

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 бакалавра
на тему: «Проект підсистеми захисту гетерогенної
мережі організації»

Виконав студент 4-го курсу групи КБ-19-1
спеціальності 125 «Кібербезпека»

 Владислав Опанасюк

Керівник старший викладач кафедри КІ та КБ

 Олександра Покотило

Рецензент старший викладач кафедри КІ та КБ

 Єлизавета Байлюк

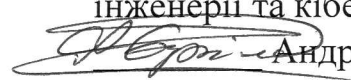
Житомир – 2023

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
2 серпня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Опанасюк Владислав Вітольдович

Тема роботи: «Проект підсистеми захисту гетерогенної мережі організації»

затверджена Наказом університету від 2 серпня 2023 р. №319/с

Термін здачі студентом закінченої роботи 23 серпня 2023 р.

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

Налаштована захищена гетерогенна мережа організації.

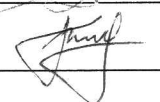
Обладнання та програмне забезпечення:

1. Мережевий емулятор GNS3, VirtualBox
2. Маршрутизатори та комутатори Cisco
3. ОС Windows, ОС Linux

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

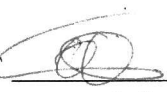
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Покотило О.А.	 02.08.23	 02.08.23
2	Покотило О.А.	 02.08.23	 02.08.23
3	Покотило О.А.	 02.08.23	 02.08.23

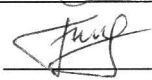
Студент  Владислав Опанасюк

Керівник  Олександра Покотило

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	10.07.2023-13.07.2023	виконано
2	Пошук та аналіз літературних джерел	14.07.2023-20.07.2023	виконано
3	Аналіз основних теоретичних відомостей про гетерогенні мережі	21.07.2023-25.07.2023	виконано
4	Проектування топології мережі	25.07.2023-31.07.2023	виконано
5	Розробка IP-адресації мережі	01.08.2023-03.08.2023	виконано
6	Вибір мережевого обладнання	04.08.2023-07.08.2023	виконано
7	Налаштування мережі в емуляторі GNS3	08.08.2023-15.08.2023	виконано
8	Тестування працездатності мережі	16.08.2023-19.08.2023	виконано
9	Оформлення пояснювальної записки	20.08.2023-22.08.2023	виконано
10	Захист кваліфікаційної роботи	28.08.2023	виконано

Студент  Владислав Опанасюк

Керівник  Олександра Покотило

АНОТАЦІЯ

В даній кваліфікаційній роботі описано повний цикл проектування, розробки та налаштування підсистеми захисту гетерогенної мережі організації. Структура роботи включає в себе вступ, три розділи, висновки, список використаної літератури та додатки. Змістовна частина охоплює 62 сторінок друкованого тексту, додаткові відомості розміщено на 9 сторінках додатків. У списку використаних джерел зазначено 14 джерел. Загальний обсяг роботи становить 71 сторінки. У роботі наведено 18 ілюстрацій та 11 таблиць, що візуально доповнюють викладену інформацію.

Метою кваліфікаційної роботи є розробка та налаштування проекту підсистеми захисту гетерогенної мережі організації.

Основні результати роботи включають аналіз принципів роботи гетерогенних мереж. Розглянуто особливості проектування та налаштування представлених мереж. В практичній роботі представлена розробка топології мережі, вибір необхідного обладнання та налаштування мережі. Наведено результати тестування працездатності мережі.

Ключові слова: ГЕТЕРОГЕННІ МЕРЕЖІ, DNS, OSPF, EIGRP, ПРОТОКОЛ, ЗАХИСТ.

					КІК.КР.Б – 125 – 11 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту гетерогенної мережі організації	Літ.	Арк.	Аркушів	
Розроб.		Опанасюк В.В.		25.08.23					
Керівник		Покотило О.А.		22.08.23			4	71	
Реценз.		Байлюк Є.М.		23.08.23		ФІКТ, Гр. КБ-19-1			
Н. контр.		Покотило О.А.		22.08.23					
Затверд.		Єфіменко А.А.		22.08.23					

ANNOTATION

This qualification work describes the full cycle of design, development and configuration of the protection subsystem of the organization's heterogeneous network. The structure of the work includes an introduction, three chapters, conclusions, a list of references and appendices. The content part covers 62 pages of printed text, additional information is placed on 9 pages of appendices. 14 sources are listed in the list of used sources. The total volume of work is 71 pages. The work contains 18 illustrations and 11 tables that visually complement the information presented.

The purpose of the qualification work is to develop and configure the project of the protection subsystem of the organization's heterogeneous network.

The main results of the work include the analysis of the principles of operation of heterogeneous networks. Features of design and configuration of the presented networks are considered. The practical work presents the development of the network topology, the selection of the necessary equipment and network settings. The results of network performance testing are presented.

Keywords: HETEROGENEOUS NETWORKS, DNS, OSPF, EIGRP, PROTOCOL, PROTECTION.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ТА АСПЕКТИ СТВОРЕННЯ	
ПІДСИСТЕМИ ЗАХИСТУ ГЕТЕРОГЕННИХ МЕРЕЖ	10
1.1 Огляд гетерогенних мереж та їх особливостей.....	10
1.2 Визначення вимог до підсистеми захисту.....	17
1.3 Огляд сучасних методів та технологій захисту гетерогенних мереж.....	21
РОЗДІЛ 2 ПРОЕКТУВАННЯ ГЕТЕРОГЕННОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ	32
2.1 Розробка топології гетерогенної мережі	32
2.2 Розробка схем адресацій мережі.....	36
2.3 Вибір мережевого обладнання для організації роботи мережі	41
2.4 Аналіз ризиків та заходи для захисту гетерогенної мережі	45
РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ОБЛАДНАННЯ	
ГЕТЕРОГЕННОЇ МЕРЕЖІ	48
3.1 Налагодження обладнання мережі	48
3.2 Перевірка працездатності мережі	56
ВИСНОВКИ	60
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	61
ДОДАТКИ	63

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

HetNet – Heterogenic Networks

ПЗ – програмне забезпечення

ПК – персональний комп'ютер

DNS – Domain Name System

IP – Internet Protocol

LAN – Local Area Network

WAN – Wide Area Network

EIGRP – Enhanced Interior Gateway Routing Protocol

OSPF – Open Shortest Path First

SSH – Secure Shell

SNMP – Simple Network Management Protocol

UDP – User Datagram Protocol

TCP – Transmission Control Protocol

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасному інформаційному середовищі вельми важлива, оскільки зростаюча роль мережевих технологій та їх розповсюдження створюють нові виклики та загрози для кібербезпеки. Підтримка ефективної та безпечної мережевої інфраструктури стає основоположним завданням для будь-якої організації, оскільки залежність від технологій набуває все більшого значення.

Зростання обсягів даних, широкий спектр пристроїв та різноманітність мережевих з'єднань створюють багато вразливостей та можливостей для кіберзлочинців. Зловмисники шукають шляхи порушення безпеки мережі, отримання конфіденційної інформації, втручання у роботу системи, що може вивести з ладу роботу організації, завдати збитків та пошкодження репутації.

У цьому контексті, розробка підсистеми захисту гетерогенної мережі організації стає важливим завданням. Реалізація ефективної системи захисту передбачає аналіз загроз та ризиків, розробку та впровадження комплексу технічних та організаційних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності даних.

Новітні технології та розширений спектр застосувань мережі підвищують складність задачі забезпечення безпеки. Важливим елементом є розробка та реалізація ефективних методів аутентифікації, авторизації та аудиту, а також використання шифрування для захисту передачі даних.

Додатковою вагомою складовою є вимоги регуляторних органів та стандарти безпеки даних. Багато секторів діяльності підлягають обов'язковим вимогам щодо захисту конфіденційної інформації, такої як особисті дані клієнтів, медичні записи, фінансові дані тощо.

Також слід враховувати, що недостатній захист може призвести до значних фінансових витрат на відновлення системи після атаки, компенсації збитків та штрафів від регуляторних органів. Тому розробка та реалізація підсистеми захисту стає необхідністю для забезпечення стабільної та безпечної діяльності організації.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

Метою кваліфікаційної роботи є розробка та реалізація комплексного проекту, спрямованого на забезпечення надійності, безпеки та стійкості гетерогенної мережевої інфраструктури організації. Головною метою є створення ефективної системи захисту, яка забезпечує конфіденційність, цілісність та доступність даних, а також запобігає можливим загрозам, атакам та невідповідностям у мережевому середовищі.

Конкретні завдання для досягнення цієї мети включають:

- Аналіз сучасних загроз та ризиків кібербезпеки, які можуть вплинути на гетерогенну мережу організації.
- Розробка топології та схеми адресації мережі, враховуючи специфіку організації та її потреби.
- Вибір та налаштування відповідного мережевого обладнання, яке відповідає вимогам безпеки та ефективності.
- Розробка плану захисту, який включає в себе заходи з аутентифікації, авторизації, шифрування, моніторингу та реагування на події.
- Налаштування протоколів маршрутизації та мережевих сервісів з урахуванням вимог безпеки та надійності.
- Проведення тестування та аудиту безпеки для перевірки ефективності заходів захисту та виявлення можливих вразливостей.

Об'єктом дослідження є захист гетерогенних мереж, зокрема, розробка та впровадження підсистеми захисту гетерогенної мережі організації.

Предметом дослідження є проект гетерогенної мережі організації.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ТА АСПЕКТИ СТВОРЕННЯ ПІДСИСТЕМИ ЗАХИСТУ ГЕТЕРОГЕННИХ МЕРЕЖ

1.1 Огляд гетерогенних мереж та їх особливостей

1.1.1 Означення та характеристика гетерогенних мереж

У середовищі сучасних телекомунікацій, що швидко розвивається, поширення різноманітних технологій і зростаючий попит на безперебійне підключення призвели до появи гетерогенних мереж (HetNets). HetNets представляють зміну парадигми в дизайні мережі, охоплюючи різноманітні мережеві елементи та технології, які співіснують, щоб забезпечити розширене покриття, пропускну здатність і якість обслуговування.

У комп'ютерних мережах гетерогенна мережа – це мережа, що з'єднує комп'ютери та інші пристрої, де операційні системи та протоколи мають суттєві відмінності. Наприклад, локальні мережі (LAN), які з'єднують персональні комп'ютери на базі Microsoft Windows і Linux з комп'ютерами Apple Macintosh, є гетерогенними. На рисунку 1.1 наведено приклад схеми гетерогенної мережі[1].

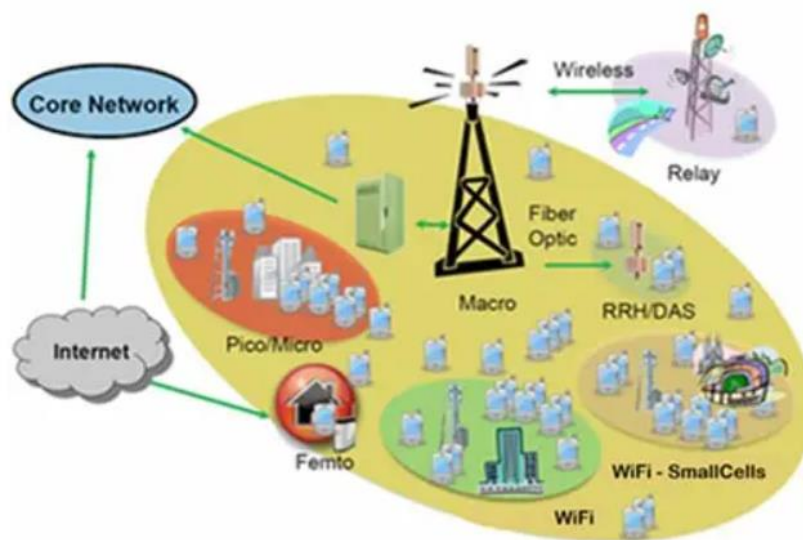


Рисунок 1.1 – Приклад схеми гетерогенної мережі

Гетерогенна мережа також описує бездротові мережі, що використовують різні технології доступу. Наприклад, бездротова мережа, яка надає послуги через бездротову локальну мережу та здатна підтримувати службу під час

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

перемикання на стільникову мережу, називається бездротовою гетерогенною мережею.

Посилання на HetNet нерідко вказує на застосування різних видів вузлів доступу в бездротових мережах. Ця глобальна мережа може складатися з різних комбінацій макростанцій, пікостанцій та фемтостанцій, щоб забезпечити безперервне бездротове покриття у різноманітних середовищах – від відкритих зовнішніх зон до офісних приміщень, житлових будівель та підземних просторів. Спеціалісти у галузі мобільних зв'язків визначають концепцію HetNet як мережу, що складається з різноманітних елементів – макростанцій, малих комірок та, в деяких випадках, WiFi-точок доступу, які взаємодіють для створення покриття, подібного мозаїці, і забезпечують плавний перехід між різними типами вузлів доступу [2].

Ця відмінність в підходах до побудови мережі забезпечує ефективність та високу якість обслуговування для різних сценаріїв використання. Наприклад, макростанції забезпечують широке охоплення та велику пропускну здатність для відкритих площ, тоді як пікостанції та фемтостанції забезпечують високу якість зв'язку в зонах високої щільності, таких як офіси та житлові приміщення. WiFi-точки доступу можуть бути використані для забезпечення додаткового бездротового покриття в місцях зі значним потоком користувачів, таких як громадські приміщення та торгові центри.

Важливою характеристикою HetNet є складна взаємодія між різними типами вузлів доступу. Це вимагає розробки та застосування нових алгоритмів управління ресурсами, які дозволяють ефективно розподіляти пропускну здатність, уникати перевантажень, та оптимізувати якість обслуговування для кожного користувача. Крім того, реалізація здатності плавного переходу між різними мережевими елементами грає ключову роль у забезпеченні безперервного зв'язку при русі користувача в межах мережі HetNet.

Гетерогенні мережі представляють трансформаційний зсув у мережевій архітектурі, що охоплює різноманітність сучасних комунікаційних технологій для створення інтегрованої та ефективної комунікаційної екосистеми. Завдяки

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

стратегічному розгортанню різних типів стільників, безперебійним механізмам передачі та вдосконаленим методам керування перешкодами, HetNets пропонують покращене покриття, ємність і якість обслуговування. Оскільки технологія продовжує розвиватися, характеристики та можливості HetNets відіграватимуть ключову роль у формуванні майбутнього бездротового зв'язку, лежачи в основі нашого пов'язаного світу [3].

1.1.2 Особливості проектування гетерогенних мереж

У сучасному динамічному та взаємопов'язаному світі попит на безперебійний та високоякісний бездротовий зв'язок ще ніколи не був таким високим. Гетерогенні мережі (HetNets) стали революційним рішенням для задоволення цих вимог шляхом інтеграції різних типів мережевих елементів і технологій. Розробка HetNets передбачає ретельний і стратегічний підхід до оптимізації покриття, пропускної здатності та загальної продуктивності мережі.

- Інтеграція різноманітних технологій:

Відмінною рисою HetNets є бездоганна інтеграція різноманітних бездротових технологій, таких як стільникові мережі, Wi-Fi і навіть нових технологій, таких як зв'язок міліметрових хвиль. Завдання при розробці HetNets полягає в тому, щоб забезпечити ефективну взаємодію та співіснування цих технологій, що забезпечує плавну передачу й оптимальний розподіл ресурсів.

- Розгортання малих клітинок:

Однією з ключових особливостей HetNets є розгортання малих осередків, включаючи мікростільники, пікосоти та фемтосоти. Ці менші типи осередків збільшують пропускну здатність мережі в зонах з високою щільністю та всередині приміщень, пом'якшуючи проблеми, пов'язані з концентрацією користувачів і потребою в даних. Ефективне розгортання малих стільникових мереж вимагає ретельного вибору місця з урахуванням таких факторів, як щільність користувачів, будівельні конструкції та шаблони перешкод.

- Управління перешкодами:

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

Співіснування кількох типів осередків у HetNets може призвести до перешкод, потенційно погіршуючи загальну продуктивність мережі. Розробка ефективних стратегій управління перешкодами має вирішальне значення для оптимізації спектральної ефективності та мінімізації погіршення сигналу. Такі методи, як координована багатоточкова передача та прийом (CoMP), формування променя та динамічний розподіл спектру, відіграють важливу роль у зменшенні перешкод.

- Підключення до мережі:

Ефективне транспортне підключення є критично важливим компонентом дизайну HetNet. Зокрема, невеликі комірки покладаються на надійні транзитні з'єднання для передачі даних до базової мережі. Вибір технологій транспортного зв'язку, таких як волоконна оптика, мікрохвильові канали зв'язку та рішення міліметрового діапазону, впливає на надійність мережі, затримку та пропускну здатність.

- Самоорганізуючі мережі (SON):

Складність HetNets вимагає інтелектуального й автоматизованого керування мережею. Функції самоорганізації мережі (SON), включаючи самоналаштування, самооптимізацію та самовідновлення, оптимізують роботу мережі та зменшують ручне втручання. Алгоритми SON безперервно контролюють стан мережі, коригують параметри та оптимізують розподіл ресурсів у режимі реального часу.

- Архітектура HetNet:

Розробка архітектури HetNets передбачає створення мережевої структури, яка бездоганно інтегрує різні типи клітинок і технології. Централізовані та розподілені архітектури пропонують різні переваги та виклики. Централізована архітектура забезпечує легшу координацію та управління, тоді як розподілена архітектура підвищує ефективність і стійкість мережі.

- Динамічний розподіл ресурсів:

HetNets вимагають механізмів динамічного розподілу ресурсів для ефективного розподілу потужності та покриття на основі попиту. Методи

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

когнітивного радіо дозволяють інтелектуально використовувати спектр, дозволяючи клітинам адаптивно регулювати свої робочі частоти та рівні потужності для оптимізації продуктивності.

- Надання якості обслуговування (QoS):

Забезпечення узгодженого QoS є першочерговим питанням у проектуванні HetNet. Різні типи стільників задовольняють різноманітні вимоги користувачів, а ефективне надання QoS передбачає встановлення пріоритетів критичних програм, керування передачами та оптимізацію балансування навантаження для підтримки безперебійної взаємодії з користувачем.

- Інструменти планування HetNet:

Проектування HetNets спирається на розширені інструменти планування та моделювання. Програмне забезпечення для планування радіозв'язку дозволяє інженерам моделювати різні конфігурації стільників, оцінювати зону покриття, аналізувати схеми перешкод і оптимізувати розподіл ресурсів перед розгортанням [5].

Проектування гетерогенних мереж є складним і багатовимірним процесом, який вимагає глибокого розуміння бездротових технологій, архітектури мережі, управління перешкодами та поведінки користувачів. Інтеграція різних типів осередків і технологій, а також ефективне пом'якшення перешкод, зворотне підключення та динамічний розподіл ресурсів формують основу ефективного дизайну HetNet. Оскільки попит на повсюдний і високоякісний бездротовий зв'язок продовжує зростати, еволюція та вдосконалення дизайну HetNet відіграватимуть ключову роль у формуванні майбутнього підключення, створюючи світ, де безперебійний зв'язок процвітає в різних середовищах і сценаріях [4].

1.1.3 Вплив гетерогенних мереж на суспільство та бізнес

Гетерогенні мережі (HetNets) стали трансформаційною силою у сфері комунікацій, революціонізувавши спосіб підключення суспільства, взаємодії та ведення бізнесу. Інтеграція різних бездротових технологій, типів клітинок і

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

мережевих елементів у HetNets започаткувала нову еру зв'язків, відкриваючи перед суспільством і бізнесом безліч можливостей і викликів. Це дослідження заглиблюється в глибокий вплив гетерогенних мереж на суспільство та бізнес, висвітлюючи трансформаційні зміни та наслідки в різних сферах.

- **Покращене підключення та доступ:**

Гетерогенні мережі змінили спосіб спілкування та доступу суспільства до інформації. Повна інтеграція макростільників, мікростільників, пікосот, фемтосот і точок доступу Wi-Fi забезпечує повсюдне покриття, дозволяючи людям залишатися на зв'язку незалежно від їх місцезнаходження. Сільські та віддалені райони, де раніше не було надійного зв'язку, тепер мають доступ до основних послуг, освіти та економічних можливостей, подолаючи цифровий розрив і сприяючи соціальній інтеграції.

- **Розширення можливостей Інтернету речей (IoT):**

Гетерогенні мережі є революцією Інтернету речей (IoT). Можливість підключати широкий спектр пристроїв і датчиків у різних секторах, від розумних будинків до промислової автоматизації, змінила спосіб взаємодії суспільства з технологіями. Пристрої з підтримкою Інтернету речей у HetNets підвищують ефективність, оптимізують процеси та надають дані в режимі реального часу, які сприяють прийняттю обґрунтованих рішень, зрештою покращуючи якість життя та стимулюючи бізнес-інновації.

- **Революціонізація бізнес-операцій:**

Підприємства різних галузей використовують потужність гетерогенних мереж для стимулювання інновацій та ефективності роботи. Роздрібні торговці використовують послуги HetNets на основі визначення місця розташування, щоб запропонувати персоналізований досвід покупок, а логістичні компанії оптимізують управління ланцюгом поставок за допомогою відстеження в реальному часі та аналізу даних. HetNets забезпечують безперебійний зв'язок між пристроями та персоналом, забезпечуючи гнучке прийняття рішень і підвищуючи конкурентоспроможність.

- **Увімкнення розумних міст:**

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

Інтеграція гетерогенних мереж є ключовим фактором розумних міст. Ці мережі є основою для безлічі взаємопов'язаних послуг, включаючи інтелектуальний транспорт, управління енергією, утилізацію відходів і громадську безпеку. Ефективно збираючи та аналізуючи дані з датчиків і пристроїв, HetNets сприяють розвитку міст, покращують розподіл ресурсів і покращують якість життя міських жителів.

- Трансформація охорони здоров'я:

HetNets відіграють значну роль у розвитку послуг охорони здоров'я. Дистанційне спостереження за пацієнтами, телемедицина та переносні пристрої для здоров'я покладаються на безперебійне підключення для безпечної передачі життєво важливих даних пацієнта. HetNets забезпечують спілкування в режимі реального часу між медичними працівниками та пацієнтами, забезпечуючи своєчасне втручання та покращуючи результати лікування пацієнтів.

- Проблеми та міркування:

Хоча вплив гетерогенних мереж, безсумнівно, позитивний, виникають проблеми та міркування. Питання безпеки та конфіденційності стають все більш складними з поширенням підключених пристроїв і обміну даними. Забезпечення надійних заходів кібербезпеки та збереження конфіденційності користувачів є обов'язковими для запобігання можливим порушенням. Крім того, потенціал для перевантаження мережі та дефіциту спектру вимагає постійної оптимізації та управління мережею.

- Економічне зростання та інновації:

HetNets стимулюють економічне зростання, заохочуючи інновації та створюючи нові можливості для бізнесу. Інтеграція різних технологій заохочує дослідження та розробки, що призводить до появи нових програм і послуг. Підприємці та стартапи можуть використовувати HetNets, щоб підірвати традиційні індустрії та запровадити трансформаційні рішення.

Гетерогенні мережі розв'язали хвилю трансформації, яка охоплює як суспільство, так і бізнес. Ці мережі переосмислили зв'язок, розширили можливості Інтернету речей, зробили революцію в бізнес-операціях, створили

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

розумні міста та трансформували послуги охорони здоров'я. Використовуючи величезний потенціал HetNets, суспільство та підприємства також повинні вирішити пов'язані з цим проблеми, забезпечивши безпеку, конфіденційність та ефективне керування мережею. Оскільки світ стає все більш взаємопов'язаним, вплив різномірних мереж продовжуватиме формувати спосіб нашого життя, роботи та взаємодії, відкриваючи нову еру зв'язку та інновацій [7].

1.2 Визначення вимог до підсистеми захисту

У сучасних організаціях, де операційна діяльність сильно залежить від інформаційних технологій та зв'язку, підсистема захисту мережі виявляється невід'ємною і надзвичайно критичною складовою. Вона виконує роль не лише технічного елемента, а й ключового фактору, що визначає успішність функціонування організації на цифровому ринку.

Підсистема захисту мережі прямо впливає на безпеку, конфіденційність та стійкість інформаційних ресурсів. Забезпечення цих аспектів важливе не лише для внутрішньої безпеки організації, але й для збереження довіри клієнтів, партнерів та інших зацікавлених сторін. Лише наявність потужної та добре налаштованої системи захисту може гарантувати захист від кіберзагроз, а також вчасну реакцію на можливі атаки.

Підсистема захисту мережі є не тільки технічним засобом, але і стратегічним інструментом, що впливає на різні аспекти діяльності організації. На її належне функціонування впливають організаційні процеси, зв'язки з клієнтами, партнерами та репутація компанії. Будь-яка недолік чи порушення в роботі підсистеми захисту може призвести до серйозних наслідків, включаючи виток конфіденційних даних, зупинку операцій чи збитки від втрати клієнтів [12].

З огляду на ріст кількості та складності кіберзагроз, підсистема захисту мережі стає важливішою ніж будь-коли. Вона вимагає постійного вдосконалення, моніторингу та адаптації до нових загроз. Організації повинні інвестувати у розробку та удосконалення цієї підсистеми, оскільки це вирішальний фактор для збереження конкурентоспроможності та довіри на ринку.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Важливість підсистеми захисту мережі проявляється у виконанні ряду важливих функцій, що демонструють її значення в сучасному інформаційному ландшафті. Розглянемо докладніше деякі з цих ключових ролей, які свідчать про необхідність належної організації та налагодження підсистеми захисту мережі:

1. Оцінка загроз та ризиків:

Перший етап формування вимог до підсистеми захисту мережі передбачає проведення глибокого аналізу потенційних небезпек, які можуть вплинути на безпеку гетерогенної мережі організації. Цей процес включає оцінку можливих атак та спроб несанкціонованого доступу до мережевих ресурсів, з урахуванням особливостей використовуваних технологій та компонентів підсистеми захисту. Більш того, аналізується потенційний вплив цих загроз на нормальне функціонування організації та нормалізовані бізнес-процеси.

Під час оцінки ризиків, спеціалісти з інформаційної безпеки ретельно вивчають можливі сценарії загроз та вимірюють ймовірність їхнього виникнення. Значимість кожної з цих загроз обговорюється в контексті можливого впливу на конфіденційність, цілісність та доступність даних, а також на репутацію та операційну діяльність організації.

2. Аутентифікація та авторизація:

Щодо аутентифікації та авторизації, підсистема захисту повинна бездоганно впроваджувати процеси перевірки облікових записів та надання прав доступу для користувачів і пристроїв, що отримують можливість підключення до мережі. Вимоги до аутентифікаційних методів ретельно формулюються з урахуванням забезпечення максимальної безпеки та зручності для кінцевого користувача.

Завдяки ефективній аутентифікації, система впевнено перевіряє правомірність доступу та ідентичності користувачів, підтримуючи найвищі стандарти безпеки. Крім того, розглядається впровадження різних аутентифікаційних факторів, таких як біометричні дані, одноразові паролі та апаратні токени, що забезпечують багаторівневий захист та підвищують надійність системи.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

У контексті авторизації, детально визначаються рівні доступу та дозволи для різних категорій користувачів та пристроїв. Це дозволяє точно контролювати, які ресурси та функціональні можливості доступні для кожної групи користувачів, забезпечуючи збалансований підхід між зручністю та безпекою. Крім того, встановлені механізми перевірки авторизації допомагають відстежувати та контролювати дії користувачів та пристроїв всередині мережі, запобігаючи можливим порушенням та недопустимому використанню ресурсів.

3. Захист даних за допомогою криптографії:

Установлення вимог до криптографічного захисту даних визначається з основною метою забезпечення високого рівня конфіденційності під час передачі та збереження інформації. Цей етап включає визначення відповідних методів шифрування, ключів та протоколів, що не лише забезпечують надійний захист, але й відповідають сучасним стандартам та вимогам кібербезпеки.

Криптографічний захист є ключовою складовою забезпечення безпеки даних, особливо в умовах зростаючої кількості кіберзагроз. Вимоги до цього заходу безпеки враховують потенційні сценарії атак та можливі загрози, які можуть виникнути при обробці, передачі та збереженні інформації. Важливо визначити оптимальні методи шифрування, вибрати надійні криптографічні алгоритми та забезпечити безпеку ключів для максимального захисту конфіденційності та цілісності даних.

4. Моніторинг та виявлення аномалій:

Однією з важливих вимог до системи моніторингу та виявлення аномалій є забезпечення безперервного нагляду за станом безпеки мережі. Це включає вчасне реагування на незвичайну активність, яка може свідчити про можливі загрози або атаки. Відповідний механізм моніторингу допомагає оперативно виявляти аномалії в мережевому трафіку, аналізувати їх і впроваджувати необхідні заходи.

Система моніторингу може використовувати різноманітні технології та алгоритми для виявлення аномальної активності, такі як машинне навчання та аналіз патернів. Це допомагає виявляти навіть найбільш субтильні зміни в

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

мережевому трафіку, що можуть вказувати на можливі загрози. Важливим аспектом є інтеграція з системами відповіді на інциденти, що дозволяє автоматично реагувати на виявлені аномалії та забезпечувати ефективний захист.

5. Стійкий захист від розподілених атак та інших загроз:

Однією з найбільш вимогливих аспектів безпеки є захист від розподілених атак (DDoS) та інших кіберзагроз, які можуть призвести до великих перебоїв у роботі мережі. Вимоги до цього виду захисту націлені на забезпечення стійкості мережі при великих навантаженнях, що можуть бути викликані зловживанням або масштабними атаками.

Забезпечення стійкого захисту від DDoS та інших атак вимагає використання спеціалізованих технологій та розробку стратегій протидії. Це може включати розгортання антивірусних шлюзів, збільшення мережевої пропускної здатності та використання розподілених ресурсів для розподілення навантаження. Додатково, система захисту може розраховувати на аналіз мережевого трафіку для виявлення підозрілих або несправедливих підключень, що допомагає вчасно реагувати на потенційні загрози.

6. Забезпечення фізичної безпеки:

Крім цифрового захисту, необхідно встановити строгі вимоги до фізичної безпеки обладнання мережі. Серед них можуть бути обмеження доступу, системи відеоспостереження та інші засоби, спрямовані на запобігання будь-якому несанкціонованому фізичному доступу.

Фізична безпека є невід'ємною частиною загальної стратегії кібербезпеки. У сучасних умовах, коли організації використовують різноманітні технології для забезпечення своєї діяльності, важливо гарантувати, що обладнання, сервери та інфраструктура фізично захищені від можливих атак або несанкціонованого доступу.

7. Безпека задач віддаленого управління:

Не менш важливою є безпека задач віддаленого управління та конфігурації мережі. Вимоги до цієї сфери встановлюють необхідні заходи для запобігання

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

будь-якому несанкціонованому доступу до управлінських інтерфейсів та важливих даних.

Сучасний бізнес вимагає гнучкості та можливості віддаленого управління, але разом з цим з'являється ризик можливих кіберзагроз та атак. Це може бути спроба злому системи з метою отримання конфіденційної інформації, або навіть зловживання правами доступу до мережі. Тому необхідно забезпечити, щоб вимоги до безпеки віддаленого управління були відповідним чином реалізовані.

8. Підвищення компетентності та свідомості користувачів:

Встановлення вимог до навчання та свідомості користувачів відіграє важливу роль у забезпеченні того, що всі працівники організації розуміють та дотримуються найкращих практик забезпечення безпеки. Навчання користувачів щодо розпізнавання потенційних загроз, використання складних паролів, а також правил поведінки в мережі може допомогти попередити багато типових атак. Отже, гарантування того, що всі користувачі розуміють, як захищати дані та відмовлятися від підозрілих дій, є ключовим для створення надійного об'єкта для кібербезпеки.

Загалом, визначення вимог до підсистеми захисту є ключовим етапом у забезпеченні безпеки мережі організації. Цей процес допомагає забезпечити високий рівень захисту даних, зберегти репутацію організації та забезпечити безпечне та безперебійне функціонування гетерогенної мережі у сучасному цифровому середовищі [13].

1.3 Огляд сучасних методів та технологій захисту гетерогенних мереж

У нашому сучасному цифровому ландшафті, де інформаційні технології займають домінуюче положення в операціях організацій, забезпечення безпеки гетерогенних мереж стає насущною та вельми важливою задачею. Зростаючі вимоги до надійності, конфіденційності та доступності даних у гетерогенних мережах, де поєднуються різноманітні обладнання, пристрої та технології, перетворюють цю проблему на ключовий пріоритет для багатьох організацій.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

Докладний огляд сучасних методів та технологій захисту гетерогенних мереж розкриває перед нами широкий спектр інноваційних підходів, спрямованих на забезпечення високого рівня кібербезпеки. Ці методи не обмежуються лише розглядом унікальних аспектів гетерогенних мереж, але також пропонують різноманітні рішення для вирішення різних викликів, що виникають у сфері захисту мережевого середовища. Вони базуються на основних принципах кібербезпеки, але враховують властивості гетерогенних мереж, щоб забезпечити оптимальну захищеність.

Застосування цих методів і технологій дозволяє організаціям ефективно реагувати на сучасні виклики в області кібербезпеки. Серед них виявлення та відсіювання аномалій у мережевому трафіку, розробка імунітету до розподілених атак (DDoS), захищені механізми аутентифікації, аналіз потенційних загроз та надання авторизованого доступу до різних ресурсів [7].

Одним із важливих методів забезпечення безпеки є використання Віртуальних Приватних Мереж (VPN). Ця технологія дозволяє створювати зашифровані та захищені канали зв'язку між різними вузлами мережі, забезпечуючи високий рівень конфіденційності даних під час їх передачі. Віртуальні Приватні Мережі особливо цінні в гетерогенних мережах, де можуть співіснувати різні типи технологій та пристроїв. Цей підхід є надзвичайно ефективним для забезпечення безпеки навіть під час обміну даними через відкриті мережі, такі як Інтернет.

Віртуальні Приватні Мережі стають незамінним інструментом для організацій, що прагнуть забезпечити безпеку своїх мереж та зберегти конфіденційність важливих даних. Завдяки застосуванню шифрування та аутентифікації, VPN дозволяють створювати захищені тунелі між вузлами мережі, що знижує ризик несанкціонованого доступу та перехоплення інформації.

У гетерогенних мережах, де може бути використано різні види пристроїв та технологій, важливо забезпечити єдність підходу до захисту. VPN дозволяють

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

об'єднати різномірні елементи мережі під спільним забезпеченим каналом, що забезпечує єдність політик та стандартів безпеки.

Застосування VPN особливо актуально для дистанційної роботи та доступу до ресурсів мережі з різних місць розташування. Він дозволяє забезпечити безпеку під час обміну даними з публічних мереж, які можуть бути вразливими до атак та перехоплення.

Системи Виявлення та Захисту від Вторгнень (IDS/IPS) є невід'ємною та надзвичайно значущою складовою сучасних методів забезпечення кібербезпеки. Ці системи виконують функцію моніторингу мережевого трафіку з метою виявлення будь-якої незвичайної або підозрілої активності, що може свідчити про можливі атаки або вторгнення в мережу. Важливість та актуальність цих IDS/IPS систем ростуть особливо в гетерогенних мережах, де велика кількість різномірних компонентів та технологій може створити додаткові точки вразливості та підвищити загрози безпеці.

Ці системи виявлення та захисту від вторгнень грають критичну роль у забезпеченні безпеки мережевого середовища. Вони не лише реагують на вже відомі шаблони атак, але й вміють реагувати на нові, поки ще невідомі загрози, використовуючи аналіз аномалій та незвичайних змін у поведінці мережі. Виявивши потенційну загрозу, ці системи можуть приймати заходи для відповідного реагування, відокремлення атакуючих елементів від мережевого середовища та запобігання подальшому розповсюдженню атаки.

У гетерогенних мережах, де різні типи обладнання, оперативних систем та пристроїв працюють разом, існує підвищена складність в управлінні безпекою. Системи IDS/IPS виступають в ролі сторожа, який постійно моніторить мережевий трафік на наявність будь-яких потенційних загроз. Завдяки їх функціоналу, можливо вчасно реагувати на загрози та атаки, забезпечуючи високий рівень безпеки в гетерогенному середовищі.

В подальшому розвитку методів забезпечення безпеки в гетерогенних мережах, системи Виявлення та Захисту від Вторгнень будуть грати все більш важливу роль. З використанням штучного інтелекту, машинного навчання та

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

аналізу великих обсягів даних, ці системи можуть стати ще більш ефективними у виявленні та запобіганні кіберзагрозам.

Системи Управління Доступом (ІАМ) відіграють роллю невід'ємної важливості у забезпеченні конфіденційності та доступності інформації. В сучасному цифровому світі, де обмін даними є невід'ємною частиною ділової та особистої взаємодії, забезпечення адекватного керування аутентифікацією та авторизацією користувачів та пристроїв є життєво важливою задачею.

Сучасні гетерогенні мережі включають різноманітні обладнання, різні рівні доступу та масштабну інфраструктуру. Ця різноманітність створює значну складність у керуванні доступом та забезпеченні безпеки. Системи ІАМ надають засоби для централізованого керування правами доступу, що допомагає підтримувати впорядкованість у такому різноманітному середовищі. Вони дозволяють організаціям визначити, хто, коли і до якої інформації має доступ, а також які дії вони можуть виконувати.

Загрози для безпеки найчастіше виникають з недостатнього контролю доступу та недбалого керування правами користувачів. Системи ІАМ забезпечують ефективну стратегію для попередження таких вразливостей. Вони дозволяють організаціям встановлювати стандарти та політики, які регулюють, які користувачі мають доступ до яких ресурсів та які дії вони можуть виконувати. Це робить можливим управління ризиками та забезпечення відповідності з внутрішніми та зовнішніми стандартами безпеки.

У гетерогенних мережах, де різноманітність є ключовою особливістю, системи ІАМ стають незамінним інструментом для управління доступом. Вони допомагають зменшити ризики, пов'язані з несанкціонованим доступом, зловживанням правами чи витоком конфіденційної інформації. Це особливо важливо в контексті зростаючих кіберзагроз та необхідності забезпечення довіри від клієнтів та партнерів.

У майбутньому, розширення можливостей систем ІАМ може включати інтеграцію з іншими сучасними технологіями, такими як штучний інтелект та

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

аналітика даних. Це може сприяти автоматизації процесів реагування на загрози, розпізнаванню аномальної поведінки та попередженню інцидентів безпеки.

У сучасному контексті забезпечення кібербезпеки, методи багатофакторної ідентифікації та аутентифікації набувають важливості через зростаючі загрози та необхідність забезпечити надійний рівень захисту. Ця підхід до ідентифікації включає в себе використання не лише традиційних методів, таких як паролі, а й біометричних даних, апаратних токенів та інших факторів, що підвищує рівень безпеки та надійності доступу до ресурсів.

У гетерогенних мережах, де різноманітність обладнання та пристроїв є нормою, застосування багатофакторної ідентифікації стає особливо актуальним. Це дозволяє організаціям встановлювати високий рівень перевірки особи, яка намагається отримати доступ до системи. Поєднання декількох факторів, таких як щось, що користувач знає (пароль), щось, що користувач має (апаратний токен) та щось, що користувач є (біометричні дані), робить процес аутентифікації більш складним для несанкціонованого доступу.

Паролі, хоча і є популярним методом ідентифікації, мають свої обмеження, такі як можливість підбору, витоку чи викрадення. Використання додаткових факторів, які важко відтворити або підмінити, додає шар додаткової безпеки. Біометричні дані, такі як відбитки пальців, розпізнавання обличчя чи сканування сітківки ока, важко підробити, і тому вони стають ефективним засобом підтвердження особи.

Крім того, застосування багатофакторної ідентифікації робить атаки, які використовують один фактор, менш ефективними. Навіть якщо зловмиснику вдалося отримати пароль, він все ще повинен зіткнутися з іншими факторами, що ускладнює процес несанкціонованого доступу.

Залежно від конкретних потреб та характеристик організації, можуть бути вибрані різні комбінації факторів для багатофакторної ідентифікації. Це дозволяє підібрати оптимальний підхід, який враховує ризики та зручність для користувачів.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Для забезпечення конфіденційності інформації в гетерогенних мережах використовуються різноманітні методи шифрування даних. Ці методи дозволяють захистити дані від несанкціонованого доступу та перехоплення. Шифрування може бути застосовано на рівні самої інформації або на рівні комунікаційних каналів, що забезпечує подвійний шар захисту та гарантує безпеку навіть у випадку можливого перехоплення даних.

Безпека гетерогенних мереж також залежить від використання методу сегментації мережі. Цей підхід полягає у розділенні великої та різноманітної мережі на менші сегменти чи підмережі. Кожен сегмент може бути незалежним, що зменшує можливість поширення атак і збільшує утриманість їх від докладних систем та цінних даних.

Сегментація мережі є ефективним методом захисту, оскільки навіть якщо один сегмент мережі стає жертвою атаки, інші сегменти залишаються відокремленими та забезпечують захист інших частин мережі. Крім того, цей метод сприяє кращому управлінню ризиками та ізоляції потенційних загроз.

Таким чином, використання методів шифрування даних та сегментації мережі в гетерогенних середовищах покращує загальний рівень безпеки, забезпечуючи конфіденційність та недоступність для несанкціонованого доступу до важливої інформації.

Надзвичайно важливим аспектом є відновлення після інцидентів та резервне копіювання, які визначають стабільність та надійність функціонування гетерогенних мереж. Створення та реалізація докладних планів відновлення в даних мережах забезпечує можливість швидко та ефективно реагувати на можливі інциденти та відновлювати операційну працездатність.

Планування відновлення після інцидентів є критично важливим етапом, який передбачає вивчення потенційних загроз та визначення оптимальних кроків для негайного відновлення систем та мережевих ресурсів. Такі плани включають не тільки технічні аспекти, але й організаційні процедури, роль та

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

відповідальність співробітників під час відновлення, а також координацію з зовнішніми сторонами, якщо це необхідно.

Резервне копіювання є невід'ємною частиною планування відновлення, яке гарантує наявність останніх копій важливих даних та налаштувань систем. Це забезпечує можливість швидкого відновлення інформації в разі виникнення інциденту або атаки, запобігаючи втраті даних та зберігаючи цінну інформацію для організації.

У сучасних умовах, коли загрози кібербезпеки стають все більш складними та розповсюдженими, важливість резервного копіювання та планів відновлення стає критично важливою. Ці заходи забезпечують відновлення після інцидентів не тільки в термінах технічних можливостей, але й в плані забезпечення неперервності діяльності організації, збереження довіри клієнтів та репутації компанії [6].

IP-адреси є зручними для ідентифікації комп'ютерів в мережі Інтернет, але вони не найзручніші для користувачів у плані використання (менш наочні, складно запам'ятовуються та можуть спричиняти помилки при введенні). Тому для полегшення доступу користувачів до ресурсів використовується літерна система доменних імен DNS (Domain Name System - система доменних імен). В рамках цієї системи, імена Web-серверів виражаються послідовностями слів, розділених крапками, що робить їх більш запам'ятовуваними та зручними для користувачів [8].

Доменне ім'я однозначно визначає сервер в Інтернеті й складається за ієрархічним принципом:

- На найвищому рівні (домен верхнього рівня) зазвичай розташовується назва країни, наприклад, uk (Велика Британія), us (Сполучені Штати Америки) або ua (Україна).
- Також замість назви країни може використовуватися скорочення, відповідне типу організації, якій належить домен: com (комерційний домен), gov (урядовий), mil (військовий), edu (освітній), net (мережний), org (інших організацій).

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

- Ліворуч від домену верхнього рівня через крапку дописується позначення міста, штату або організації. Однак цієї частини імені може не бути.
- Ліворуч від позначення міста (організації) - позначення серверу, яке займає відповідно крайню ліву позицію у доменному імені.

У результаті доменне ім'я серверу (простіше, домен) може мати такий вигляд:

- autoland.com.ua - комерційний сервер, присвячений автомобілям, країна ua (Україна);
- kyivstar.net - сервер оператора мобільного зв'язку, домен верхнього рівня net.

Відповідність між IP-адресами та доменними іменами встановлюється за допомогою баз даних, розташованих на спеціальних серверах DNS (Domain Name System). Сервери DNS виконують щоденну рутинну роботу, яка є необхідною для правильної роботи системи доменних імен.

DNS-сервер є програмою, яка відповідає на запити DNS згідно відповідного протоколу. Крім цього, термін "DNS-сервер" може використовуватися для позначення хоста, на якому запущена відповідна програма. Нижче на рисунку 1.2 наведено схему взаємодії між сервером та клієнтом.

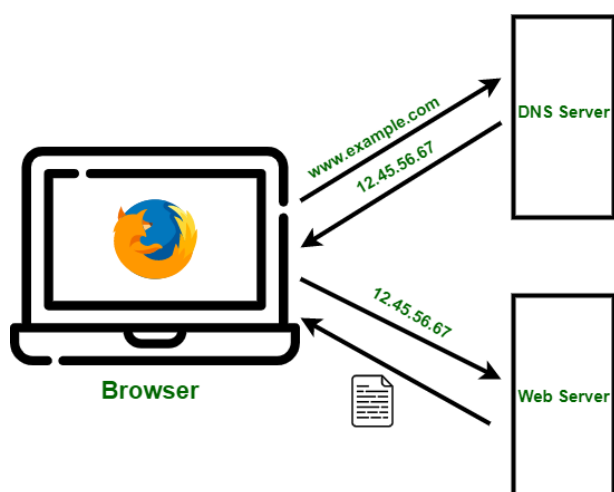


Рисунок 1.2 – Схема взаємодії веб-застосунку клієнта та DNS серверу

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

За виконуваними функціями DNS-сервери поділяються на декілька груп. Залежно від конфігурації, конкретний сервер може відноситися до декількох типів:

1. Авторитетний DNS-сервер — сервер, що відповідає за свою зону.

- Головний або первинний сервер (в термінології BIND) — сервер, що має право на внесення змін в окремі зони. Зазвичай для зони буває тільки один головний сервер. У випадку Microsoft DNS-сервера і його інтеграції з Active Directory, головних серверів може бути декілька (так як реплікація змін здійснюється не засобами DNS-сервера, а засобами Active Directory, за рахунок чого забезпечується рівноправність серверів і актуальність даних);

- Підлеглий або вторинний сервер, що не має права на внесення змін в дані зони і отримує повідомлення про зміни від головного сервера. На відміну від головного сервера їх може бути (практично) необмежена кількість. Підлеглий так само є авторитетним сервером (і користувач не може розрізнити головний і підлеглий сервери, різниця з'являється тільки на етапі конфігурування/внесення змін до налаштувань зони);

2. Кеш-сервер DNS — сервер, який обслуговує запити клієнтів, (отримує рекурсивний запит, виконує його за допомогою нерекурсивних запитів до авторитетних серверів, або передає рекурсивний запит DNS-серверу, що стоїть вище в ієрархії);

3. Локальний DNS-сервер; використовується для обслуговування DNS-клієнтів, які працюють на локальній машині. Фактично, це різновид кешувального DNS-сервера, сконфігурованого для обслуговування локальних додатків;

4. Перенаправний DNS-сервер (англ. forwarder внутрішній DNS-сервер); сервер, що перенаправляє отримані рекурсивні запити кеш-серверу, що стоїть вище в ієрархії, у вигляді рекурсивних запитів. Використовується переважно для зниження навантаження на сервер кешу DNS;

5. Кореневий DNS-сервер — сервер, який є авторитетним у кореневій зоні. Загальноновживаних корневих серверів у світі всього 13, їх доменні імена

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

знаходяться в зоні root-servers.net і називаються a.root-servers.net, b.root-servers.net, ..., m.root-servers.net. У певних конфігураціях локальної мережі можлива ситуація налаштування локальних кореневих серверів;

6. Реєстраційний DNS-сервер. Сервер, що приймає динамічні оновлення від користувачів. Часто поєднується з DHCP-сервером. У Microsoft DNS-сервер при роботі на контролері домену сервер працює в режимі реєстраційного DNS-сервера, приймаючи від комп'ютерів домену інформацію про відповідність імені та IP комп'ютера і оновлюючи відповідно дані зони домену;

7. DNSBL-сервер (сервер з чорними списками адрес та імен). Формально, такий сервер не входить в ієрархію DNS, однак використовує той же механізм і протокол для роботи, що і DNS-сервери.

Записи, які пов'язані з певним доменом, отримали назву "зони DNS". Це окремі сегменти в просторі імен домену, за які зазвичай відповідає юридична особа - організація або компанія. Вони несуть відповідальність за підтримку регіональних зв'язків у веб-просторі. Зона DNS представляє собою адміністративну функцію, яка дозволяє детально контролювати різні компоненти DNS, такі як авторитетні сервери імен [9].

Коли веб-браузер або інший мережевий пристрій потребує знайти IP-адресу для імені хоста, наприклад, "example.com", він здійснює пошук DNS, що по суті є перевіркою відповідної зони DNS. Для цього він звертається до сервера DNS, який керує зоною, вказаною у запиті для даного імені хоста. Цей сервер відомий як офіційний сервер імен для домену. Далі, офіційний сервер імен виконує запит DNS, надаючи IP-адресу або інші відомості щодо запитаного імені хоста.

Основні сервери розбивають зону на різні сегменти. Вони визначають домени верхнього рівня, такі як ".org" або ".com", домени другого рівня, наприклад, "ukraine.com.ua", і домени третього рівня, відомі також як піддомени, наприклад, "support.ukraine.com.ua". Кожен з цих рівнів може становити окрему зону DNS.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

Наприклад, кореневий домен "ukraine.com.ua" делегується компанією "Хостинг Україна". Вона приймає на себе відповідальність за налаштування основного DNS-сервера, який містить вірні записи DNS для цього домену.

Висновки до першого розділу

В даному розділі було проведено аналіз теоретичних основ та ключових аспектів створення підсистеми захисту гетерогенних мереж. Результати цього дослідження відображають важливість забезпечення безпеки і надійності мережевого середовища для сучасних організацій.

У першому підрозділі розділу проведено огляд гетерогенних мереж та їх особливостей. Виявлено, що гетерогенні мережі є складними утвореннями, які об'єднують різноманітне обладнання, пристрої та технології. Це створює специфічні виклики для забезпечення їх безпеки та надійності.

Далі, у другому підрозділі, було визначено вимоги до підсистеми захисту гетерогенних мереж. З'ясовано, що ці вимоги визначають технічні та організаційні параметри підсистеми захисту, які сприятимуть забезпеченню надійної, стійкої та безпечної роботи мережі.

Третій підрозділ описує огляд сучасних методів та технологій захисту гетерогенних мереж. Виявлено, що для забезпечення безпеки в таких мережах використовуються різноманітні підходи та інноваційні технології. Вони включають в себе використання Віртуальних Приватних Мереж (VPN), систем Виявлення та Захисту від Вторгнень (IDS/IPS), Систем Управління Доступом (IAM) та інші. Кожен з цих методів має свої особливості та переваги, які допомагають ефективно забезпечувати безпеку мережі.

У цілому, цей розділ надає глибокий уявлення про те, як важливою та складною є задача забезпечення безпеки гетерогенних мереж. На основі аналізу різних аспектів і методів захисту можна зробити висновок, що розробка ефективної підсистеми захисту є важливою складовою для забезпечення безпеки та надійності мережевого середовища організації.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

РОЗДІЛ 2 ПРОЕКТУВАННЯ ГЕТЕРОГЕННОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

2.1 Розробка топології гетерогенної мережі

Створення ефективної топології гетерогенної мережі організації є критичним етапом, спрямованим на забезпечення оптимальної функціональності та безпеки мережевої інфраструктури компанії. При розробці такої топології важливо враховувати унікальні аспекти, пов'язані з гетерогенним характером мережі, яка об'єднує різноманітне обладнання та технології.

Процес розробки топології гетерогенної мережі включає кілька важливих етапів, спрямованих на оптимізацію її функціональності та надійності. Першим кроком є вибір відповідної топологічної структури, який залежить від потреб компанії, розміру та географічного розташування її філіалів. Важливим аспектом є також розгляд масштабованості, маршрутизації та можливості резервування мережі.

Розташування мережних пристроїв, таких як маршрутизатори, комутатори та файрволи, у мережі має бути обдуманим та оптимізованим для забезпечення найкращої шляху передачі даних. Такий підхід допомагає мінімізувати затримки та забезпечити високий рівень доступності. Враховуючи фізичну та логічну структуру мережі, розташування пристроїв обирається з метою забезпечення оптимальної комунікації між різними вузлами мережі.

Ключовим аспектом є проектування з'єднань між мережними пристроями, що визначає ефективність мережі. Важливо обрати відповідний тип з'єднань, враховуючи потреби компанії та можливості мережевого обладнання. Також слід розгортати фізичні та логічні з'єднання для забезпечення безпеки та ефективності мережі.

Одним із важливих аспектів при створенні топології є розробка схеми адресації. Ефективна схема допомагає уникнути конфліктів IP-адрес та забезпечити правильну маршрутизацію пакетів даних.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

Загалом, успішна розробка топології гетерогенної мережі організації є ключовим кроком для створення функціонального, надійного та безпечного мережевого середовища, що відповідає потребам та вимогам компанії.

Для гетерогенних мереж підприємства найбільш вдалою може бути застосування ієрархічної моделі мережі з трьома рівнями.

Ця модель передбачає визначення та організацію трьох основних рівнів:

- Рівень ядра (Core layer)
- Рівень розподілу (Distribution layer)
- Рівень доступу (Access layer)

Кожен з цих рівнів несе на собі певні функціональні завдання, сприяючи ефективній та безпечній роботі мережі. Варто відзначити, що хоча ці рівні визначають ролі та завдання, вони є логічними концепціями, і їх фізична реалізація може бути різною, залежно від потреб та особливостей підприємства.

Такий підхід до організації мережі спирається на логічний розподіл обов'язків між різними рівнями, сприяючи оптимальному функціонуванню системи. Схожий принцип застосовується і в інших моделях, таких як OSI, де логічні рівні також визначаються для розділення функцій.

Важливо зауважити, що фізична реалізація мережі може відрізнятися від логічної ієрархії. Декілька фізичних пристроїв може спільно функціонувати на одному рівні, а один пристрій може виконувати завдання кількох логічних рівнів. Така гнучкість дозволяє вирішувати специфічні вимоги та виклики підприємства.

Таким чином, ієрархічна модель мережі з трьома рівнями надає структурований та ефективний підхід до побудови мережевої інфраструктури, допомагаючи оптимізувати функціонування та забезпечувати безпеку мережі в гетерогенному середовищі підприємства.

Для створення топології гетерогенної мережі організації було використано графічний редактор Draw.io. На рисунку 2.1 наведено загальна топологія мережі, що дозволяє одним поглядом ознайомитися з основною структурою мережі та розташуванням основних компонентів.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

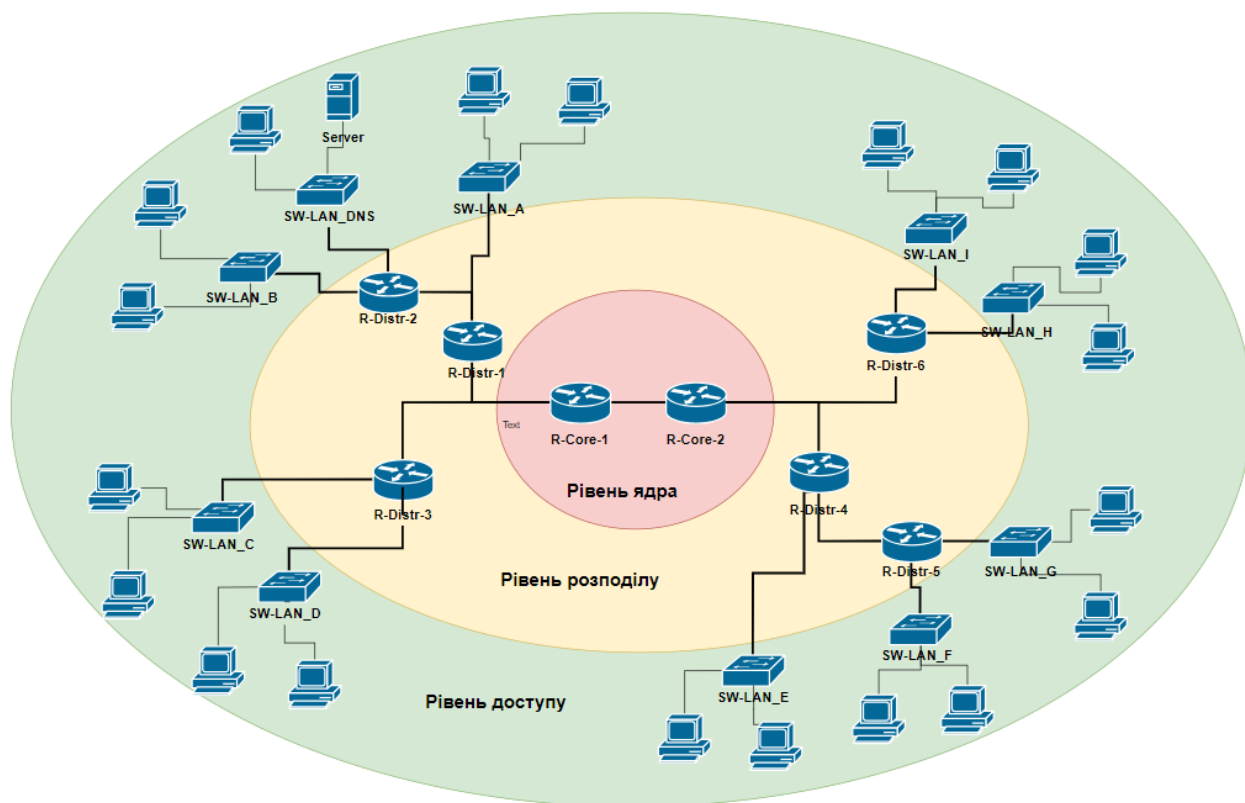


Рисунок 2.1 – Загальна топологія гетерогенної мережі

Існує низка факторів, що підтверджують важливість використання 3-рівневої ієрархічної моделі мережі Cisco:

- Масштабованість: Цей підхід забезпечує гнучке пристосування до майбутнього росту мережі. Шляхи зв'язку на різних рівнях ієрархії дозволяють ефективно розширювати мережу, додавати нові сегменти і забезпечувати оптимальний рівень пропускної здатності.
- Спрощене управління і виправлення неполадок: Модель сприяє ефективному управлінню мережею і спрощує процес виявлення та усунення проблем. Кожен рівень відповідає за конкретні завдання і може мати власні протоколи та політики управління.
- Легкість фільтрації та застосування політик: Це дозволяє зручно створювати та застосовувати фільтри та політики в мережі. Кожен рівень може мати власні правила фільтрації, що полегшує контроль над рухом даних і забезпечує виконання правил безпеки.

- Зайвисть та стійкість до відмов: Ієрархічна архітектура сприяє стійкості та високій надійності мережі. У разі збою або відмови одного пристрою, інші здатні прийняти його функції і забезпечити безперебійну роботу мережі.

- Висока продуктивність: 3-рівнева ієрархія розроблена для підтримки високої пропускної здатності та продуктивності мережі. Кожен рівень відіграє свою роль, сприяючи ефективному розподілу навантаження та забезпечуючи високу швидкодію базової інфраструктури.

- Модульність: 3-рівневий підхід надає гнучкість у проектуванні мережі та спрощує впровадження та виправлення проблем. Кожен рівень може бути незалежним модулем, що дозволяє легко вносити зміни без суттєвого впливу на решту мережі. Такий підхід сприяє адаптації мережі до змін вимог і технологічного розвитку компанії.

Рівень ядра є центральним компонентом мережі, відповідальним за критичні функції передачі даних. Розташований у верхній частині ієрархії, цей рівень має за мету забезпечити швидку та надійну передачу значних обсягів трафіку. Він складається з 2 маршрутизаторів, які сполучені високошвидкісними зв'язками на базі технології Gigabit Ethernet. Саме на цьому рівні реалізується з'єднання з глобальною мережею Інтернет.

Рівень розподілу виконує роль зв'язуючого елемента між рівнем доступу та ядром. Його основною місією є забезпечення маршрутизації, фільтрації та доступу до глобальної мережі, а також визначення, як пакети можуть досягти ядра. Рівень розподілу визначає оптимальний шлях для запитів мережевих служб, наприклад, як запити на файли передаються на сервери, і при необхідності передаються на рівень ядра. Зазвичай, цей рівень містить маршрутизатори та багаторівневі комутатори. У загальній топології рівень розподілу включає 6 маршрутизаторів.

На рівні доступу знаходяться комутатори другого рівня та точки доступу, що забезпечують з'єднання з робочими станціями та серверами. Цей рівень надає можливість контролювати доступ та встановлювати політики, створювати окремі домени та гарантувати безпеку портів на рівні доступу. Комутатори рівня

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

доступу відповідають за передачу пакетів до кінцевих пристроїв, що забезпечує швидку та надійну комунікацію всередині мережі.

В загальному вигляді мережа складається з 8 маршрутизаторів та 10 комутаторів. Також мережа має 10 локальних мереж.

У мережі також існує потенціал для подальшого розширення та масштабування. Важливо враховувати, що у міру зростання потреб і обсягів даних, мережева інфраструктура повинна бути гнучкою та готовою впоратися з новими вимогами. Це може передбачати додавання нових вузлів, розширення фізичної і логічної інфраструктури, а також адаптацію мережевих пристроїв до змінюючихся потреб. Завдяки можливості розширення, мережа зможе ефективно впоратися з ростом бізнесу та забезпечити стабільну та надійну інфраструктуру для підтримки діяльності компанії.

2.2 Розробка схем адресації мережі

Під час стадії розробки мережевої топології, однією з найсуттєвіших етапів є створення схеми адресації. Цей крок виявляється важливим для запобігання можливим дублікатам IP-адрес та забезпечення функціонування мережі в майбутньому. Процес планування адресації має в собі глибокий аналіз та врахування великої кількості чинників, що впливають на ефективне використання IP-адрес.

Під час вирішення завдання адресації, особлива увага надається досягненню оптимальності розподілу IP-адрес. Важливим є уникнення надмірної витрати або недостатку адрес, що може призвести до труднощів у майбутньому масштабуванні. Враховуючи майбутні потреби компанії та її мережевої інфраструктури, планування адресації здійснюється з урахуванням можливих розширень та змін. Такий підхід дозволяє підтримувати гнучкість та ефективність мережі відповідно до зростаючих вимог та внутрішніх процесів компанії.

З метою спрощення організації та розподілу IP-адрес, була підготовлена таблиця 2.1, яка включає розрахунки IP-адрес для пристроїв на рівні ядра та їх

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

взаємодії з пристроями на рівнях розподілу та доступу. Ця таблиця є неоцінним інструментом для точності та структурованості в процесі конфігурації мережевої адресації.

Таблиця 2.1 – Параметри адресації рівнів ядра та розподілу

Пристрій	Мережа
R-Core-1 R-Core-2	192.191.1.0/30
R-Core-1 R-Distr-1	192.191.2.0/30
R-Core-1 R-Distr-3	192.191.3.0/30
R-Distr-1 R-Distr-2	192.191.4.0/30
R-Core-2 R-Distr-4	192.191.5.0/30
R-Core-2 R-Distr-6	192.191.6.0/30
R-Distr-4 R-Distr-5	192.191.7.0/30

Глибокий розгляд та аналіз належать деталізації, яка вимагає проведення розрахунків IP-адрес для локальних мереж. Під час цих розрахунків важливо визначити IP-адрес мережі, використовувані маски, діапазон адрес та інші параметри, що сприяють оптимальному використанню ресурсів доступної мережі.

Для кращого розуміння і наочності розподілу IP-адрес усередині даного проекту, знадобиться докладне ознайомлення з таблицями 2.2 – 2.11. Ця інформація стає не лише важливою вказівкою для налагодження і конфігурації мережі, але й допомагає забезпечити високу пропускну здатність та ефективність функціонування всіх підсистем мережі.

Таблиця 2.2 – Параметри адресації мережі LAN_DNS

Призначення	IP-адреса
Адреса мережі	193.191.1.0
Маска мережі	255.255.255.0
Префікс мережі	24

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Продовження таблиці 2.2 – Параметри адресації мережі LAN_DNS

Призначення	ІР-адреса
Інвертована маска	0.0.0.255
Мінімальна адреса	193.191.1.1
Максимальна адреса	193.191.1.254
Широкомовна маска	193.191.1.255
Шлюз за замовчуванням	193.191.1.1
Діапазон адрес комутаторів	193.191.1.2-193.191.1.10
Діапазон адрес ПК	193.191.1.11-193.191.1.145
Діапазон вільних адрес	193.191.1.146-193.191.1.254

Таблиця 2.3 – Параметри адресації мережі LAN_A

Призначення	ІР-адреса
Адреса мережі	193.191.2.0
Маска мережі	255.255.255.0
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	193.191.2.1
Максимальна адреса	193.191.2.254
Широкомовна маска	193.191.2.255
Шлюз за замовчуванням	193.191.2.1
Діапазон адрес комутаторів	193.191.2.2-193.191.2.10
Діапазон адрес ПК	193.191.2.11-193.191.2.145
Діапазон вільних адрес	193.191.2.146-193.191.2.254

Таблиця 2.4 – Параметри адресації мережі LAN_B

Призначення	ІР-адреса
Адреса мережі	193.191.3.0
Маска мережі	255.255.255.0
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	193.191.3.1
Максимальна адреса	193.191.3.254
Широкомовна маска	193.191.3.255
Шлюз за замовчуванням	193.191.3.1
Діапазон адрес комутаторів	193.191.3.2-193.191.3.10
Діапазон адрес ПК	193.191.3.11-193.191.3.145
Діапазон вільних адрес	193.191.3.146-193.191.3.254

Таблиця 2.5 – Параметри адресації мережі LAN_C

Призначення	ІР-адреса
Адреса мережі	193.191.4.0
Маска мережі	255.255.255.0
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	193.191.4.1
Максимальна адреса	193.191.4.254
Широкомовна маска	193.191.4.255
Шлюз за замовчуванням	193.191.4.1
Діапазон адрес комутаторів	193.191.4.2-193.191.4.10
Діапазон адрес ПК	193.191.4.11-193.191.4.145
Діапазон вільних адрес	193.191.4.146-193.191.4.254

Таблиця 2.6 – Параметри адресації мережі LAN_D

Призначення	ІР-адреса
Адреса мережі	193.191.5.0
Маска мережі	255.255.255.0
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	193.191.5.1
Максимальна адреса	193.191.5.254
Широкомовна маска	193.191.5.255
Шлюз за замовчуванням	193.191.5.1
Діапазон адрес комутаторів	193.191.5.2-193.191.5.10
Діапазон адрес ПК	193.191.5.11-193.191.5.145
Діапазон вільних адрес	193.191.5.146-193.191.5.254

Таблиця 2.7 – Параметри адресації мережі LAN_E

Призначення	ІР-адреса
Адреса мережі	193.191.6.0
Маска мережі	255.255.255.0
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	193.191.6.1
Максимальна адреса	193.191.6.254
Широкомовна маска	193.191.6.255
Шлюз за замовчуванням	193.191.6.1

Продовження таблиці 2.7 – Параметри адресації мережі LAN_E

Призначення	ІР-адреса
Діапазон адрес комутаторів	193.191.6.2-193.191.6.10
Діапазон адрес ПК	193.191.6.11-193.191.6.145
Діапазон вільних адрес	193.191.6.146-193.191.6.254

Таблиця 2.8 – Параметри адресації мережі LAN_F

Призначення	ІР-адреса
Адреса мережі	193.191.7.0
Маска мережі	255.255.255.0
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	193.191.7.1
Максимальна адреса	193.191.7.254
Широкомовна маска	193.191.7.255
Шлюз за замовчуванням	193.191.7.1
Діапазон адрес комутаторів	193.191.7.2-193.191.7.10
Діапазон адрес ПК	193.191.7.11-193.191.7.145
Діапазон вільних адрес	193.191.7.146-193.191.7.254

Таблиця 2.9 – Параметри адресації мережі LAN_G

Призначення	ІР-адреса
Адреса мережі	193.191.8.0
Маска мережі	255.255.255.0
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	193.191.8.1
Максимальна адреса	193.191.8.254
Широкомовна маска	193.191.8.255
Шлюз за замовчуванням	193.191.8.1
Діапазон адрес комутаторів	193.191.8.2-193.191.8.10
Діапазон адрес ПК	193.191.8.11-193.191.8.145
Діапазон вільних адрес	193.191.8.146-193.191.8.254

Таблиця 2.10 – Параметри адресації мережі LAN_H

Призначення	ІР-адреса
Адреса мережі	193.191.9.0
Маска мережі	255.255.255.0

Продовження таблиці 2.10 – Параметри адресації мережі LAN_H

Призначення	ІР-адреса
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	193.191.9.1
Максимальна адреса	193.191.9.254
Широкомовна маска	193.191.9.255
Шлюз за замовчуванням	193.191.9.1
Діапазон адрес комутаторів	193.191.9.2-193.191.9.10
Діапазон адрес ПК	193.191.9.11-193.191.9.145
Діапазон вільних адрес	193.191.9.146-193.191.9.254

Таблиця 2.11 – Параметри адресації мережі LAN_I

Призначення	ІР-адреса
Адреса мережі	193.191.10.0
Маска мережі	255.255.255.0
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	193.191.10.1
Максимальна адреса	193.191.10.254
Широкомовна маска	193.191.10.255
Шлюз за замовчуванням	193.191.10.1
Діапазон адрес комутаторів	193.191.10.2-193.191.10.10
Діапазон адрес ПК	193.191.10.11-193.191.10.145
Діапазон вільних адрес	193.191.10.146-193.191.10.254

2.3 Вибір мережевого обладнання для організації роботи мережі

Вибір мережевого обладнання виявляється критично важливим етапом у процесі розробки та будівництва мережі, бо саме на ньому базується функціональність, продуктивність та надійність цієї мережі. Обладнання є не просто складовою, але і фундаментальною основою, що забезпечує передачу даних, забезпечує взаємозв'язок між пристроями та забезпечує безпеку у мережевому середовищі. Справжній вибір апаратної складової мережі може мати суттєвий вплив на її продуктивність та результативність.

Процес розгортання мережі невіддільно пов'язаний з урахуванням унікальних вимог та потреб організації. Кожна мережа має свою специфіку та

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

конкретні вимоги, і тому обладнання має бути налаштоване так, щоб задовольняти ці унікальні потреби та завдання. Завдяки відомій якості, надійності та широкому асортименту продуктів, вибір мережевого обладнання від компанії Cisco може бути надзвичайно перспективним.

Однією з ключових переваг обрання обладнання Cisco є можливість вибору з багатої гами продуктів, які відповідають вимогам різноманітних мереж та розгортань. Велика кількість моделей і опцій дозволяє точно вибрати обладнання, яке оптимально відповідає вимогам конкретної мережевої інфраструктури. Безумовно, правильно вибране мережеве обладнання стане надійною основою для забезпечення безперебійної та ефективної роботи мережі.

Під час обрання моделі маршрутизатора для гетерогенної мережі, необхідно враховувати декілька ключових факторів. Перш за все, це кількість портів, яка повинна задовольняти потребам підключення різноманітних пристроїв, включаючи робочі станції, сервери, інші маршрутизатори чи комутатори. Крім того, важливо переконатися, що обрана модель маршрутизатора підтримує необхідні технології та протоколи, які використовуються в мережі.

Збалансований вибір моделі маршрутизатора має враховувати потреби мережі в розширенні та зростанні. Обраний маршрутизатор повинен бути достатньо гнучким, щоб враховувати майбутні розширення мережі та можливість підключення нових пристроїв та технологій. Важливо, щоб модель маршрутизатора була готовою відповідати потребам мережі не лише на сьогодні, але й на завтра.

Використання маршрутизатора Cisco 4461 забезпечить ефективну роботу мережі, оскільки він має достатню кількість портів для підключення пристроїв та відповідає усім потрібним вимогам.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				42
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 2.2 – Маршрутизатор Cisco 4461

Маршрутизатори Cisco ISR (Integrated Services Routers) 4000 серії включає моделі Cisco ISR4300 і Cisco ISR4400 підсерії. Ці пристрої відрізняються високою продуктивністю від 50 Мбіт/с до 2 Гбіт/с, вбудованими WAN портами Gigabit Ethernet та SFP портами. Функціональність платформи Cisco ISR4300 та Cisco ISR4400 можна розширити за допомогою інтерфейсних модулів NIM. Платформа підтримує 2 або 3 слоти розширення, залежно від моделі. Об'єм пам'яті DRAM 4GB з можливістю розширення до 16GB дозволяє справлятися із завданнями з високою швидкістю. Моделі Cisco ISR4400 підтримують функцію резервного живлення.

Маршрутизатори Cisco ISR4000 серії надають замовникам користувацькі послуги найвищої якості, високу масштабованість архітектури, захист інвестицій та мінімальні витрати на встановлення.

Крім цього, важливим і невід'ємним елементом нашої мережі є комутатор. Він виявляє значний вплив на ефективність та загальну функціональність мережевої інфраструктури. У випадку нашої гетерогенної мережі, де безпроводні з'єднання не є вимогою, вибір правильного комутатора є надзвичайно важливим для забезпечення безперебійної та ефективної роботи мережі.

При обранні комутатора для нашої мережі було враховано кілька ключових аспектів. Перш за все, необхідно було звернути увагу на кількість доступних портів, оскільки вона повинна задовольнити потреби підключення всіх пристроїв у мережі. Додатково, обраний комутатор повинен бути оснащений необхідними функціями, які дозволять успішно налаштувати та управляти схемою мережі.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

Після аналізу було встановлено, що найбільш оптимальним рішенням є обрання комутатора моделі WS-C2960+24TC-L. Цей комутатор є лінійним і володіє жорсткою конфігурацією, включаючи порти Fast Ethernet та Gigabit Ethernet. Крім того, він підтримує можливість розширення мережі, що дозволяє планувати масштабування та збільшення мережевої інфраструктури в майбутньому. Завдяки цим рисам, цей комутатор є ідеальним рішенням для вирішення всіх потреб і забезпечує необхідну функціональність для ефективної роботи всієї мережі.



Рисунок 2.3 – Комутатор Cisco WS-C2960+24TC-L

Комутатори серії Cisco Catalyst 2960-Plus - це комутатори Fast Ethernet із фіксованою конфігурацією, які забезпечують комутацію рівня 2 корпоративного класу для філій, звичайних робочих місць та інфраструктурних програм. Вони забезпечують надійну та безпечну роботу з нижчою загальною вартістю володіння завдяки ряду програмних функцій Cisco IOS, включаючи Cisco Catalyst SmartOperations.

Переваги комутатора включають:

- Надійна якість обслуговування (QoS), яка надає пріоритет голосу та критичним бізнес-додаткам
- Гнучкі функції безпеки, які можуть обмежити доступ до мережі та зменшити загрози
- Інструменти, які знижують загальну вартість володіння за рахунок спрощених операцій і автоматизації

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

2.4 Аналіз ризиків та заходи для захисту гетерогенної мережі

Гетерогенні мережі вимагають специфічного підходу до аналізу ризиків та розробки стратегій захисту. Загрози безпеці можуть виникати з більшої кількості джерел, і тому аналіз ризиків є критичним етапом в процесі планування та реалізації мережі.

Однією з основних загроз є можливість несанкціонованого доступу до мережі та її ресурсів. Це може призвести до витоку конфіденційної інформації, порушення прав доступу або навіть крадіжки даних. Особливо вразливими можуть бути пристрої з застарілими версіями операційних систем або слабкими точками входу. Для уникнення таких ризиків, рекомендується регулярно оновлювати програмне забезпечення, встановлювати сильні паролі та використовувати механізми двухфакторної аутентифікації.

Іншою загрозою є атаки на мережевий трафік, такі як атаки "людина посередині" (man-in-the-middle) або "переповнення буфера" (buffer overflow). Такі атаки можуть дозволити зловмисникам перехоплювати, змінювати або використовувати дані, що пересилаються між пристроями. Для запобігання таким ризикам, рекомендується використовувати шифрування трафіку, встановлювати брандмауери та системи виявлення вторгнень.

Віруси та шкідливі програми також можуть становити серйозну загрозу для гетерогенної мережі. Різноманітність компонентів може ускладнити процес виявлення та лікування інфікованих пристроїв. Для запобігання цим ризикам, важливо встановлювати антивірусне програмне забезпечення, виконувати регулярну перевірку пристроїв на вразливості та обмежувати можливість встановлення програм від ненадійних джерел.

Додатковою загрозою може бути недостатня захищеність фізичного обладнання мережі. Несанкціонований фізичний доступ до пристроїв може призвести до втрати даних, зміни налаштувань або навіть фізичної шкоди обладнанню. Для захисту від цього ризику, рекомендується фізично обмежувати

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

доступ до серверних кімнат, використовувати механізми аутентифікації для фізичного доступу та моніторити фізичну безпеку мережі.

Однак, з метою забезпечення високого рівня безпеки мережі та запобігання можливим загрозам, можна вжити різноманітні заходи та практики, які належить ретельно розглянути:

- Налаштування брандмауерів та систем виявлення вторгнень: Перш за все, важливо ретельно налаштовувати брандмауери та системи виявлення вторгнень. Це сприяє моніторингу та фільтрації мережевого трафіку, що дозволяє реагувати на підозрілі або небезпечні дії у мережі. Додатково, належить регулярно оновлювати ці системи, щоб вони відповідали актуальним загрозам.

- Шифрування трафіку: Застосування шифрування до мережевого трафіку допомагає забезпечити конфіденційність даних під час їх передачі. Використання протоколів шифрування, таких як SSL / TLS, ускладнює можливість перехоплення та зловживання інформацією з боку недоброзичливих акторів.

- Використання антивірусного програмного забезпечення: Для захисту від вірусів та шкідливих програм важливо встановити та регулярно оновлювати антивірусне програмне забезпечення на всіх пристроях мережі. Це дозволить виявити та нейтралізувати потенційні загрози до безпеки мережі.

- Регулярне оновлення програмного забезпечення: Постійне оновлення операційних систем та програмного забезпечення на всіх пристроях мережі є ключовим для зниження ризику використання вразливостей зловмисниками. Це надає можливість використовувати останні заходи захисту та виправлення вразливостей.

- Підвищення рівня аутентифікації: Важливо встановити сильні паролі для доступу до ресурсів мережі та використовувати механізми двофакторної аутентифікації. Це допоможе ускладнити несанкціонований доступ до важливих даних та зменшити ризик несанкціонованих дій.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

- Навчання персоналу з кібербезпеки: Навчання персоналу з питань кібербезпеки є надзвичайно важливим. Інформований персонал може вчасно розпізнати підозрілі ситуації, уникнути соціального інженерінгу та поводитися відповідно, щоб уникнути можливих загроз.

- Проведення аудитів безпеки мережі: Регулярні аудити безпеки допомагають виявити потенційні вразливості та недоліки у системі захисту. Це дозволяє вчасно вжити заходів для їх усунення та підвищення рівня безпеки мережі.

- Розробка планів реагування на інциденти: Рекомендується розробити плани реагування на інциденти безпеки. У разі загрози або інциденту ефективний план дій допоможе оперативно та ефективно впоратися з ситуацією та запобігти подальшим наслідкам.

Висновки до другого розділу

У даному розділі було проведено докладне дослідження та аналіз проектування гетерогенної мережі для організації. Була розглянута розробка топології гетерогенної мережі, де було обговорено ключові аспекти створення мережевої інфраструктури, включаючи рівні доступу, розподілу та ядра. Також було визначено основні пристрої та з'єднання між ними для забезпечення ефективного обміну даними. Також була детально розглянута розробка схем адресації мережі, де було акцентовано на важливості уникнення дублікатів IP-адрес та оптимізації використання ресурсів для майбутнього зростання мережі.

Далі була розглянута проблематика вибору мережевого обладнання для організації роботи гетерогенної мережі. Були враховані вимоги до функціональності, продуктивності та надійності мережі при виборі конкретних моделей маршрутизаторів та комутаторів. Також був проведений аналіз ризиків безпеки та розроблені відповідні заходи для захисту гетерогенної мережі.

У цілому, даний розділ надав глибокий інсайт у процес проектування гетерогенної мережі для організації, від вибору топології та адресації до вибору обладнання та забезпечення безпеки.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ОБЛАДНАННЯ ГЕТЕРОГЕННОЇ МЕРЕЖІ

3.1 Налаштування обладнання мережі

Для забезпечення належного функціонування мережі необхідно дотримуватися налаштувань та параметрів, які відповідають характеристикам та потребам організації. При врахуванні спроектованої топології, яка була обговорена у другому розділі, ми застосовуємо вже розраховані параметри. Проте, важливо також надати належну увагу послідовності налаштувань та переконатися у застосуванні вірних параметрів для кожного з компонентів мережі. Цей процес гарантує не лише оптимальну продуктивність, але і ефективну передачу даних, а також захист від можливих проблем та перешкод в мережевому середовищі.

Першим етапом в реалізації проекту є встановлення та налаштування параметрів IP-адресації на всіх мережевих пристроях. Це включає призначення унікальних IP-адрес для кожного пристрою та правильне налаштування масок підмереж. Далі ми розглянемо приклад конфігурації для маршрутизатора R-Core-1:

```
R-Core-1#configure terminal
R-Core-1(config)#interface fa0/0
R-Core-1(config-if)#description LINK_TO_R-Core-2
R-Core-1(config-if)#ip address 192.191.1.1 255.255.255.252
R-Core-1(config-if)#no shutdown
R-Core-1(config-if)#exit
R-Core-1(config)#interface fa1/0
R-Core-1(config-if)#description LINK_TO_R-Distr-1
R-Core-1(config-if)#ip address 192.191.2.1 255.255.255.252
R-Core-1(config-if)#no shutdown
R-Core-1(config-if)#exit
R-Core-1(config)#interface fa1/1
```

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

```

R-Core-1(config-if)#description LINK_TO_R-Distr-3
R-Core-1(config-if)#ip address 192.191.3.1 255.255.255.252
R-Core-1(config-if)#no shutdown
R-Core-1(config-if)#exit

```

Тим же методом здійснюється конфігурація IP-адресації для всіх інших компонентів мережі.

Далі необхідно перейти до налаштування маршрутизації на маршрутизаторах за допомогою протоколів OSPF та EIGRP. Процес налаштування цих протоколів є ключовим для забезпечення ефективної маршрутизації даних у мережі.

Для початку, налаштовуємо протокол OSPF на маршрутизаторі R-Distr-1:

```

R-Distr-1(config)#router ospf 191
R-Distr-1(config-router)#network 192.191.2.0 0.0.0.3 area 0
R-Distr-1(config-router)#network 192.191.4.0 0.0.0.3 area 0
R-Distr-1(config-router)#network 193.191.2.0 0.0.0.255 area 0
R-Distr-1(config-router)#exit

```

Налаштування протоколу EIGRP на маршрутизаторі R-Distr-6 наведено нижче:

```

R-Distr-6(config)#router eigrp 191
R-Distr-6(config-router)#network 192.191.6.0 0.0.0.3
R-Distr-6(config-router)#network 193.191.9.0 0.0.0.255
R-Distr-6(config-router)#network 193.191.10.0 0.0.0.255
R-Distr-6(config-router)#exit

```

Для того щоб маршрутизатори, що використовують різні протоколи маршрутизації, могли ефективно обмінюватися інформацією про доступні підмережі, необхідно налаштувати процес редистрибуції на маршрутизаторі R-Core-1. Цей процес полягає в передачі інформації про маршрути з одного протоколу до іншого, забезпечуючи взаємодію між різними протоколами.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R-Core-1(config)#router ospf 191
R-Core-1(config-router)#network 192.191.2.0 0.0.0.3 area 0
R-Core-1(config-router)#network 192.191..0 0.0.0.3 area 0
R-Core-1(config-router)#network 192.191.3.0 0.0.0.3 area 0
R-Core-1(config-router)#redistribute eigrp 191
% Only classful networks will be redistributed
R-Core-1(config-router)#exit
R-Core-1(config)#router eigrp 191
R-Core-1(config-router)#network 192.191.1.0 0.0.0.3
R-Core-1(config-router)#redistribute ospf 191 metric 1000000 1 255 1 1500
R-Core-1(config-router)#exit

```

У якості DNS-серверів будемо використовувати пристрій на операційній системі Windows. Для WinServer2019 у першу чергу встановимо сервіс DNS. Встановлення сервісу показано на рисунку 3.1.

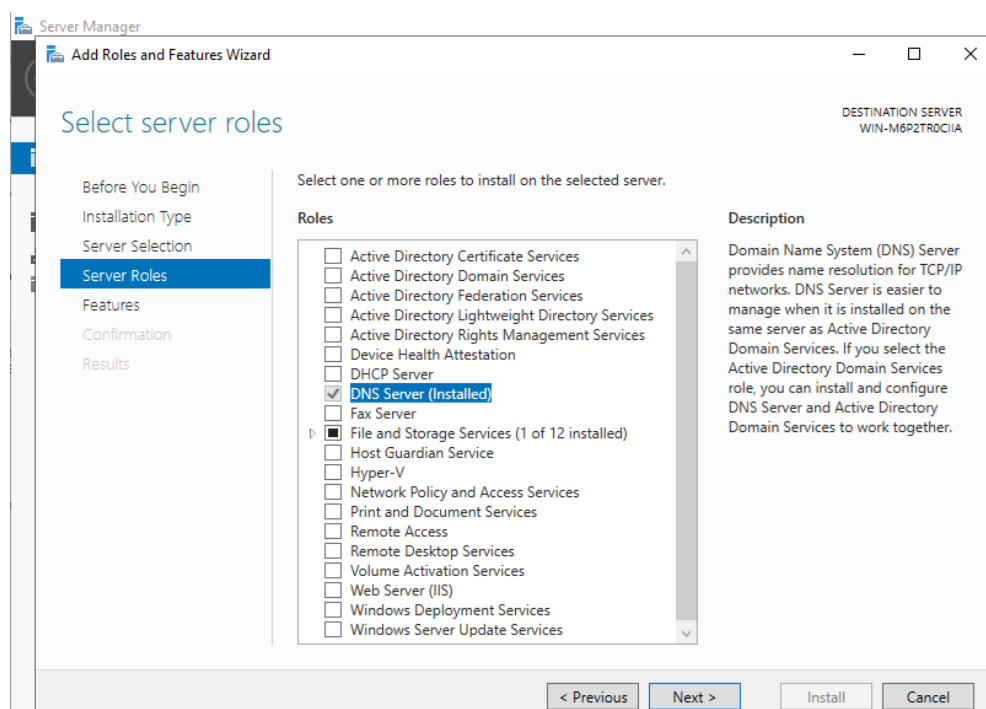
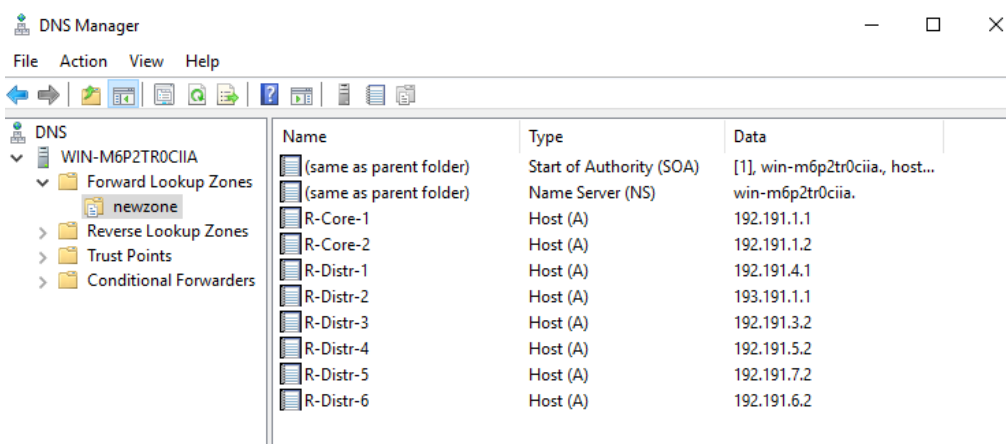


Рисунок 3.1 – Встановлення сервісу DNS

Після успішного встановлення сервісу DNS необхідно перейти до процесу налаштування DNS-записів та засобів забезпечення безпеки. Це дозволить

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

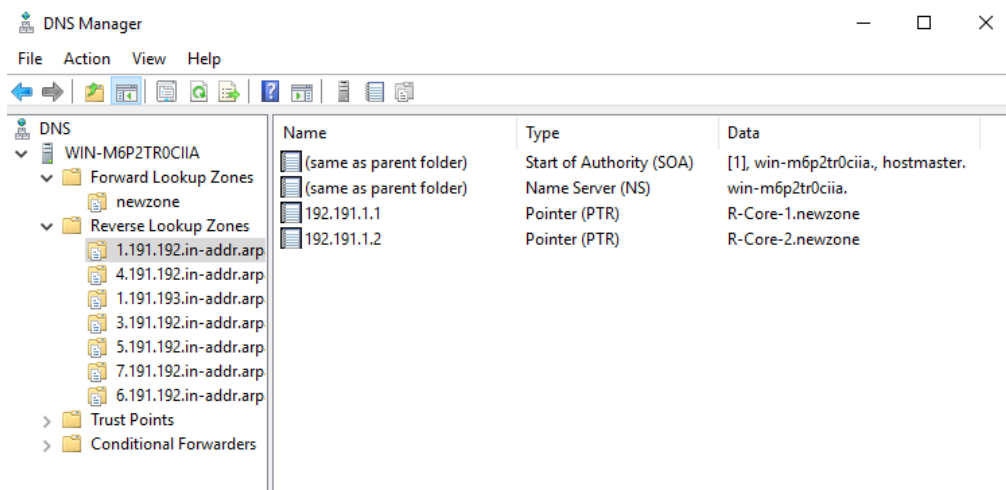
ефективно управляти ідентифікацією та адресацією різних компонентів мережі. Налагоджені записи наведені на рисунках 3.2 та 3.3.



The screenshot shows the DNS Manager console tree with 'Forward Lookup Zones' expanded. The 'newzone' folder is selected. The main pane displays a list of DNS records:

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], win-m6p2tr0ciia, host...
(same as parent folder)	Name Server (NS)	win-m6p2tr0ciia.
R-Core-1	Host (A)	192.191.1.1
R-Core-2	Host (A)	192.191.1.2
R-Distr-1	Host (A)	192.191.4.1
R-Distr-2	Host (A)	193.191.1.1
R-Distr-3	Host (A)	192.191.3.2
R-Distr-4	Host (A)	192.191.5.2
R-Distr-5	Host (A)	192.191.7.2
R-Distr-6	Host (A)	192.191.6.2

Рисунок 3.2 – Налагодження Forward lookup zones



The screenshot shows the DNS Manager console tree with 'Reverse Lookup Zones' expanded. The '1.191.192.in-addr.arpa' zone is selected. The main pane displays a list of DNS records:

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], win-m6p2tr0ciia., hostmaster.
(same as parent folder)	Name Server (NS)	win-m6p2tr0ciia.
192.191.1.1	Pointer (PTR)	R-Core-1.newzone
192.191.1.2	Pointer (PTR)	R-Core-2.newzone

Рисунок 3.3 – Налагодження Reverse lookup zones

Далі здійснимо налаштування методів захисту DNSSEC на сервері. Перш за все, ми здійснимо реєстрацію нашої зони у системі. На наступному етапі, ми візьмемо на себе завдання налаштування параметрів для ключів DNSSEC, які будуть використовуватися для підпису даних у нашій зоні.

Зокрема, в кожній DNS-зоні ми матимемо пару ключів: відкритий та закритий. Закритий ключ використовується власником зони для підписування DNS-даних у цій зоні та генерації цифрових підписів для цих даних. Як зрозуміло з назви "закритий ключ", інформація про цей ключ є конфіденційною та відомою тільки власнику зони. Проте відкритий ключ зони розголошується публічно та

доступний для всіх зацікавлених. Будь-який рекурсивний клієнт, що виконує запити до цієї зони, також отримує відкритий ключ цієї зони та використовує його для перевірки цілісності та достовірності DNS-даних.

Застосування технології DNSSEC допомагає усунути багато загроз безпеки, пов'язаних з DNS, та забезпечує перевірку даних між клієнтами та DNS-серверами. У високозабезпечених мережових середовищах впровадження DNSSEC є необхідною складовою для забезпечення надійної та захищеної інфраструктури DNS.

The screenshot shows the 'New Key Signing Key (KSK)' dialog box. It has a title bar with a close button. The dialog is divided into several sections: 'Guid' with a text box containing a GUID; 'Key Generation' with two radio buttons, 'Generate new signing keys.' being selected; 'Key Properties' with dropdown menus for 'Cryptographic algorithm' (RSA/SHA-256), 'Key length (Bits)' (2048), and 'Select a key storage provider to generate and store keys:' (Microsoft Software Key Storage Prov), and a spinner for 'DNSKEY RRSET signature validity period (hours)' (168); and 'Key Rollover' with a checked checkbox 'Enable automatic rollover', a spinner for 'Rollover frequency (days)' (755), and a spinner for 'Delay the first rollover by (days)' (0). At the bottom are 'OK' and 'Cancel' buttons.

Рисунок 3.4 – Параметри відкритого ключа

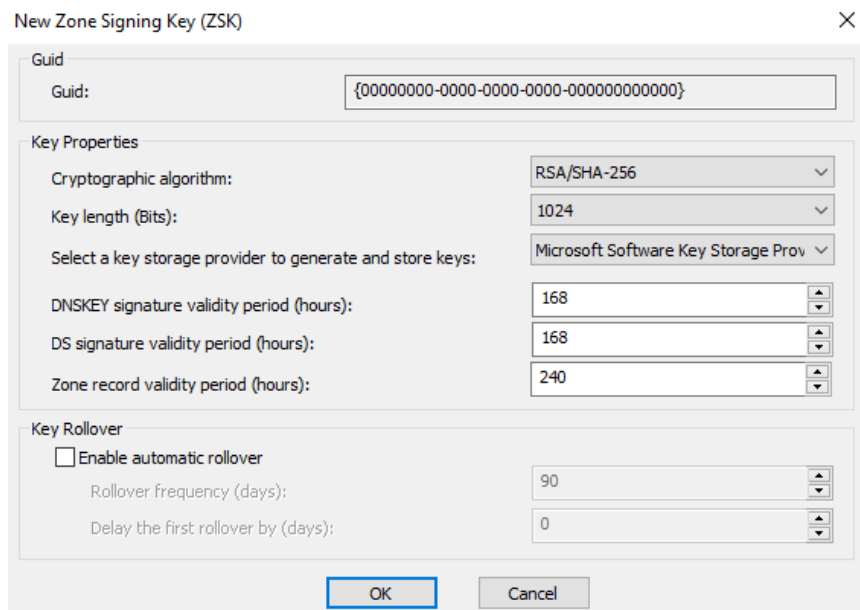


Рисунок 3.5 – Параметри закритого ключа

Таким чином, після створення ключів, давайте розглянемо вміст зони. Зараз у зоні присутні записи, що пов'язані з впровадженими заходами безпеки. Детальний огляд вмісту цієї зони представлено на рисунку 3.6.

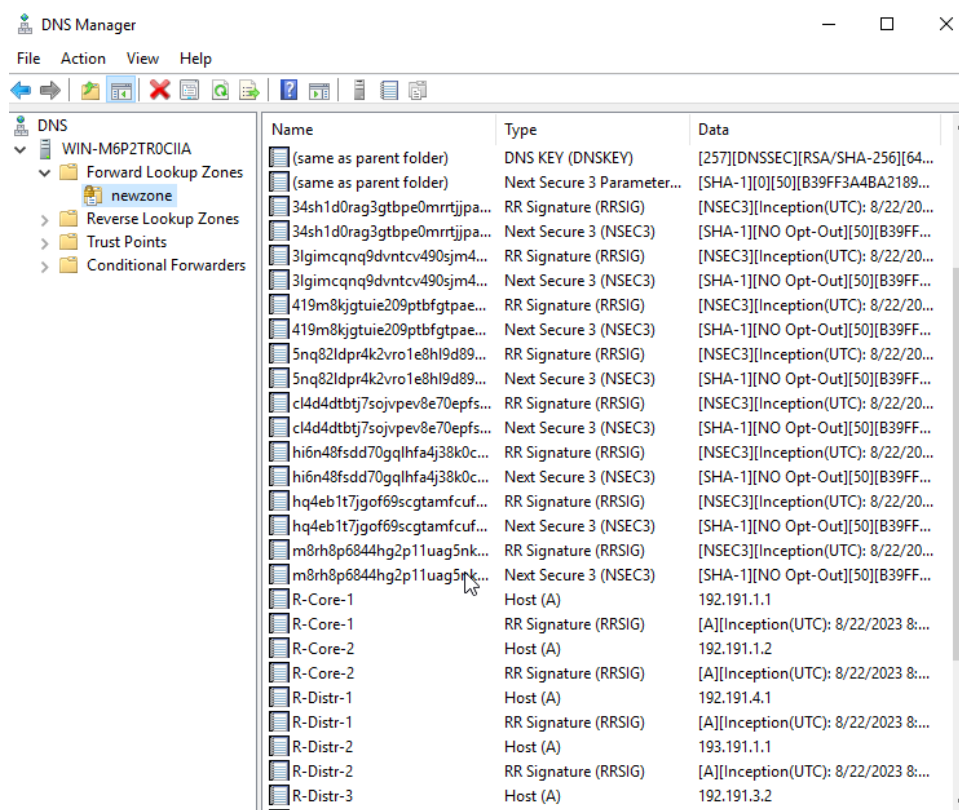


Рисунок 3.6 – Вміст зони після налагодження засобів безпеки

Після встановлення ключів, важливо також провести додаткове налаштування політик безпеки. Деталі параметрів для налаштування цих політик можна знайти на рисунку 3.7.

Рисунок 3.7 – Налагодження політик безпеки

Додатковий рівень безпеки можна забезпечити шляхом впровадження аутентифікації у протоколах маршрутизації EIGRP і OSPF. Це стане додатковим механізмом захисту, який дозволить перевіряти та підтверджувати легітимність комунікації між маршрутизаторами:

```
R-Core-1(config)#key chain priv
R-Core-1(config-keychain)#key 1
R-Core-1(config-keychain-key)#key-string qwerty123
R-Core-1(config-keychain-key)#exit
R-Core-1(config-keychain)#exit
R-Core-1(config)#interface fa0/0
R-Core-1(config-if)#ip authentication mode eigrp 191 md5
R-Core-1(config-if)#ip authentication key-chain eigrp 191 priv
R-Core-1(config-if)#exit
R-Core-1(config)#interface fa1/0
```

```

R-Core-1(config-if)#ip ospf authentication message-digest-key 1 md5
qwerty123
R-Core-1(config-if)#ip ospf authentication message-digest
R-Core-1(config-if)#exit
R-Core-1(config)#interface fa1/1
R-Core-1(config-if)#ip ospf authentication message-digest-key 1 md5
qwerty123
R-Core-1(config-if)#ip ospf authentication message-digest
R-Core-1(config-if)#exit

```

Також на кожному маршрутизаторі та комутаторі виконується налаштування протоколу SSH для забезпечення безпечного віддаленого доступу. Нижче наведено приклад налаштування протоколу SSH на маршрутизаторі R-Core-1:

```

R-Core-1(config)#crypto key generate rsa
R-Core-1(config)#service password-encryption
R-Core-1(config)#username admin privilege 15 secret adminpass
R-Core-1(config)#username user1 privilege 1 secret user1pass
R-Core-1(config)#username user4 privilege 4 secret user4pass
R-Core-1(config)#enable secret mypass
R-Core-1(config)#aaa new-model
R-Core-1(config)#line vty 0 4
R-Core-1(config-line)#transport input ssh
R-Core-1(config-line)#logging synchronous
R-Core-1(config-line)#exec-timeout 60 0

```

І на завершальному етапі ми займаємося налаштуванням протоколів SNMP, NTP та системного журналу. Ці протоколи відіграють важливу роль у керуванні та моніторингу мережі, а також у забезпеченні синхронізації часу та запису подій. Нижче наведено приклад налаштування цих протоколів для забезпечення їх правильної роботи у мережі:

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R-Core-1(config)#ip access-list standard PERMIT-SNMP
R-Core-1(config-std-nacl)#permit 193.191.1.0 0.0.0.255
R-Core-1(config-std-nacl)#exit
R-Core-1(config)#snmp-server view SNMP-R iso included
R-Core-1(config)#$ group SNMP-G v3 priv read SNMP-R access PERMIT-
SNMP
R-Core-1(config)#$-Admin SNMP-G v3 auth sha Authpass priv des56
Encrypass
R-Core-1(config)#ntp authentication-key 1 md5 NTPpassword
R-Core-1(config)#ntp trusted-key 1
R-Core-1(config)#ntp authenticate
R-Core-1(config)#ntp server 193.191.1.1
R-Core-1(config)#service timestamps log datetime msec
R-Core-1(config)#logging host 193.191.1.12
R-Core-1(config)#logging trap warning

```

3.2 Перевірка працездатності мережі

Перевірка працездатності мережі виявляється як невід'ємний компонент у забезпеченні надійного та оптимального функціонування гетерогенної інфраструктури. Під час проведення такої перевірки ми звертаємо увагу на різні ключові аспекти, такі як функціональність, якість з'єднань, правильність маршрутизації, рівень безпеки та загальна надійність. Цей аналіз допомагає переконатися, що мережа працює оптимально та відповідає вимогам корпоративного середовища, готова впоратися з завданнями будь-якого рівня складності.

У першу чергу перевіримо налаштування маршрутизації на пристроях мережі. Поглянемо на таблицю маршрутизації на пристрої R-Distr-6, таблицю маршрутизації показано на рисунку 3.8.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

```

R-Distr-6#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    193.191.9.0/24 is directly connected, FastEthernet0/1
D    193.191.8.0/24 [90/35840] via 192.191.6.1, 00:01:29, FastEthernet1/0
C    193.191.10.0/24 is directly connected, FastEthernet0/0
D EX 193.191.5.0/24 [170/30976] via 192.191.6.1, 00:00:45, FastEthernet1/0
     192.191.4.0/30 is subnetted, 1 subnets
D EX 192.191.4.0 [170/30976] via 192.191.6.1, 00:00:45, FastEthernet1/0
D EX 193.191.4.0/24 [170/30976] via 192.191.6.1, 00:00:45, FastEthernet1/0
D    192.191.5.0/24 [90/30720] via 192.191.6.1, 00:01:29, FastEthernet1/0
D    193.191.7.0/24 [90/35840] via 192.191.6.1, 00:01:29, FastEthernet1/0
     192.191.6.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.191.6.0/30 is directly connected, FastEthernet1/0
D    192.191.6.0/24 is a summary, 00:01:32, Null0
D    193.191.6.0/24 [90/33280] via 192.191.6.1, 00:01:29, FastEthernet1/0
D    192.191.7.0/24 [90/33280] via 192.191.6.1, 00:01:31, FastEthernet1/0
D EX 193.191.1.0/24 [170/30976] via 192.191.6.1, 00:00:37, FastEthernet1/0
D    192.191.1.0/24 [90/30720] via 192.191.6.1, 00:01:31, FastEthernet1/0
D EX 193.191.3.0/24 [170/30976] via 192.191.6.1, 00:00:37, FastEthernet1/0
     192.191.2.0/30 is subnetted, 1 subnets
D EX 192.191.2.0 [170/30976] via 192.191.6.1, 00:01:31, FastEthernet1/0
D EX 193.191.2.0/24 [170/30976] via 192.191.6.1, 00:00:47, FastEthernet1/0
     192.191.3.0/30 is subnetted, 1 subnets
D EX 192.191.3.0 [170/30976] via 192.191.6.1, 00:01:31, FastEthernet1/0
R-Distr-6#

```

Рисунок 3.8 – Таблиця маршрутизації

Як можна спостерігати, у таблицю маршрутизації були додані не лише підмережі, що відносяться до одного конкретного протоколу маршрутизації, а також мережі, які використовують інші протоколи. Це підтверджує успішну реалізацію процесу обміну маршрутною інформацією між різними протоколами.

Далі перевіряється безперервний зв'язок між пристроями за допомогою команд ping та tracert/traceroute:

```

R-Distr-3#ping 193.191.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 193.191.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 700/812/1000 ms
R-Distr-3#ping 193.191.7.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 193.191.7.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1004/1149/1220 ms
R-Distr-3#

```

Рисунок 3.9 – Перевірка зв'язку за допомогою команди ping

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

```

R-Distr-5#traceroute 193.191.2.1

Type escape sequence to abort.
Tracing the route to 193.191.2.1

 0 192.191.7.1 80 msec 360 msec 328 msec
 1 192.191.5.1 484 msec 220 msec 656 msec
 2 192.191.1.1 624 msec 672 msec 812 msec
 3 192.191.2.2 968 msec 1112 msec 1044 msec
R-Distr-5#traceroute 193.191.9.1

Type escape sequence to abort.
Tracing the route to 193.191.9.1

 0 192.191.7.1 152 msec 220 msec 264 msec
 1 192.191.5.1 552 msec 544 msec 480 msec
 2 192.191.6.2 784 msec 936 msec 704 msec
R-Distr-5#

```

Рисунок 3.10 – Перевірка зв'язку за допомогою команди traceroute

```

student@student-VirtualBox:~$ ping 193.191.4.1
ЛУНА-ІМПУЛЬС 193.191.4.1 (193.191.4.1) 56(84) байтів даних.
64 байтів з 193.191.4.1: icmp_seq=1 ttl=255 час=43.3 мс
64 байтів з 193.191.4.1: icmp_seq=2 ttl=255 час=29.0 мс
64 байтів з 193.191.4.1: icmp_seq=3 ttl=255 час=31.6 мс
64 байтів з 193.191.4.1: icmp_seq=4 ttl=255 час=31.8 мс
^C
--- Статистика луна-імпульсів 193.191.4.1 ---
Передано 4 пакетів, отримано 4, втрачено 0% пакетів, час 3004 мс
rtt мін/сер/макс/mdev = 28.956/33.905/43.279/5.527 мс
student@student-VirtualBox:~$ ping 193.191.9.1
ЛУНА-ІМПУЛЬС 193.191.9.1 (193.191.9.1) 56(84) байтів даних.
64 байтів з 193.191.9.1: icmp_seq=1 ttl=252 час=207 мс
64 байтів з 193.191.9.1: icmp_seq=2 ttl=252 час=154 мс
64 байтів з 193.191.9.1: icmp_seq=3 ttl=252 час=136 мс
64 байтів з 193.191.9.1: icmp_seq=4 ttl=252 час=168 мс
^C
--- Статистика луна-імпульсів 193.191.9.1 ---
Передано 4 пакетів, отримано 4, втрачено 0% пакетів, час 3004 мс
rtt мін/сер/макс/mdev = 135.955/166.144/206.538/25.892 мс
student@student-VirtualBox:~$

```

Рисунок 3.11 – Перевірка зв'язку на ОС Linux

Наступний етап це перегляд налагодження параметрів аутентифікації для протоколів маршрутизації:

```

R-Core-1
!
interface FastEthernet0/0
 description LINK_TO_R-Core-2
 ip address 192.191.1.1 255.255.255.252
 ip authentication mode eigrp 191 md5
 ip authentication key-chain eigrp 191 priv
 duplex auto
 speed auto
!

```

Рисунок 3.12 – Перевірка налагодження аутентифікації для протоколів маршрутизації

Далі переходимо до перевірки роботи DNS-сервера. Для забезпечення належної функціональності мережі важливо впевнитися в коректному

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

функціонуванні DNS-серверу, оскільки він відіграє значущу роль у розрізненні та перетворенні доменних імен на відповідні IP-адреси.

```
C:\Users\Administrator>ping R-Distr-1.newzone

Pinging R-Distr-1.newzone [192.191.4.1] with 32 bytes of data:
Reply from 192.191.4.1: bytes=32 time=128ms TTL=254
Reply from 192.191.4.1: bytes=32 time=163ms TTL=254
Reply from 192.191.4.1: bytes=32 time=251ms TTL=254
Reply from 192.191.4.1: bytes=32 time=88ms TTL=254

Ping statistics for 192.191.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 88ms, Maximum = 251ms, Average = 157ms

C:\Users\Administrator>ping R-Distr-6.newzone

Pinging R-Distr-6.newzone [192.191.6.2] with 32 bytes of data:
Reply from 192.191.6.2: bytes=32 time=495ms TTL=251
Reply from 192.191.6.2: bytes=32 time=427ms TTL=251
Reply from 192.191.6.2: bytes=32 time=497ms TTL=251
Reply from 192.191.6.2: bytes=32 time=446ms TTL=251

Ping statistics for 192.191.6.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 427ms, Maximum = 497ms, Average = 466ms
```

Рисунок 3.13 – Перевірка працездатності DNS-сервісу

Висновки до третього розділу.

Третій розділ присвячено детальному аналізу процесу налагодження та тестування обладнання корпоративної мережі. Починаючи з опису налагодження обладнання мережі, у цьому розділі було розглянуто комплексний процес конфігурування маршрутизаторів, комутаторів та інших компонентів мережі.

Процес налагодження був впроваджений відповідно до вимог та конкретних потреб гетерогенної мережі. Під час цього етапу було важливо дотримуватися стандартів безпеки та враховувати особливості гетерогенної інфраструктури мережі.

Після завершення налагодження наступив етап перевірки працездатності мережі. Основна мета цього етапу полягала в підтвердженні успішності налагодження та виявленні можливих недоліків або проблем, які можуть виникнути під час реальної експлуатації мережі.

Цей етап дозволив ідентифікувати можливі проблеми та вразливості, які можуть виникнути під час експлуатації мережі в реальних умовах.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

ВИСНОВКИ

В ході дослідження, охопленого даною кваліфікаційною роботою, було проведено аналіз та розробка підсистеми захисту для гетерогенної мережі організації. Основним завданням було створення ефективної та надійної інфраструктури захисту, яка б відповідала специфіці гетерогенної мережі та забезпечувала високий рівень безпеки в умовах сучасних викликів кібербезпеки.

У першому розділі були розглянуті теоретичні аспекти та особливості гетерогенних мереж, що дозволило отримати загальне уявлення про їх характеристики та складності. Визначення вимог до підсистеми захисту дало можливість визначити конкретні цілі та об'єкти створення захисту для гетерогенної мережі. Огляд сучасних методів і технологій захисту гетерогенних мереж розкрив широкий спектр можливостей та підходів до створення надійного захисту, що стало основою для подальшого проектування.

Другий розділ був присвячений проектуванню гетерогенної мережі організації. Розробка топології мережі, схеми адресації та вибір мережевого обладнання були здійснені з урахуванням вимог до безпеки та ефективності мережі. Аналіз ризиків та заходи для захисту гетерогенної мережі допомогли виявити потенційні небезпеки та розробити стратегію забезпечення безпеки.

В третьому розділі було виконано налагодження та тестування обладнання корпоративної мережі. Налагодження обладнання, яке включало налаштування маршрутизаторів, комутаторів, протоколів маршрутизації та безпеки, було здійснене згідно з вимогами та потребами мережі. Далі було проведено перевірку працездатності мережі. Цей етап допоміг виявити можливі недоліки та забезпечити високу надійність та працездатність мережі.

Завершуючи роботу, можна визначити, що створений проект підсистеми захисту гетерогенної мережі організації відповідає сучасним вимогам безпеки та є ефективним інструментом для забезпечення цілісності, конфіденційності та доступності інформаційного середовища. Реалізація запропонованого проекту підсилює безпековий стандарт організації та сприяє створенню стійкої мережевої інфраструктури в умовах постійно зростаючих загроз кібербезпеці.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ПРОЕКТ ПІДСИСТЕМИ ЗАХИСТУ ГЕТЕРОГЕННОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ НА БАЗІ ПРИСТРОЇВ МІКРОТІК ТА CISCO [Електронний ресурс] – Режим доступу до ресурсу: <https://conf.ztu.edu.ua/wp-content/uploads/2022/02/32.pdf>.
2. Heterogeneous network [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Heterogeneous_network.
3. HETNET - ГЕТЕРОГЕННІ МЕРЕЖІ [Електронний ресурс] – Режим доступу до ресурсу: <https://jak.koshachek.com/articles/hetnet-geterogenni-merezhi-heterogenic-networks.html>.
4. Гетерогенні комп'ютерні мережі [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%93%D0%B5%D1%82%D0%B5%D1%80%D0%BE%D0%B3%D0%B5%D0%BD%D0%BD%D1%96_%D0%BA%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%96_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96.
5. Heterogeneous Network [Електронний ресурс] – Режим доступу до ресурсу: <https://www.sciencedirect.com/topics/computer-science/heterogeneous-network>.
6. Next Generation Heterogeneous Wireless Networks [Електронний ресурс] – Режим доступу до ресурсу: <https://www.wipro.com/communications-service-management-in-next-generation-heterogeneous-wireless-net/>.
7. Heterogeneous Network [Електронний ресурс] – Режим доступу до ресурсу: <https://academic-accelerator.com/encyclopedia/heterogeneous-network>.
8. What Is DNS and How Does It Work [Електронний ресурс] – Режим доступу до ресурсу: <https://www.hostinger.com/tutorials/what-is-dns>.
9. Domain Name System [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Domain_Name_System.
10. Маршрутизатор Cisco ISR4461/K9 [Електронний ресурс] – Режим доступу до ресурсу: <https://stack-systems.com.ua/marshrutizator-cisco-isr4461-k9>.

		Опанасюк В.В.			<i>КІК.КР.Б – 125 – 11 – ПЗ</i>	Арк.
		Покотило О.А.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

11. Cisco 4461 Integrated Services Router [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/routers/4461-integrated-services-router/model.html>.

12. Технології захисту інформації в інформаційних системах та комп'ютерних мережах [Електронний ресурс] – Режим доступу до ресурсу: https://stud.com.ua/50143/informatika/tehnologiyi_zahistu_informatsiyi_informatsiy_nih_sistemah_kompyuternih_merezhah.

13. Комплексні системи захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/rozdil7.html.

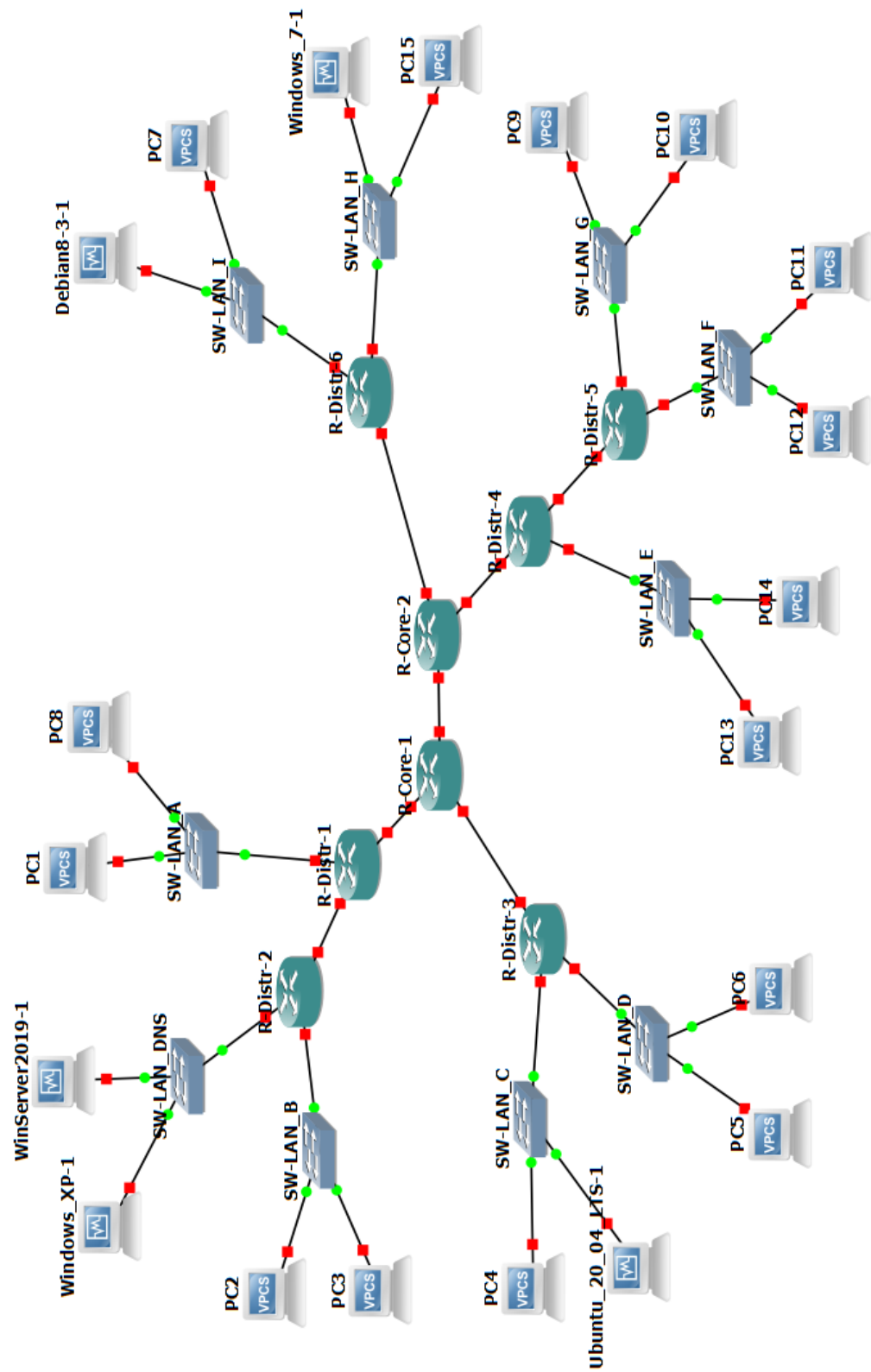
14. Network Security [Електронний ресурс] – Режим доступу до ресурсу: <https://www.itarian.com/network-security.php>.

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

ДОДАТКИ

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток А – Детальна схема побудованої схеми



Додаток Б – Лістинг конфігураційних файлів пристроїв

```
R-Core-1#show run
Building configuration...
Current configuration : 2272 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R-Core-1
boot-start-marker
boot-end-marker
enable secret 5
$1$xXmV$3GFT3jmvChqvVIZOAMEyc1
aaa new-model
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip domain name opanasiuk.net
key chain priv
key 1
key-string 7 00150403164F12575D72
username admin privilege 15 secret 5
$1$eXCD$WsyYdzGFSYeEHTwQmgwAd/
username user1 secret 5
$1$uEDZ$5MjmjYZ8N1uhf1MEmwKzX0
username user4 privilege 4 secret 5
$1$Y4kO$4OmGbnYjoKGArSasfQXVIO
ip tcp synwait-time 5
interface FastEthernet0/0
description LINK_TO_R-Core-2
ip address 192.191.1.1 255.255.255.252
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 priv
duplex auto
speed auto
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet1/0
description LINK_TO_R-Distr-1
ip address 192.191.2.1 255.255.255.252
ip ospf authentication message-digest
duplex auto
speed auto
interface FastEthernet1/1
description LINK_TO_R-Distr-3
ip address 192.191.3.1 255.255.255.252
ip ospf authentication message-digest
duplex auto
```

```
speed auto
router eigrp 191
redistribute connected
redistribute ospf 191 metric 1000000 1 255 1
1500
network 192.191.1.0 0.0.0.3
auto-summary
router ospf 191
log-adjacency-changes
redistribute eigrp 191
network 192.191.2.0 0.0.0.3 area 0
network 192.191.3.0 0.0.0.3 area 0
no ip http server
no ip http secure-server
ip access-list standard PERMIT-SNMP
permit 193.191.1.0 0.0.0.255
logging trap warnings
logging 193.191.1.12
snmp-server group SNMP-G v3 priv read SNMP-
R access PERMIT-SNMP
snmp-server view SNMP-R iso included
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 60 0
logging synchronous
transport input ssh
ntp authentication-key 1 md5
12373127020A1F173D24362C 7
ntp authenticate
ntp trusted-key 1
ntp server 193.191.1.1
end
```

```
R-Core-2#show run
Building configuration...
Current configuration : 1230 bytes
version 12.4
service timestamps debug datetime msec
```

		Опанасюк В.В.			<i>КІК.КР.Б – 125 – 11 – ПЗ</i>	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

```

service timestamps log datetime msec
service password-encryption
hostname R-Core-2
boot-start-marker
boot-end-marker
enable secret 5
$1$xXmV$3GFT3jmvChqvVIZOAMEyc1
aaa new-model
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip domain name opanasiuk.net
key chain priv
key 1
key-string 7 00150403164F12575D72
username admin privilege 15 secret 5
$1$eXCD$WsyYdzGFSYeEHTwQmgwAd/
username user1 secret 5
$1$uEDZ$5MjmjYZ8N1uhf1MEmwKzX0
username user4 privilege 4 secret 5
$1$Y4kO$4OmGbnYjoKGArsasfQXVIO
ip tcp synwait-time 5
interface FastEthernet0/0
description LINK_TO_R-Core-1
ip address 192.191.1.2 255.255.255.252
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 priv
duplex auto
speed auto
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet1/0
description LINK_TO_R-Distr-6
ip address 192.191.6.1 255.255.255.252
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 priv
duplex auto
speed auto
interface FastEthernet1/1
description LINK_TO_R-Distr-4
ip address 192.191.5.1 255.255.255.252
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 priv
duplex auto
speed auto
router eigrp 191
network 192.191.1.0 0.0.0.3
network 192.191.5.0 0.0.0.3

```

```

network 192.191.6.0 0.0.0.3
auto-summary
no ip http server
no ip http secure-server
ip access-list standard PERMIT-SNMP
permit 193.191.1.0 0.0.0.255
logging trap warnings
logging 193.191.1.12
snmp-server group SNMP-G v3 priv read SNMP-R
access PERMIT-SNMP
snmp-server view SNMP-R iso included
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 60 0
logging synchronous
transport input ssh
ntp authentication-key 1 md5
12373127020A1F173D24362C 7
ntp authenticate
ntp trusted-key 1
ntp server 193.191.1.1
end

```

```

R-Distr-1#show run
Building configuration...
Current configuration : 1256 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R-Distr-1
boot-start-marker
boot-end-marker
enable secret 5
$1$xXmV$3GFT3jmvChqvVIZOAMEyc1
aaa new-model
aaa session-id common
no ip icmp rate-limit unreachable
ip cef

```

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

```

no ip domain lookup
ip domain name opanasiuk.net
key chain priv
  key 1
    key-string 7 00150403164F12575D72
username admin privilege 15 secret 5
$1$eXCD$WsyYdzGFSYeEHTwQmgwAd/
username user1 secret 5
$1$uEDZ$5MjmjYZ8N1uhf1MEmwKzX0
username user4 privilege 4 secret 5
$1$Y4kO$4OmGbnYjoKGArsasfQXVIO
ip tcp synwait-time 5
interface FastEthernet0/0
  description LINK_TO_LAN-A
  ip address 193.191.2.1 255.255.255.0
  ip ospf authentication message-digest
  duplex auto
  speed auto
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
interface FastEthernet1/0
  description LINK_TO_R-Core-1
  ip address 192.191.2.2 255.255.255.252
  ip ospf authentication message-digest
  duplex auto
  speed auto
interface FastEthernet1/1
  description LINK_TO_R-Distr-2
  ip address 192.191.4.1 255.255.255.252
  ip ospf authentication message-digest
  duplex auto
  speed auto
router ospf 191
  log-adjacency-changes
  network 192.191.2.0 0.0.0.3 area 0
  network 192.191.4.0 0.0.0.3 area 0
  network 193.191.2.0 0.0.0.255 area 0
no ip http server
no ip http secure-server
ip access-list standard PERMIT-SNMP
  permit 193.191.1.0 0.0.0.255
logging trap warnings
logging 193.191.1.12
snmp-server group SNMP-G v3 priv read SNMP-
R access PERMIT-SNMP
snmp-server view SNMP-R iso included
no cdp log mismatch duplex
control-plane
gatekeeper

```

```

shutdown
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  exec-timeout 60 0
  logging synchronous
  transport input ssh
ntp authentication-key 1 md5
12373127020A1F173D24362C 7
ntp authenticate
ntp trusted-key 1
ntp server 193.191.1.1
end

```

```

R-Distr-2#show run
Building configuration...
Current configuration : 1255 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R-Distr-2
boot-start-marker
boot-end-marker
enable secret 5
$1$xXmV$3GFT3jmvChqvVlZOAMEyc1
aaa new-model
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip domain name opanasiuk.net
key chain priv
  key 1
    key-string 7 00150403164F12575D72
username admin privilege 15 secret 5
$1$eXCD$WsyYdzGFSYeEHTwQmgwAd/
username user1 secret 5
$1$uEDZ$5MjmjYZ8N1uhf1MEmwKzX0
username user4 privilege 4 secret 5
$1$Y4kO$4OmGbnYjoKGArsasfQXVIO
ip tcp synwait-time 5
interface FastEthernet0/0
  description LINK_TO_LAN-DNS

```

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ІІЗ	Арк.
		Покотило О.А.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip address 193.191.1.1 255.255.255.0
ip ospf authentication message-digest
duplex auto
speed auto
interface FastEthernet0/1
description LINK_TO_LAN-B
ip address 193.191.3.1 255.255.255.0
ip ospf authentication message-digest
duplex auto
speed auto
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet1/1
description LINK_TO_R-Distr-1
ip address 192.191.4.2 255.255.255.252
ip ospf authentication message-digest
duplex auto
speed auto
router ospf 191
log-adjacency-changes
network 192.191.4.0 0.0.0.3 area 0
network 193.191.1.0 0.0.0.255 area 0
network 193.191.3.0 0.0.0.255 area 0
no ip http server
no ip http secure-server
ip access-list standard PERMIT-SNMP
permit 193.191.1.0 0.0.0.255
logging trap warnings
logging 193.191.1.12
snmp-server group SNMP-G v3 priv read SNMP-
R access PERMIT-SNMP
snmp-server view SNMP-R iso included
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 60 0
logging synchronous

```

```

transport input ssh
ntp authentication-key 1 md5
12373127020A1F173D24362C 7
ntp authenticate
ntp trusted-key 1
ntp server 193.191.1.1
end

R-Distr-3#show run
Building configuration...
Current configuration : 1252 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R-Distr-3
boot-start-marker
boot-end-marker
enable secret 5
$1$xXmV$3GFT3jmvChqvVlZOAMEyc1
aaa new-model
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip domain name opanasiuk.net
key chain priv
key 1
key-string 7 00150403164F12575D72
username admin privilege 15 secret 5
$1$eXCD$WsyYdzGFSYeHTwQmgwAd/
username user1 secret 5
$1$uEDZ$5MjmjYZ8N1uhf1MEmwKzX0
username user4 privilege 4 secret 5
$1$Y4kO$4OmGbnYjoKGArsasfQXVIO
ip tcp synwait-time 5
interface FastEthernet0/0
description LINK_TO_LAN-C
ip address 193.191.4.1 255.255.255.0
ip ospf authentication message-digest
duplex auto
speed auto
interface FastEthernet0/1
description LINK_TO_LAN-D
ip address 193.191.5.1 255.255.255.0
ip ospf authentication message-digest
duplex auto
speed auto
interface FastEthernet1/0
no ip address
shutdown

```

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

```

duplex auto
speed auto
interface FastEthernet1/1
description LINK_TO_R-Core-1
ip address 192.191.3.2 255.255.255.252
ip ospf authentication message-digest
duplex auto
speed auto
router ospf 191
log-adjacency-changes
network 192.191.3.0 0.0.0.3 area 0
network 193.191.4.0 0.0.0.255 area 0
network 193.191.5.0 0.0.0.255 area 0
no ip http server
no ip http secure-server
ip access-list standard PERMIT-SNMP
permit 193.191.1.0 0.0.0.255
logging trap warnings
logging 193.191.1.12
snmp-server group SNMP-G v3 priv read SNMP-
R access PERMIT-SNMP
snmp-server view SNMP-R iso included
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 60 0
logging synchronous
transport input ssh
ntp authentication-key 1 md5
12373127020A1F173D24362C 7
ntp authenticate
ntp trusted-key 1
ntp server 193.191.1.1
end

```

```

R-Distr-4#show run
Building configuration...
Current configuration : 1217 bytes
version 12.4
service timestamps debug datetime msec

```

```

service timestamps log datetime msec
service password-encryption
hostname R-Distr-4
boot-start-marker
boot-end-marker
enable secret 5
$1$xXmV$3GFT3jmvChqvVIZOAMEyc1
aaa new-model
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip domain name opanasiuk.net
key chain priv
key 1
key-string 7 00150403164F12575D72
username admin privilege 15 secret 5
$1$eXCD$WsyYdzGFSYeEHTwQmgwAd/
username user1 secret 5
$1$uEDZ$5MjmjYZ8N1uhf1MEmwKzX0
username user4 privilege 4 secret 5
$1$Y4kO$4OmGbnYjoKGArSasfQXVIO
ip tcp synwait-time 5
interface FastEthernet0/0
description LINK_TO_LAN-E
ip address 193.191.6.1 255.255.255.0
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 priv
duplex auto
speed auto
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet1/0
description LINK_TO_R-Distr-5
ip address 192.191.7.1 255.255.255.252
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 priv
duplex auto
speed auto
interface FastEthernet1/1
description LINK_TO_R-Core-2
ip address 192.191.5.2 255.255.255.252
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 priv
duplex auto
speed auto
router eigrp 191
network 192.191.5.0 0.0.0.3
network 192.191.7.0 0.0.0.3

```

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

```

network 193.191.6.0
auto-summary
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
end

R-Distr-5#show run
Building configuration...
Current configuration : 1204 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R-Distr-5
boot-start-marker
boot-end-marker
enable secret 5
$1$xXmV$3GFT3jmvChqvVIZOAMEyc1
aaa new-model
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip domain name opanasiuk.net
key chain priv
key 1
key-string 7 00150403164F12575D72
username admin privilege 15 secret 5
$1$eXCD$WsyYdzGFSYeEHTwQmgwAd/
username user1 secret 5
$1$uEDZ$5MjnjYZ8N1uhf1MEmwKzX0
username user4 privilege 4 secret 5
$1$Y4kO$4OmGbnYjoKGArsasfQXVI0
ip tcp synwait-time 5
interface FastEthernet0/0
description LINK_TO_LAN-G

```

```

ip address 193.191.8.1 255.255.255.0
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 priv
duplex auto
speed auto
interface FastEthernet0/1
description LINK_TO_LAN-F
ip address 193.191.7.1 255.255.255.0
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 priv
duplex auto
speed auto
interface FastEthernet1/0
description LINK_TO_R-Distr-4
ip address 192.191.7.2 255.255.255.252
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 priv
duplex auto
speed auto
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
router eigrp 191
network 192.191.7.0 0.0.0.3
network 193.191.7.0
network 193.191.8.0
auto-summary
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
end

R-Distr-6#show run
Building configuration...
Current configuration : 1205 bytes

```

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R-Distr-6
boot-start-marker
boot-end-marker
enable secret 5
$1$xXmV$3GFT3jmvChqvVIZOAMEyc1
aaa new-model
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip domain name opanasiuk.net
key chain priv
key 1
key-string 7 00150403164F12575D72
username admin privilege 15 secret 5
$1$eXCD$WsyYdzGFSYeEHTwQmgwAd/
username user1 secret 5
$1$uEDZ$5MjmjYZ8N1uhf1MEmwKzX0
username user4 privilege 4 secret 5
$1$Y4kO$4OmGbnYjoKGArsasfQXVIO
ip tcp synwait-time 5
interface FastEthernet0/0
description LINK_TO_LAN-I
ip address 193.191.10.1 255.255.255.0
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 priv
duplex auto
speed auto
interface FastEthernet0/1
description LINK_TO_LAN-H
ip address 193.191.9.1 255.255.255.0
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 priv
duplex auto
speed auto
interface FastEthernet1/0

```

```

description LINK_TO_R-Core-2
ip address 192.191.6.2 255.255.255.252
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 priv
duplex auto
speed auto
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
router eigrp 191
network 192.191.6.0 0.0.0.3
network 193.191.9.0
network 193.191.10.0
auto-summary
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
end

```

		Опанасюк В.В.			КІК.КР.Б – 125 – 11 – ПЗ	Арк.
		Покотило О.А.				71
Змн.	Арк.	№ докум.	Підпис	Дата		