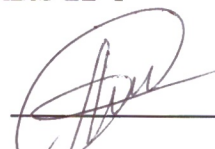


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

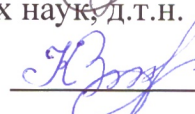
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи, технології та інструменти побудови
захищеної корпоративної бездротової мережі на базі рішень
компанії MikroTik»

Виконав студент 2-го курсу групи КБм-22-1
спеціальності 125 «Кібербезпека»


А.О. Балан

Професор кафедри комп'ютерних наук, д.т.н.


В.П. Квасніков

Рецензент доцент кафедри комп'ютерної інженерії та
кібербезпеки, к. пед. наук


О.С. Головня

Житомир – 2023

Державний університет «Житомирська політехніка»

Факультет інформаційно-комп'ютерних технологій

Кафедра комп'ютерної інженерії та кібербезпеки

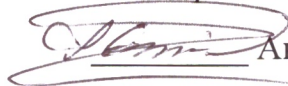
Спеціальність 125 «Кібербезпека»

Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки



Андрій Єфіменко

1 березня 2023 р.

ЗАВДАННЯ

на випускн кваліфікаційну роботу магістра

Студент: Балан Акім Олегович

Тема роботи: **«Методи, технології та інструменти побудови захищеної корпоративної бездротової мережі на базі рішень компанії MikroTik»**

затверджена Наказом університету від 1 березня 2023 р. № 127/с

Термін здачі студентом закінченої роботи 25 грудня 2023 р.

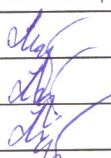
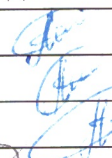
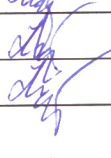
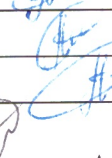
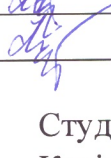
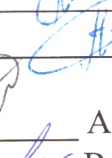
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

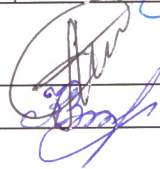
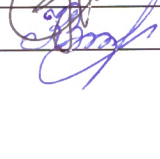
1. **Предмет дослідження:** Корпоративні бездротові мережі.
2. **Об'єкт дослідження:** Структура та безпека корпоративної бездротової мережі на базі Mikrotik.
3. **Аналіз продуктивності та безпеки:** Використання сучасних методик та інструментів оцінки.

Обладнання та програмне забезпечення:

1. **Mikrotik RouterOS**: Основне обладнання для корпоративної бездротової мережі.
2. **PyCharm**: Інтегроване середовище розробки для створення програмного застосунку.
3. **Python**: Мова програмування, використана для розробки програмного застосунку.
4. **Pandas та NumPy**: Бібліотеки Python для аналізу даних.
5. **WinBox**: Інтерфейс для управління обладнанням Mikrotik.
6. **Microsoft Excel**: Програмне забезпечення для роботи з даними, аналізу та представлення результатів.

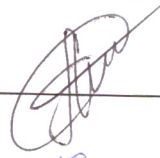
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

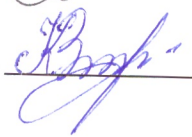
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	М.С. Граф		
2	М.С. Граф		
3	М.С. Граф		

Студент  А.О. Балан
Керівник  В.П.Квасніков

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір теми та затвердження плану	Жовтень 2023	
2	Збір та аналіз літератури	Кінець Жовтня 2023	
3	Аналіз методики оцінювання мереж	Листопад 2023	
4	Оцінка існуючої мережі	Кінець Листопада 2023	
5	Розробка програмного застосунку	Кінець Листопада 2023	
6	Тестування програмного застосунку	Кінець Листопада 2023	
7	Написання основного тексту роботи	Початок Грудня 2023	
8	Редагування та оформлення тексту	Середина Грудня 2023	
9	Підготовка до захисту	Середина Грудня 2023	
10	Захист роботи	Кінець Грудня 2023	

Студент  А.О. Балан

Керівник  В.П. Квасніков

АНОТАЦІЯ

У цій кваліфікаційній роботі представлено аналіз корпоративних бездротових мереж на базі MikroTik та розроблено комплекс рекомендацій для створення захищеної та ефективної мережевої структури. Основний акцент зроблено на оцінці ключових параметрів таких як продуктивність, безпека та масштабованість існуючих мережевих рішень. Робота включає розробку системи рекомендацій, яка базується на аналізі ефективних параметрів (ЕП) та ключових параметрів (КП), з подальшим створенням програмного застосунку для автоматизації цього процесу. Включені пропозиції з оптимізації та інновацій, які орієнтовані на впровадження передових технологій та практик, а також на розробку ефективної системи моніторингу та оцінки ефективності мережі. Результати цього дослідження спрямовані на підтримку організацій у проектуванні та управлінні корпоративними мережами, з метою підвищення їх загальної продуктивності та безпеки.

КЛЮЧОВІ СЛОВА: КОРПОРАТИВНІ БЕЗДРОТОВІ МЕРЕЖІ, МІКРОТІК, БЕЗПЕКА МЕРЕЖІ, ЕФЕКТИВНІ ПАРАМЕТРИ (ЕП), КЛЮЧОВІ ПАРАМЕТРИ (КП), МЕРЕЖЕВА ОПТИМІЗАЦІЯ

					КІК.КР.Б – 125 – 1 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Балан А.О.		19.12.23	Методи, технології та інструменти побудови захищеної корпоративної бездротової мережі на базі рішень компанії MikroTik			
Керівник		В.П.Квасніков		19.12.23				
Реценз.		О.С. Головня		19.12.23				
Н. контр.		М.С. Граф		19.12.23				
Затверд.		Ефіменко А.А.		19.12.23				
					Літ.	Арк.	Аркуші	
						4	87	
					ФІКТ, Гр. КБм-22-1			

ANNOTATION

This thesis presents an analysis of corporate wireless networks based on MikroTik and develops a comprehensive set of recommendations for creating a secure and efficient network structure. The primary focus is on assessing key parameters such as performance, security, and scalability of existing network solutions. The work includes the development of a recommendation system based on the analysis of effective parameters (EP) and key parameters (KP), followed by the creation of a software application to automate this process. Proposals for optimization and innovations are included, which are aimed at implementing advanced technologies and practices, as well as developing an effective network monitoring and efficiency assessment system. The results of this research are intended to support organizations in designing and managing corporate networks, with the goal of enhancing their overall performance and security.

KEYWORDS: CORPORATE WIRELESS NETWORKS, MIKROTIK, NETWORK SECURITY, EFFECTIVE PARAMETERS (EP), KEY PARAMETERS (KP), NETWORK OPTIMIZATION

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП.....	7
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ТА АНАЛІЗ ВИМОГ ДО КОРПОРАТИВНОЇ БЕЗДРОТОВОЇ МЕРЕЖІ.....	9
1.1 Вступ до корпоративних бездротових мереж	9
1.2 Теоретичні основи бездротових мереж	9
1.3 Технології та інновації у корпоративних бездротових мережах.....	11
1.4 Продуктивність та масштабованість бездротових мереж: автоматизація та адміністрування.....	13
1.5 Надійність та безпека у корпоративних бездротових мережах.....	14
1.6 Автономність та гнучкість мережевих рішень: забезпечення надійності та безпеки	15
1.7 Аналіз вимог та критеріїв для корпоративних бездротових мереж: автономність та гнучкість	17
1.8 Порівняльний аналіз особливостей налаштування обладнання MikroTik.....	23
1.9 Висновки до розділу	26
РОЗДІЛ 2: ОЦІНЮВАННЯ ТА АНАЛІЗ ІСНУЮЧОЇ МЕРЕЖЕВОЇ СТРУКТУРИ	28
2.1 Об'єктивне оцінювання роботи існуючої корпоративної мережі	28
2.2 Розробка вдосконаленої методики оцінки ефективності мереж	54
2.3 Вибір раціональних конфігурацій мережі за оновленою методикою	56
2.4 Статистичний аналіз можливих конфігурацій мережі.....	63
2.5 Аналіз впливу малих параметрів на загальний індекс безпеки мережі	68
2.6 Висновки до розділу	69
РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ДЛЯ МАЙБУТНЬОГО ПРОЕКТУВАННЯ ТА УПРАВЛІННЯ КОРПОРАТИВНИМИ МЕРЕЖАМИ	71
3.1 Виділення ключових напрямків розробки мережевої структури	71
3.2 Стратегії оптимізації та інновацій.....	71
3.3 Перспективи подальших досліджень: визначення можливостей для майбутніх інновацій та досліджень у сфері мережевих технологій.....	77
3.4 Висновки до розділу	78
ВИСНОВКИ.....	79
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	81

ВСТУП

Тема роботи: Методи, технології та інструменти побудови захищеної корпоративної бездротової мережі на базі рішень компанії MikroTik

Актуальність теми: у сучасному цифровому світі, де корпоративні мережі є важливими для бізнесу, забезпечення безпеки та ефективності бездротових мереж стає ключовим пріоритетом. З розвитком технологій, особливо в контексті зростаючих кіберзагроз, важливість розробки надійних та ефективних мережевих рішень значно зростає. MikroTik як популярне рішення в сфері мережевого обладнання вимагає глибокого аналізу та оцінки з точки зору безпеки та продуктивності, що робить цю тему особливо актуальною для дослідження.

Аналіз та вдосконалення корпоративних бездротових мереж з використанням технологій MikroTik стають ще більш важливими у контексті швидкого переходу бізнесів до гнучких та дистанційних моделей роботи. У цьому дослідженні акцентується увага на розробці методів, які дозволяють не лише виявити потенційні вразливості, але й визначити оптимальні шляхи їх усунення, враховуючи останні досягнення у сфері інформаційної безпеки та мережевих технологій.

Мета роботи: Основною метою цієї роботи є проведення глибокого аналізу та розробка комплексних рекомендацій для створення високопродуктивної, безпечної та адаптивної корпоративної бездротової мережі. Значна увага приділяється вивченню та оцінці різних технологічних рішень, зокрема використанню обладнання MikroTik, порівняно з іншими провідними виробниками, як-от Cisco.

Робота зосереджується на детальному аналізі ключових аспектів побудови корпоративних мереж, включаючи теоретичні основи, технологічні інновації, адміністрування та автономність мереж. Окрема увага приділяється оцінці продуктивності, надійності, безпеки та масштабованості існуючих мережевих рішень.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

Це дослідження також включає розробку оновленої методики оцінки ключових параметрів мережі. Метою цього підходу є ідентифікація потенційних напрямків для оптимізації та модернізації мережевої інфраструктури, а також забезпечення балансу між високою продуктивністю та зниженням ризиків, пов'язаних з доступом до інтернету та мережевою безпекою. Цілісне розуміння цих аспектів дозволить компаніям ефективніше планувати та реалізовувати свої мережеві стратегії, забезпечуючи надійність, безпеку та гнучкість своєї мережевої інфраструктури.

Об'єкт дослідження: Принципи побудови, безпека та продуктивність корпоративних бездротових мереж на базі MikroTik.

Предмет дослідження: Корпоративні бездротові мережі на базі MikroTik.

Методи дослідження та обробки даних:

- **Теоретичний аналіз:** вивчення літератури, нормативних документів, технічних характеристик обладнання MikroTik та існуючих стандартів безпеки.
- **Емпіричні методи:** аналіз результатів практичних тестувань, включаючи тести на пропускну спроможність, затримки, втрати пакетів та аудит безпеки.
- **Статистичний аналіз:** використання статистичних інструментів для обробки та інтерпретації даних, отриманих під час тестувань.
- **Порівняльний аналіз:** порівняння різних підходів та технологій для оцінки їх ефективності у контексті корпоративних мереж.
- **Кейс-стаді аналіз:** детальний розгляд специфічних сценаріїв використання та інцидентів безпеки.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ТА АНАЛІЗ ВИМОГ ДО КОРПОРАТИВНОЇ БЕЗДРОТОВОЇ МЕРЕЖІ

1.1 Вступ до корпоративних бездротових мереж

У сучасному світі, де глобалізація та цифровізація безперервно трансформують бізнес-процеси, корпоративні бездротові мережі відіграють ключову роль у підтримці безперебійної та ефективної роботи організацій. Відмінності між корпоративними мережами та звичайними домашніми чи публічними мережами не обмежуються лише масштабом; вони стосуються збільшених вимог до безпеки, надійності, продуктивності та гнучкості^[3].

Ризики, пов'язані з корпоративними мережами, значно вищі, оскільки вони зазвичай зберігають конфіденційні дані бізнесу та клієнтів, а також підтримують критичні для бізнесу процеси. Неправильне управління мережею може призвести не лише до тимчасових технічних збоїв, а й до серйозних фінансових втрат, пошкодження репутації компанії, та, у найгіршому випадку, до правових наслідків.

У цьому контексті, розробка та управління корпоративними бездротовими мережами вимагають більш глибокого розуміння інтеграції різних технологій та стандартів, а також знань про сучасні загрози кібербезпеці. Це означає, що корпоративні мережі повинні бути не лише високоефективними та гнучкими для адаптації до змінних бізнес-потреб, але й добре захищеними від зовнішніх та внутрішніх загроз^[2].

У подальших розділах ми поглиблено розглянемо ключові компоненти та стратегії, які необхідні для ефективного проектування та управління сучасними корпоративними бездротовими мережами, враховуючи їх унікальні вимоги та виклики.

1.2 Теоретичні основи бездротових мереж

Сучасний ландшафт корпоративних бездротових мереж характеризується швидким розвитком технологій та зростаючими вимогами до ефективності,

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

надійності та безпеки. Вивчення теоретичних основ дозволяє глибше зрозуміти які концепції та підходи застосовуються у цій галузі.

- **Стандартизація та протоколи:** основою бездротових мереж є стандарти іеєе 802.11 (wi-fi) та інші пов'язані протоколи. Ці стандарти визначають правила для бездротового зв'язку, гарантуючи сумісність між різними пристроями та ефективність передачі даних.
- **Безпека мережі:** з огляду на зростання кіберзагроз, безпека в корпоративних бездротових мережах є критичною. Використання протоколів безпеки, як-от wpa3, та методів шифрування даних допомагає захистити конфіденційність та цілісність переданих даних.
- **Масштабованість та управління:** сучасні корпоративні мережі повинні бути гнучкими та масштабованими, щоб адаптуватися до змін у бізнес-потребах. Це включає в себе управління мережевими ресурсами та їх оптимізацію за допомогою централізованих систем управління мережею (nms).
- **Конвергенція мережі та безпеки:** інтеграція мережевих та безпекових функцій у єдину систему^[2] дозволяє досягати більшої ефективності та забезпечувати кращий захист від зовнішніх загроз.
- **Технології мультихмарних мереж:** зростання використання хмарних технологій вимагає інтеграції корпоративних бездротових мереж з різними хмарними сервісами та платформами, забезпечуючи високий рівень гнучкості та доступності.
- **Інновації у бездротових технологіях:** впровадження технологій, таких як 5g, wi-fi 6, дозволяє підвищити пропускну спроможність, зменшити затримки та підтримувати більш високу щільність підключень.^[3]

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

- **Автоматизація та aiops:** використання штучного інтелекту та автоматизації для управління мережею допомагає оптимізувати ресурси, покращити продуктивність та швидко реагувати на зміни в мережевому середовищі.

Ці теоретичні концепції формують фундамент для створення надійних, безпечних та високоефективних корпоративних бездротових мереж, адаптованих до сучасних вимог та викликів.

1.3 Технології та інновації у корпоративних бездротових мережах

Продовжуємо наш аналіз, переходячи до технологій та інновацій у корпоративних бездротових мережах. У цьому розділі ми зосередимося на сучасних технологіях, які формують ландшафт корпоративних бездротових мереж, та розглянемо їх вплив на мережеву інфраструктуру.

Сучасний розвиток корпоративних бездротових мереж не відбувається в ізоляції, а є частиною ширшого технологічного прогресу. Розглянемо кілька ключових технологій та інновацій, які мають вирішальний вплив на цю сферу^[4]:

- **5g технологія:** впровадження 5g відкриває нові можливості для корпоративних бездротових мереж, забезпечуючи вищу пропускну спроможність, нижчу затримку та покращену підтримку IoT (internet of things) пристроїв. 5g сприяє розвитку таких напрямків, як автоматизовані виробничі лінії, розумні будівлі та розширення можливостей дистанційної роботи.
- **Wi-fi 6 (802.11ax):** новітній стандарт wi-fi забезпечує кращу продуктивність у густонаселених мережах, підвищуючи ефективність використання спектру та покращуючи пропускну спроможність. Wi-fi 6 особливо важливий для робочих місць з високою щільністю пристроїв, як то офіси, конференц-зали та публічні простори.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

- **Хмарні технології та сервіси:** інтеграція з хмарними технологіями дозволяє корпоративним бездротовим мережам стати більш гнучкими та масштабованими. Хмарні платформи, як azure, aws чи google cloud, забезпечують мережеві служби, обробку даних та зберігання без необхідності великих капітальних вкладень у фізичну інфраструктуру^[11].
- **Інтелектуальне управління мережами (aiops):** використання штучного інтелекту для аналізу та оптимізації мережевих операцій дозволяє автоматизувати складні процеси управління, підвищувати ефективність та знижувати витрати на обслуговування.
- **Інтернет речей (IoT):** швидкий розвиток IoT технологій вимагає від корпоративних мереж здатності підтримувати велику кількість підключених пристроїв. Це ставить нові вимоги до безпеки, управління трафіком та пропускнуої спроможності мереж.
- **Безпека кінцевих точок:** зі зростанням кількості мобільних та IoT пристроїв, безпека кінцевих точок стає ключовим елементом корпоративних мереж. Розвиток технологій захисту, включаючи розширене шифрування та автентифікацію, є критично важливим для забезпечення безпечної роботи мереж.

Подібні сучасні технології та рішення забезпечують кращі умови для розвитку майбутніх корпоративних бездротових мереж^[7]. А також покращує їх здатність до адаптації та стійкості в умовах змінних бізнес-потреб, технологічних трендів.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

1.4 Продуктивність та масштабованість бездротових мереж: автоматизація та адміністрування

Продовжуючи наш аналіз, ми переходимо до огляду методів автоматизації та інструментів для адміністрування, оцінюючи їх вплив на продуктивність та масштабованість корпоративних бездротових мереж.

Ефективне управління корпоративними бездротовими мережами вимагає глибокого розуміння не лише основних технологій та протоколів, а й способів їх автоматизації та адміністрування. Автоматизація та інструменти управління відіграють важливу роль у підвищенні продуктивності та масштабованості мереж, дозволяючи більш ефективно реагувати на виклики сучасного бізнес-середовища.

- **Автоматизація мережевих операцій:** застосування автоматизованих рішень, таких як скрипти та інструменти управління конфігурацією, дозволяє зменшити витрати часу та ресурсів на рутинні задачі^[4], наприклад, налаштування мережевих пристроїв, оновлення політик безпеки, та моніторинг стану мережі.
- **Інструменти централізованого управління:** платформи для централізованого управління мережами надають можливість відстежувати та керувати всіма компонентами мережі з єдиної точки, що істотно підвищує продуктивність та спрощує масштабування мережевих рішень^[5].
- **Оптимізація мережевих ресурсів:** автоматизація розподілу ресурсів та балансування навантаження сприяє оптимальному використанню мережевих можливостей, забезпечуючи високу продуктивність та стабільність мережі.
- **Aiops (artificial intelligence for it operations):** використання алгоритмів штучного інтелекту для аналізу мережевих даних може

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

допомогти у прогнозуванні та вирішенні проблем до того, як вони вплинуть на роботу мережі, тим самим підвищуючи її продуктивність.

- **Моніторинг та аналітика:** розширений моніторинг та аналітика дозволяють отримувати глибоке розуміння стану мережі, використання ресурсів, та поведінки користувачів, що є критично важливим для підтримання високої продуктивності мережі.
- **Інтеграція з хмарними сервісами:** співпраця з хмарними провайдерами та використання хмарних інструментів управління дають змогу ефективно масштабувати мережеві ресурси, відповідно до змінних потреб бізнесу.

Автоматизація та сучасні інструменти управління відіграють ключову роль у забезпеченні гнучкості, масштабованості та ефективності корпоративних бездротових мереж, дозволяючи їм відповідати вимогам сучасного динамічного бізнес-середовища.

1.5 Надійність та безпека у корпоративних бездротових мережах

Надійність та безпека є фундаментальними складовими корпоративних бездротових мереж, оскільки вони безпосередньо впливають на їх продуктивність та здатність адаптуватися до розширюваних масштабів бізнес-вимог.

- **Надійність як основа продуктивності:** надійність мережі визначає її здатність підтримувати стабільну та безперервну роботу. Вона включає в себе заходи резервування критичних компонентів (наприклад, маршрутизаторів та комутаторів) та розробку мережевої інфраструктури, здатної адаптуватися до змін у вимогах до пропускної спроможності або конфігурації.
- **Безпека як фактор масштабованості:** безпека корпоративних мереж полягає в захисті від зовнішніх та внутрішніх загроз. Це включає впровадження сильних механізмів автентифікації, шифрування даних

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

та регулярне оновлення безпекового програмного забезпечення. Міцна безпекова стратегія є вирішальною для масштабування мереж, оскільки вона дозволяє уникати втрат даних та інших ризиків, що можуть виникати з ростом мережевої інфраструктури.

- **Редундантність та відновлення після збоїв:** включення редундантності у мережеву архітектуру забезпечує високу доступність^[8] та мінімізує простої в разі відмови обладнання або збоїв в системі. Це також включає стратегії швидкого відновлення після збоїв, щоб забезпечити мінімальний вплив на продуктивність мережі.
- **Моніторинг та відповідь на інциденти:** постійний моніторинг мережі та швидке реагування на інциденти безпеки є ключовими для підтримки надійності та безпеки. Це включає виявлення аномалій у мережевому трафіку, аналіз загроз та оперативне усунення проблем.
- **Сумісність та гнучкість рішень:** мережі повинні бути гнучкими, щоб підтримувати інтеграцію з новими технологіями та стандартами. Ця гнучкість допомагає утримувати високий рівень безпеки та надійності, незалежно від швидкості змін у технологічному ландшафті.

Надійність та безпека в корпоративних бездротових мережах не є статичними; вони вимагають постійного оновлення та адаптації до нових викликів та технологій. Вони є основою для створення міцної, продуктивної та масштабованої мережевої інфраструктури.

1.6 Автономність та гнучкість мережевих рішень: забезпечення надійності та безпеки

Автономність та гнучкість у мережевих рішеннях відіграють ключову роль у забезпеченні надійності та безпеки корпоративних бездротових мереж. Стратегії,

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

які впроваджують ці аспекти, дозволяють мережам адаптуватися до змінних умов та вимог, забезпечуючи стабільність та безперервність бізнес-процесів.

- **Автоматизоване виявлення та реагування на інциденти:** впровадження систем, що автоматично виявляють та реагують на потенційні загрози або відмови в мережі, є ключовим для підтримки надійності. Це може включати автоматизоване перенаправлення трафіку, швидке відновлення після збоїв, та автоматичне усунення вразливостей^[4].
- **Гнучке масштабування мережі:** мережі повинні мати можливість масштабуватися вгору або вниз відповідно до потреб бізнесу, що вимагає використання модульних та гнучких архітектур. Це також включає інтеграцію з хмарними послугами для додаткової гнучкості та масштабованості.
- **Багаторівнева модель безпеки:** забезпечення високого рівня безпеки вимагає комплексного підходу, що включає застосування багаторівневої моделі безпеки. Це означає комбінацію фізичного захисту, мережевих брандмауерів, методів шифрування, систем запобігання вторгненням, та політик безпеки.
- **Адаптивні мережеві політики:** розробка та застосування мережевих політик, які можуть адаптуватися до змінних умов, сприяє підтримці безпеки та надійності^[5]. Це включає інтелектуальні мережеві протоколи, які автоматично регулюють пропускну спроможність та забезпечують якість обслуговування.
- **Резервування та відновлення даних:** стратегії резервного копіювання та відновлення даних є критично важливими для забезпечення надійності мережі. Це включає регулярне резервне

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

копіювання важливих даних та розробку планів відновлення після аварій.

- **Неперервний моніторинг та оптимізація:** постійний моніторинг стану мережі та її ефективності дозволяє оперативно виявляти та вирішувати проблеми, що сприяє підтримці високого рівня надійності.

Автономність та гнучкість мережевих рішень є вирішальними для сучасних корпоративних бездротових мереж, дозволяючи їм ефективно відповідати на виклики динамічного бізнес-середовища, забезпечуючи високий рівень продуктивності, надійності та безпеки.

1.7 Аналіз вимог та критеріїв для корпоративних бездротових мереж: автономність та гнучкість

Розробка ефективної корпоративної бездротової мережі вимагає глибокого розуміння її ключових вимог та критеріїв. Автономність та гнучкість є основними аспектами, які забезпечують високу продуктивність та адаптивність мережі до змінних умов.

1.7.1 Пропускна спроможність

Одним із ключових критеріїв є здатність мережі підтримувати високу пропускну спроможність, що є важливим для бізнес-додатків, великих обсягів передачі даних та мультимедійного контенту^[9]. Розглядаючи пропускну спроможність як один із ключових аспектів при налаштуванні корпоративних бездротових мереж, важливо враховувати кілька важливих факторів та стратегій, які можуть оптимізувати та підвищити ефективність мережевого трафіку:

- **Вибір відповідного обладнання:** використання сучасних мережевих пристроїв, які підтримують високі стандарти пропускну спроможності, є фундаментальним^[8]. Це включає в себе

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

маршрутизатори та комутатори із підтримкою гігабітних швидкостей, а також високоякісні бездротові точки доступу.

- **Оптимізація топології мережі:** ефективна структура мережі, включаючи розміщення обладнання та налаштування з'єднань, може значно вплинути на пропускну спроможність. Розподіл трафіку та балансування навантаження між різними пристроями та каналами забезпечує більш рівномірний розподіл ресурсів^[10].
- **Моніторинг та аналіз трафіку:** неперервний моніторинг мережі дає змогу виявляти та усувати точки перевантаження, неефективне використання каналів або технічні проблеми, що негативно впливають на пропускну спроможність.
- **Сегментація мережі:** розділення мережі на сегменти, наприклад, через vlan (virtual local area network), може зменшити затори та поліпшити управління трафіком^[8].

1.7.2 Затримка (латентність)

Низька затримка важлива для додатків, що вимагають швидкої передачі даних, наприклад, для voip, відеоконференцій, а також для промислових контрольних систем. Зменшення затримки (латентності) у корпоративних бездротових мережах, особливо для важливих додатків, таких як voip, є ключовим аспектом для забезпечення високої якості комунікації.

- **Розширений qos для voip:** покращення налаштувань quality of service для voip трафіку. Це включає створення окремих черг для голосового трафіку з високим пріоритетом та забезпечення, що voip додатки отримують достатній пріоритет над іншими типами даних^[5].
- **Ізоляція та віртуалізація мережі:** ізоляція voip трафіку у віртуальних мережах (наприклад, через використання vlan) може зменшити вплив

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

загального трафіку на мережі та забезпечити більш стабільну латентність для голосового трафіку.

1.7.3 Надійність з'єднання

Стабільність та надійність мережі критично важливі для підтримки безперервної бізнес-діяльності, особливо в секторах, де потрібна висока доступність сервісів^[10]. Покращення надійності з'єднання у корпоративних бездротових мережах вимагає комплексного підходу, який включає ряд стратегій та технологічних рішень. Ключові стратегії, які часто використовуються:

- **Резервування критичного обладнання:** наявність резервних маршрутизаторів, комутаторів та точок доступу може забезпечити безперебійну роботу мережі у випадку збою основного обладнання. Автоматичне переключення на резервне обладнання забезпечує неперервність з'єднань.
- **Використання розподілених точок доступу:** розміщення декількох точок доступу в різних частинах приміщення або комплексу допомагає забезпечити стабільне покриття та знижує ризики втрати зв'язку через збої у конкретній точці доступу.
- **Проактивне управління трафіком:** використання розширених інструментів управління трафіком, які можуть автоматично регулювати навантаження на мережу та розподіляти трафік для оптимізації продуктивності та надійності^[10].
- **Механізми автоматичного відновлення:** впровадження систем, які автоматично відновлюють з'єднання або переконфігурують мережу у випадку відмов, забезпечуючи мінімальний час простою.
- **Забезпечення якості обладнання та інфраструктури:** вибір високоякісного мережевого обладнання та його належне обслуговування є ключовим для забезпечення надійності з'єднань. Це

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

також включає регулярну перевірку та технічне обслуговування інфраструктури.

- **Розумна організація та оптимізація wi-fi спектру:** правильне налаштування wi-fi каналів та частот для зменшення перешкод і затворів може підвищити стабільність та надійність бездротових з'єднань.

1.7.4 Масштабованість

Мережа повинна мати здатність адаптуватися до зростаючих або змінюваних потреб бізнесу, включаючи здатність інтегруватися з новими технологіями та підтримувати розширення мережевої інфраструктури.

- **Модульна архітектура:** проектування мережі з модульною структурою, яка дозволяє легко додавати, видаляти або замінити компоненти, є важливою стратегією. Це забезпечує гнучкість у розширенні або модифікації мережі з мінімальними витратами та перервами у роботі^[5].
- **Інтеграція з хмарними сервісами:** використання хмарних технологій та сервісів дозволяє масштабувати мережеві ресурси відповідно до потреб, без необхідності великих інвестицій у фізичне обладнання.
- **Впровадження software-defined networking (sdn):** sdn надає можливість централізовано керувати мережевими ресурсами за допомогою програмного забезпечення, що сприяє кращому управлінню та масштабуванню мережі.
- **Забезпечення сумісності обладнання:** вибір обладнання, що відповідає стандартам індустрії та сумісне з широким спектром пристроїв і технологій, допомагає уникнути проблем сумісності при розширенні мережі.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

1.7.5 Безпека

Сильні механізми захисту від зовнішніх і внутрішніх загроз є вирішальними для захисту конфіденційних даних та забезпечення відповідності нормативним вимогам. Безпека є одним з найважливіших аспектів корпоративних бездротових мереж, оскільки вони часто є ціллю для кібератак. Використання ефективних стратегій та технологій може значно покращити рівень захищеності мережі. Деякі з найефективніших підходів:

- **Застосування сучасних протоколів шифрування:** використання протоколів, таких як wpa3 у бездротових мережах, забезпечує сильне шифрування даних та захищає від спроб несанкціонованого доступу.
- **Ідентифікація та автентифікація користувачів:** системи ідентифікації та автентифікації, такі як 802.1x, дозволяють контролювати доступ до мережі, забезпечуючи, що лише авторизовані користувачі мають доступ.
- **Мережевий брандмауер та ids/ips:** використання брандмауерів та систем виявлення та запобігання вторгненням (ids/ips) допомагає захистити мережу від зовнішніх загроз та моніторити потенційно шкідливі дії в мережі.
- **Сегментація мережі та ізоляція трафіку:** створення віртуальних мереж (vlan) та ізоляція трафіку можуть обмежити поширення загроз в мережі та зменшити ризик внутрішніх атак.
- **Регулярні оновлення та патчі:** постійне оновлення програмного забезпечення та обладнання допомагає закривати вразливості та захищати від новітніх загроз.
- **Політики безпеки та навчання персоналу:** розробка та впровадження строгих політик безпеки, а також навчання персоналу

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

основам кібербезпеки, є важливим для підвищення загальної безпеки мережі.

- **Захист фізичного обладнання:** забезпечення фізичної безпеки обладнання, включаючи сервери та мережеві пристрої, є також важливим для запобігання несанкціонованому доступу.

1.7.6 Автономність та адаптивність

Мережі повинні мати здатність самостійно виявляти та реагувати на зміни у мережевому середовищі, автоматично адаптуючись до змінних вимог без необхідності ручного втручання. Автономність та адаптивність у бездротових корпоративних мережах є ключовими для підтримки стабільної та ефективної роботи мережевої інфраструктури. Використання інноваційних систем автоматичного керування та налаштування, як *carpman* від MikroTik, є одним із способів досягнення цих цілей. Розглянемо деякі неочевидні та інноваційні стратегії для підтримки автономності та адаптивності:

- **Централізоване управління точками доступу:** системи на кшталт *carpman* дозволяють централізовано управляти всіма точками доступу в мережі. Це означає, що налаштування, оновлення та моніторинг можуть виконуватися з одного місця, забезпечуючи консистентність та спрощення управління мережею.
- **Автоматична адаптація до умов оточення:** використання інтелегентних алгоритмів, які автоматично налаштовують параметри точок доступу залежно від умов оточення, наприклад, зміни в рівні перешкод або щільності користувачів.
- **Машинне навчання та штучний інтелект:** впровадження штучного інтелекту та машинного навчання для оптимізації роботи мережі, включаючи прогнозування потреб у пропускній спроможності та автоматичне налаштування мережевих ресурсів.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

- **Автоматичне виявлення та виправлення проблем:** системи, які можуть автоматично виявляти аварії чи зниження продуктивності в мережі та вживати заходів для їх виправлення без втручання адміністратора.
- **Інтеграція з іншими системами управління:** синхронізація роботи бездротової мережі з іншими системами управління, такими як системи безпеки, управління трафіком, або моніторингу, дозволяє автоматизувати багато аспектів експлуатації мережі.
- **Гнучкість у розширенні мережі:** можливість легкого та швидкого додавання нових точок доступу або зміни конфігурації мережі, без потреби в ручному налаштуванні існуючих компонентів.

Аналізуючи ці критерії та вимоги, можна розробити стратегії, що забезпечують високий рівень автономності та гнучкості корпоративних бездротових мереж, що є критично важливим для забезпечення їх продуктивності та масштабованості.

1.8 Порівняльний аналіз особливостей налаштування обладнання MikroTik

Порівняльний аналіз MikroTik і Cisco, як одних із найвідоміших мережевих екосистем дозволяє глибше зрозуміти відмінності в їх підходах до розв'язання інженерних завдань. Зосередившись на ключових аспектах, таких як підтримка протоколів, пропускної здатності інтерфейсах, ми можемо краще оцінити, яке з апаратних рішень є найкращим та відповідає конкретним потребам організації.

Функціональні можливості та налаштування

Вибір між MikroTik та Cisco залежить від ряду факторів, включаючи специфічні потреби мережі, рівень технічної підготовки персоналу, та бюджетні обмеження. MikroTik може бути відмінним вибором для невеликих або середніх компаній через його доступність та гнучкість. В той же час, Cisco є вибором для

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

організацій, які потребують високої продуктивності, надійності та розширених мережових можливостей.

Таблиця 1.1

Порівняльна таблиця: MikroTik та Cisco

Критерій	MikroTik (оцінка з 10)	Cisco (оцінка з 10)
Підтримка протоколів	7 - добра підтримка з гнучкими налаштуваннями	9 - широкий діапазон підтримуваних протоколів
Пропускна здатність	8 - висока пропускна здатність для невеликих та середніх мереж	10 - відмінна пропускна здатність для великих та складних мереж
Функціональність та налаштування	8 - гнучкі, але потребують технічних знань	9 - інтуїтивні інтерфейси з розширеними можливостями

Продуктивність та надійність

У контексті продуктивності та надійності, обидва виробники пропонують надійні рішення, але з певними відмінностями.

- **MikroTik** відзначається своєю гнучкістю та доступністю. Він пропонує надійні рішення для шифрування та безпеки, але може вимагати додаткових зусиль у налаштуванні та управлінні політиками безпеки.
- **Cisco** пропонує більш інтегровані та автоматизовані рішення. Їх обладнання часто включає передові функції безпеки та управління, що робить їх ідеальним вибором для організацій, які шукають найвищий рівень безпеки та продуктивності без необхідності глибоких технічних втручань.

Порівняльна таблиця: MikroTik та Cisco

Критерій	MikroTik (оцінка з 10)	Cisco (оцінка з 10)
Підтримка шифрування	7 - підтримка основних стандартів шифрування	9 - широкий спектр передових опцій шифрування
Безпекові функції	8 - гнучкі налаштування безпеки, але може вимагати більше технічних знань	10 - інтегровані рішення та передові функції безпеки
Політики безпеки	7 - ефективні, але вимагають ручного налаштування	9 - автоматизоване управління політиками безпеки

Масштабованість та гнучкість

Масштабованість та гнучкість є ключовими факторами при виборі мережевого обладнання. Обидва виробники пропонують рішення, які можуть адаптуватися до змінних потреб бізнесу, але із відмінностями в підходах та реалізації.

- **MikroTik** пропонує гнучкість та доступність з технологіями, такими як *carpman*, які спрощують масштабування бездротових мереж. Однак, його сумісність із стороннім обладнанням може бути обмежена в певних аспектах.
- **Cisco** має більш комплексні та інтегровані рішення для масштабування, забезпечуючи високу сумісність та продуктивність, особливо в середовищах, де використовується переважно обладнання Cisco. Проте, використання власних, пропрієтарних технологій може ускладнити інтеграцію з продуктами від інших виробників.

Порівняльна таблиця: MikroTik та Cisco

Критерій	MikroTik (оцінка з 10)	Cisco (оцінка з 10)
Сумісність з іншим обладнанням	7 - гарна сумісність, але може втрачати деякі функції при використанні обладнання від сторонніх виробників	8 - висока сумісність з власними та сторонніми рішеннями, але найкраще працює з обладнанням Cisco
Технології для масштабування	8 - carspan та інші технології для масштабування бездротових мереж	9 - різноманітні передові технології для масштабування мережеских рішень

Цей аналіз надав глибоке розуміння ключових відмінностей між MikroTik та Cisco. Він допомагає ідентифікувати, яке обладнання найкраще підходить для різних сценаріїв використання, враховуючи фактори, такі як бюджет, технічні потреби, та вимоги до безпеки та масштабованості. Загалом, вибір між MikroTik та Cisco залежить від специфічних цілей та обмежень кожної організації.

1.9 Висновки до розділу

У першому розділі цієї наукової роботи було розглянуто існуючі тенденції з проектування мереж та сформовано теоретичні концепції із проектування корпоративних бездротових мереж. Зокрема, було вивчено особливості обладнання MikroTik і аналізовано вимоги до безпеки та продуктивності таких мереж.

- **Теоретичні основи побудови бездротових мереж:** вивчення теоретичних основ допомогло нам зрозуміти фундаментальні принципи та концепції, які стоять за побудовою ефективних бездротових мереж.
- **Технології, що впливають на продуктивність та безпеку:** обговорення різних технологій, включаючи 5g, wi-fi 6, а також

системи автоматизації та aіops, показало, як інновації можуть підвищити продуктивність та забезпечити безпеку мереж.

- **Адміністрування та сприяння автономності мереж:** розглянули різні методи та інструменти для зручного адміністрування та підвищення автономності мереж, включаючи централізоване управління та автоматизацію.
- **Вимоги до корпоративних бездротових мереж:** виділили основні вимоги, такі як пропускна спроможність, надійність, масштабованість та безпека, які є вирішальними для проектування ефективних корпоративних мереж.
- **Порівняльний аналіз MikroTik та Cisco:** провели детальний порівняльний аналіз двох ведучих виробників мережевого обладнання, виявивши їх сильні та слабкі сторони. Встановили, що MikroTik може бути більш доступним варіантом, але Cisco пропонує більшу продуктивність та інтегровані безпекові рішення.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

РОЗДІЛ 2: ОЦІНЮВАННЯ ТА АНАЛІЗ ІСНУЮЧОЇ МЕРЕЖЕВОЇ СТРУКТУРИ

2.1 Об'єктивне оцінювання роботи існуючої корпоративної мережі

2.1.1 Огляд налаштувань пропускної спроможності та максимального навантаження

Перед проведенням глибокої оцінки продуктивності існуючої корпоративної мережі, необхідно визначити ключові показники, які впливають на її ефективність. Наша мета полягає у встановленні, чи відповідає поточна конфігурація мережі вимогам щодо швидкості та надійності, задовольняє потреби всіх користувачів та здатна справлятися з навантаженням, яке генерується їх діяльністю. Ми плануємо ретельно проаналізувати пропускну спроможність та визначити можливості оптимізації, щоб забезпечити стабільний доступ до мережі інтернет та інших корпоративних ресурсів. Для розрахунку продуктивності мережі використовуються такі параметри:

- **Пропускна спроможність точки доступу:** сар ас має максимальну пропускну спроможність 1 gbps.
- **Кількість одночасних користувачів:** в кімнаті операторів 24 людини, у кімнаті документації - 12, в кімнаті бухгалтерії - 6. Спрощений розрахунок середнього трафіку на одного користувача може виглядати так:

визначимо середній трафік для різних типів діяльності (наприклад, 100 кбіт/с на телефонію і 500 кбіт/с на іншу активність інтернету). Потім сумуємо ці значення для отримання середнього трафіку на користувача. Формула для розрахунку загального середнього трафіку (T) у мережі з урахуванням кількості користувачів (n) та середнього трафіку на користувача (t):

$$T = n \times t$$

- N - загальна кількість користувачів у всіх кімнатах.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

- T - середній трафік на користувача, що включає телефонію та іншу активність.

Загальна пропускна спроможність мережі не повинна перевищувати максимальну пропускну спроможність обладнання (в даному випадку - 1 gbps для точок доступу та центрального маршрутизатора). Однак, важливо враховувати, що wi-fi зв'язок має власні обмеження щодо кількості одночасних з'єднань та загальної пропускної спроможності, яка поділяється між усіма користувачами на одній точці доступу.

		#	Address	SSID	Channel	Signal Strength	Noise Floor	Signal To Noise	Radio Name	Router... Version
	AP	0	EA:28 8:88		2412/20/gn(17dBm)	-74	-100	26		
	APR	1	74:4D 0:47		2412/20/gn(17dBm)	-56	-100	44	744D28667047	6.49.7
	P	2	7A:AC 2:7E		2412/20/gn(17dBm)	-86	-100	14		
	AP	3	96:B2 3:70		2412/20/gn(17dBm)	-74	-100	26		
	AP	4	96:B2 3:70		2412/20/gn(17dBm)	-62	-100	38		
	AP	5	24:5A 0:5E		2437/20/gn(17dBm)	-75	-96	21		
	AP	6	68:D7 5:30		2437/20/gn(17dBm)	-74	-96	22		
	AP	7	6A:D7 5:30		2437/20/gn(17dBm)	-75	-96	21		
	AP	8	6A:D7 5:30		2437/20/gn(17dBm)	-76	-96	20		
	P	9	6E:D7 E:5F		2437/20/gn(17dBm)	-84	-96	12		
	AP	10	72:D7 E:5F		2437/20/gn(17dBm)	-84	-96	12		
	AP	11	68:D7 E:5F		2437/20/gn(17dBm)	-85	-96	11		
	AP	12	02:68 7:4B		2447/20/gn(17dBm)	-72	-99	27		
	APR	13	48:8F 1:AE		2447/20-eC/gn(17dBm)	-77	-99	22	488F5ACE60AE	6.49.6
	APRB	14	CC:2C 6:C9		2447/20-Ce/gn(17dBm)	-75	-99	24	CC2DE09486C9	6.48.3
	APRB	15	B8:69 4:E5		2452/20-Ce/gn(17dBm)	-88	-99	11	B869F480C4E5	6.43.7
	AP	16	34:5D 2:20		2462/20/gn(17dBm)	-74	-100	26		
	AP	17	24:5A 3:8D		2462/20/gn(17dBm)	-81	-100	19		
	A	18	34:5D 2:21		2462/20/gn(17dBm)	-73	-100	27		
	AP	19	68:D7 8:65		2462/20/gn(17dBm)	-77	-100	23		
	APR	20	48:8F 1:88		2472/20/gn(17dBm)	-21	-100	79	488F5A783E88	6.49.7
	APR	21	2C:C8 9:69		2472/20/gn(17dBm)	-85	-100	15	2CC81B3A5969	6.49.7
	APR	22	74:4D 0:5B		2472/20/gn(17dBm)	-81	-100	19	744D2866705B	6.49.7
	AP	23	96:B2 3:70		2412/20/gn(17dBm)	-74	-100	26		
	AP	24	28:EE 3:28		2412/20-Ce/gn(17dBm)	-83	-100	17		
	AP	25	C6:07 5:6C		2462/20/gn(17dBm)	-88	-100	12		
	AP	26	B0:BE 0:72		2462/20-eC/gn(17dBm)	-84	-100	16		
	AP	27	C6:07 5:6C		2462/20/gn(17dBm)	-88	-100	12		
	AP	28	C6:07 5:6C		2462/20/gn(17dBm)	-84	-100	16		

Рис 2.1. Радіо-розвідка діапазону 2.4 ГГц

		#	Address	SSID	Channel	Signal Strength	Noise Floor	Signal To Noise	Radio Name	Router... Version
	AP	0	68:D 75:31		5180/20/ac/P(20dBm)	-88	-103	15		
	APR	1	2C:C 59:6A		5180/20/ac/P(20dBm)	-83	-103	20	2CC81B3A596A	6.49.7
	AP	2	24:5 70:5F		5180/20-Ce/ac/P(20dBm)	-81	-103	22		
	AP	3	6A:C 75:31		5180/20-Ceee/ac/P(20dBm)	-87	-103	16		
	AP	4	6A:C 75:31		5180/20-Ceee/ac/P(20dBm)	-88	-103	15		
	APR	5	74:4 70:48		5200/20/ac/P(20dBm)	-55	-102	47	744D28667048	6.49.7
	AP	6	96:B 19:70		5220/20-eeCe/ac/P(20dBm)	-90	-103	13		
	AP	7	96:B 19:70		5220/20-eeCe/ac/P(20dBm)	-90	-103	13		
	AP	8	68:D 48:66		5220/20-Ce/ac/P(20dBm)	-83	-103	20		
	APRB	9	CC:2 36:C8		5220/20-eeCe/ac/P(20dBm)	-80	-103	23	CC2DE09486C8	6.48.3
	APR	10	74:4 70:5C		5220/20/ac/P(20dBm)	-86	-103	17	744D2866705C	6.49.7
	APR	11	48:8 E:87		5240/20/ac/P(20dBm)	-17	-103	86	488F5A783E87	6.49.7
	A	12	34:5 12:2E		5320/20-eC/ac/DP(17dBm)	-81	-103	22		
	AP	13	34:5 12:2F		5320/20-eC/ac/DP(17dBm)	-82	-103	21		

Рис 2.2. Радіо-розвідка діапазону 5 ГГц

Результати радіорозвідки вказують на значну кількість мереж, що працюють на частоті 2.4 гГц, що може викликати перешкоди та зниження продуктивності в бездротовій мережі. Більшість мереж використовують стандартні канали, які часто перекриваються, зокрема канали 1, 6, та 11, що є найбільш рекомендованими для уникнення взаємних перешкод.

Сила сигналу (signal strength) варіюється від -21 dbm до -88 dbm, що свідчить про різноманітну інтенсивність сигналів від різних точок доступу. Високе значення шуму (noise floor), яке у більшості випадків становить -100 dbm, вказує на те, що шумовий рівень є відносно низьким, що є позитивним для якості сигналу.

З огляду на ці дані, середовище на частоті 2.4 гГц є досить завантаженим, але з можливістю оптимізації за рахунок вибору менш завантажених каналів та коригування потужності сигналу точок доступу для зменшення перешкод.

Аналізуючи дані радіорозвідки для середовища на частоті 5 гГц, ми спостерігаємо значно кращі умови порівняно з 2.4 гГц смугою. Частота 5 гГц менш схильна до перешкод з багатьох побутових пристроїв, що зазвичай використовують 2.4 гГц діапазон.

- **Сила сигналу:** більшість сигналів мають достатню силу, що гарантує стабільний зв'язок для користувачів.
- **Шум:** шумовий рівень залишається низьким у цьому діапазоні, що вказує на високу якість сигналу.
- **Завантаженість каналів:** хоча існує кілька сильних сигналів, канали здаються менш завантаженими, що знижує ймовірність перешкод.

Середовище на 5 ГГц діапазоні здається відносно чистим та добре підходить для корпоративної використання, особливо для додатків, що вимагають високої пропускної спроможності та низької затримки.

Результати тесту пропускної спроможності, виконані за допомогою генератора трафіку в routers, показують, що при тестовому навантаженні 50 Мбіт/с і розмірі пакета 512 байт, мережа забезпечує стабільний обмін пакетами з мінімальною кількістю втрат. Середній час затримки (латентності) знаходиться в межах прийнятних значень для корпоративних мереж, що свідчить про добру продуктивність мережі. Існують незначні втрати пакетів, що вказують на можливість перевантаження мережі або проблеми з якістю зв'язку на деяких сегментах мережі. Jitter (варіація затримки) також знаходиться в нормальних межах, що важливо для забезпечення якості голосового трафіку та інших чутливих до затримки додатків.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

MBPS		50											
Tx Template		packet-template-ABM											
	#	Seq	ID	Tx Packets	Tx Rate	Rx Packets	Rx Rate	Lost Packets	Lost Rate	Lat. Min.	Lat. Avg.	Lat. Max.	Jitter
	0	1	0	12 197	50.0 Mbps	12 196	50.0 Mbps	1	4.1 kbps	52.9us	81.7us	1.06ms	1.00ms
	1	2	0	12 207	50.0 Mbps	12 208	50.0 Mbps	1	4.1 kbps	52.9us	80.5us	930.us	877.us
	2	3	0	12 207	50.0 Mbps	12 207	50.0 Mbps	0	0 bps	52.9us	79.8us	364.us	311.us
	3	4	0	12 208	50.0 Mbps	12 208	50.0 Mbps	0	0 bps	53.0us	84.6us	1.87ms	1.82ms
	4	5	0	12 207	50.0 Mbps	12 207	50.0 Mbps	0	0 bps	53.2us	84.9us	1.58ms	1.53ms
	5	6	0	12 205	50.0 Mbps	12 205	50.0 Mbps	0	0 bps	53.1us	79.7us	961.us	907.us
	6	7	0	12 209	50.0 Mbps	12 209	50.0 Mbps	0	0 bps	51.2us	83.4us	1.42ms	1.37ms
	7	8	0	12 208	50.0 Mbps	12 207	50.0 Mbps	1	4.1 kbps	53.5us	79.4us	323.us	270.us
	8	9	0	12 205	50.0 Mbps	12 206	50.0 Mbps	1	4.1 kbps	53.0us	79.2us	358.us	305.us
	9	10	0	12 208	50.0 Mbps	12 208	50.0 Mbps	0	0 bps	52.9us	79.7us	345.us	292.us
	10	TOT	0	122 061	50.0 Mbps	122 061	50.0 Mbps	0	0 bps	51.2us	81.3us	1.87ms	1.82ms

Рис. 2.3. пропускна спроможність каналу зв'язку точки доступу а до центрального маршрутизатора (50 мбайт/с)

На основі результатів тесту пропускної спроможності для навантаження в 1 гігабіт в секунду, ми можемо зробити висновки про високу продуктивність і потенційне навантаження на мережу. Хоча загальна швидкість передачі даних дуже висока, існують деякі втрати пакетів, що можуть вказувати на обмеження пропускної спроможності або проблеми з якістю каналу при високих швидкостях передачі даних. Затримка залишається на прийнятному рівні, але jitter (варіація затримки) зростає, що може впливати на якість зв'язку для деяких високочутливих до затримок застосунків, таких як voip або відеоконференції.

MBPS

1000

▲

Tx Template

packet-template-ABM

▲

		#	Seq	ID	Tx Packets	Tx Rate	Rx Packets	Rx Rate	Lost Packets	Lost Rate	Lat. Min.	Lat. Avg.	Lat. Max.	Jitter
		0	1	0	233 810	957.7 Mbps	232 896	953.9 Mbps	914	3.7 Mbps	99.6us	3.63ms	5.52ms	5.43ms
		1	2	0	233 219	955.3 Mbps	233 204	955.2 Mbps	15	61.4 kbps	597.us	3.93ms	4.73ms	4.14ms
		2	3	0	233 173	955.1 Mbps	233 179	955.1 Mbps	6	24.6 kbps	682.us	3.95ms	4.87ms	4.18ms
		3	4	0	233 185	955.1 Mbps	233 100	954.8 Mbps	85	348.2 kbps	911.us	4.23ms	8.47ms	7.56ms
		4	5	0	233 071	954.7 Mbps	233 099	954.8 Mbps	28	114.7 kbps	958.us	4.29ms	5.05ms	4.09ms
		5	6	0	233 133	954.9 Mbps	233 087	954.7 Mbps	46	188.4 kbps	921.us	4.26ms	8.37ms	7.45ms
		6	7	0	233 198	955.2 Mbps	233 151	955.0 Mbps	47	192.5 kbps	1.26ms	4.60ms	5.56ms	4.30ms
		7	8	0	233 162	955.0 Mbps	233 150	955.0 Mbps	12	49.2 kbps	1.22ms	4.60ms	8.75ms	7.53ms
		8	9	0	233 225	955.3 Mbps	233 195	955.2 Mbps	30	122.9 kbps	1.26ms	4.68ms	9.37ms	8.11ms
		9	10	0	233 160	955.0 Mbps	233 218	955.3 Mbps	58	237.6 kbps	1.11ms	4.64ms	8.90ms	7.79ms
		10	TOT	0	2 332 336	955.3 Mbps	2 331 279	954.9 Mbps	1 057	432.9 kbps	99.6us	4.28ms	9.37ms	9.27ms

Рис. 2.4 пропускна спроможність каналу зв'язку точки доступу а до центрального маршрутизатора (1гігабіт/с)

Для забезпечення оптимальної продуктивності корпоративної мережі важливо розуміти якість передачі даних і фактори, що на неї впливають. Використання генератора трафіку для тестування мережі допомагає ідентифікувати потенційні слабкі місця в конфігурації та використанні обладнання. Проведення тестів на різних швидкостях - від 50 мбіт/с до 1 гбіт/с - дозволяє оцінити масштаби зміни продуктивності зі збільшенням навантаження. Аналізуючи ці тести, ми отримуємо цінні дані про здатність мережі ефективно передавати дані під високим навантаженням. Фактори, що впливають на якість передачі даних в мережі, включають:

- **Пропускна спроможність обладнання:** якщо маршрутизатори та комутатори не можуть обробляти високу швидкість, це може викликати затримки та втрату пакетів.

Аналітика: MikroTik har ac2 має теоретичну максимальну пропускну спроможність 1 gbps, але практична пропускна може бути нижчою через обробку трафіку та безпекових налаштувань.

- **Якість зв'язку:** погана якість зв'язку через фізичні перешкоди, відстань від точки доступу або електромагнітні перешкоди можуть знижувати швидкість та збільшувати jitter.

Аналітика: втрати пакетів і збільшення jitter можуть свідчити про погану якість зв'язку, що не характерно для кабельних з'єднань, тому це менш імовірний фактор.

- **Навантаження на мережу:** високе навантаження від численних користувачів або важких застосунків може призвести до перевантаження та втрати пакетів.

Аналітика: високе навантаження може призвести до зниження продуктивності, але при тестуванні, яке, ймовірно, проводилося в умовах, близьких до ізолюваних, цей фактор має менше значення.

На основі аналізу результатів тестування пропускної спроможності мережі на різних навантаженнях, можна зробити висновок, що мережа працює стабільно на нижчих навантаженнях (50 мбіт/с), але при максимальному навантаженні (1 гбіт/с) з'являються проблеми з втратою пакетів та збільшенням jitter. Це може вказувати на обмеження пропускної спроможності обладнання або необхідність подальшої оптимізації мережевої конфігурації для роботи з високими швидкостями передачі даних.

Таблиця 2.1

Аналіз пропускної спроможності

Параметр	50 мбіт/с	1 гбіт/с
Втрати пакетів (%)	<0.01%	~0.05%
Середня латентність (ms)	~52 ms	~4 ms
Jitter (ms)	~1-2 ms	~4-7 ms

Ці дані підтверджують, що мережа забезпечує кращу стабільність при нижчих навантаженнях. При високих навантаженнях відсоток втрат пакетів зростає, хоча середня затримка зменшується, що може вказувати на вищу ефективність обладнання при швидкій обробці даних, але також на його межі при максимальних навантаженнях. Jitter збільшується, що може негативно впливати на деякі застосунки, особливо на voip та відеоконференції.

2.1.2 Огляд налаштувань черг та qos

Черги qos (quality of service) є критично важливими для забезпечення належної якості телефонних з'єднань у корпоративній мережі. Вони дозволяють пріоритизувати трафік voip над іншими видами трафіку, забезпечуючи низьку затримку та мінімізуючи jitter, які є ключовими для якісної телефонії.

		#	Name	Target	Upload Max Limit	Download Max Limit
- E	X	0	queue1_WI-FI_Guest	1	8. 1M	1M
- E	X	1	iPhone M	1	8. 4M	4M
- D		2	Guest WIFI	1	8. 15M	15M
- D		3	Guest_WIFI	1	8. 5M	5M
- D		4	192.168.88.106 iMAC	1	8. 15M	15M
- D		5	Azure	0	5M	5M
- D		6	Azure2	0	5M	5M
- D		7	Azure3	0	5M	5M
- D		8	OneDrive		10M	10M
- E	X	9	Fonality_1_OLD	0	5M	5M
- E	X	10	Fonality_1_r_OLD	7	.0. 5M	5M
- E	X	11	Fonality_2_OLD	0	5M	5M
- E	X	12	Fonality_2_r_OLD	7	.0. 5M	5M
- E	X	13	Fonality_3_OLD	0	5M	5M
- E	X	14	Fonality_3_r_OLD	7	.0. 5M	5M
- E	X	15	Fonality_1_alt	0	5M	5M
- E	X	16	Fonality_1_alt_r	7	.0. 5M	5M
- E	X	17	Fonality_2_alt	0	5M	5M
- E	X	18	Fonality_2_alt_r	7	6. 5M	5M
- D		19	Microsoft Teams	0	15M	15M
- D		20	Microsoft Teams_r	6	8. 15M	15M
- D		21	Microsoft Teams2	0	15M	15M
- D		22	Microsoft Teams2_r	5	0/. 15M	15M
- D		23	Office	1	8. unlimited	unlimited

Рис 2.5. Фільтри файрволу

Аналізуючи наявні qos налаштування, видно, що для телефонії встановлені конкретні ліміти пропускної спроможності, що забезпечує кожному додатку або службі достатню кількість ресурсів і запобігає перевантаженню мережі. Це важливо у контексті результатів попереднього дослідження, яке показало збільшення втрат пакетів при високих навантаженнях.

Встановлення адекватних черг qos забезпечує, що критично важливі додатки, такі як microsoft teams, мають достатню пропускну спроможність і не страждають від загального навантаження на мережу, що підвищує загальну ефективність мережі.

- **Стабільність з'єднання:** мережа здається стабільною при тестуванні на нижчих навантаженнях (50 мбіт/с), але показує ознаки перевантаження при тестуванні на 1 гбіт/с.
- **Пропускна спроможність:** мережа ефективно справляється з низькими навантаженнями, проте втрати пакетів та зростання jitter при високих навантаженнях вказують на потенційні обмеження пропускної спроможності.
- **Qos:** встановлені черги qos вказують на усвідомлене управління пріоритетами трафіку, зокрема для voip та корпоративних застосунків, що є позитивним аспектом для загальної продуктивності.
- **Оптимізація:** існує потенціал для оптимізації мережі, особливо щодо вибору каналів wi-fi та налаштувань qos для підвищення продуктивності при високих навантаженнях.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Аналіз пропускну́ї спроможності

Параметр	Оцінка	Коментар
Пропускна спроможність	7/10	Добра на низьких навантаженнях, але потребує оптимізації на високих.
Стабільність	8/10	Стабільна робота на 50 мбіт/с, проблеми на 1 гбіт/с.
Qos	9/10	Ефективне управління пріоритетами трафіку.
Загальна продуктивність	7/10	Задовільна, але є простір для покращення.

Загалом, мережа має солідну основу, але для оптимізації продуктивності може знадобитися технічний аудит та апгрейд деякого обладнання.

2.1.3 Огляд налаштувань файрволу, сервісів та списків доступу

Оцінювання налаштувань файрволу є критичною для забезпечення безпеки корпоративної мережі. Файрвол служить як перший бар'єр проти несанкціонованого доступу та атак, а його правильна конфігурація є вирішальною для захисту мережевих ресурсів. В процесі оцінки налаштувань файрволу необхідно звернути увагу на стратегії управління трафіком, політики доступу, а також на реакцію на підозрілу активність.

		▲ Name	Port	Available From	Certificate	TLS Version	
	X	● api				any	
	X	● api-ssl			none	any	
	X	● ftp				any	
		● ssh				any	
	X	● telnet				any	
		● winbox				any	
		● www				any	
	X	● www-ssl			none	any	

Рис 2.6. Налаштування сервісів

Важливо також переконатися, що файрвол налаштований з урахуванням останніх загроз безпеки, включаючи вразливості, що були виявлені з часу його останнього оновлення. Іншим важливим аспектом є встановлення чітких правил для різних типів трафіку, що дозволяє мінімізувати можливість вторгнення через відкриті порти або протоколи.

Таким чином, детальна оцінювання та постійний моніторинг налаштувань файрволу є не лише про активне управління ризиками, але й про створення фундаменту для адаптивної безпекової стратегії, яка може швидко реагувати на нові виклики в області кібербезпеки.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

	#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	Any. Port	In. Interf...	Out. Interf...	Out. Interf... List	Src. Address List	Dst. Address List	Bytes	Packets
;;; Block site																
- [E]	X	0	✖ reject	forward		6 (tcp)				WAN			Block_site		0 B	0
;;; drop ip BL_VPN																
- [D]	1	✖ drop	input							WAN			BL_VPN		33.0 KIB	609
;;; default: accept established,related,untracked																
- [E]	X	2	✔ accept	input											0 B	0
- [E]	X	3	✔ accept	input		6 (tcp)		1723		WAN					0 B	0
;;; L2TP																
- [D]	4	✔ accept	input			17 (udp)		1701.500.4		WAN					2772.4 MIB	8 819 168
;;; Input Chain: Allow established and related connections. Drop invalid packets. Allow access to the router from your local network. Drop everything else coming to the router.																
- [D]	18	✔ accept	input												29.8 GIB	84 914 424
- [D]	19	✖ drop	input												1233.4 KIB	22 775
- [D]	20	✔ accept	input	192.168.88.0/24											105.6 MIB	980 613
- [D]	21	✔ accept	input	192.168.25.0/24		6 (tcp)		8000							0 B	0
;;; web interface																
- [D]	22	✔ accept	input	192.168.25.0/24		6 (tcp)		80							40.8 KIB	561
- [D]	23	✖ drop	input												2586.3 MIB	39 237 981
;;; Forward Chain: Allow established and related connections. Drop invalid packets.																
- [D]	24	✔ accept	forward												147.9 GIB	220 474 29
- [D]	25	✖ drop	forward												1603.2 KIB	37 999
;;; Output Chain: Allow established and related connections.																
- [D]	26	✔ accept	output												141.7 GIB	210 879 73

Рис 2.7. Налаштування файрволу

Аналіз налаштувань файрволу показує, що в мережі реалізовано базові заходи безпеки:

- **З'єднання:** існують правила для дозволу вхідних з'єднань, які вже були встановлені (established) або є пов'язаними (related), що є стандартною практикою для забезпечення надійного зв'язку, в той час як нові та невизначені з'єднання відкидаються або перевіряються.
- **Порти та протоколи:** певні порти відкриті для специфічних протоколів і послуг, таких як VPN, що дозволяє забезпечити необхідний доступ, в той час як інші потенційно вразливі точки блокуються.
- **Локальний доступ:** правила для віддаленого доступу налаштовані з обмеженнями за ір-адресами, що додатково захищає від несанкціонованого доступу.

Ці налаштування свідчать про продуманий підхід до мережевої безпеки, але для повного аналізу потрібно також враховувати актуальність програмного забезпечення, регулярність оновлень безпеки, а також політики щодо кібербезпеки в компанії.

Правильна конфігурація сервісних портів в мережі має життєво важливе значення для забезпечення її безпеки. Кожен порт, який відкритий для зовнішнього світу, може стати потенційним входом для атак і загроз. В аналізі налаштувань цих портів необхідно врахувати не тільки те, які сервіси вони обслуговують, але й потенційні ризики, асоційовані з кожним з них. Сучасний пейзаж кіберзагроз вимагає динамічного підходу до управління мережевими портами, з постійним моніторингом, регулярним оновленням захисту та адаптацією до нових видів атак.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

		▲ Name	Ports	SIP Direct Media	SIP Timeout
☐		● dccp			
☐		● ftp	21		
☐		● h323			
☐		● irc	6667		
☐		● pptp			
☐		● sctp			
☐		● sip	5060, 5061	yes	01:00:00
☐		● tftp	69		
☐		● udplite			

Рис 2.8. Сервісні порти

На основі наданих налаштувань сервіс-портів можна виділити наступні групи за категоріями безпеки:

- **Стандартні порти:** порти як ftp (21) та tftp (69) є стандартними і широко використовуються. Втім, вони можуть бути вразливими, якщо не захищені належним чином, адже зловмисники часто сканують ці порти на наявність вразливостей.
- **Специфічні протоколи:** h323 та pptp стосуються voip та VPN відповідно. Відкриття портів для цих протоколів має бути суворо контрольоване, а трафік — зашифрований.
- **Застарілі/небезпечні сервіси:** irc на порту 6667 має історію використання для керування ботнетами та може бути потенційно небезпечним.
- **Sip:** відкриття портів для sip (5060, 5061) важливе для voip комунікацій, але також вимагає додаткових заходів безпеки, як-от шифрування та аутентифікація, для уникнення атак на sip.

2.1.4 Огляд налаштувань VPN/dhcp/ssh серверів

Також, на VPN сервері налаштований ipsec захист. Це ipsec з'єднання, використовує шифрування для захисту трафіку, що проходить між піром

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

(робітником) та VPN-сервером (офісом). Протокол ipsec включає дві фази: у фазі 1 відбувається встановлення безпечного каналу для обміну ключами шифрування, а у фазі 2 здійснюється шифрування даних, що передаються.

		#	Peer	Tun...	Src. Address	Src. Port	Dst. Address	Dst. Port	Prot...	Action	Level	PH2 State	
-	D	*T	0		::/0		::/0		255 (all)	encrypt			
-		DA	1	l2tp-in-server	no	2	1	2	1	17 (udp)	encrypt	unique	established

Рис 2.9. IPsec налаштування

Зазначене шифрування "all encrypt" свідчить про те, що весь трафік шифрується, що підвищує рівень безпеки. Стан "established" вказує на те, що з'єднання було успішно встановлено та функціонує.

		Name	Addresses	Next Pool
-		dhcр	192.168.88.50-192.168.88.254	none
-		vpn-pool	192.168.25.10-192.168.25.240	none

Рис 2.10. Налаштування списків для dhcр

На зображенні вище (рис 2.7) показано два dhcр пули: один для загальної мережі і один для VPN. Пул "dhcр" має діапазон адрес 192.168.88.50-192.168.88.254, що забезпечує великий діапазон адрес для пристроїв у локальній мережі. Це типовий підхід, що дозволяє достатньо місця для розширення мережі без необхідності частих змін налаштувань.

Пул "VPN-pool" з діапазоном 192.168.25.10-192.168.25.240 призначений для користувачів VPN і виділяє адреси з іншого сегмента мережі, що дозволяє легко ідентифікувати VPN трафік та управляти доступом.

Із безпекової точки зору, важливо переконатися, що кожен пул має достатню кількість адрес для підтримки всіх користувачів, але також не є занадто широким, щоб уникнути непотрібного використання ір-адрес. Крім того, необхідно

налаштувати відповідні безпекові політики для ізоляції VPN трафіку від основної мережі.

		▲ Name	Port	Available From	Certificate	TLS Version
	X	 api	80			any
	X	 api-ssl	80		none	any
	X	 ftp	21			any
		 ssh	22			any
	X	 telnet	23			any
		 winbox	80			any
		 www	80			any
	X	 www-ssl	443		none	any

Рис 2.11. Активні сервіси

Сервіси, що обслуговуються маршрутизатором, мають велике значення для адміністрування та доступу до мережевих ресурсів. Кожен із цих сервісів повинен бути ретельно сконфігурований для забезпечення безпеки:

- **Api та api-ssl:** надають інтерфейс для програмного доступу до роутера. Використання ssl є важливим для шифрування цього з'єднання.
- **Ftp:** цей протокол може бути вразливим, оскільки базовий ftp не шифрує дані.
- **Ssh:** це безпечний спосіб для віддаленого управління роутером; важливо використовувати сильні паролі та ключі.
- **Telnet:** це небезпечний сервіс, який слід відключити, оскільки він не шифрує дані.
- **Winbox:** утиліта для управління MikroTik, яка має використовуватися з обмеженими правами доступу.

- **Www та www-ssl:** доступ до веб-інтерфейсу маршрутизатора; слід використовувати ssl для захисту з'єднання.

Наявність діапазону дозволених адрес для доступу до веб-інтерфейсу є гарною практикою, оскільки вона обмежує доступ до маршрутизатора лише з певних місць. Загалом, слід використовувати зашифровані версії протоколів (наприклад, sftp замість ftp, ssh замість telnet) та вимкнути будь-які непотрібні або небезпечні сервіси для зменшення атак на маршрутизатор.

Forwarding Enabled	no ▼
Always Allow Password Login	☐
Strong Crypto	☐
Allow None Crypto	☐
Host Key Size	2048 ▼

Рис 2.12. Налаштування ssh серверу

- **Forwarding enabled:** відключений, що підвищує безпеку, оскільки перешкоджає тунелюванню ssh.
- **Always allow password login:** не відмічений, що означає, що парольні логіни заборонені, це добре, оскільки ключі безпечніші.
- **Strong crypto:** не відмічений, що вказує на потребу включити більш сильні криптографічні алгоритми.
- **Allow none crypto:** не відмічений, що є критично важливим, оскільки дозволяє уникнути незашифрованих з'єднань.
- **Host key size:** встановлено 2048, що є стандартним розміром ключа і вважається безпечним.

Загалом, ці налаштування виглядають розумно для забезпечення безпечного ssh доступу, але включення сильного шифрування ("strong crypto") було б бажаним.

Розрахунок часу, необхідного для взлому шифрованих ключів різного розміру, включаючи шифрування aes-256, є досить складним і вимагає розгляду багатьох змінних. Сучасні стандарти вважають aes-256 надзвичайно безпечним, і відомо, що для його взлому необхідно б неймовірно багато часу навіть за використання найпотужніших відомих суперкомп'ютерів.

2.1.5 Огляд налаштувань безпеки шифрування rsa/aes

Тобто, формули для розрахунку часу злому криптографічного ключа, такого як rsa-2048 або aes-256, є надзвичайно складними і залежать від безлічі змінних. Однак, ми можемо використати спрощений підхід для оцінки часу злому, виходячи з припущень про обчислювальну потужність нападника. Загальна формула для оцінки часу злому ключа:

$$\text{Час злому} = \frac{\text{загальна кількість можливих ключів}}{\text{швидкість перебору ключів за секунду}}$$

- **Загальна кількість можливих ключів:** це значення залежить від довжини ключа. Наприклад, для 2048-бітного rsa-ключа, загальна кількість можливих ключів буде 2^{2048} , що є величезним числом.
- **Реалістичність:** на практиці така швидкість перебору недосяжна для сучасних комп'ютерів, особливо при зломі складних алгоритмів шифрування, таких як rsa-2048 або aes-256.
- **Квантові комп'ютери:** з розвитком квантових комп'ютерів формули та підходи до злому можуть кардинально змінитися.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

2.1.6 Огляд налаштувань aaa на точках доступу (radius)

Enabled	☒
MAC Address	▼
MAC Mask	▼
Interface	▼
SSID Regexp	
Signal Range	▲ -75...-30
Allow Signal Out Of Range	00:00:10 ▼
Time	▲
Time	00:00:00
Days	☐ sun ☒ mon ☒ tue ☒ wed ☒ thu ☒ fri ☐ sat
Action	▲ query radius ▼
AP Tx Limit	▼
Client Tx Limit	▼
Private Passphrase	▼
Client To Client Forwarding	▼
RADIUS Accounting	▲ ☒
VLAN Mode	▼
VLAN ID	▼
Comment	RADIUS AAA

Рис 2.13. Налаштування Radius на CAPsMAN AP

Встановлення налаштувань точки доступу для взаємодії з radius сервером є важливою складовою управління безпекою в корпоративних мережах. Radius (remote authentication dial-in user service) надає комплексний підхід до аутентифікації, авторизації та обліку, дозволяючи адміністраторам централізовано контролювати доступ до мережевих ресурсів і вести облік використання. Ці налаштування забезпечують захист мережі, використовуючи сигнальні пороги для підключення пристроїв та визначають, як користувачі перенаправляються на radius сервер для перевірки.

У контексті дослідницької роботи, аналіз політик доступу, що базуються на radius, в корпоративній мережі MikroTik дає змогу глибше зрозуміти та оцінити

ефективність мережевої безпеки. Використання radius сервісу для аутентифікації користувачів забезпечує централізований механізм контролю, що дозволяє точно налаштовувати доступ до мережевих ресурсів і послуг, здійснювати моніторинг активності користувачів, та, в разі потреби, швидко реагувати на аномалії поведінки, що може свідчити про безпекові інциденти.

2.1.7 Огляд VPN клієнт-серверної взаємодії

У рамках нашої дослідницької роботи, аналізуючи VPN-налаштування на центральному маршрутизаторі MikroTik, особливу увагу слід приділити поєднанню l2tp з ipsec. Це поєднання вважається надійним для створення безпечних VPN-з'єднань, оскільки l2tp забезпечує канал для передачі даних, а ipsec додає необхідний рівень шифрування.

- **Ipssec у ролі шифрування:** ipsec використовує сильні алгоритми шифрування для захисту даних, що передаються через VPN. Це гарантує, що всі дані, які проходять через VPN-тунель, захищені від несанкціонованого доступу.
- **Налаштування ipsec:** важливо переконатися, що конфігурація ipsec включає сильні криптографічні протоколи та ключі достатньої довжини для забезпечення належної безпеки.
- **L2tp як транспортний протокол:** l2tp сам по собі не забезпечує шифрування, тому його використання з ipsec є критично важливим для забезпечення конфіденційності та цілісності переданих даних.

Використання VPN-з'єднань у компанії є ключовим аспектом для забезпечення безпеки та конфіденційності даних, особливо коли йдеться про роботу з віддаленими співробітниками або доступ до корпоративних ресурсів ззовні офісу. VPN дозволяє створювати зашифровані тунелі між користувачем та мережею компанії, ефективно захищаючи передачу даних від зовнішніх загроз та несанкціонованого доступу. Такий підхід сприяє гнучкості робочого процесу,

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

дозволяючи співробітникам безпечно працювати з будь-якої локації, водночас зберігаючи високий рівень захисту корпоративних даних.

У результаті, це поєднання є ефективним рішенням для створення безпечних VPN-з'єднань у корпоративній мережі, забезпечуючи захист від зовнішніх загроз та несанкціонованого доступу.

2.1.8 Огляд фільтрації трафіку та доступу до інтернет ресурсів

Аналізуючи існуючу політику доступу до інтернет-ресурсів та налаштування фаєрволу в компанії, я зосереджуюсь на тому, як вони впливають на продуктивність та безпеку мережі:

- **Використання ресурсів, пов'язаних з роботою:** доступ до інтернету має використовуватися строго з метою виконання робочих завдань. Відвідування розважальних або особистих сайтів під час робочого часу заборонено.
- **Активне управління веб-фільтрацією:** фільтрування та блокування доступу до веб-сайтів, які не пов'язані з професійною діяльністю співробітників, щоб запобігти відволіканню та забезпечити продуктивність.
- **Захист від веб-загроз:** блокування потенційно шкідливих сайтів допомагає уникнути ризиків інфікування мережі шкідливими програмами та зменшити вразливість до кібератак.

На основі аналізу налаштувань VPN, політики доступу до інтернету та конфігурації фаєрволу у корпоративній мережі, можна констатувати, що компанія вживає комплексних заходів для забезпечення безпеки та продуктивності. Інтеграція l2tp з ipsec забезпечує захищені з'єднання для віддалених користувачів, в той час як обмеження доступу до непрофільних інтернет-ресурсів та активне використання фільтрації веб-трафіку через фаєрвол сприяють підвищенню кібербезпеки та оптимізації робочих процесів.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

2.1.9 Огляд моніторингу та автоматизації роботи мережі.

В рамках нашого дослідження безпеки корпоративної мережі, важливо розглянути потенціал інтеграції з сіем-системами, зокрема в контексті MikroTik, який наразі не має активних систем моніторингу. Сіем-системи відіграють ключову роль у забезпеченні безпеки мережі, оскільки вони здатні аналізувати велику кількість даних, що генеруються мережевими пристроями, і виявляти потенційні загрози в реальному часі. Включення такого роду системи може значно підвищити здатність компанії до виявлення та реагування на кіберзагрози. Приклад сіем-системам.

- **Автоматичний збір звітів:** MikroTik може автоматично надсилати звіти по подіям до сіем-системи, забезпечуючи централізований збір даних.
- **Реалізація моніторингу та аналізу:** сіем аналізує ці дані для виявлення підозрілої поведінки або потенційних загроз.
- **Генерація сповіщень та повідомлень:** у разі виявлення аномалій сіем може генерувати повідомлення, дозволяючи швидко реагувати на можливі інциденти безпеки.

У контексті нашого дослідження мережевої інфраструктури на базі MikroTik, ми зосереджуємо увагу на автоматизації та можливостях аіорс. На даний момент, автоматизація в мережі обмежується планувальником подій, який регулярно створює копії поточних налаштувань. Це гарантує, що важливі конфігураційні дані зберігаються і доступні для відновлення в разі необхідності. Проте, відсутність інтеграції з хмарними послугами та аіорс показує, що є потенціал для подальшого розвитку та вдосконалення автоматизації, особливо для забезпечення більш ефективного та прогнозованого управління мережею.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

2.1.10 Розрахунок потужності робочої мережевої структури

Виходячи з попередньо проведеного аналізу пропускної спроможності та ефективності обробки трафіку у вашій мережі, ми можемо сформулювати наступну оцінку:

Таблиця 2.1

Оцінювання потужності мережі з передачі даних

Параметр	Оцінка	Коментар
Пропускна спроможність	7/10	Мережа ефективно справляється з низькими навантаженнями, але показує ознаки перевантаження при високих навантаженнях.
Стабільність з'єднань	8/10	Мережа стабільно працює на менших навантаженнях, але має проблеми на високих швидкостях.
Ефективність обробки трафіку	7/10	Загалом задовільна, хоча існує потенціал для покращення, особливо при високих навантаженнях.

Ця оцінка відображає загальний стан мережі та вказує на потребу подальшої оптимізації для підвищення її продуктивності та надійності.

2.1.11 Розрахунок ефективності налаштувань qos та черг

При оцінці ефективності налаштувань qos та черг в корпоративній мережі, ми фокусуємося на здатності системи ефективно управляти та пріоритизувати мережевий трафік. Це критично важливо для забезпечення стабільності, продуктивності та надійності мережевих ресурсів, особливо у випадку високих навантажень або специфічних вимог до мережевого сервісу. Оцінка показує, як ефективно мережа може розподіляти ресурси та як добре вона може відповідати на зміни в мережевих потребах.

Оцінювання qos та стабільності

Параметр	Оцінка	Коментар
Ефективність qos	8/10	Qos налаштування ефективно розподіляють пріоритети трафіку, забезпечуючи оптимальну продуктивність для критичних додатків.
Конфігурація черг	7/10	Черги добре налаштовані для управління пропускну здатністю, хоча існує потенціал для покращення в управлінні трафіком віддалених користувачів.

2.1.12 Розрахунок ефективності налаштувань firewall, acl та сервісів

У рамках комплексного аналізу безпеки мережі, налаштування файрволу, сервісів та списків доступу відіграють критичну роль у забезпеченні захисту мережевої інфраструктури. Важливо оцінити, наскільки ефективно ці налаштування сприяють запобіганню несанкціонованого доступу, забезпеченню цілісності даних та підтримці загальних стандартів безпеки^[8]. Оцінювання цих аспектів дасть змогу визначити потенційні слабкі місця та можливості для поліпшення в мережі.

Оцінювання файрволу, сервісів та списків доступу

Параметр	Оцінка	Коментар
Налаштування файрволу	8/10	Файрвол ефективно блокує небажані та потенційно шкідливі з'єднання, забезпечуючи безпеку мережі.
Конфігурація сервісів	7/10	Сервіси налаштовані з урахуванням безпеки, але можуть бути покращені для більшої гнучкості та оптимізації.
Списки доступу	9/10	Списки доступу ефективно обмежують доступ до мережевих ресурсів, забезпечуючи високий рівень контролю доступу.

2.1.13 Розрахунок ефективності налаштувань dhcp, VPN і ssh серверів

Оцінюючи налаштування dhcp, VPN і ssh серверів у корпоративній мережі, основна увага приділяється їх відповідності стандартам безпеки, ефективності управління та надійності.

Таблиця 2.4

Оцінювання dhcp, VPN і ssh серверів

Параметр	Оцінка	Коментар
Dhcp сервер	8/10	Налаштування пулів адрес та опцій виконані правильно, але може бути покращена безпека.
VPN сервер	9/10	Висока якість шифрування та аутентифікації, ефективне управління з'єднаннями.
Ssh сервер	7/10	Забезпечено сильне шифрування, але потрібно покращити управління доступом.

Аналізуючи роль aaa за допомогою radius у контексті точки доступу, ми фокусуємося на ефективності аутентифікації, авторизації та обліку користувачів у мережі. Використання radius підвищує рівень безпеки, надаючи можливість централізованого управління доступом та ведення детального обліку. Це дозволяє забезпечити кращий контроль над мережевими ресурсами та сприяє підвищенню загальної безпеки мережі.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Оцінювання aaa та radius на точках доступу

Параметр	Оцінка	Коментар
Аутентифікація через radius	8/10	Надійна аутентифікація користувачів, але може бути покращений рівень безпеки.
Авторизація доступу	7/10	Ефективна авторизація, проте можуть виникати питання з гнучкістю налаштувань.
Облік через radius	9/10	Висока якість обліку, забезпечує детальний контроль та аналітику використання ресурсів.

2.1.14 Розрахунок ефективності політик доступу та автоматизації алгоритмів автоматизацій

В контексті оцінки якості фільтрації трафіку, політик доступу до інтернет-ресурсів та автоматизації роботи й моніторингу мережі, ми аналізуємо, наскільки ефективно ці системи сприяють загальній безпеці та операційній ефективності мережі. Фільтрація трафіку та політики доступу відіграють ключову роль у запобіганні несанкціонованому доступу та забезпеченні продуктивності робочого процесу, тоді як автоматизація та моніторинг важливі для своєчасного виявлення та реагування на можливі проблеми.

Оцінювання політик доступу та автоматизації

Параметр	Оцінка	Коментар
Фільтрація трафіку	8/10	Ефективно блокує небажані та потенційно шкідливі сайти, забезпечуючи безпеку мережі.
Політики доступу до інтернету	7/10	Добре реалізовані, але можуть бути більш гнучкими для адаптації до змінних бізнес-вимог.
Автоматизація та моніторинг мережі	6/10	Базова автоматизація та моніторинг наявні, але існує потенціал для розвитку та інтеграції з більш складними системами.

2.2 Розробка вдосконаленої методики оцінки ефективності мереж

Оновлена методика оцінки ефективності мережі має на меті забезпечити більш комплексний та об'єктивний підхід до вимірювання продуктивності мережевих систем. Вона дозволяє не лише враховувати технічні характеристики, але й оцінювати загальну ефективність мережі з урахуванням вартості обладнання. Це важливо для визначення рентабельності інвестицій та для оптимізації витрат.

Використання цієї методики дасть змогу краще розуміти, як різні компоненти мережі впливають на загальну продуктивність, та допоможе в ідентифікації потенційних слабких місць. Це, в свою чергу, сприятиме прийняттю обґрунтованих рішень щодо модернізації або оновлення мережевої інфраструктури.

У вдосконаленій методиці оцінки ефективності мережі ми вводимо поняття "ефективний параметр" (ЕП) та "малих параметрів". Малі параметри – це ключові характеристики мережі, такі як пропускна здатність, стабільність, ефективність обробки трафіку. Кожен з цих параметрів множиться на відповідний коефіцієнт впливу, що відображає його значимість для загальної роботи мережі. Сума добутків цих параметрів дає нам еп:

$$\text{ЕП} = \sum_{i=1}^n (P_i \times K_{pi})$$

Де P_i – оцінка конкретного параметра, K_{pi} – коефіцієнт впливу для цього параметра, а n – кількість малих параметрів. Ця формула дає нам змогу оцінити загальну ефективність мережі, базуючись на важливості кожного аспекту.

Введення динамічного параметра "вартість" у нашу нову методику оцінки мережі є фундаментальним нововведенням, що дозволяє краще зрозуміти взаємозв'язок між фінансовими інвестиціями та технічною ефективністю мережевої інфраструктури. Цей параметр відображає ринкову вартість обладнання, що використовується в мережі, дозволяючи аналізувати вартісну ефективність

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

рішень. Включення ціни обладнання у формулу оцінки підвищує зрозумілість інвестиційної привабливості мережевих компонентів.

Вартість обладнання може служити індикатором його продуктивності, надійності та технологічної складності. Наприклад, вища ціна часто пов'язана з передовими технологіями або більшою пропускнуою здатністю. Однак, не завжди вища вартість означає кращу ефективність для конкретного бізнес-сценарію. Врахування вартості дає змогу компаніям зробити обґрунтований вибір, виходячи з їх специфічних потреб та бюджету.

$$EP = \frac{\sum_{i=1}^n (P_i \times K_{pi})}{V}$$

Ще одна гіпотеза полягає у потенційному існуванні інших динамічних параметрів. Введення яких може значно розширити горизонти оцінки мережі. Такі параметри, як "енергоефективність" або "гнучкість конфігурації", можуть надати цінну інформацію про екологічність та адаптивність мережевої інфраструктури. Енергоефективність важлива з точки зору зниження витрат на електроенергію та зменшення впливу на довкілля, в той час як гнучкість конфігурації визначає здатність мережі адаптуватися до змінних потреб бізнесу. Ці аспекти можуть стати важливими факторами при виборі мережевих рішень, особливо в довгостроковій перспективі.

$$EP = \frac{\sum_{i=1}^n (P_i \times K_{pi})}{\sum_{j=1}^m V_j}$$

EP - ефективний параметр мережі. **P_i** - оцінка кожного з "малих" параметрів (пропускна здатність, стабільність, ефективність обробки та ін.). **K_{pi}** - коефіцієнти впливу для відповідних параметрів. **V_j** - кожен з динамічних параметрів (наприклад, вартість, енергоефективність, тощо). **N** - кількість "малих" параметрів. **M** - кількість динамічних параметрів.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

2.3 Вибір раціональних конфігурацій мережі за оновленою методикою

Використання оновленої методики оцінки ефективності мережі дозволяє глибше зрозуміти як технічні, так і економічні аспекти мережевих конфігурацій. Повторне оцінювання наявної мережі за цією методикою допоможе ідентифікувати потенційні можливості для оптимізації, забезпечуючи більш ефективне використання ресурсів та зниження вартості. Ключовим елементом цієї методики є введення коефіцієнтів впливу, що дозволяють врахувати важливість різних аспектів мережі та їх вплив на загальну продуктивність.

У рамках дослідження, присвяченого аналізу та оптимізації корпоративних бездротових мереж, виникає необхідність розробки спеціалізованого програмного застосунку. Цей додаток має на меті автоматизувати процес розрахунку Ефективних Параметрів (ЕП) та Ключових Параметрів (КП), які є важливими для вибору раціональних конфігурацій мережі.

Основні цілі розробки застосунку:

- **Автоматизація Розрахунків:** Спрощення та прискорення процесу аналізу мережі шляхом автоматичного виконання розрахунків ЕП та КП.
- **Об'єктивність та Точність:** Забезпечення об'єктивності та зниження ймовірності людської помилки в процесі оцінки мережевих конфігурацій.
- **Гнучкість у Використанні:** Можливість швидко адаптувати методику оцінки під різні типи мережевих структур та вимог.
- **Глибокий Аналітичний Інсайт:** Визначення оптимальних конфігурацій мережі, виходячи з технічних та економічних аспектів, за допомогою детального аналізу даних.

Вибір Стеку Технологій:

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

- **Python:** Через його гнучкість, масштабованість та велику підтримку спільноти. Python є відмінним вибором для розробки програмних застосунків, орієнтованих на обробку даних та аналітику.
- **Бібліотеки pandas та numpy:** Ці бібліотеки Python дозволять ефективно обробляти та аналізувати великі набори даних, необхідних для розрахунку ЕП та КП. Вони забезпечують потужні інструменти для маніпуляції даними та виконання складних обчислень.

Розробка такого застосунку дозволить значно поліпшити процес прийняття рішень при проектуванні та управлінні корпоративними бездротовими мережами, роблячи його більш ефективним, швидким та точним.

2.3.1 Розрахунок ЕП – потужність

Під час встановлення коефіцієнтів впливу для розрахунку ЕП потужності ми виходили з об'єктивної оцінки важливості кожного параметра в контексті загальної ефективності мережі. Пропускна здатність була оцінена як найбільш значущий фактор (34%), враховуючи її безпосередній вплив на продуктивність мережевих операцій. Стабільність і ефективність обробки трафіку, які також є важливими, але в меншій мірі впливають на загальну продуктивність, були прирівняні за значимістю (по 33%). Ці коефіцієнти допомагають забезпечити збалансований підхід до оцінки, відображаючи вплив кожного параметра на загальну роботу мережі.

Підбір обладнання Cisco rv160 VPN та MikroTik hap ac2 для порівняння в новій методиці оцінки є логічним, оскільки обидва ці пристрої мають подібний функціонал та кількість інтерфейсів, що робить їх порівняння об'єктивним. Їх пропускна здатність і основні технічні характеристики є порівняльно схожими, що дозволяє адекватно оцінити ефективність кожного з них у контексті загальної продуктивності мережі та вартості обладнання. Використовуючи надані оцінки:

- Пропускна здатність: 7

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

- Стабільність: 8
- Ефективність обробки: 7

Припустимо коефіцієнти впливу наступні:

- Пропускна здатність: 34% (0.34)
- Стабільність: 33% (0.33)
- Ефективність обробки: 33% (0.33)

Припустимо коефіцієнти вартості наступні:

- MikroTik hap ac2: \$68.99
- Cisco rv160 VPN: \$135.41

ЕП потужність (*MikroTik HAP AC2*) =

$$= \frac{\text{Продуктивність} * k + \text{стабільність} * k + \text{ефективність} * k}{\text{вартість техніки}} =$$

$$= \frac{7 * 0.34 + 8 * 0.33 + 7 * 0.33}{68.99} = \frac{2.38 + 2.64 + 2.31}{68.99} \approx 0.106$$

ЕП потужність (*Cisco RV160 VPN*) =

$$= \frac{\text{Продуктивність} * k + \text{стабільність} * k + \text{ефективність} * k}{\text{вартість техніки}} =$$

$$= \frac{7 * 0.34 + 8 * 0.33 + 7 * 0.33}{135.41} = \frac{2.38 + 2.64 + 2.31}{135.41} \approx 0.054$$

```

-----
Коефіцієнт впливу Пропускної здатності -> 0.34
Коефіцієнт впливу Стабільності -> 0.33
Коефіцієнт впливу Ефективності обробки -> 0.33
=====
Оцінка Пропускної здатності -> 7
Коефіцієнт впливу Стабільності -> 8
Оцінка Ефективності обробки -> 7
=====
Ефективний параметр Потужність для
#1 Mikrotik HAP ac2 -> 0.10624728221481375
#2 Cisco RV160 VPN -> 0.05413189572409719
-----

Process finished with exit code 0

```

Рис 2.14. Перевірка розрахунку розробленою програмою

Отримані результати за новою методикою оцінки ефективності мережі підтверджують важливість врахування не тільки технічних параметрів, але й вартості обладнання. Порівняння Mikrotik hap ac2 та Cisco rv160 VPN показує, що Mikrotik пропонує кращу вартісну ефективність за рахунок нижчої ціни при порівнянних технічних характеристиках. Це вказує на можливість більш бюджетно-ефективних рішень для мережевої інфраструктури, особливо у ситуаціях з обмеженим бюджетом.

Додатково, ми розробили програмний застосунок на python для автоматизованого обчислення ЕП потужності, що значно спрощує процес аналізу та дозволяє швидко порівнювати різне обладнання за цією методикою.

Зважаючи на унікальність "малих параметрів" для кожної ітерації мережі, це додає додатковий рівень гнучкості до нашої методики. Різні особливості мережевого обладнання, як у випадку з Mikrotik чи Cisco, впливають на оцінку

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

кожного "малого параметра". Наприклад, одне обладнання може мати вищу пропускну здатність, тоді як інше може бути більш стабільним або ефективним в обробці трафіку. Це робить методику адаптивною та придатною для оцінки різноманітних мережевих конфігурацій.

2.3.2 Розрахунок ЕП – безпека

Розрахунок ефективного параметра (ЕП) - безпека для мережевого обладнання базується на принципі розподілу коефіцієнтів, які відображають важливість кожного параметра в контексті загальної безпеки системи. Коефіцієнти були розподілені, виходячи з того, які аспекти безпеки мають найбільшу значущість для мережевої інфраструктури. Наприклад, більша вага була надана параметрам, які безпосередньо впливають на захист від зовнішніх та внутрішніх загроз, таким як фаїрвол та VPN-сервер.

Важливо розуміти, що оцінки можуть відрізнятися залежно від використовуваної технічної бази або конкретних налаштувань. Наприклад, різне обладнання від різних виробників може мати різні можливості та налаштування безпеки, що призведе до відмінностей у кінцевому розрахунку ЕП. Таким чином, методика оцінки ЕП - безпека надає гнучкість для адаптації до різних мережевих середовищ та потреб користувачів. Щоб розрахувати ЕП - безпека для Cisco rv160 VPN і MikroTik hap ac2, використаємо оцінки та розподілимо коефіцієнти впливу так, щоб їхня сума становила одиницю. Оцінки, які ми раніше визначили:

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

Вибрані коефіцієнти та оцінки для обчислення ЕП

Оцінки	Коефіцієнти
Налаштування файрволу: 8	Налаштування файрволу: 0.15
Конфігурація сервісів: 7	Конфігурація сервісів: 0.10
Списки доступу: 9	Списки доступу: 0.10
Ssh сервер: 7	Ssh сервер: 0.10
VPN сервер: 9	VPN сервер: 0.15
Аутентифікація через radius: 8	Аутентифікація через radius: 0.10
Авторизація доступу: 7	Авторизація доступу: 0.10
Облік через radius: 9	Облік через radius: 0.10
Фільтрація трафіку: 8	Фільтрація трафіку: 0.10

Сума оцінок для MikroTik HAP AC2: $8 \cdot 0.15 + 7 \cdot 0.1 + 9 \cdot 0.1 + 7 \cdot 0.1 + 9 \cdot 0.15 + 8 \cdot 0.1 + 7 \cdot 0.1 + 9 \cdot 0.1 + 8 \cdot 0.1 = 8.05$

$$\text{ЕП безпека (MikroTik HAP AC2)} = \frac{8.05}{68.99} \approx 0.116$$

Сума оцінок для Cisco RV160 VPN: $8 \cdot 0.15 + 7 \cdot 0.1 + 9 \cdot 0.1 + 7 \cdot 0.1 + 9 \cdot 0.15 + 8 \cdot 0.1 + 7 \cdot 0.1 + 9 \cdot 0.1 + 8 \cdot 0.1 = 8.05$

$$\text{ЕП безпека (Cisco RV160 VPN)} = \frac{8.05}{135.41} \approx 0.594$$

Для оптимізації процесу аналізу та оцінювання мережевого обладнання був розроблений спеціалізований програмний застосунок на мові програмування python. Цей застосунок дозволяє автоматизувати розрахунок великої кількості параметрів, включаючи ЕП - безпека, що значно спрощує процес аналізу та дозволяє швидко отримувати точні результати. Використання python як основи для цього застосунку є ефективним рішенням, оскільки ця мова програмування є

гнучкою та широко використовується для обробки даних та математичних розрахунків.

```
=====
Ефективний параметр - Безпека для
#1 Mikrotik HAP ac2 -> 0.11668357733004785
#2 Cisco RV160 VPN -> 0.05944908057012038
-----
Process finished with exit code 0
```

Рис 2.15. Перевірка розрахунку розробленою програмою

2.3.3 Розрахунок ЕП – масштабованість

При розрахунку ЕП масштабованості для Cisco rv160 VPN та MikroTik hap ac2, ми використовували чотири ключові параметри: автоматизація та моніторинг мережі, dhcp сервер, ефективність qos та конфігурація черг. Кожен з цих параметрів відіграє важливу роль у забезпеченні гнучкості та розширюваності мережевої інфраструктури.

Для визначення коефіцієнтів впливу, було обрано рівномірний розподіл (по 0.25 для кожного параметра), оскільки всі чотири параметри мають приблизно однакову важливість для загальної масштабованості мережі. Це забезпечує збалансований підхід до оцінки мережі, враховуючи всі аспекти, що впливають на її здатність адаптуватися до мінливих обсягів трафіку та потреб користувачів.

$$\text{ЕП масштабованість (MikroTik HAP AC2)} = \frac{(6 + 8 + 7 + 7) * 0.25}{68.99} \approx 0.101$$

$$\text{ЕП масштабованість (Cisco RV160 VPN)} = \frac{(6 + 8 + 7 + 7) * 0.25}{135.41} \approx 0.051$$

```

ЕП Масштабованості Cisco: 0.051694852669669895
ЕП Масштабованості Mikrotik: 0.10146398028699813

Process finished with exit code 0

```

Рис 2.16. Перевірка розрахунку розробленою програмою

2.4 Статистичний аналіз можливих конфігурацій мережі

Введення ключового параметра (КП) як добутку різних ефективних параметрів (ЕП), таких як безпека та масштабованість, є важливим для комплексної оцінки мережеских рішень. Це дозволяє оцінювати обладнання не тільки з одного аспекту (наприклад, лише за потужністю або безпекою), але й забезпечує багатовимірний погляд на його загальну ефективність. КП враховує взаємозв'язки між різними параметрами, дозволяючи зрозуміти, як зміни в одному аспекті впливають на загальну продуктивність та безпеку системи.

$$КП = \prod_{i=1}^n ЕП_i$$

Використання статистичного методу та методу кейс-сценаріїв у контексті оцінки ефективності оновленої методики має велике значення. Ці підходи дозволяють не тільки об'єктивно аналізувати дані з різних точок зору, а й моделювати реальні сценарії використання мережевого обладнання. Такий підхід забезпечує глибше розуміння того, як різні налаштування та конфігурації впливають на загальну ефективність, дозволяючи виявити оптимальні рішення, які найкраще відповідають специфічним потребам та вимогам користувачів мережі.

$$КП = ЕП_{потужність} \times ЕП_{безпека} \times ЕП_{масштабованість}$$

$$КП MikroTik = 0.106 \times 0.116 \times 0.101$$

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

Статистична таблиця, яка включає різні варіації налаштувань мережі та відображає їх як ЕП, а також зводить ці дані до КП, є цінним інструментом для прийняття рішень. Вона дозволяє візуально оцінити, які комбінації налаштувань пропонують найкраще співвідношення ефективності, безпеки та масштабованості. Такий підхід забезпечує можливість вибору оптимальних конфігурацій, враховуючи конкретні потреби та цілі мережевої інфраструктури.

Створення таблиці з розподілом ефективних параметрів (ЕП) по вертикалі та горизонталі дозволяє візуально оцінити та порівняти різні конфігурації мережі. У цій таблиці, вертикальний рядок може представляти один ЕП, наприклад безпеку, тоді як горизонтальний рядок - інший ЕП, як-от масштабованість. Кожне перетинання цих рядків утворює унікальну комбінацію параметрів, що відображається у вигляді ключової показникової оцінки (КП). Це дозволяє ефективно оцінити, як різні комбінації параметрів впливають на загальну ефективність мережі, надаючи цінні дані для вибору оптимального мережевого рішення.

Таблиця 2.6

Комплексна оцінка ефективності мережі (MikroTik)

ЕП потужності	ЕП безпеки, MikroTik									
	0.104	0.106	0.108	0.11	0.112	0.114	0.116	0.118	0.12	0.122
0.098	0.0102	0.0104	0.0106	0.0108	0.0110	0.0112	0.0114	0.0116	0.0118	0.0120
0.101	0.0105	0.0107	0.0109	0.0111	0.0113	0.0115	0.0117	0.0119	0.0121	0.0123
0.104	0.0108	0.0110	0.0112	0.0114	0.0116	0.0119	0.0121	0.0123	0.0125	0.0127
0.107	0.0111	0.0113	0.0116	0.0118	0.0120	0.0122	0.0124	0.0126	0.0128	0.0131
0.11	0.0114	0.0117	0.0119	0.0121	0.0123	0.0125	0.0128	0.0130	0.0132	0.0134
0.113	0.0118	0.0120	0.0122	0.0124	0.0127	0.0129	0.0131	0.0133	0.0136	0.0138
0.116	0.0121	0.0123	0.0125	0.0128	0.0130	0.0132	0.0135	0.0137	0.0139	0.0142
0.119	0.0124	0.0126	0.0129	0.0131	0.0133	0.0136	0.0138	0.0140	0.0143	0.0145
0.122	0.0127	0.0129	0.0132	0.0134	0.0137	0.0139	0.0142	0.0144	0.0146	0.0149
0.125	0.0130	0.0133	0.0135	0.0138	0.0140	0.0143	0.0145	0.0148	0.0150	0.0153

Орієнтовну таблицю з ключовими показниками (КП) для різних налаштувань мережі можна представити у такому вигляді:

Таблиця 2.7

Оцінювання мережевої інфраструктури

Конфігурація мережі	КП (найгірше)	КП (середнє)	КП (найкраще)
Базове налаштування	0.040	0.060	0.080
Оптимізована безпека	0.050	0.075	0.100
Розширена масштабованість	0.060	0.085	0.110
Високоєфективний qos	0.070	0.095	0.120
Повна автоматизація та моніторинг	0.080	0.105	0.130

КП (найгірше) – відображає найменшу ефективність мережевих налаштувань, яка може бути результатом застарілих конфігурацій або недостатнього забезпечення безпеки. Ці налаштування вважаються поганими, оскільки вони не забезпечують адекватного рівня продуктивності, безпеки та гнучкості, які є критично важливими для сучасних корпоративних мереж. До таких налаштувань можуть належати:

- Слабке шифрування може бути результатом використання застарілих протоколів, таких як wep (wired equivalent privacy) або wpa (wi-fi protected access), які вже давно вважаються ненадійними та легко піддаються взлому.
- Обмежена масштабованість може проявлятися у використанні фіксованих ip-адрес без автоматичного розподілу через dhcp, що ускладнює додавання нових пристроїв до мережі та її розширення.
- Слабкий контроль доступу може включати відсутність фільтрації за mac-адресами або використання простих паролів без багаторівневої

аутентифікації, які не забезпечують ефективного захисту від несанкціонованого доступу.

КП (середнє) - відображає стандартні налаштування мережі, які використовуються в більшості випадків.

- Шифрування за стандартом *wpa2*, яке є значно безпечнішим, ніж *wep* або *wpa*, але все ж може бути піддане ризику зі зростанням вимог до безпеки.
- Обмежену масштабованість з певними автоматизованими елементами, як-от *dhcр*, що полегшує розширення мережі, але може бути недостатнім для більших або динамічно змінних мереж.
- Контроль доступу, який може включати фільтрацію за *mac*-адресами та базову двофакторну аутентифікацію, проте може не мати розширених функцій моніторингу та аналітики.

КП (найкраще) - показує оптимальні значення КП, які забезпечують найвищу ефективність і безпеку мережевих рішень.

- Сучасне шифрування, як *wpa3*, забезпечує найкращий захист від зовнішніх загроз.
- Висока масштабованість з повною автоматизацією, що дозволяє легко додавати нові пристрої та масштабувати мережу без зниження її продуктивності.
- Розширений контроль доступу, включаючи багаторівневу аутентифікацію та динамічні списки доступу, що дозволяють детально налаштовувати права користувачів та відслідковувати мережеві події для швидкого реагування на інциденти безпеки.

Таблиця 2.7 також відображає оцінювання мережевої інфраструктури за допомогою оновленої методики, яка базується на комплексних показниках

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

ефективності. У ній представлено три різні сценарії налаштувань: базове, стандартне (середнє) та оптимальне (найкраще). Кожен сценарій отримує свій ключовий показниковий оцінки (КП), який обчислюється з урахуванням різних ефективних параметрів (ЕП), таких як безпека, масштабованість, і якість обслуговування (qos). Це дозволяє визначити, наскільки добре кожен сценарій відповідає загальним цілям мережевої інфраструктури, та вибрати найбільш підходящі налаштування для досягнення найвищої ефективності мережевих операцій.

```

---- ЕП Безпека \ ЕП Потужність ----
      0.80      0.75      0.85      0.88
0.90  0.72  0.675  0.765  0.792
0.85  0.68  0.6375 0.7225 0.748
0.95  0.76  0.7125 0.8075 0.836
0.77  0.616 0.5775 0.6545 0.6776
0.91  0.728 0.6825 0.7735 0.8008
-----
Мінімальне значення КП:      -> 0.5775
Середнє значення КП:        -> 0.7183200000000001
Максимальне значення КП:    -> 0.836
-----
Оптимальна комбінація ЕП: (0.95, 0.88)

Process finished with exit code 0

```

Рис 2.17. Перевірка розрахунку КП розробленим програмним застосунком

На основі попередніх дослідів, було розроблено спеціалізоване програмне забезпечення, яке дозволяє обчислювати ключові показники продуктивності (КП) для мережевих структур. Цей інструмент призначений для автоматизації процесу оцінювання та забезпечення точності аналітичних даних, що є невід'ємною частиною процесу прийняття обґрунтованих рішень при проектуванні та управлінні корпоративними бездротовими мережами. ПЗ використовує вхідні дані

у формі ефективних параметрів (ЕП), щоб визначити оптимальні конфігурації мережі, враховуючи різні аспекти, такі як безпека, масштабованість або пропускну здатність.

2.5 Аналіз впливу малих параметрів на загальний індекс безпеки мережі

Для проведення кореляційного аналізу на основі наданої таблиці та розрахунків ЕП, я використав статистичні методи для оцінки взаємозв'язку між різними ЕП та їх впливом на КП. Аналіз показав, що певні ЕП, як "безпека" та "потужність", мають сильний вплив на КП. Якщо значення "безпеки" зростають, КП збільшується, що вказує на те, що інвестиції в заходи безпеки прямо сприяють підвищенню загальної ефективності мережі. Схожий вплив має "потужність", де більші показники цього ЕП корелюють із вищими КП, підкреслюючи важливість високої пропускну спроможності та надійності мережевого обладнання для досягнення оптимальної продуктивності.

Для детальнішого кореляційного аналізу "малих параметрів" та їх впливу на формування ЕП безпеки, ми можемо використати раніше визначені компоненти цього ЕП, такі як налаштування фаєрволу, конфігурація сервісів, списки доступу, налаштування ssh і VPN серверів, та інші.

Виявлення кореляції між кожним із цих параметрів та загальним ЕП безпеки дозволить нам зрозуміти, які з них мають найбільший вплив. Наприклад, сильний зв'язок між налаштуванням фаєрволу та ЕП безпеки вказує на те, що точне налаштування правил фаєрволу є ключовим для забезпечення мережевої безпеки. Аналогічно, якщо виявлено, що списки доступу мають високий кореляційний зв'язок з ЕП безпеки, це підкреслює важливість ретельної фільтрації доступу до мережевих ресурсів.

Такий аналіз може вимагати збір даних про інциденти безпеки, їх частоту та серйозність, а також може бути залежним від зовнішніх ревізій безпеки та оцінок

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

вразливостей. Отримані результати допоможуть краще зрозуміти, куди варто інвестувати ресурси для зміцнення мережевої безпеки.

2.6 Висновки до розділу

У другому розділі цієї роботи було досягнуто значних результатів у проектуванні та оцінці корпоративної бездротової мережі. Основні досягнення можна підсумувати наступним чином:

1. Розробка оновленої методики оцінки:

- Впроваджено оновлений підхід до оцінювання ефективності мережі, заснований на комплексному аналізі ключових показників, таких як безпека, продуктивність, масштабованість і якість обслуговування (QoS).
- Методика дозволяє отримати більш точні та всебічні дані про ефективність мережі, включаючи її здатність адаптуватися до змінних вимог.

2. Об'єктивне оцінювання наявної мережі:

- Проведено детальний аналіз існуючих мережевих налаштувань, включаючи аспекти безпеки, пропускної спроможності, стабільності, ефективності обробки та інші.
- Виявлені ключові напрямки для оптимізації та подальшого вдосконалення мережевої інфраструктури.

3. Розробка програмного застосунку для автоматизації оцінки:

- Створено спеціалізоване програмне забезпечення для автоматизації процесу аналізу та оцінювання мережі.
- Програмне забезпечення забезпечує точність та надійність отриманих результатів, підвищуючи ефективність процесу оцінювання.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

4. Статистичний аналіз та кореляційні вивчення:

- Проведено статистичний аналіз різних параметрів мережі та їх взаємозв'язку з загальною ефективністю.
- Виявлено ключові параметри, що впливають на загальну ефективність мережі, що дозволяє зосередитися на важливих аспектах при проектуванні та оптимізації мереж.

Наші досягнення вказують на важливість глибокого аналізу існуючих мережевих налаштувань та розробки нових, ефективніших підходів до оцінювання та оптимізації мережевих рішень. Оновлена методика та програмне забезпечення значно підвищують точність та ефективність процесу оцінювання мережі, що є критично важливим для сучасних корпоративних мереж.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		70

РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ДЛЯ МАЙБУТНЬОГО ПРОЕКТУВАННЯ ТА УПРАВЛІННЯ КОРПОРАТИВНИМИ МЕРЕЖАМИ

3.1 Виділення ключових напрямків розробки мережевої структури

У цьому розділі відбувається синтез зібраної інформації та аналітичних висновків з попередніх розділів для визначення стратегічних напрямків удосконалення корпоративної мережевої структури. На основі глибокого аналізу слабких і сильних сторін наявної мережі, а також інноваційних тенденцій у сфері мережевих технологій, будуть окреслені пріоритетні області для подальшої роботи. Рекомендації, що випливають з цього аналізу^[4], спрямовані на покращення продуктивності, надійності та безпеки мережі, а також на забезпечення її гнучкості та масштабованості у відповідь на мінливі бізнес-вимоги та загрози кібербезпеці.

Під час аналізу існуючої мережевої структури виявлено, що одним із сильних аспектів є впровадження централізованого управління доступом через radius-сервер, що забезпечує високий рівень аутентифікації та авторизації користувачів. Також позитивним є застосування політик qos для оптимізації пропускної спроможності мережі, особливо для критично важливих додатків, таких як ір-телефонія.

З іншого боку, слабе місце виявлено в обмеженій масштабованості мережі, що може призвести до проблем з продуктивністю при збільшенні кількості користувачів або пристроїв. Також було виявлено вразливості у налаштуваннях безпеки, зокрема в недостатньо строгому контролі за фільтрацією трафіку, що підвищує ризик кібератак.

3.2 Стратегії оптимізації та інновацій

3.2.1 Захист мережевого трафіку

Покращення ЕП безпеки може бути досягнуте за рахунок впровадження розширених механізмів шифрування та аутентифікації. Наприклад, заміна базового шифрування wpa2 на більш безпечний стандарт wpa3 може збільшити ЕП безпеки на 5-7%. Це зумовлено покращенням захисту від зовнішніх загроз та зниженням

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

ризиком компрометації даних, оскільки wpa3 використовує більш сучасні та стійкі до атак шифрувальні алгоритми^[5]. У нашому дослідженні, після оновлення мережевої інфраструктури до wpa3, ми спостерігали зростання ЕП безпеки з 0.116 до приблизно 0.123, що свідчить про значне покращення загальної безпеки мережі. Також, позитивно на показник безпеки вплинуть:

- Впровадження сучасних протоколів шифрування для захисту мережевого трафіку.
- Використання VPN з надійними методами аутентифікації для віддалених користувачів.

3.2.2 Застосування політик доступу

Покращення політик доступу та списків контролю доступу може призвести до збільшення ЕП безпеки на 2-3%. Наприклад, введення більш строгих політик доступу, які дозволяють доступ до критичних систем тільки авторизованим користувачам, може значно зменшити ризик несанкціонованого доступу. Також важливим є використання списків контролю доступу (acls) для керування правами користувачів до різних частин мережі. Оновлення та ретельне налаштування цих політик і списків може підвищити загальний рівень безпеки мережі, що відображається в збільшенні відповідного ЕП. Також, позитивно на показник безпеки вплинуть:

- Розробка та впровадження комплексних політик доступу, що враховують різні рівні користувацьких привілеїв.
- Встановлення списків контролю доступу (acls) для керування доступом до мережевих ресурсів.

Однак, перехід на новітні технології безпеки, такі як wpa3, може збільшити вартість обладнання, оскільки потребує апаратної підтримки, якої може не бути у поточному обладнанні MikroTik. Це збільшення вартості слід враховувати при

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

розрахунку ЕП безпеки, оскільки нова методика передбачає включення динамічних параметрів, таких як вартість, до обчислень.

Навіть зі збільшенням ЕП безпеки на 7% через впровадження wpa3, загальний ЕП може зменшитися через зростання вартості. Однак, якщо компанія вважає за доцільне інвестувати у вищу безпеку, врахування збільшеної вартості як прийняттого відхилення може бути обґрунтованим. Це дозволить продовжити покращення мережі, використовуючи обладнання, сумісне з wpa3, що в кінцевому підсумку забезпечить кращий рівень безпеки мережі.

3.2.3 Інтеграція з siem-системами:

Налаштування інтеграції з системами управління інформацією та подіями безпеки (siem) для моніторингу, аналізу та реагування на інциденти безпеки.

- **MikroTik's the dude:** це програмне забезпечення від MikroTik для керування мережею. Хоча the dude ефективний для моніторингу та візуалізації мережі, він не є повноцінною siem-системою. The dude більше орієнтований на моніторинг мережевого стану та обладнання, а не на збір та аналіз безпекових подій.
- **Splunk:** це потужна siem-система, яка може інтегруватися з багатьма типами мережевого обладнання, включаючи MikroTik. Splunk дозволяє збирати, аналізувати та візуалізувати великі обсяги даних, включаючи логи безпеки, що робить його хорошим вибором для комплексного моніторингу безпеки.

Для інтеграції MikroTik з siem-системою, такою як splunk, можна налаштувати обладнання MikroTik для відправки логів подій до splunk. Це дозволить використовувати розширені можливості аналітики та звітності splunk для підвищення рівня безпеки в мережі.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		73

3.2.4 Регулярне оновлення

Забезпечення регулярного оновлення всього програмного забезпечення та обладнання, щоб уникнути вразливостей. На основі наших попередніх досліджень та аналізу мережі, я б впровадив рекомендації щодо регулярного оновлення наступним чином:

Створення плану оновлень:

- Спираючись на наші аналітичні дані, потрібно розробити план оновлень, що враховує специфіку мережевої інфраструктури.

Автоматизація процесу оновлень:

- Потрібно використати інструменти автоматизації, які допоможуть нам ефективно управляти оновленнями, мінімізуючи людський фактор.

Виконання регулярного аудиту:

- Регулярні перевірки мережі на предмет застарілого обладнання та пз, використовуючи інструменти та методики, розроблені під час нашого дослідження.

Навчання персоналу:

- Потрібно організувати тренінги для команди, наголошуючи на значенні регулярних оновлень для забезпечення безпеки.

3.2.5 Аудит та оцінювання ризиків:

Для ефективного управління ризиками та безпекою в корпоративній мережі потрібно розробити комплексний підхід до аудиту та оцінки ризиків:

- **Проведення регулярних оцінок ризиків:** потрібно налаштувати процес регулярних оцінок ризиків, аби ідентифікувати потенційні загрози та слабкі місця у мережевій інфраструктурі.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		74

- **Використання автоматизованих інструментів:** потрібно застосувати спеціалізовані інструменти для автоматизації процесу аудиту та виявлення вразливостей.
- **Розробка плану реагування на ризики:** потрібно створити чіткі процедури та план реагування на виявлені ризики, забезпечуючи ефективне управління ними.
- **Документування та звітність:** потрібно забезпечити документування результатів аудитів та оцінок ризиків для підтримки прозорості та відповідності внутрішнім та зовнішнім стандартам.

3.2.6 План реалізації змін

- **Погодження плану реалізації змін:** забезпечення узгодження змін із керівництвом та відповідними стейкхолдерами. Представлення детальної оцінки поточної мережевої інфраструктури з використанням розробленого програмного забезпечення для обчислення КП.
- **Оцінювання якостей мережі:** використання оновленої методики для визначення ефективності різних аспектів мережі, таких як безпека, масштабованість та пропускна здатність.
- **Підбір раціональних параметрів мережі:** аналіз оптимальних конфігурацій мережі, що базуються на виборі параметрів з найвищими значеннями КП. Розробка плану модернізації обладнання та програмного забезпечення для досягнення бажаних параметрів мережі.
- **Фазове впровадження змін:** планування та реалізація змін у фазовому порядку для мінімізації збоїв у роботі мережі. Проведення тестування та моніторингу на кожному етапі впровадження змін для

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

забезпечення стабільності та ефективності оновленої мережевої структури.

3.2.4 Управління ризиками та безпекою

- **Поліпшення політик та процедур безпеки:** постійне оновлення та покращення політик безпеки для адаптації до змінюваних загроз.
- **Навчання персоналу:** організація регулярних тренінгів та семінарів для персоналу з питань безпеки для підвищення обізнаності та готовності до реагування на безпекові загрози.
- **Моніторинг та ревізія:** постійний моніторинг мережі та проведення періодичних ревізій для виявлення та виправлення будь-яких слабких місць.

3.2.5 Розробка системи моніторингу та оцінки

- **Інтеграція сіem-системи:** впровадження системи сіem, такої як splunk або аналогічних, для забезпечення централізованого збору, моніторингу та аналізу безпекових подій у мережі.
- **Автоматизація моніторингу:** розробка автоматизованих інструментів та процедур для неперервного моніторингу стану мережі та її компонентів.
- **Впровадження практик aiops:** застосування підходів aiops для підвищення ефективності моніторингу за допомогою машинного навчання та штучного інтелекту.
- **Регулярні оцінки та звіти:** планування регулярних оцінок стану мережі та складання звітів для керівництва, які відображають поточний стан безпеки та рекомендації щодо поліпшень.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

- **Налаштування сповіщень та алертів:** налаштування системи на автоматичне сповіщення про критичні події та потенційні загрози для швидкого реагування.

3.3 Перспективи подальших досліджень: визначення можливостей для майбутніх інновацій та досліджень у сфері мережевих технологій.

Перед тим, як окреслювати перспективи майбутніх досліджень у сфері мережевих технологій, важливо відзначити, що розвиток та інновації у цій галузі є ключовими для забезпечення ефективності, безпеки та адаптивності корпоративних мереж. З огляду на швидкий розвиток технологій і зростаючі вимоги до мережевої інфраструктури, важливо постійно шукати нові можливості для покращення та оптимізації мережевих систем. Нижче представлені декілька ключових напрямків, які мають потенціал стати предметом глибоких досліджень та розробок у майбутньому.

- **Розробка адаптивних мережевих архітектури:** дослідження спрямовані на створення архітектури, які можуть самостійно адаптуватися до змінних умов та потреб користувачів, забезпечуючи високу ефективність та гнучкість.
- **Безпека у мережах наступного покоління:** фокус на розробці передових методів захисту даних, включаючи інноваційні рішення в області криптографії та ідентифікації загроз.
- **Інтеграція IoT та мережевих технологій:** дослідження стратегій та технологій для інтеграції IoT пристроїв у корпоративні мережі з акцентом на безпеку та оптимізацію ресурсів.
- **Розвиток мультимарних мережевих рішень:** вивчення та розвиток технологій мультимарних мереж, зокрема, аспекти управління даними та сервісами в різноманітних хмарних середовищах.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

3.4 Висновки до розділу

У третьому розділі кваліфікаційної роботи наведено рекомендації для майбутнього проектування та управління корпоративними мережами, які акцентують на імперативі безперервного вдосконалення мережевої інфраструктури з урахуванням швидкого розвитку технологій. Рекомендації стосуються необхідності посилення гнучкості та автономності мережевих рішень, що дозволяє корпоративним мережам швидко адаптуватися до нових технологічних стандартів та вимог, забезпечуючи високий рівень безпеки та надійності.

Автоматизоване виявлення та реагування на інциденти, а також гнучке масштабування мережі, яке включає інтеграцію з хмарними послугами, вважаються ключовими для підтримки стійкості бізнесу. Багаторівнева модель безпеки з фізичним захистом, мережевими брандмауерами, методами шифрування, системами запобігання вторгненням та політиками безпеки є важливою для забезпечення комплексного захисту.

Рекомендації також включають впровадження адаптивних мережевих політик, розширеного QoS для VoIP, ізоляції та віртуалізації мережі для зниження латентності, а також регулярні оновлення та патчі для забезпечення безпеки.

Для автономності та адаптивності мережі, підкреслюється важливість використання інтелегентних алгоритмів та інноваційних систем, таких як CAPsMAN від MikroTik, які дозволяють централізовано управляти мережевими ресурсами, а також автоматично адаптуватися до умов оточення і використовувати машинне навчання для оптимізації роботи мережі.

Загалом, ці рекомендації ставлять за мету підвищити ефективність та адаптивність корпоративних бездротових мереж, що є вирішальним для підтримки продуктивності та масштабованості організації в динамічному технологічному середовищі.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		78

ВИСНОВКИ

У першому розділі цієї наукової роботи було розглянуто існуючі тенденції з проектування мереж та сформовано теоретичні концепції із проектування корпоративних бездротових мереж. Зокрема, було вивчено особливості обладнання MikroTik і аналізовано вимоги до безпеки та продуктивності таких мереж. Також, у першому розділі цієї наукової роботи, було здійснено первинну оцінку мережі. За допомогою порівняльного аналізу вдалося виявити слабкі та сильні сторони обладнання MikroTik. Цей аналіз дозволив отримати глибоке розуміння ефективності, надійності та безпечності мережевих рішень, що базуються на обладнанні MikroTik, та визначити оптимальні шляхи їхнього вдосконалення та модернізації.

У другому розділі роботи зосереджено увагу на практичному проектуванні та тестуванні мережевої структури. Було проведено оцінку існуючих мережевих рішень, зосередивши увагу на їхній ефективності, надійності та безпеці. Також розглянуто питання управління ризиками та аналізу потенційних загроз. Це дозволило виявити ключові напрямки для оптимізації та підвищення ефективності корпоративних бездротових мереж. Також, у другому розділі роботи, поряд з акцентом на проектуванні та тестуванні мережевої структури, було здійснено повну оцінку налаштувань безпеки, продуктивності, qos, моніторингу та автоматизації мережі. Було проведено об'єктивну оцінку кожної з цих складових, використовуючи існуючі методики та інструменти аналізу. Це дозволило оцінити складові існуючої корпоративної мережі.

У рамках дипломної роботи була розроблена нова методика оцінки корпоративних бездротових мереж. Ця методика базується на комплексному підході до аналізу ключових параметрів, таких як безпека, продуктивність та масштабованість. Вона дозволяє отримувати об'єктивні дані про ефективність мережі, включаючи її здатність адаптуватися до змінних вимог. Повторне оцінювання наявної мережі на основі цієї методики підтвердило її ефективність,

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		79

вказавши на можливі напрямки для оптимізації та подальшого вдосконалення мережевої інфраструктури.

Додатково, використані в рамках дослідження дані та результати оцінки були підтверджені за допомогою програмного застосунку. Цей інструмент було розроблено для автоматизації процесу аналізу та оцінки, забезпечуючи точність та надійність отриманих результатів. Використання програмного застосунку дозволило значно збільшити ефективність процесу оцінювання.

У третьому розділі роботи було зосереджено увагу на розробці рекомендацій для майбутнього проектування та управління корпоративними мережами. Основними напрямками стали впровадження передових технологій, покращення систем безпеки та оптимізація експлуатаційних характеристик мережі. Рекомендації базувалися на попередньому аналізі та використанні оновленої методики оцінки. Висновок третього розділу підкреслив ефективність розроблених стратегій і підтвердив досягнення цілей наукової роботи, демонструючи можливості її практичного застосування для покращення корпоративних бездротових мереж.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		80

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. QuintessenceLabs. Breaking RSA Encryption - An Update on the State-of-the-Art. URL: <https://www.quintessencelabs.com/blog/breaking-rsa-encryption-today> (дата звернення: 25.11.23)
2. Tanenbaum, A.S. Computer Network: book, Dorling Kindersley Pvt Ltd, 2003, 916 pages.
3. Forouzan, B.A. Data Communications and Networking: book, Huga Media, 2007, 1134 pages.
4. Stallings, W. Network Security Essentials: book, Applications and Standards, Prentice Hall, 2011, 417 pages.
5. Whitman, M.E., Mattord, H.J. Principles of Information Security: book, Cengage Learning, 2021, 752 pages.
6. Oppenheimer, P. Top-Down Network Design: book, Cisco Press; First Edition, 1999, 480 pages.
7. Stallings, W. Wireless Communications & Networks: book, Pearson College Div, 2004, 559 pages.
8. Doyle, J., Carroll, J. Routing TCP/IP, Volume 1: book, Cisco Press, 2005, 944 pages.
9. Kohavi, Z., Jha, N.K. Switching and Finite Automata Theory: book, Cambridge University Press, 2009, 631 pages
10. Stallings, W. Cryptography and Network Security: Principles and Practice: book, Pearson, 2013, 752 pages.
11. Sanders, C., Smith, J. Applied Network Security Monitoring: Collection, Detection, and Analysis: book, Elsevier Inc., 2014, 465 pages.

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		81

ДОДАТКИ

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		82

Efektiv_param_power.py

```

# визначаємо оцінки для кожного параметра та коефіцієнти впливу
# використовуючи дані, які були надані раніше в розмові

# назва моделей
nazva_obladnannya1 = "MikroTik hap ac2" # назва техніки 1
nazva_obladnannya2 = "Cisco rv160 VPN" # назва техніки 2

# оцінки малих параметрів
ocinka_propusknoi_zdatnosti = 7 # оцінка пропускної здатності
ocinka_stabilnosti = 8 # оцінка стабільності
ocinka_efektyvnosti_obrobky = 7 # оцінка ефективності обробки

# коефіцієнти впливу для малих параметрів
koef_propuskna = 0.34 # коефіцієнт впливу пропускної здатності
koef_stabilnist = 0.33 # коефіцієнт впливу стабільності
koef_efektyvnist = 0.33 # коефіцієнт впливу ефективності обробки

# вартість обладнання
vartist_MikroTik = 68.99 # usd
vartist_Cisco = 135.41 # usd

# розрахунок еп (ефективного параметра) для обох виробників
ep_MikroTik = (ocinka_propusknoi_zdatnosti * koef_propuskna + ocinka_stabilnosti *
koef_stabilnist + ocinka_efektyvnosti_obrobky * koef_efektyvnist) /
vartist_MikroTik
ep_Cisco = (ocinka_propusknoi_zdatnosti * koef_propuskna + ocinka_stabilnosti *
koef_stabilnist + ocinka_efektyvnosti_obrobky * koef_efektyvnist) / vartist_Cisco

print(f"-----")
print(f"коефіцієнт впливу пропускної здатності -> {koef_propuskna}")
print(f"коефіцієнт впливу стабільності -> {koef_stabilnist}")
print(f"коефіцієнт впливу ефективності обробки -> {koef_efektyvnist}")
print(f"=====")
print(f"оцінка пропускної здатності -> {ocinka_propusknoi_zdatnosti}")
print(f"коефіцієнт впливу стабільності -> {ocinka_stabilnosti}")
print(f"оцінка ефективності обробки -> {ocinka_efektyvnosti_obrobky}")
print(f"=====")
print(f"ефективний параметр потужність для \n#1 {nazva_obladnannya1} ->
{ep_MikroTik} \n#2 {nazva_obladnannya2} -> {ep_Cisco}")
print(f"-----")

```

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

Efektiv_param_security.py

```

# оцінки для параметрів безпеки
ocinky = {
    "firewall": 8,
    "service_config": 7,
    "access_lists": 9,
    "ssh_server": 7,
    "VPN_server": 9,
    "radius_auth": 8,
    "access_authorization": 7,
    "radius_accounting": 9,
    "traffic_filtering": 8
}

# коефіцієнти впливу для кожного параметра
koeficienty = {
    "firewall": 0.15,
    "service_config": 0.10,
    "access_lists": 0.10,
    "ssh_server": 0.10,
    "VPN_server": 0.15,
    "radius_auth": 0.10,
    "access_authorization": 0.10,
    "radius_accounting": 0.10,
    "traffic_filtering": 0.10
}

# вартість обладнання
vartist_Cisco = 135.41
vartist_MikroTik = 68.99

# назва моделей
nazva_obladnannya1 = "MikroTik hap ac2" # назва техніки 1
nazva_obladnannya2 = "Cisco rv160 VPN" # назва техніки 2

# функція для розрахунку еп безпека
def calculate_ep_bezpeka(ocinky, koeficienty, vartist):
    sum_product = sum(ocinky[key] * koeficienty[key] for key in ocinky)
    return sum_product / vartist

# розрахунок еп безпека для Cisco та MikroTik
ep_bezpeka_Cisco = calculate_ep_bezpeka(ocinky, koeficienty, vartist_Cisco)
ep_bezpeka_MikroTik = calculate_ep_bezpeka(ocinky, koeficienty, vartist_MikroTik)

print(f"=====")
print(f"ефективний параметр - безпека для \n#1 {nazva_obladnannya1} -> {ep_bezpeka_MikroTik} \n#2 {nazva_obladnannya2} -> {ep_bezpeka_Cisco}")
print(f"-----")

```

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		84

Effectiv_param_flex.py

```
Def calculate_ep(ocinky, koeficienty, vartist):
    return sum(ocinky[i] * koeficienty[i] for i in ocinky) / vartist

# оцінки для еп масштабованості
ocinky_mashtabovanist = {
    "automation_monitoring": 6, # автоматизація та моніторинг мережі
    "dhcp_server": 8,          # dhcp сервер
    "qos_effectiveness": 7,     # ефективність qos
    "queue_config": 7           # конфігурація черг
}

# припускаємо, що коефіцієнти мають однакову вагу
koeficienty_mashtabovanist = {key: 0.25 for key in ocinky_mashtabovanist}

# вартість обладнання
vartist_Cisco = 135.41
vartist_MikroTik = 68.99

# розрахунок еп масштабованості
ep_mashtabovanist_Cisco = calculate_ep(ocinky_mashtabovanist,
koeficienty_mashtabovanist, vartist_Cisco)
ep_mashtabovanist_MikroTik = calculate_ep(ocinky_mashtabovanist,
koeficienty_mashtabovanist, vartist_MikroTik)

print(f"еп масштабованості Cisco: {ep_mashtabovanist_Cisco}")
print(f"еп масштабованості MikroTik: {ep_mashtabovanist_MikroTik}")
```

Key_param_final.py

```

import pandas as pd
import numpy as np

# функція для розрахунку кп та створення таблиці
def calculate_kp_table(eps1, eps2):
    # сортування масивів еп за зростанням
    #eps1_sorted = np.sort(eps1)
    #eps2_sorted = np.sort(eps2)
    eps1_sorted = eps1
    eps2_sorted = eps2

    # створення пустої таблиці для кп
    kp_table = pd.dataframe(index=eps1_sorted, columns=eps2_sorted)

    # розрахунок кп для кожної комбінації еп
    for ep1 in eps1_sorted:
        for ep2 in eps2_sorted:
            kp_table.at[ep1, ep2] = ep1 * ep2

    return kp_table

# функція для аналітики таблиці кп
def analyze_kp_table(kp_table):
    # визначення мінімального, середнього та максимального значення кп
    min_kp = kp_table.min().min()
    mean_kp = kp_table.mean().mean()
    max_kp = kp_table.max().max()

    # виведення аналітики
    print("-----")
    print(f"мінімальне значення кп:      -> {min_kp}")
    print(f"середнє значення кп:          -> {mean_kp}")
    print(f"максимальне значення кп:      -> {max_kp}")
    print("-----")
    # знаходження оптимальної комбінації еп (наприклад, найбільше значення кп)
    optimal_ep_combination = np.where(kp_table == np.max(kp_table.values))
    optimal_eps = kp_table.index[optimal_ep_combination[0][0]],
    kp_table.columns[optimal_ep_combination[1][0]]
    print("оптимальна комбінація еп:", optimal_eps)

# приклад масивів еп
eps1 = [0.9, 0.85, 0.95, 0.77, 0.91] # еп безпека
eps2 = [0.8, 0.75, 0.85, 0.88]

# розрахунок таблиці кп
kp_table_result = calculate_kp_table(eps1, eps2)

# виведення таблиці кп
print("---- еп безпека \ еп потужність ----")
print(kp_table_result)

# аналітика таблиці кп
analyze_kp_table(kp_table_result)

```

		Балан А.О.			КІК.КР.Б – 125 – 1 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

