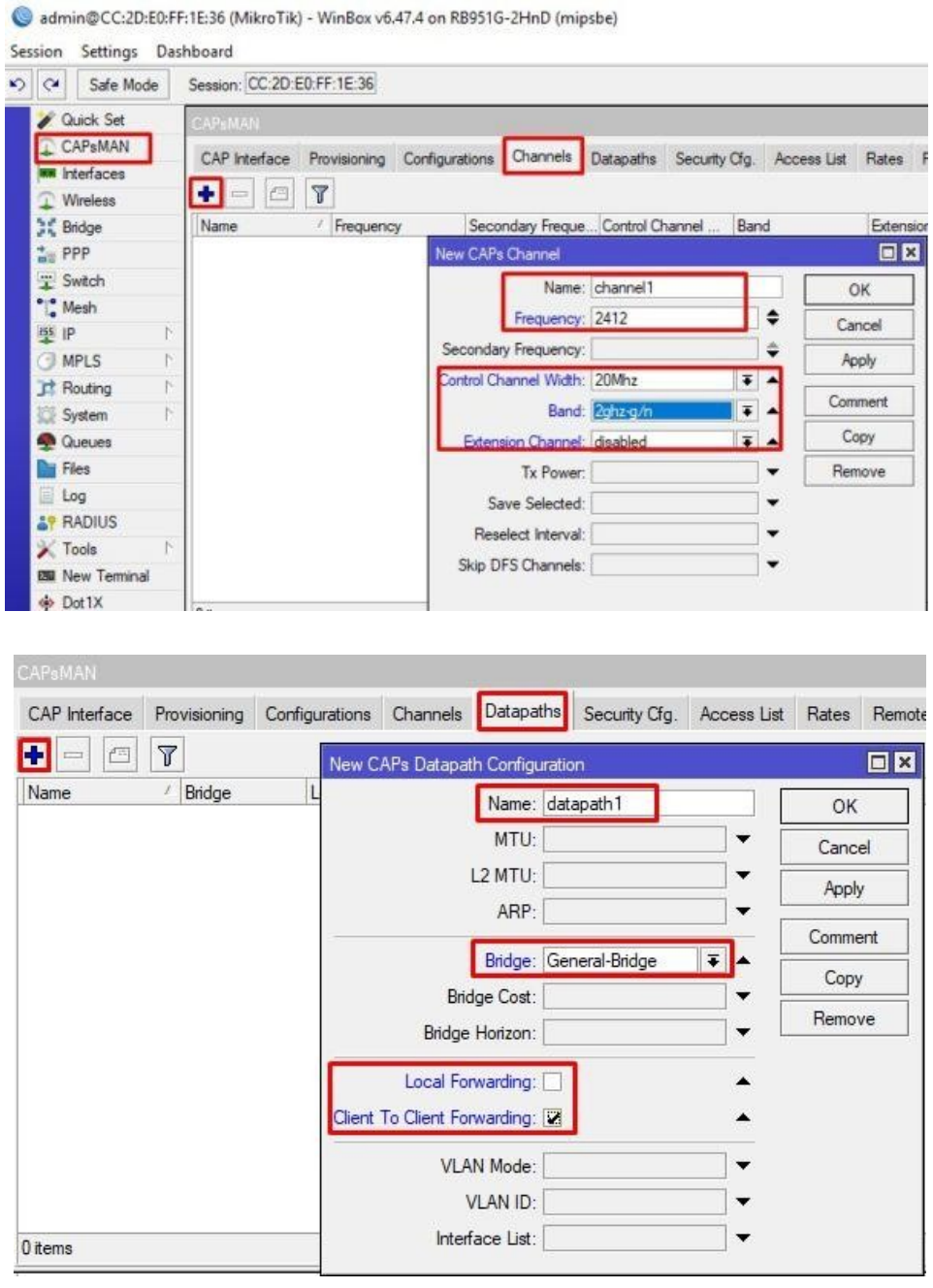


Рисунок 3.1– Створення каналу роботи безпровідної мережі зверху, знизу встановлення параметрів конгфігурації

Безпека. Налаштуємо профіль безпеки для мережі із захистом, враховуючи (див.рис.3.2):

- Найменування профілю
- Метод аутентифікації
- Тип шифрування
- Пароль

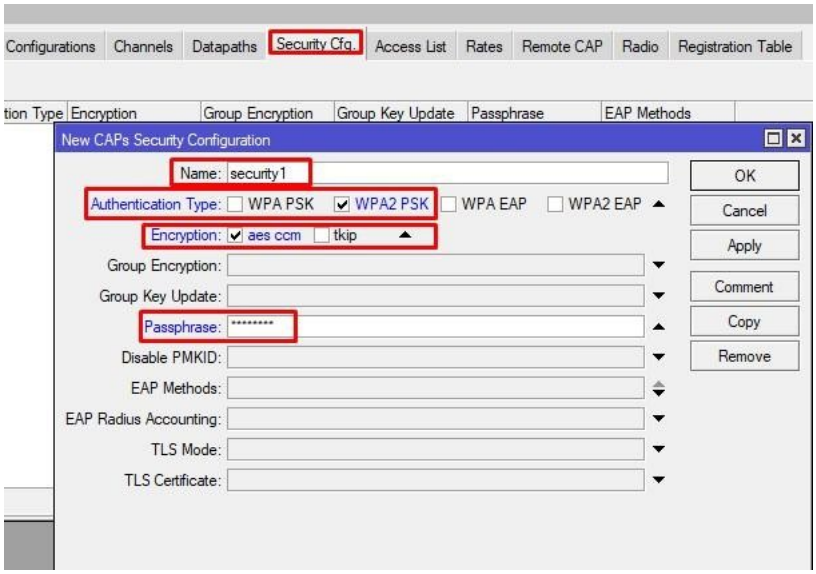


Рисунок 3.2– Встановлення параметрів безпеки

Налаштування додаткового профілю для публічної мережі, без завдання методів шифрування, ключів доступу та іншого

Налаштування. (див.рис.3.3) На цьому етапі виконуємо налаштування параметрів. Оскільки у нас передбачені як захищені, і публічні мережі, нам знадобляться дві конфігурації. Для першої у розділі бездротового зв'язку вказуємо:

- Назва конфігурації
- Режим функціонування

- SSID
- Локація
- Переважний режим безпеки
- Діапазон
- Обмеження за кількістю користувачів

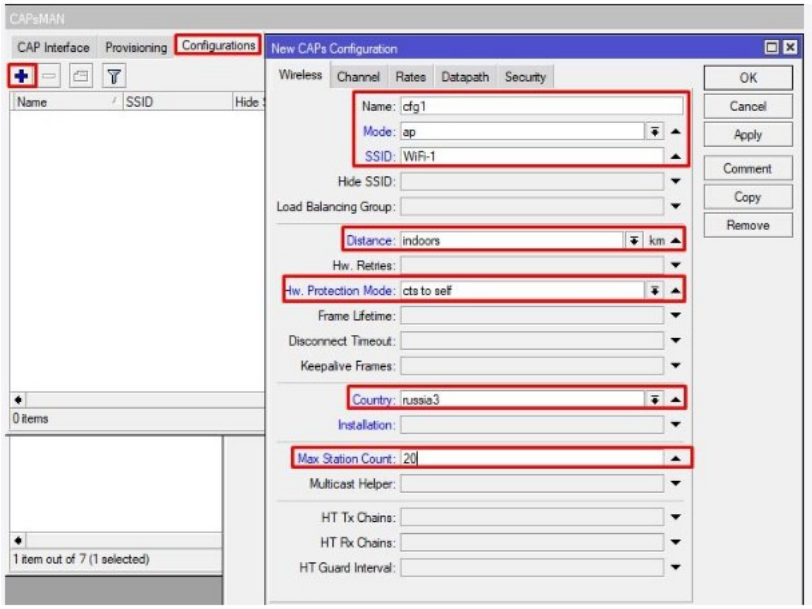


Рисунок 3.3– Створення конгфігурації захисту безпровідної мережі

Перейдемо до розділу Datapath і виберемо першу конфігурацію

Необхідно вибрати перший профіль безпеки

Сформуємо другу конфігурацію з невеликими відмінностями (див.рис. 3.4)

Для Datapath та Security Profile оберемо другі у списку

Забезпечення. Встановлюємо параметри для ініціалізації. Клієнти будуть ідентифікуватися за IP-адресою, хоча можливі й інші варіанти, наприклад, по імені системи або MAC-адреси, або комбінація всіх варіантів.

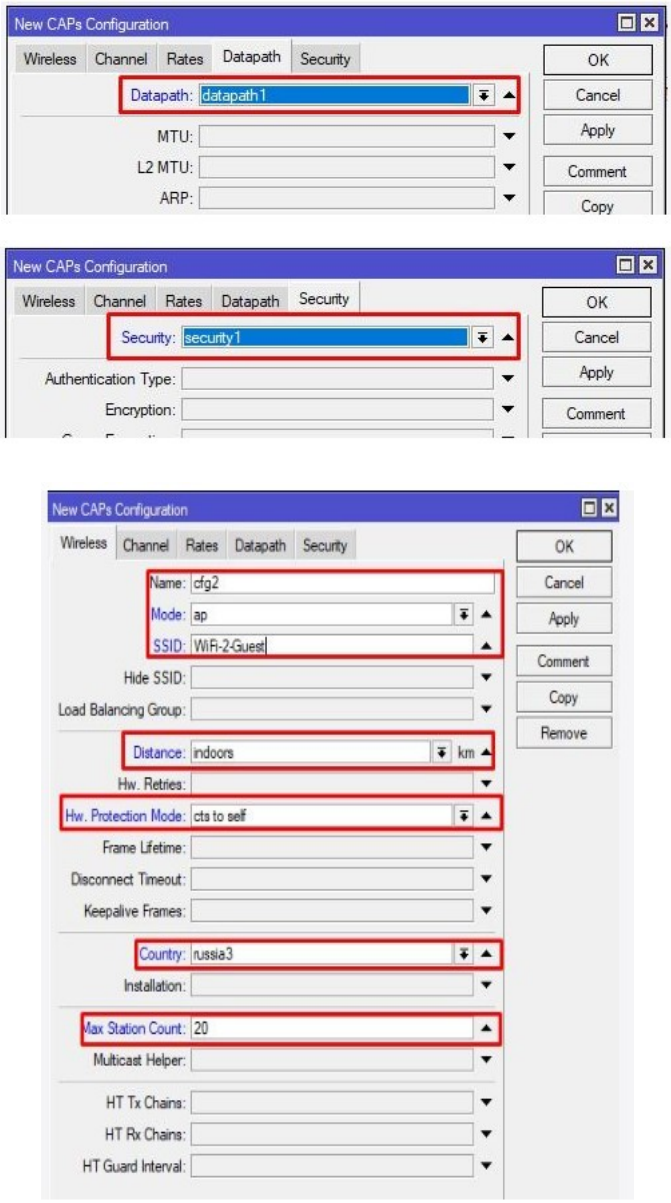


Рисунок 3.4– Створення альтернативної конгфігурації параметрів без-провідної мережі

Доступні дії:

- None – без дій
- Create enabled – створюються статичні інтерфейси
- Create disabled – створення у неактивному стані
- Create dynamic enabled – застосовується для початкових перевірок, після яких рекомендується перейти на Create enabled

Активація CAPsMAN. Так багато зусиль всього для однієї цінної галочки (див.рис.3.5)

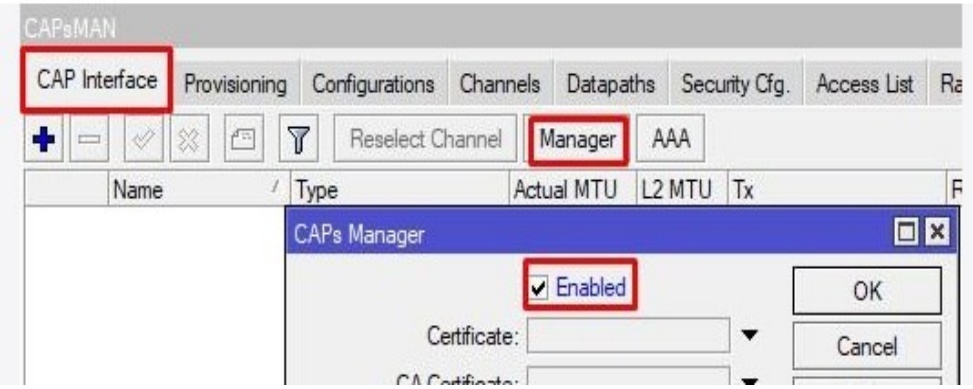


Рисунок 3.5– Активація CAPsMAN

Налаштування AP. Приєднаємося до MikroTik та розглянемо його конфігурацію.

Щоб застосувати конфігурацію, перейдіть до розділу Wireless – CAP :

- Активуйте CAP
- Interface – інтерфейс, до якого будуть застосовані налаштування
- CAPsMAN Address – вкажіть адресу контролера. Якщо у вас є резервні адреси, можна вказати їх
- Bridge – міст, до якого буде додано інтерфейси з конфігурацією, отриманою від контролера

Як можна побачити, з'явився відповідний коментар, тепер цією точкою доступу управляє контролер.(див.рис. 3.6)

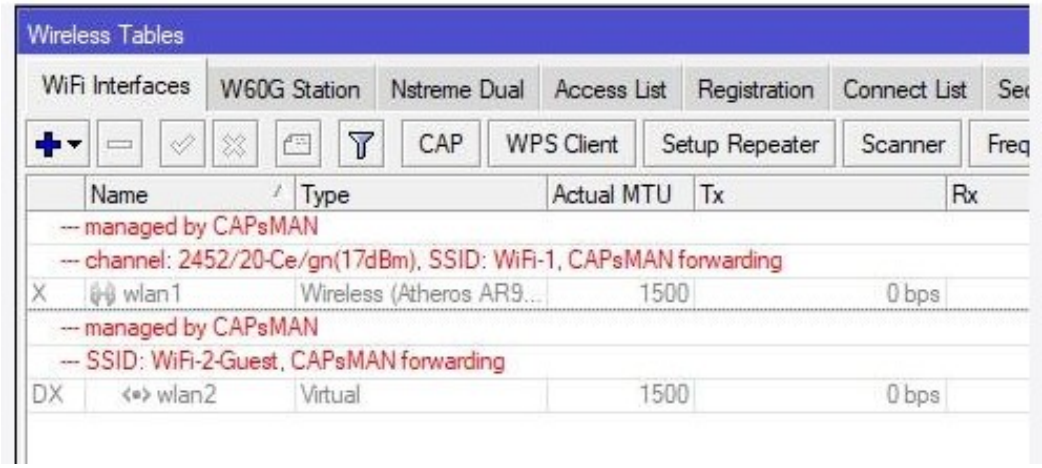


Рисунок 3.6– Приєднана точка доступу до контролера

Безперебійний роумінг. Інтернет повний заяв на тему "налаштування безперебійного Wi-Fi (роумінг) на MikroTik", але реальність така, що це лише ілюзія безшовного роумінгу. Для істинно безшовного підключення необхідний протокол 802.11R, якого немає в пристроях MikroTik, але який підтримується іншими дорогими пристроями. Багато посібників направляють нас на «тонке налаштування» Access List з метою примусового відключення клієнта при досягненні певного рівня сигналу. Однак, такий підхід позбавляє користувача можливості псевдо роумінгу.

Ключовий момент полягає в правильному розміщенні точок доступу. Під "правильно" мається на увазі, щоб сигнал до клієнтського пристрою був у діапазоні -70-75 дБм. У цьому випадку CAPsMAN визначить, що якість сигналу у вас недостатня і переключить вас на найближчу доступну точку (якщо вона коректно встановлена і її сигнал кращий). Перемикання в цій ситуації відбудеться на другому етапі аутентифікації, а не з самого початку, що робить процес швидшим, ніж при примусовому відключенні. Це додаткова функція, а чи не повноцінна реалізація роумінгу.

Access List використовується для інших цілей, таких як керування доступом до точок. У рамках CAPsMAN таке управління здійснюється централізовано.

Подивіться, чи є можливість дозволяти або забороняти підключення до певних або всіх точок доступу для конкретних MAC-адрес.

Ми почали з одного підходу та перейшли до іншого. Сподіваємось, що тепер все стало ясніше для вас.Налаштування сертифікатів

На жаль, початкова версія мала недоліки, що давало змогу легко імітувати роботу AP.

Перейдіть до Manager , потім у розділі Certificate та CA Certificate , де слід вибрати опцію auto.

Після підтвердження налаштувань, роутер створить CA та сертифікат для себе. Виберіть їх зі списку замість попереднього значення «auto» (див.рис. 3.7)

Рисунок 3.7– Прописування сертифікатів роутера

Після цього клієнтська сторона надішле запит на контролер для отримання сертифіката. Як тільки сертифікат буде отримано, змініть значення «auto» на назву отриманого сертифіката у списку, що випадає. Також рекомендується встановити значення для CAPsMAN Certificate Common Name. Активуючи опцію Lock To CAPsMAN, ви створюєте строгу прив'язку до контролера. Однак, якщо ви анулюєте сертифікат контролера, точки доступу перестануть функціонувати.

Якщо все пройшло успішно, конфігурація буде використана без помилок. Застосуйте аналогічні дії для решти точок доступу. Потім на контролері активуйте опцію «Вимагати сертифікат учасника» (Require Peer Certificate).

Тепер ми встановлюємо обов'язкову умову наявності сертифіката для точок доступу.

3.3 Налаштовуємо мережеве сховище - FreeNAS 9.1.1 [12]

Встановлення та налаштування FreeNAS

За основу ми візьмемо найпопулярніший дистрибутив, заточений під ці цілі – FreeNAS . Системні вимоги спочатку невеликі, але продуктивність мережевого сховища залежить від продуктивності заліза.

FreeNAS можна встановити на жорсткий диск або флешку USB. У цьому система займає весь обсяг носія який встановлюється , незалежно від ємності, проте мережні ресурси для зберігання інформації розміщуються інших жорстких дисках. Тому якщо у вас є лише один жорсткий диск, то ми вам рекомендуємо встановлювати систему на USB-флешку, при цьому головне щоб комп'ютер підтримував завантаження з USB носіїв. Місткість флешки має бути не менше 2 Гб.

Додатково є два жорсткі диски, щоб отримати можливість резервування важливої інформації на основі роботи програмного RAID. Це особливо буде цікаво тим, хто дбає про надійність зберігання своєї інформації.

У разі використання програмного RAID ви працюєте тільки з одним диском з двох, а другий FreeNAS використовує як точну копію першого диска в режимі реального часу. Тобто вся записувана інформація одночасно пишеться на обидва диски . Якщо раптом один із дисків вийде з ладу, система продовжить працювати на другому диску, як ні в чому не бувало. Потім ви змінюєте несправний диск на новий і він автоматично синхронізується з наявним диском. При використанні RAID , обсяг доступний для даних дорівнюватиме об'єму найменшого з двох дисків.

Описувати встановлення програми не будем, оскільки це стандартна прроцедура. Початкове налаштування

Після перезапуску ми побачимо екран FreeNAS. Цей екран нам буде корисним для налаштування мережеої плати.

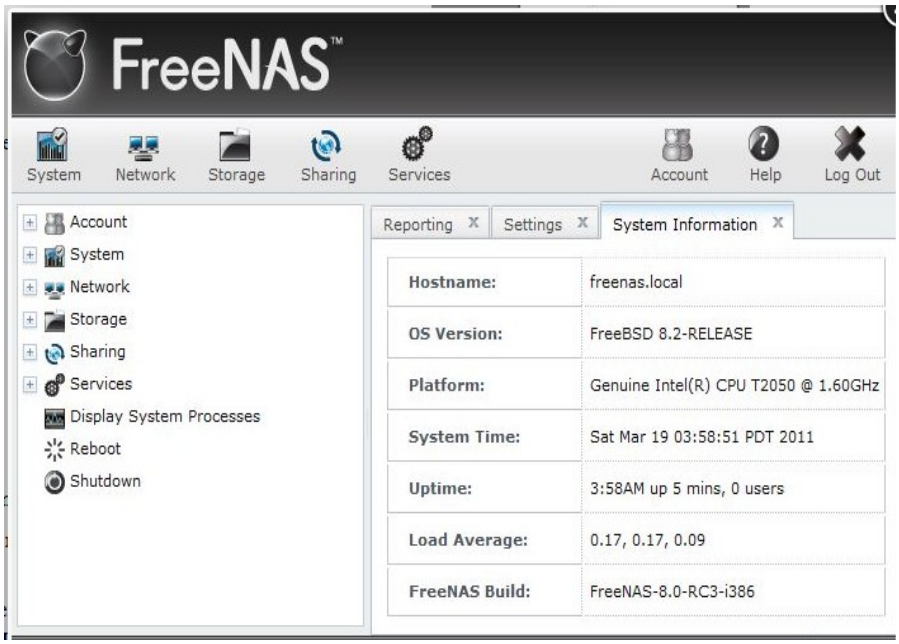


Рисунок 3.8– Вікно зведеної конгфігурації про систему

Заходимо на FreeNAS через Firefox або Chrome.

Насамперед заходимо на Web-інтерфейс FreeNAS і логінимся там з параметрами за замовчуванням: логін - admin і пароль - freenas

Потім ми потрапимо до основного меню нашої системи, де буде представлена зведена інформація про ПК (див.рис.3.8)

Насамперед ми перейдемо в закладку Settings і поміняємо там часовий пояс, щоб логи нашого FreeNAS велися правильно.

Не зайвим буде ще вказати DNS- сервер в налаштуваннях мережі, для цього тиснемо по кнопці Network у верхній панелі і в полі Nameserver 1 вписуємо IP-адресу нашого маршрутизатора (або виділеного DNS-сервера, якщо він є). Не забуваймо зберегти налаштування. Щодо мережі FreeNAS має одну дуже корисну функцію - Link Aggregation. Простіше кажучи, якщо ми вставимо в ПК кілька мережевих плат, всі вони зможуть працювати одночасно для підсумовування швидкості доступу до нашого мережевого сховища . Налаштовується Link Aggregation у відповідній закладці. Не зайвим буде поміняти стандартний пароль адміна: у лівій панелі необхідно зайти в Account – My Account – Change Password.

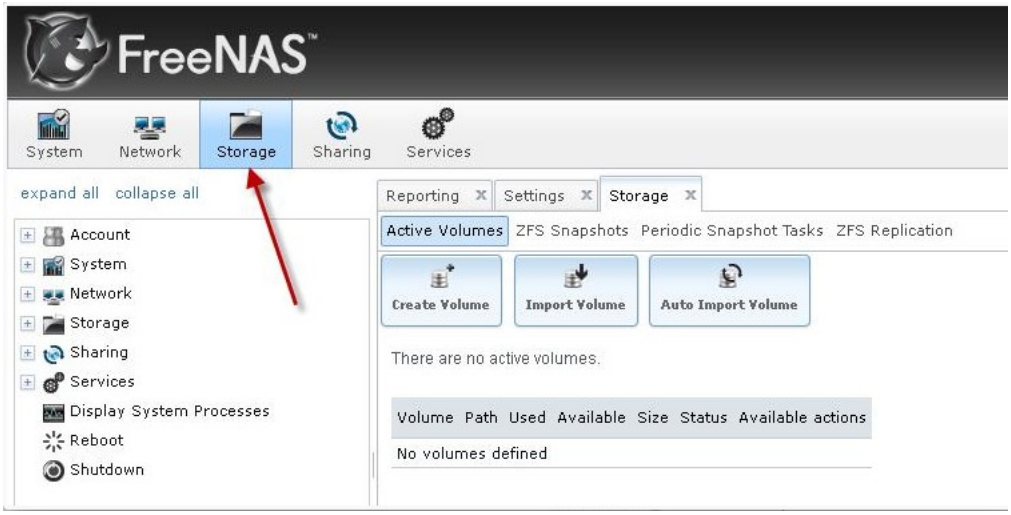


Рисунок 3.9– Вікно добавлення дисків в систему

Тепер нам потрібно додати жорсткі диски до системи (див.рис. 3.9) та визначити файлову систему. Робиться це у розділі Storage (кнопка у верхній панелі).

У правій частині з'явиться три кнопки, за допомогою яких можна додати диски як нові або імпортувати диски з існуючою інформацією.

Давайте розглянемо процес додавання, натискаємо кнопку Create Volume і перед нами з'явиться нове вікно (див.рис. 3.10):

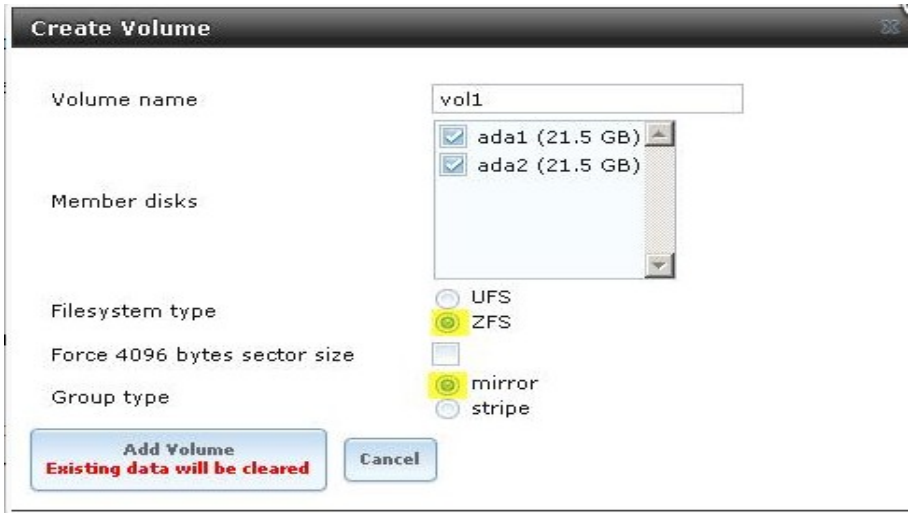


Рисунок 3.10– Вікно вибору дсків

Тут у списку ми вибираємо обидва жорсткі диски та опцію mirror , якщо хочемо зробити RAID , або один жорсткий диск, якщо функціонал RAID нам не потрібен.

У полі Volume name вказуємо ім'я тома.

Тепер потрібно вибрати файлову систему. FreeNAS підтримує дві файлові системи - це UFS та ZFS. Найкращою вважається ZFS, її варто вибрати.

Якщо всі параметри встановлено, натисніть кнопку Add Volume .

Щоб оновлена інформація стала доступною, закрийте закладку Storage і ще раз клацніть по ній у верхній частині інтерфейсу.

Останнє, що треба зробити, це встановити права для всіх датасетів. Якщо ви вперше налаштовуєте FreeNAS, то ми вам рекомендуємо зробити все просто. Для цього зайдіть у призначення прав кожного датасета (кнопки позначені стрілками на скріншоті вище) і виставте як показано на малюнку (див.рис. 3.11):

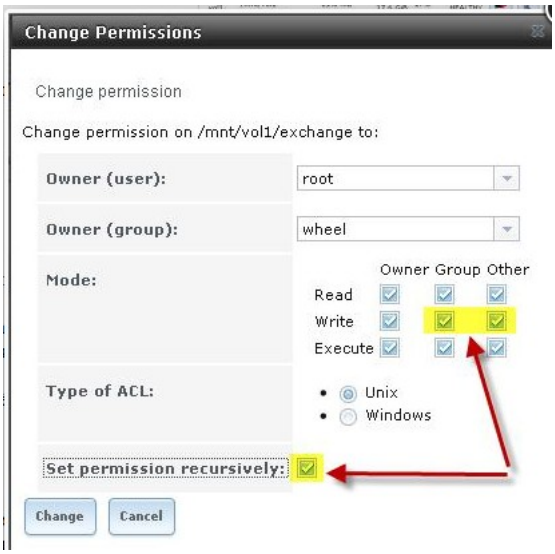


Рисунок 3.11– Встановлення прав клієнтів

Перш ніж ми почнемо створювати мережеві ресурси, нам потрібно визначитися зі схемою доступу до сховища мережі. Варіантів два: або використовувати персональні логіни з паролями, або використовувати вільний доступ.

Всі дані про користувачів та групи зберігаються в розділі Accounts лівої панелі веб-інтерфейсу. Для створення користувача використовується пункт Add User , а для перегляду всіх існуючих користувачів – View All Users .

При створенні нового користувача заповнюється стандартна форма, де вказується його логін, пароль , ім'я, електронна пошта.

FreeNAS вміє робити ресурси всім платформ: для Apple (AFP), для UNIX-систем (NFS) і Windows (CIFS). І це крім універсальних FTP тощо. Розглянемо створення ресурсу для Windows комп'ютерів.

Ідемо в розділ Sharing , Windows і натискаємо кнопку Add Windows Share (див.рис. 3.12)

Рисунок 3.12– Вікно створення Windows Share

Перед нами з'явиться вікно, в якому ми вкажемо ім'я створюваного ресурсу (exchange), вкажемо зрозумілий коментар, потім у полі Path треба вибрати той датасет, який ми зробили під файли.

Далі промотуємо весь список опцій до кінця та внизу вікна натискаємо кнопку OK . Наш ресурс готовий. Про всяк випадок ось ще список цікавих параметрів, які можна вказати при створенні ресурсу:

Export Read Only – зробити ресурс тільки для читання

Browsable to Network Clients – Видимість ресурсу в мережевому оточенні. Якщо прапорець зняти, ми зробимо приховану кулі.

Inherit permissions - успадковувати дозволи

Export Recycle Bin - додати кошик, тобто. дані з пулу спочатку видалятимуться в кошик

Show Hidden Files - відображення прихованих файлів

Guest Account - гостьовий обліковий запис. Краще залишити такий

Allow Guest Access - дозволяти гостьовий вхід (тобто в кулі можна буде увійти без будь-яких паролів тощо)

Only Allow Guest Account - тільки гостьовий вхід. Не можна буде окремо ввести пароль при вході в кулі, щоб підвищити свої права

Host Allow - список IP-адрес, з яких можна заходити в пул. Як роздільник можна використовувати пропуск

Host Deny - список IP-адрес, з яких не можна заходити в пул. Як роздільник можна використовувати пробіл

Тепер перейдемо до налаштування служби CIFS. Ідемо до розділу Services , а там натискаємо на значок гайкового ключа навпроти служби CIFS

У вікні нам потрібно вказати ряд параметрів:

Authentication Model – схема доступу. Можливі варіанти: анонімний доступ (Anonymous) та за логінами (Local User). Вибираємо потрібне

NetBIOS Name – ім'я комп'ютера в мережі

Workgroup – ім'я робочої групи. Треба ставити таким же, як у ваших інших комп'ютерів у мережі

Description - якщо це поле взагалі не заповнювати, то FreeNAS натомість підставляє неінформативну службову інфу. Тому ми вам рекомендуємо в цьому полі написати хоча б пропуск

Вибір кодувань (DOS charset і UNIX charse t) - можете встановити все так, як показано на скріншоті вище

Local Master - визначити FreeNAS головним комп'ютером в робочій групі

Time Server for Domain - зробити FreeNAS сервером точного часу для комп'ютерів мережі

Guest Account - допускати гостьовий вхід до мережевих ресурсів. Не встановлюйте цю галку, якщо використовуєте схему доступу за логіном та паролем (Local User) File Mask - маска доступу для створюваних файлів. Спочатку краще встановити це значення 0777

Directory Mask - теж саме що File Mask, тільки для каталогів

Інші параметри можна залишити як є. Перейдіть до кінця сторінки і натисніть OK . Залишається просто увімкнути службу CIFS, для цього треба клацнути мишею по значку OFF навпроти назви служби. За кілька секунд його статус зміниться на ON.

Тепер можна спробувати зайти на наше сховище з будь-якого комп'ютера мережі. На ньому будуть представлені два створені нами ресурси.

Якщо ви вибрали схему доступу Local User (за логінами та паролями), то в exchange ви зможете потрапляти вільно, а у documents у вас запитають логін та пароль.

3.4 Тестування мережі

Тестування мережі за допомогою команд ping, tracert та інших є важливим етапом діагностики та перевірки її працездатності. Ці інструменти дозволяють визначити наявність з'єднання, затримки, втрати пакетів та маршрут проходження даних. Ось опис основних команд та їх використання:

1. ping

Команда ping є однією з найпростіших та найчастіше використовуваних для перевірки базового з'єднання між двома вузлами в мережі.

Як працює:

ping відправляє на вказану IP-адресу або доменне ім'я ехо-запит (ICMP Echo Request).

Якщо вузол призначення доступний і налаштований на відповідь на такі запити, він надсилає у відповідь ехо-відповідь (ICMP Echo Reply).

У результаті виконання команди відображається час затримки (round-trip time, RTT) кожного пакета, а також інформація про втрачені пакети.

Використання:

Перевірка доступності вузла: ping <IP-адреса> або ping <доменне ім'я> (наприклад, ping 192.168.1.1 або ping google.com).

Визначення затримки: Час, що відображається у відповіді, показує, скільки часу знадобилося пакету, щоб дістатися до призначення та повернутися. Висока затримка може свідчити про проблеми з мережею.

Виявлення втрати пакетів: Якщо у звіті ping вказано втрачені пакети, це може вказувати на нестабільне з'єднання або проблеми на шляху проходження даних.

Безперервний пінг: У Windows можна використовувати команду ping -t <IP-адреса> для безперервного відправлення запитів до зупинки вручну (Ctrl+C). У Linux команда ping за замовчуванням працює безперервно до зупинки.

Інтерпретація результатів:

Reply from <IP-адреса>: Означає, що вузол призначення відповідає.

Time=...ms: Час затримки в мілісекундах.

TTL (Time To Live): Значення, що зменшується з кожним проходженням через маршрутизатор. Початкове значення може дати уявлення про кількість маршрутизаторів на шляху.

- Request timed out: Вказує на те, що відповідь від вузла призначення не була отримана протягом встановленого часу очікування. Це може бути пов'язано з недоступністю вузла, блокуванням ICMP-пакетів брандмауером або проблемами з мережею.
- Destination host unreachable: Повідомлення про те, що мережа не знає, як дістатися до вказаного хоста.

2. tracert (Windows) / traceroute (Linux, macOS)

Команда tracert (в Windows) або traceroute (в Linux та macOS) використовується для відстеження маршруту, яким пакети даних прямують до вказаного вузла призначення.

Як працює:

- Команда відправляє серію пакетів UDP (в Linux) або ICMP (в Windows) з поступово збільшуваним значенням Time To Live (TTL).
- Перший пакет має TTL=1, тому він "гине" на першому ж маршрутизаторі, який відправляє назад повідомлення "Time Exceeded".
- Наступний пакет має TTL=2, і так далі. Таким чином, команда крок за кроком визначає всі проміжні маршрутизатори на шляху до призначення.
- Для кожного проміжного вузла відображається його IP-адреса (та, за можливості, доменне ім'я) та час затримки трьох послідовних запитів.

Використання:

- Визначення маршруту: Дозволяє побачити шлях, яким дані досягають віддаленого хоста.
- Виявлення проблемних ділянок мережі: Висока затримка або відсут-

ність відповіді на певному проміжному вузлі може вказувати на проблему саме на цій ділянці.

- Діагностика проблем з підключенням: Якщо `ping` до кінцевого вузла не проходить, `tracert` може допомогти визначити, на якому етапі виникає проблема.

Приклад використання:

tracert google.com (в Windows)

traceroute google.com (в Linux/macOS)

Інтерпретація результатів:

- Кожен рядок у виводі представляє один "стрибок" (хоп) - проміжний маршрутизатор.
- Перший стовпець - номер стрибка.
- Наступні три стовпці - час затримки в мілісекундах для трьох відправлених пакетів.
- Останній стовпець - IP-адреса та (якщо доступно) доменне ім'я маршрутизатора.
- `* * * Request timed out` на певному стрибку може означати, що маршрутизатор не відповідає на запити `tracert` (можливо, через налаштування безпеки), але це не завжди свідчить про проблему з прохідністю трафіку.

3. Інші корисні команди для тестування мережі:

- `ipconfig` (Windows) / `ifconfig` (Linux, macOS): Відображає поточні налаштування мережевих інтерфейсів, такі як IP-адреса, маска підмережі, шлюз за замовчуванням, DNS-сервери. Корисна для перевірки локальних налаштувань мережі.
- `ipconfig /all` (Windows) - відображає повну інформацію, включаючи MAC-адресу, інформацію про DHCP та DNS.
- `netstat` (Windows, Linux, macOS): Відображає активні мережеві

з'єднання, таблиці маршрутизації, статистику інтерфейсів. Допомагає відстежувати, які програми використовують мережеві з'єднання та які порти відкриті.

- `netstat -ano` (Windows) - відображає всі активні TCP-з'єднання та порти прослуховування, а також PID процесів, які їх використовують.
- `netstat -tuln` (Linux) - відображає TCP, UDP та UNIX сокети, що прослуховуються, у числовому форматі.
- `nslookup` (Windows, Linux, macOS): Використовується для запиту DNS-серверів для отримання інформації про доменні імена або IP-адреси. Дозволяє перевірити, чи правильно працює розпізнавання імен.
- `nslookup <доменне ім'я>` - повертає IP-адресу для вказаного домену.
- `nslookup <IP-адреса>` - виконує зворотний DNS-запит і намагається знайти доменне ім'я для вказаної IP-адреси.
- `arp` (Windows, Linux, macOS): Відображає та змінює ARP-таблицю (Address Resolution Protocol), яка містить відповідність між IP-адресами та MAC-адресами в локальній мережі. Корисна для діагностики проблем з локальною комунікацією.
- `arp -a` - відображає поточну ARP-таблицю.
- `route` (Windows, Linux, macOS): Відображає та змінює таблиці маршрутизації, які визначають, яким шляхом повинні прямувати пакети до різних мереж призначення. Корисна для діагностики проблем з маршрутизацією.
- `route print` (Windows) - відображає таблицю маршрутизації.
- `netstat -r` (Windows, Linux) - також відображає таблицю маршрутизації.
- `route -n` (Linux) - відображає таблицю маршрутизації в числовому

форматі.

- `telnet` (Windows, Linux, macOS): Використовується для встановлення TCP-з'єднання з віддаленим хостом на вказаний порт. Хоча зараз рідко використовується для віддаленого доступу, може бути корисним для перевірки, чи прослуховується певний порт на віддаленому сервері (наприклад, `telnet <IP-адреса> <порт>`).
- `curl` (Linux, macOS, Windows): Потужний інструмент командного рядка для передачі даних з або на сервер. Часто використовується для тестування вебсервісів та API.
- `curl <URL>` - відправляє HTTP-запит GET на вказаний URL і відображає відповідь.

Розуміння та вміле використання цих команд є важливим навиком для будь-якого адміністратора мережі або фахівця з інформаційних технологій для діагностики та усунення проблем з мережею.

3.5 Моделювання мережі в Cisco Packet Tracer [13]

Cisco Packet Tracer - це багатофункціональна програма моделювання мереж, яка дозволяє експериментувати з поведінкою мережі і оцінювати можливі сценарії.

У верхній частині знаходиться головне меню (див.рис. 3.13).

Воно містить такі кнопки: File, Edit, Options, View, Tools, Extensions, Help.(1)

Рисунок 3.13 - Головне меню програми

Під головним меню розташовується панель (2) з найпотрібнішими і найбільш часто вживаними елементами головного меню.

Категорія File містить стандартні пункти, такі як: створити новий файл, відкрити файл, зберегти файл, надрукувати файл, вийти (див.рис. 3.14).

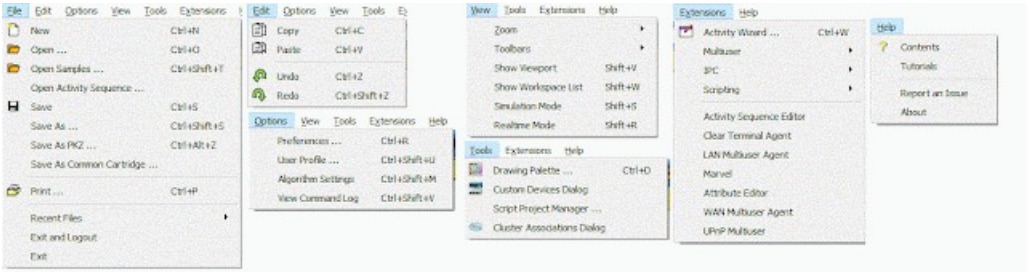


Рисунок 3.14 - Категорія File програми

Ще нижче розташовується перемикач між логічною та фізичною організацією мережі (див.рис. 3.15).

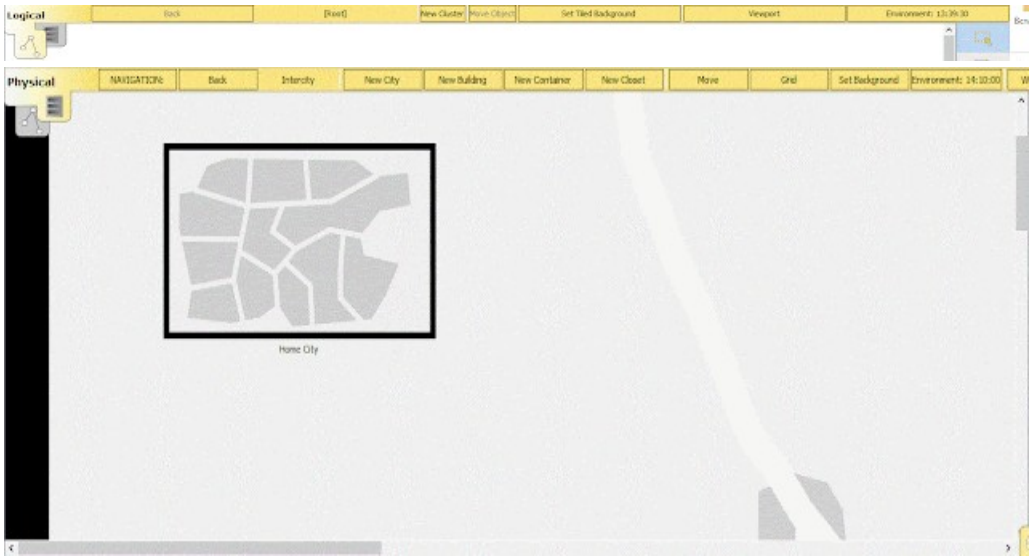


Рисунок 3.15 - Перемикач між логічною та фізичною організацією мережі (зверху), та фізична карта мережі

При зміні на фізичну організацію мережі, порожній бланк замінюється на фізичну карту, на яку можна додавати міста, будівлі, шафи, встановлювати фон. Натомість у логічній організації можна додавати кластери. Тобто фізичній організації мережі ми створюємо зовнішню структуру нашої мережі(місто->будинок->офіс).

А в логічній ми всі ланки нашої структури організовуємо відповідно до заданої задачі.

В обох вкладках ми можемо змінювати характеристику(сила вітру, погодні умови, радіація і т.д) навколишнього середовища при натисканні кнопки Environment.

Зміни певних значень в цьому вікні будуть позначатись на характеристиках мережі.

Знизу зліва міститься панель з присторями (див.рис. 3.16).

На ній містяться різновиди хабів, свічів, роутерів, бездротових девайсів, з'єднань, кінцевих пристороїв, безпеки, емуляція глобальної мережі, з'єднання мультиюзера, кастомні пристрої.

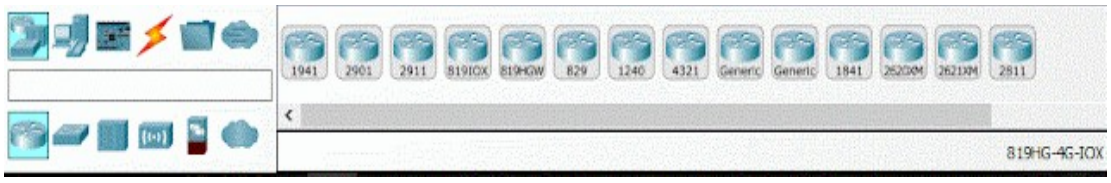


Рисунок 3.16 - Панель з присторями

Один раз натиснувши на пристрій отримаємо фізичне зображення пристрою. Тут ми можемо додавати різні модулі до комп’ютера (див.рис. 3.17).

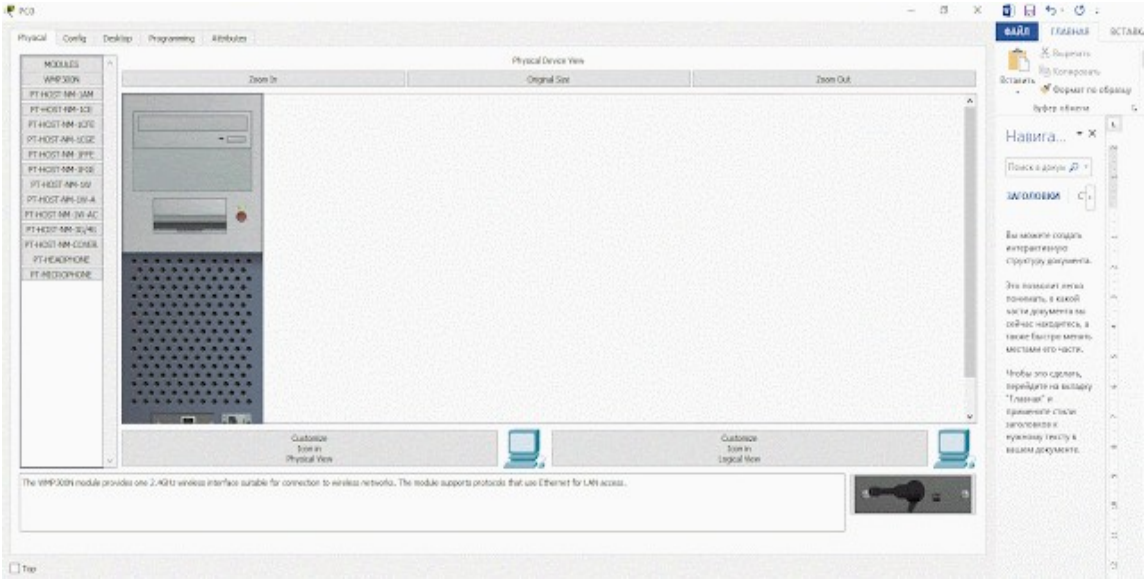


Рисунок 3.17 - Добавляння пристроїв в компютер

Вкладка Desktop представляє собою уявний робочий стіл з якого ми можемо керувати обраним комп’ютером (див.рис. 3.18).

Ми можемо налаштувати IP конфігурації, зайти в термінал, виконати певні команди в командному рядку, зайти до веб-браузеру, щоб перевірити під’єднання обраного комп’ютеру до мережі Інтернет.

Рисунок 3.18 - Вкладка Desktop для симуляції роботи з компютером

Ось як виглядає вікно налаштування адреси IP (див.рис. 3.19).

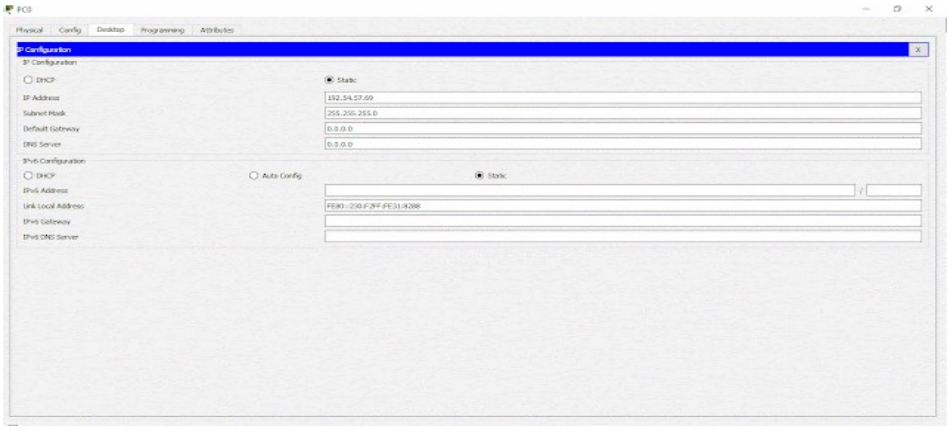


Рисунок 3.19 - Вікно налаштування адреси IP

Для зєднання пристроїв в мережу існують кнопки. вкладки Connnections

В результаті проектування моделі мережі, в нас получиться така схема, яка показана на рисунку 3.20.

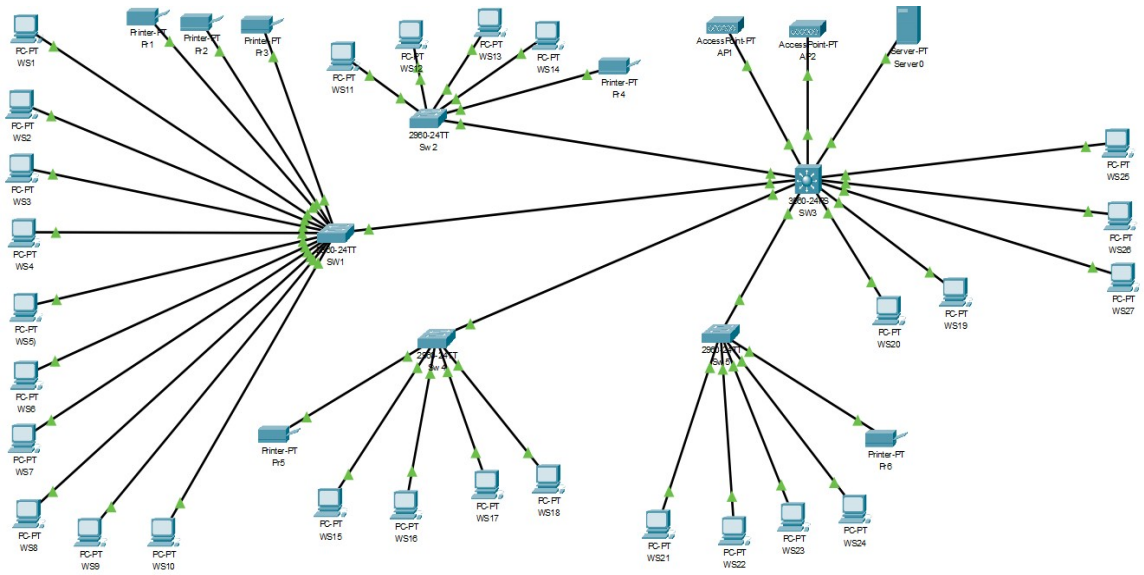


Рисунок 3.20 — Створена модель мережі

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки комп'ютерної мережі для компанії «Авто-ком» 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	16
2	Монтаж кабельних каналів	Технік	30
3	Монтаж активного та пасивного мережевого обладнання	Технік	12
4	Тестування мережі. Моніторинг основних параметрів	Інженер	18

Продовження таблиці 4.1

1	2	3	4
5	Налагодження мережі та створення технічної документації	Інженер	12
Разом		-	88

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

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

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

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

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

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

Основна заробітна плата розраховується за формулою:

$$Зосн.=Тс * Кг , \quad (4.1)$$

де Тс – тарифна ставка, грн.;

Кг – кількість відпрацьованих годин.

Отже, основна заробітна плата для:

- керівника проекту: Зосн1 = 16*150 = 2400,00 грн.
- інженера: Зосн2 = 42 * 140 = 5880,00 грн.
- техніка: Зосн3 = 30 * 120= 3600,00 грн.

Сумарна основна заробітна плата становить:

Зосн = 2400,00+ 5880,00+ 3600,00 = 11880,00 грн

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

$$Здод.=Зосн.* Кдопл , \quad (4.2)$$

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

Отже, додаткова заробітна плата по категоріях працівників становить:

1. керівника проекту: Здод1= 2400,00 · 0,15 = 360,00 грн.
2. інженера: Здод2= 5880,00 · 0,15 = 882,00 грн.
3. техніка: Здод3= 3600,00 · 0,15 = 540,00 грн.

Загальна додаткова заробітна плата становить:

Здод = 360,00 + 882,00 + 540,00 = 1782,00 грн.

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

$$Во.п.=Зосн.+Здод , \quad (4.3)$$

Во.п = 11880,00 + 1782,00= 13662,00 грн

Крім того, слід врахувати суму нарахування на заробітну плату:

- фонд страхування на випадок безробіття – 1,6 %;
- фонд по тимчасовій втраті працездатності – 1,4 %;
- пенсійний фонд – 33,2 %;

- внески на страхування від нещасного випадку на виробництві та професійного захворювання - 1,4%.

Загальна сума зазначених відрахувань становить 37,6 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.} = ФОП \cdot 0,376, \quad (4.4)$$

де ФОП – фонд оплати праці, грн.

$$В_{с.з.} = 13662,00 \cdot 0,376 = 5136,91 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додатк. зароб. плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тариф. Ставка, грн.	К-сть відпр. год.	Факт. нарах. з/пл., грн.			
1	Керівник проекту	150	16	2400,00	360,00	-	-
2	Інженер	140	42	5880,00	882,00		
3	Технік	120	30	3600,00	540,00	-	-
Разом				11880,00	1782,00	5136,91	18798,91

Отже, загальні витрати на оплату праці становлять 18798,91 грн.

4.3 Розрахунок матеріальних витрат

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

$$МВі = qі \cdot рі \quad (4.5)$$

де qі – кількість витраченого матеріалу і-го виду;

рі – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$Зм.в. = \sum МВі \quad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. вим.	шт	Ціна 1-ці, грн.	Загальна сума витрат, грн.
1	комутатор Zyxel GS1100-16	шт	3	3000,00 грн.	9000,00 грн.
3	Комутатор MikroTik CRS328-24P-4S+RM	шт	1	1700,00 грн.	1700,00 грн.
4	MikroTik cAP AC RBcAPGi-5acD2nD	шт	2	2600,00 грн.	5200,00 грн.
5	Сервер Lenovo ThinkSystem ST50 V2	шт	2	40000,00 грн.	80000,00 грн
5	Комутаційна шафа	шт	1	7120,00 грн.	7120,00 грн.
6	Кабель мережевий	шт	4	2800,00 грн.	9200,00 грн.
7	Короб 20х40х2000	шт	45	39,00 грн.	1755,00 грн.
Разом					115975,00 грн.

Отже, загальна сума матеріальних витрат дорівнюють Зм.в = 115975,00 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$Зе=W \cdot T \cdot S, \quad (4.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 14 годин, споживана потужність - 0,5 кВт/год, вартість електроенергії 6,5 грн.

Тому:

$Зе = 0,5 \cdot 14 \cdot 6,5 = 45,5$ грн.

4.5 Визначення транспортних затрат

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

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

де Тв – транспортні витрати.

Отже,

$Тв = 115975,00 \cdot 0,08 = 9278,00$ грн.

4.6 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному вигляді 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:

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

де А – амортизаційні відрахування за звітний період, грн.

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

$Н_А$ – норма амортизації, %;

Т – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 14 год., балансова вартість ПК – 28500,00 грн., тому:

$А = 28500 \cdot 0,04 /150 \cdot 14 = 133,00$ 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.

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

де Нв – накладні витрати.

Нв = 18798,91 · 0,50 = 9399,46 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	1 8798,91	11,84
Відрахування на соціальні заходи	5136,91	3,24
Матеріальні витрати	115975,00	73,05
Витрати на електроенергію	45,50	0,03
Транспортні витрати	9278,00	5,84
Амортизаційні відрахування	133,00	0,08
Накладні витрати	9399,456	5,92
Собівартість	158766,78	100

Собівартість (Св) НДР розрахуємо за формулою:

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

Отже, собівартість дорівнює

Св =158766,78 грн

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

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

де Св – собівартість виконання НДР;

Ррен. – рівень рентабельності,

ПДВ – ставка податку на додану вартість,

Ц = 158766,78· (1+0,3) · (1+0,2) = 236244,97 грн.

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва - категорія, яка характеризує результативність виробництва. Вона свідчить не лише про приріст обсягів виробництва, а й про те, якими витратами ресурсів досягається цей приріст, тобто свідчить про якість економічного зростання.

Прибуток розраховується за формулою:

$$П = Ц - С_в \quad (4.13)$$

П = 236244,97 — 158766,78 = 77478,19 грн.

Економічна ефективність (Ер) полягає у відношенні результату виробництва до затрачених ресурсів і розраховується за формулою 4.14.

$$Е_р = П / С_в, \quad (4.14)$$

де П – прибуток;

$С_в$ – собівартість.

$Е_р$ = 77478,19 / 158766,78 = 0,48

Поряд із економічною ефективністю розраховують (формула 4.15) термін окупності капітальних вкладень (Тр):

$$T_р = 1 / E_р \qquad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку

$$T_р=1/0,48=2,08$$

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.	158766,78
2.	Плановий прибуток, грн.	77478,19
3.	Ціна, грн.	236244,97
4.	Термін окупності, рік	2,08

Загальна вартість розробленої комп'ютерної мережі компанії «Автоком» становить 236244,97 грн. Термін окупності становить 2,08 роки.

5. ОХОРОНА ПРАЦІ, ТЕХНІКИ БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1 Способи і засоби пожежогасіння в компанії «Авто-ком»

Одним з елементів забезпечення пожежної безпеки в офісі є первинні засоби пожежогасіння. Необхідно утримувати їх в належному стані та навчити персонал користуватися ними у випадку виникнення надзвичайної ситуації.

До первинних засобів пожежогасіння належать: вогнегасники, кошма (покривало з негорючого теплоізоляційного полотна), ящики з піском, бочки з водою, пожежні відра, багри, ломи, сокири тощо.

Найбільш зручними для використання в умовах офісу є вогнегасники.

Попри обладнання будівель будь-якими типами установок пожежогасіння, пожежної сигналізації або внутрішніми пожежними кранами, офісні приміщення також мають бути забезпечені первинними засобами пожежогасіння.

Відповідальними за своєчасне та повне оснащення об’єктів засобами пожежогасіння, забезпечення їх технічного обслуговування, навчання працівників правил користування ними є власники або орендарі об’єктів.

В кожній організації наказом або розпорядженням керівника повинна бути призначена особа, відповідальна за експлуатацію вогнегасників.

Це може бути особа відповідальна за дотримання вимог пожежної безпеки на об’єкті або спеціаліст відповідної категорії з іншої організації, наприклад, пункту технічного обслуговування вогнегасників.

Успішне гасіння пожежі залежить від правильного вибору типу та виду вогнегасника. Вибір типу та необхідна кількість вогнегасників здійснюється відповідно до Правил експлуатації та типових норми належності вогнегасни-

ків, затверджених наказом Міністерства внутрішніх справ України від 15 січня 2018 р. № 25 (далі — Правила).

Експлуатація вогнегасників без призначення відповідального за організацію цієї роботи не допускається.

Згідно з Правилами, будинки адміністративного призначення на кожному поверсі повинні мати не менше двох переносних (порошкових, водопінних або водяних) вогнегасників з масою заряду вогнегасної речовини 5 кг і більше.

Крім того, на 20 м² площі підлоги в офісних приміщеннях з оргтехнікою, слід передбачати по одному газовому вогнегаснику з величиною заряду вогнегасної речовини 3 кг і більше.

Приміщення, у яких розміщено оргтехніку, слід оснащувати переносними газовими вогнегасниками з розрахунку один вогнегасник ВВК-1,4 чи ВВК-2, але не менше ніж один вогнегасник зазначених типів на приміщення.

Додатково будинки та офісні приміщення можуть оснащуватися пристроєм вогнегасним водопінним аерозольним (ВВПА), з масою заряду вогнегасної речовини 400 г і більше.

Для гасіння пожежі в початковій стадії в офісах, крім вогнегасників доречно мати ще кошму. Пожежні покривала повинні бути розміром не менше ніж 1 х 1 м. У місцях застосування та зберігання ЛЗР та ГР1 мінімальні розміри пожежних покривал збільшуються до величин: 2 х 1,5 м і 2 х 2 м відповідно.

Необхідна кількість первинних засобів пожежогасіння повинна визначатися відповідальним за пожежну безпеку на об’єкті окремо для кожного поверху та приміщення з урахуванням специфіки даного офісу.

Купувати вогнегасники слід лише в спеціалізованих організаціях, які мають ліцензію на такий вид діяльності й продукція яких сертифікована в

Україні.Перед розміщенням вогнегасників на об’єкті особі, відповідальній за пожежну безпеку, необхідно обов’язково провести їх огляд. Після проведення огляду вогнегасникам присвоюються облікові (інвентарні) номери за прийнятою на об’єкті системою нумерації. Особі, відповідальній за пожежну безпеку на об’єкті, необхідно вести журнал обліку вогнегасників встановленого зразка (додаток 2 до Правил).

Не рідше одного разу на місяць особою, відповідальною за пожежну безпеку має проводитись огляд вогнегасників при їх експлуатації.

Особа, що відповідає за пожежну безпеку, зобов’язана організувати технічне обслуговування вогнегасників у таких випадках:

- пошкодження або відсутність маркування, пломб або пристроїв блокування на них;
- наявність механічних пошкоджень і слідів корозії на їх корпусах або запірно-пускових пристроях;
- відсутність робочого тиску в корпусі та (або) наявність надмірного тиску (для вогнегасників закачного типу);
- після використання за призначенням;
- після закінчення гарантійного терміну експлуатації, передбаченого експлуатаційною документацією виробника.

Технічне обслуговування вогнегасників слід довіряти лише пунктам технічного обслуговування вогнегасників (далі — ПТОВ), що мають відповідну ліцензію з надання послуг і виконання робіт протипожежного призначення відповідно до вимог ДСТУ 4297:2004 «Пожежна техніка.

Технічне обслуговування вогнегасників. Загальні технічні вимоги». Приймання вогнегасників після технічного обслуговування оформлюється актом, який складається не менше ніж у двох примірниках і підписується представниками споживача послуг та ПТОВ.

Під час огляду вогнегасників, після надходження з технічного обслуговування, відповідальний за пожежну безпеку має перевірити наявність на корпусі вогнегасника етикетки ПТОВ, встановленого зразка (додаток 3 до Правил).

Рекомендуємо ознайомитись зі статтею «Вимоги до первинних засобів пожежогасіння на підприємстві» в ОППБ № 8-2018 та спецвипуском з охорони праці та пожежної безпеки «Пожежна безпека підприємства: мінімізуємо ризики» № 3-2020.

Враховуючи те, що в офісних приміщеннях багато апаратури, приладів та документів, щоб запобігти їх псуванню при гасінні, краще користуватись газовими (вуглекислотними) вогнегасниками. Застосування порошкових вогнегасників для гасіння таких пожеж прийнятне лише за відсутності газових вогнегасників. Під час застосування газових або порошкових вогнегасників для гасіння електрообладнання, що перебуває під напругою до 1000 В, необхідно дотримуватися рекомендацій, зазначених у паспортах вогнегасників.

Забороняється!

Гасити обладнання, що перебуває під напругою, водяними та водопінними вогнегасниками. При користуванні газовими вогнегасниками необхідно враховувати можливість зниження концентрації кисню в повітрі приміщення, особливо якщо воно невелике за об’ємом. Якщо через використання газових вогнегасників може створитись небезпечна для життя людини концентрація газів у повітрі слід використовувати засоби індивідуального захисту органів дихання.

Усі працівники офісу повинні знати, як користуватися первинними засобами пожежогасіння.

На рисунку 5.1 нанесено розміщення засобів пожежогасіння в компанії.

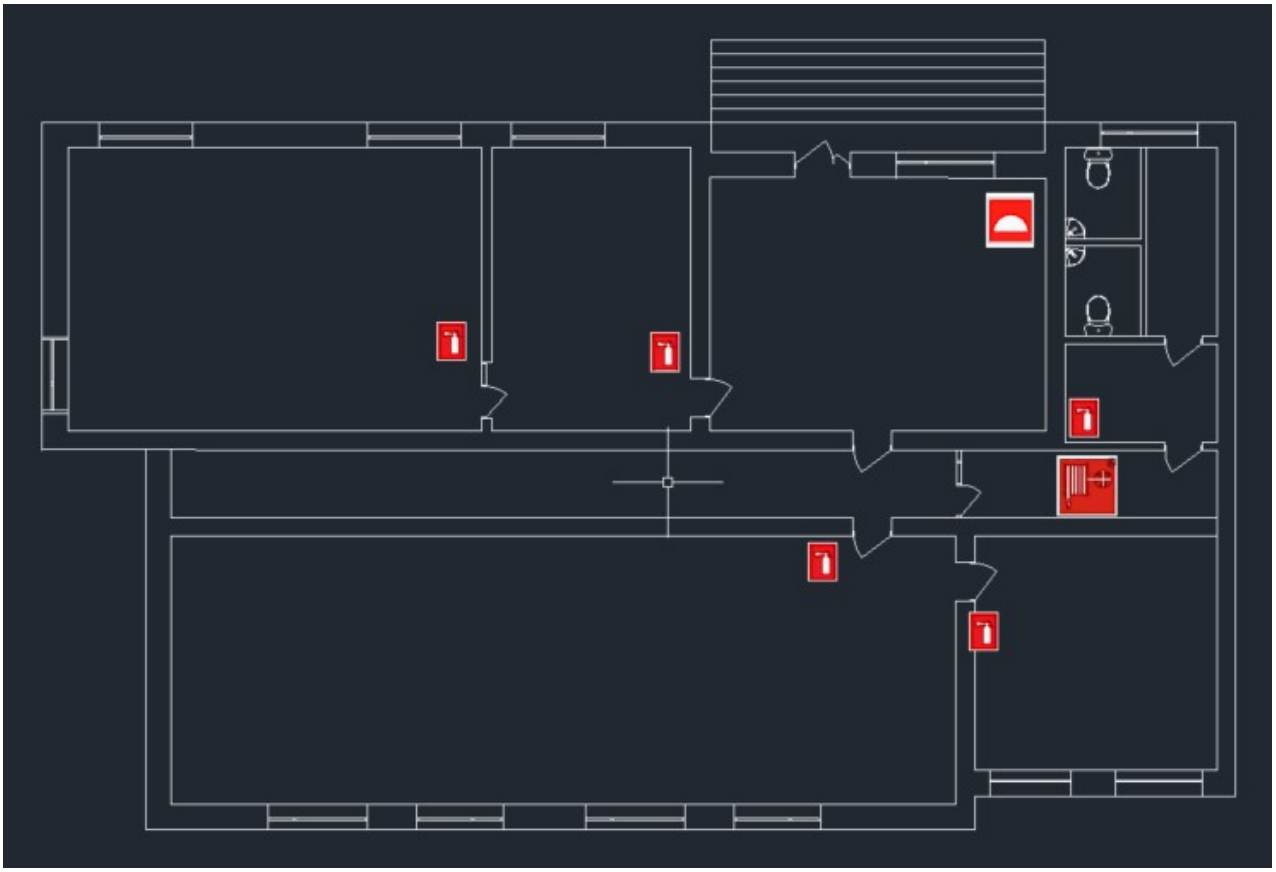


Рисунок 5.1 - Розміщення засобів пожежогасіння в компанії

5.2 Вплив шуму на організм людини та розробка заходів щодо його зниженню до допустимих величин

5.2.1 Вплив шуму на організм людини

Інтенсивний шумовий вплив викликає в звуковому аналізаторі людини зміни, які спричиняють відповідну реакцію всього організму. В цьому плані характерною рисою звукового аналізатора людини є ефект адаптації, який виражається в часовому зсуві (підвищенні) порогів слухової чутливості (Іо). Цей ефект викликається тривалим впливом акустичних коливань (шуму) підвищеного рівня. Підвищення слухових порогів, тобто постійне зміщення порогу

слуху, виражається в розвитку професійного захворювання, яке називається глухуватістю (погіршенням слуху).

Серед численних проявів несприятливого впливу шуму на організм людини виділяють: погіршення слуху, зниження розбірливості мови, розвиток втомлення, порушення сну, серцебиття.

Літературні дані показують, що збільшення виробничого шуму на 10 дБ виражається в підвищенні рівня захворюваності працюючих в 1,2...1,3 рази.

З цього виходить, що несприятливий вплив шуму на організм людини має істотні як фізіологічні, так і економічні наслідки.

5.2.2 Заходи і засоби захисту працюючих від шкідливої дії виробничого шуму

Заходи з боротьби із шумом підрозділяються на організаційні, медико-профілактичні, архітектурно-планувальні, технічні.

Організаційні й архітектурно – планувальні заходи:

- угруповання приміщень з підвищеним рівнем шуму в одній зоні будинку, відділення їх коридорами, підсобними, допоміжними, складськими приміщеннями;
- застосування результатів математичного прогнозування рівня шуму на етапі проектування будівництва або реконструкції;
- проектування по можливості більшої кількості виробничих приміщень витягнутої форми, висотою 6...7 м. При цьому забезпечується зменшення числа відбиття звукових хвиль;
- заборонено діючим стандартом перебування працюючих у зонах з рівнями звукового тиску L > 135 дБ у будь-якій октавній смузі.

Медико-профілактичні:

- проведення попередніх та періодичних медичних оглядів,

диспансерне спостереження за здоров'ям працюючих в умовах підвищеного рівня шуму протягом першого року роботи (через індивідуальну чутливість людини відносно дії шуму);

- підвищення опірності організму працюючих до впливу шуму (щоденнийприйом вітамінів В1, С протягом 2-х тижнів);
- використання кімнат психологічного розвантаження, санітарно-курортноголікування.

Технічні засоби захисту від шкідливої дії шуму передбачають використання трьох головних напрямків:

- усунення причин виникнення шуму або зниження його рівня в джерелі;
- ослаблення шуму на шляху його поширення;
- індивідуальний захист працюючих.

Найбільш ефективним шляхом зниження шуму є заміна гучних технологічних операцій на малошумні, наприклад, штампування – пресуванням, заміна клепки – зварюванням і т. п.

Так як реалізація таких методів захисту не завжди реальна та доцільна з економічної точки зору, то застосовують зниження шуму в джерелі: застосування в механізмах матеріалів із звуковбирними властивостями, своєчасне проведення профілактики й планово-попереджувальних ремонтів.

Одним з найбільш простих рішень щодо зниження шуму на шляху його поширення є застосування звукоізолюючих кожухів – звуковідбиваючих або звукопоглинаючих.

Звуковідбиваючі кожухи забезпечують зниження рівня звуку за рахунок високого коефіцієнта відбиття. Такі кожухи можуть знизити рівень звукового тиску на 20...25 дБ.

Звукопоглинаючі кожухи забезпечують зменшення звуку за рахунок перетворення кінетичної енергії звукових хвиль у теплову при коливанні

малих об’ємів повітря в порах звукопоглинаючого матеріалу. Такі кожухи можуть знизити рівень звукового тиску на 20...30 дб.

Ослаблення аеродинамічного шуму, створюваного компресорами, систе мами пневмотранспорту і т. п. здійснюють глушителями різних типів.

При великих габаритах машин, устаткування передбачають спеціальні кабіни для операторів.

Значний ефект зниження шуму від устаткування дає застосування акустичних екранів, які обгороджують джерело шуму від робочого місця або зони обслуговування. Дія такого екрана може бути заснована на ефекті створення акустичної тіні, за рахунок поглинання або відбиття звукової енергії. При цьому слід пам'ятати, що ефект екранного захисту виявляється найбільш помітно лише в області високих та середніх частот і менш ефективний в області низьких частот через дифракцію хвиль, яка може призводити до огинання захисного екрана звуковим полем через невідповідність довжини хвилі і розміру екрана.

Одним з розповсюджених заходів зниження шуму є акустична обробка

приміщень. Застосування такого технічного рішення дозволяє знизити шум у результаті дії механізму поглинання. Ефективність захисту в цьому разі також залежить від співвідношення розміру пор в облицювальному матеріалі й довжини звукової хвилі і, природно, характеризується найбільшим коефіцієнтом на високих і середніх частотах.

У багатоповерхових промислових будинках важливий захист приміщень і від структурного шуму, який виникає при закріпленні устаткування, що характеризується підвищеним шумом, на елементах конструкції будинку. Ослаблення передачі такого шуму по будинку здійснюється шумоізоляцією і шумопоглинанням, а також влаштуванням так званих «плаваючих підлог» – підлог виробничих приміщень, які не зв'язані жорстко з конструктивними елементами будинку.

Як індивідуальні засоби захисту від шуму застосовують спеціальні вкладиші у вушну раковину – беруші, а також шумозахисні навушники.

Даний розділ роботи написано за матеріалами інтернет ресурсів

ВИСНОВКИ

В ході роботи над кваліфікаційною роботою спроектовано комп’ютерну мережу компанії «Авто-ком». 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.

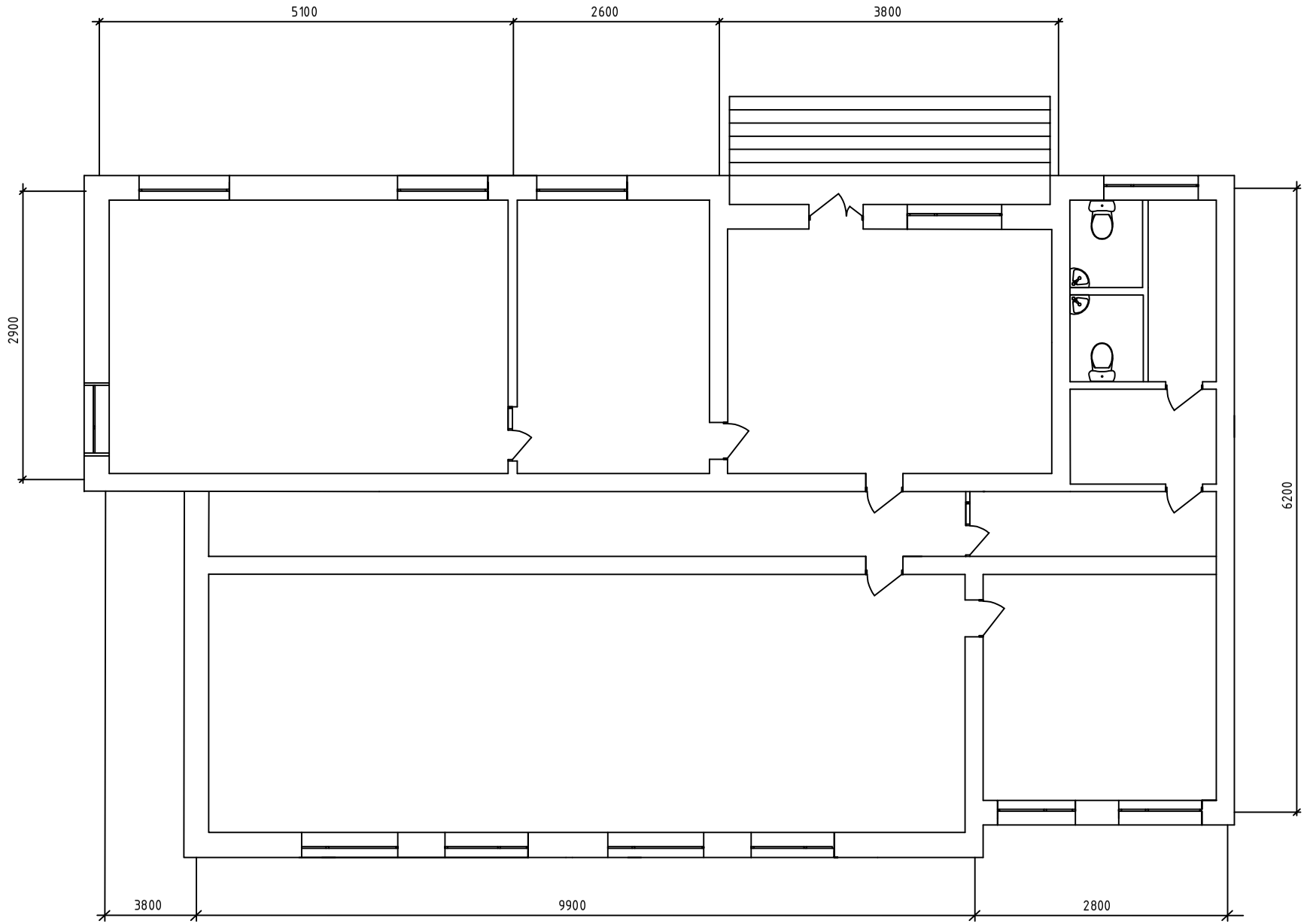
ПЕРЕЛІК ПОСИЛАНЬ

1. Альваро Ретана, Дон Слайс, Расс Уайт. Принципы проектирования корпоративных IP-сетей. - М.: АБФ, 2003. – 435с.
2. Антонов В.М. Сучасні комп'ютерні мережі. Підручник — К.: "МК-Прес", 2005. — 480 с.
3. Буров Є. Комп'ютерні мережі, 2-е видання. - БаК, 2004. – 584 с.: іл.
4. Комп’ютерні мережі: навч. посіб. / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник/ Львів. Магнолія 2006. 2013. 256 с.
5. Джеймс Куроуз, Кит Росс. Компютерні мережі. М.: Эксмо, 2016. — 912 с.
6. Додонов О. Г., Ланде Д. В., Путятін В. Г. — К.: Наук, думка, 2009. — 295 с
7. Жуков І.А., Дрововозов В.І., Махновський Б.Г. Експлуатація комп’ютерних систем та мереж. Київ: НАУ. 2007. 361с. .
8. Шорошев В. В. Теоретичні і практичні аспекти організації і побудови архітектури захищених комп’ютерних систем. Монографія. - К.: ДУПСТ, 2011. - с.257.
9. Комутатори [Електронний ресурс] – Режим доступу до ресурсу: http://hotline.ua/computer/kommutatory/ – Дата доступу: 11.04.2025.
10. Охорона праці – Москальова В.М. [Електронний ресурс] – Режим доступу до ресурсу: http://studentbooks.com.ua /content/view/1327/76/ – . (дата звернення: 11.05.2025).
11. FreeNAS 9.1.1 — Створюємо мережеве сховище. URL: https://habr.com/articles/196744/. (дата звернення: 29.04.2025).
12. Організація компютерних мереж Cisco-packet-tracer URL: http://nickshevtsov.blogspot.com/2023/10/cisco-packet-tracer.html. (дата звернення: 21.04.2025).
13. Технології компютерних мереж URL:

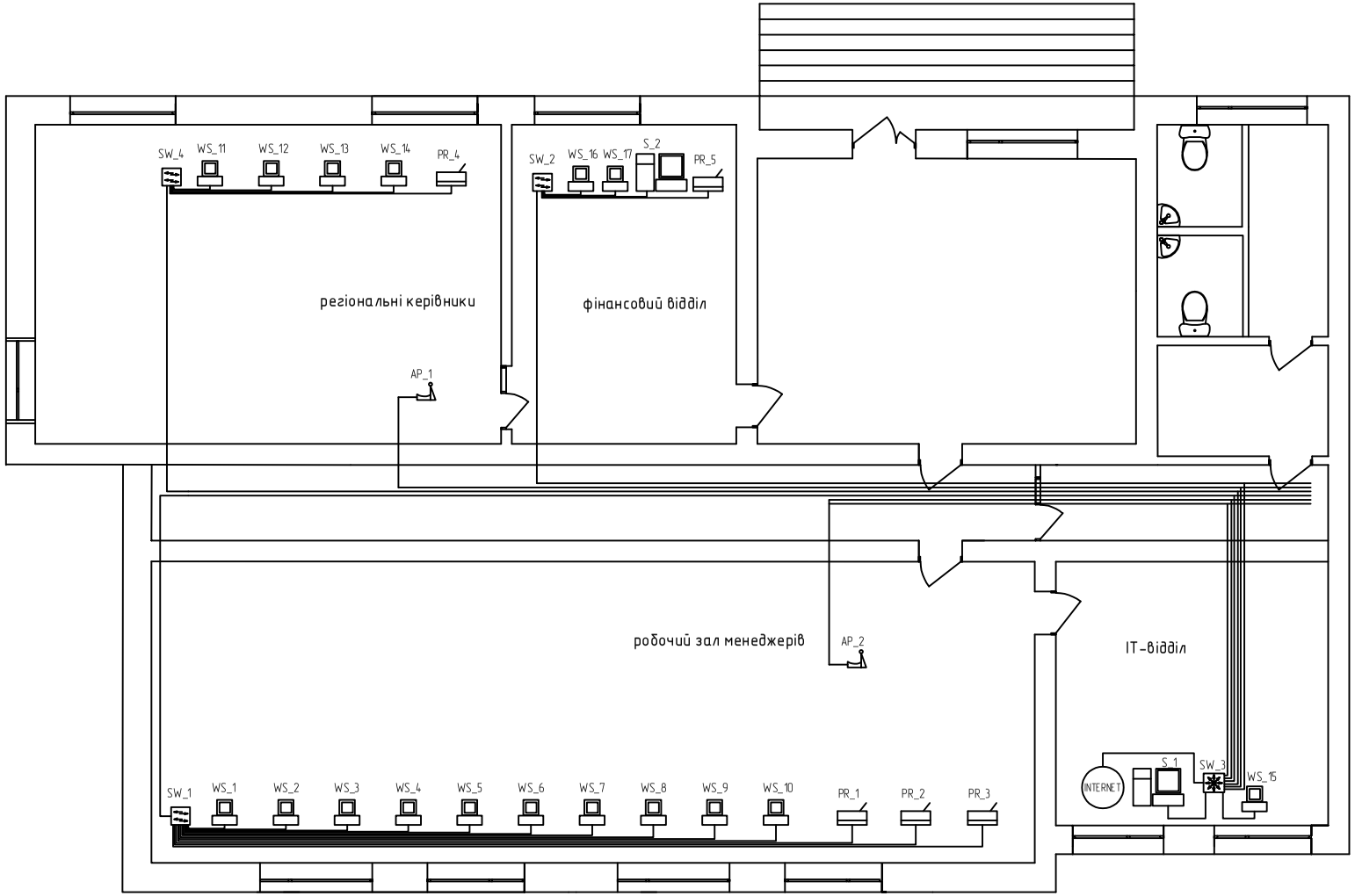
https://ukrquru.ru/tehnoloqii/127525-lan-tester-opis-priznachennia.html. (дата звернення: 18.04.2025).

14. Мережі на витій парі URL: https://ua.gecid.com/netlan/seti_na_vitoyi_pare_ot_ethernet_do_100_gigabit_ethernet/.(дата звернення: 12.04.2025).

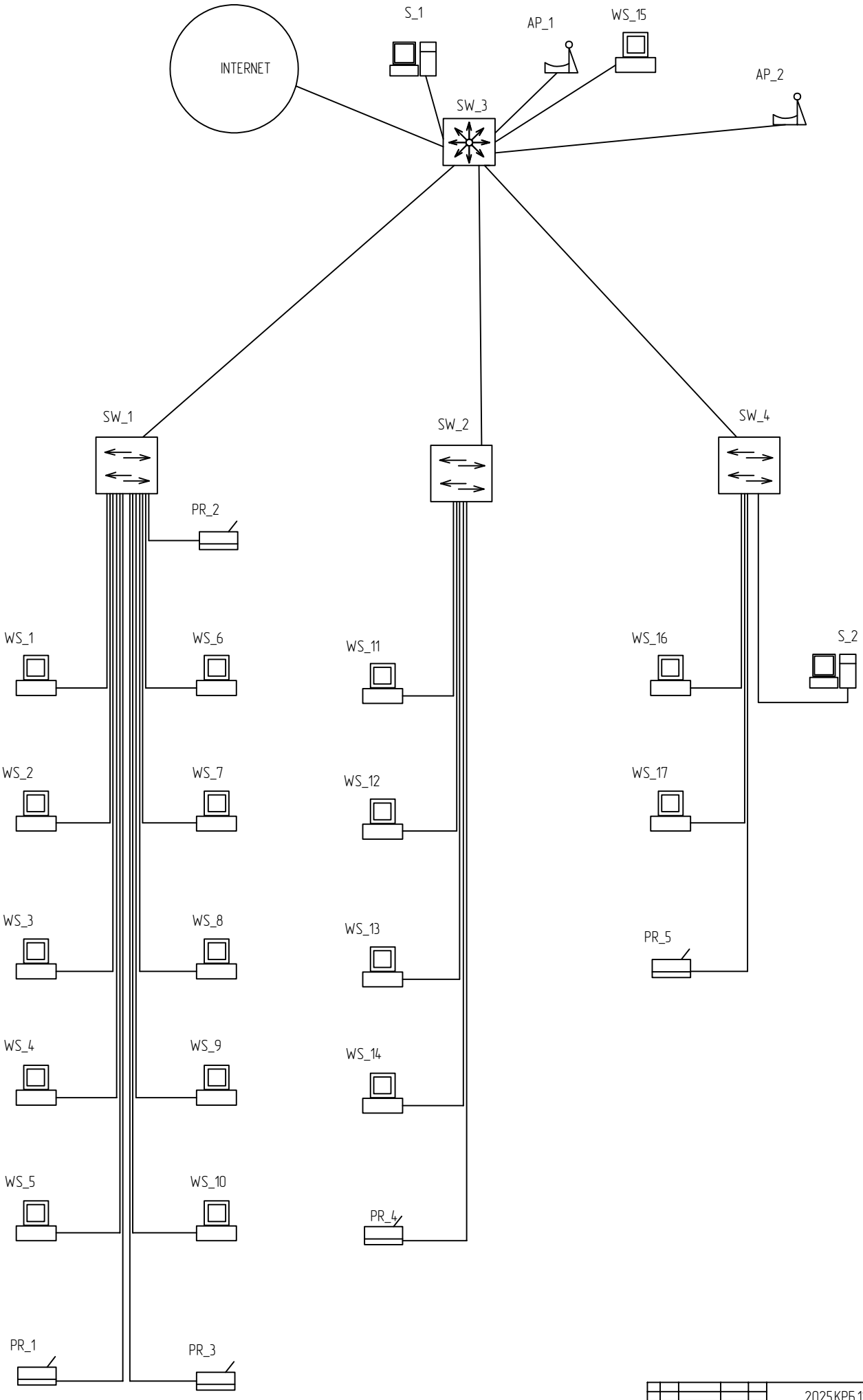
2025КРБ.123.602.01.00.00 ПП



						2025.КРБ.123.602.01.00.00 ПП	
Зм.	Арк.	№Докум.	Підпис	Дат.			
Розроб.		Абдикарич А.М.			Розробка проекту комп'ютерної мережі компанії «Авто-ком» План приміщень	Літ.	Маса	Масшт.
Керів.		Пцж. В. С.						1:100
Нконтр.		Пришмак В. А.				Аркуш 1	Аркушів 1	
Рецензія						ВСП ТФК ТНТУ КІБ-602 м.Тернопіль		
затв.								



						2025.КРБ.123.602.01.00.00 ФТ		
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі компанії «Авто-ком» Фізична топологія	Літ.	Маса	Масшт.
Розроб.		Абдикарович А.М.						1:100
Керів.		Пшк В. Є.						
Н.контр.		Приймак В.А.				Аркуш 1	Аркушів 1	
Рецензія						ВСП ТФК ТНТУ КІБ-602 м.Тернопіль		
затв.								



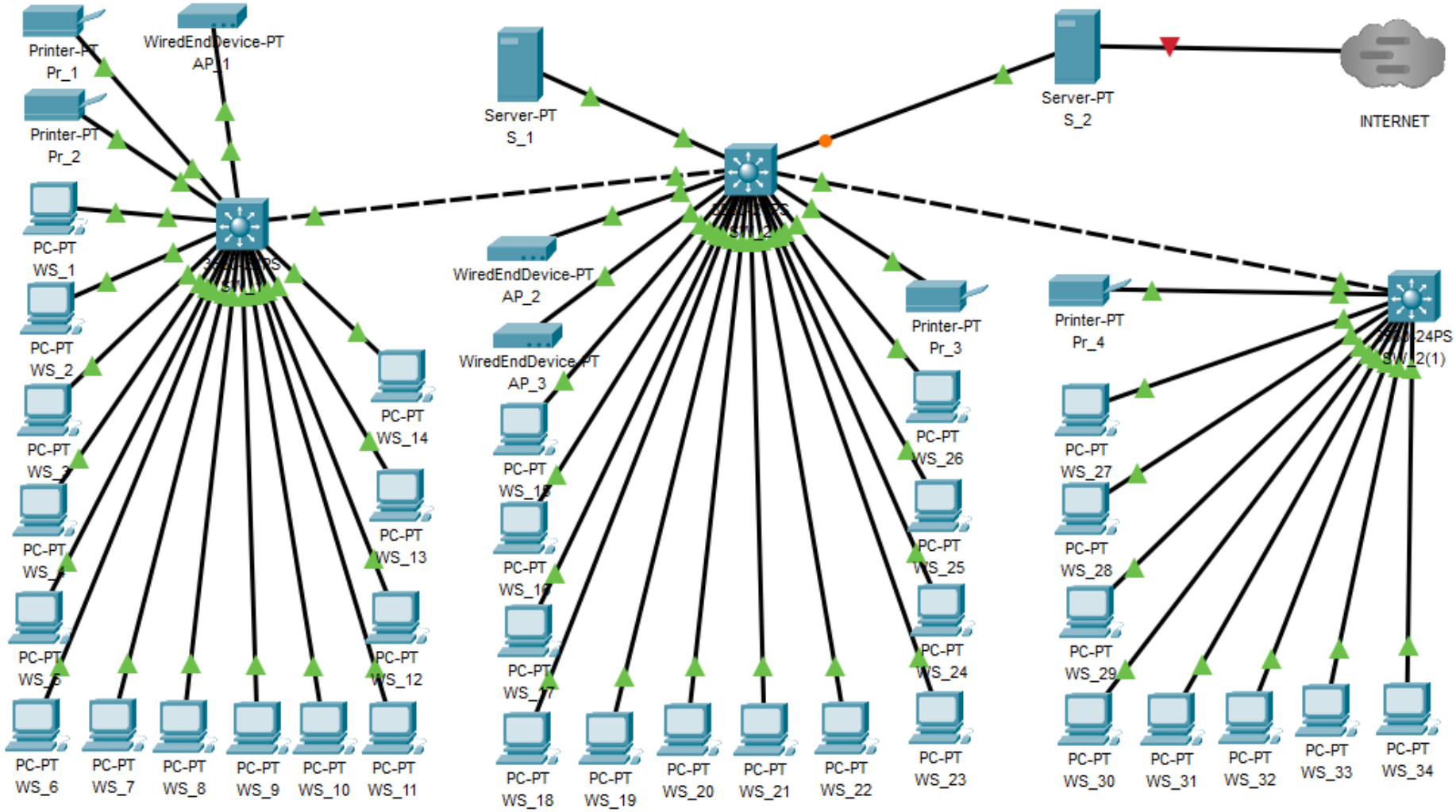
						2025.КРБ.123.602.01.00.00 /ЛТ	
Зм.	Арк.	№Докум.	Підпис	Дат.			
Розроб.		Абдикабич А.М.			Розробка проекту комп'ютерної мережі компанії «Авто-ком» /Логічна топологія	Літ.	Маса	Масшт.
Керів.		Пиж В.С.				Н		
Н.контр.		Пришмак В.А.				Аркуш 1	Аркушів 1	
Рецензія						ВСП ТФК ТНТУ КІБ-602 м.Тернопіль		

ТАБЛИЦЯ IP-АДРЕСАЦІЇ В МЕРЕЖІ						
номер	НАЗВА	IP-АДРЕСА	МАСКА	НОМЕР Vlan	коментар	порт головного комутатора
1	WS_1-WS_10	192.168.100.0	255.255.255.0	100	office	2-9
2	PR_1-PR_3					
3	WS_11-WS_14					
4	PR_4					
5	WS_15-WS_18					
6	PR_5					
7	WS_19-WS_20					
8	WS_21-WS_24	192.168.110.0	255.255.255.0	110	бухгалтерія	21
9	S2					
10	PR_6					
11	WS_25-WS_27	192.168.120.0	255.255.255.0	120	IT	10-20
12	AP_1-AP_2					
13	S2	192.168.100.0	255.255.255.0	100	office	5
14	SW_3	провайдер призначає статично				1
15	15	192.168.1.0	255.255.255.0	1	відділ IT	22-24

							2025.КРБ.123.602.01.00.02 ТА	
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі компанії «Авто-ком» Таблиця IP адрес		Літ.	Маса	Масшт.
Розроб.		Абайкович А.М.							
Керів.		Пшк В.С.					Аркуш 1	Аркушів 1	
Нконтр.		Приймак В.А.					ВСП ТФК ТНТУ КІБ-602 м.Тернопіль		
Рецензія									
затв.									

ТАБЛИЦЯ ТЕХНІКО-ЕКОНОМІЧНИХ ПОКАЗНИКІВ							
№ n\n	параметр	одиниці виміру	значення	№ n\n	параметр	одиниці виміру	значення
1	технологія мережі	–	ethernet 1000	9	операційна система NAS	–	FreeNAS 9.1.1
2	топологія мережі	–	гібридна	10	операційна система робочих станцій	–	windows 10
3	середовище передачі	–	Вита пара кат. 5Е	11	тип доступу до інтернет	–	вита пара
4	кількість вузлів мережі	шт	36	12	термін окупності	рік	2,08
5	марка головного комутатора	–	MikroTik CRS328-24P-4S+RM	13	плановий прибуток	грн	77478,19
6	марка 8-ти портового комутатора	–	Zyxel GS1100-16	14	транспортні витрати	грн	9278,00
7	марка сервера	–	Lenovo ThinkSystem ST50 V2	15	собівартість	грн	158766,78
8	марка точки доступу	–	MikroTik cAP AC RBcAPGi-5acD2nD	16	ціна	грн	236244,97

						2025.КРБ.123.602.01.00.01 ТБ	
Зм.	Арк.	№докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі компанії «Авто-ком» Таблиця техніко-економічних показників	Літ.	Маса	Масшт.
Розроб.		Абдикабич А.М.						
Керів.		Пик В.І.				Н		
Н.контр.		Приймак В.А.				Аркуш 1	Аркушів 1	
Рецензія						ВСП ТФК ТНТУ КІБ-602 м.Тернопіль		
затв.								


Printer-PT
Pr_1
WiredEndDevice-PT
AP_1
Printer-PT
Pr_2
PC-PT
WS_1
PC-PT
WS_2
PC-PT
PC-PT
PC-PT
PC-PT
WS_6
PC-PT
WS_7
PC-PT
WS_8
PC-PT
WS_9
PC-PT
WS_10
PC-PT
WS_11
PC-PT
WS_12
PC-PT
WS_13
PC-PT
WS_14
Server-PT
S_1
WiredEndDevice-PT
AP_2
WiredEndDevice-PT
AP_3
PC-PT
PC-PT
PC-PT
PC-PT
PC-PT
WS_18
PC-PT
WS_19
PC-PT
WS_20
PC-PT
WS_21
PC-PT
WS_22
PC-PT
WS_23
PC-PT
WS_24
PC-PT
WS_25
PC-PT
WS_26
Printer-PT
Pr_3
Server-PT
S_2
INTERNET
Printer-PT
Pr_4
PC-PT
WS_27
PC-PT
WS_28
PC-PT
WS_29
PC-PT
WS_30
PC-PT
WS_31
PC-PT
WS_32
PC-PT
WS_33
PC-PT
WS_34