Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Факультет комп'ютерних наук та технологій
Кафедра комп'ютерних систем та мереж

Пояснювальна записка

до дипломного проєкту (роботи)
магістра
(ступінь вищої освіти)

на тему **СИСТЕМА УПРАВЛІННЯ ІНФРАСТРУКТУРОЮ РОЗПОДІЛЕНИХ МЕРЕЖ ІЗ ЗАСТОСУВАННЯМ ХМАРНИХ СЕРВІСІВ**

Виконав: студент 2 курсу, групи КНТ-513м
спеціальності
123 Комп'ютерна інженерія
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Комп'ютерні системи та мережі

ЦЕЛУЙКО Р. О.
(ПРІЗВИЩЕ та ініціали)
Керівник КИРИЧЕК Г.Г.
(ПРІЗВИЩЕ та ініціали)
Рецензент КОЗІНА Г.Л.
(ПРІЗВИЩЕ та ініціали)

2024

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет Комп'ютерних наук і технологій
Кафедра «Комп'ютерні системи та мережі»
Ступінь вищої освіти магістерський
Спеціальність 123 Комп'ютерна інженерія
(код і найменування)

Освітня програма (спеціалізація) «Комп'ютерні системи та мережі»
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ
Зав. кафедри Кудерметов Р.К.
_____
"____" _____ 2024 року

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

ЦЕЛУЙКО Руслана Олександровича
(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Система управління інфраструктурою розподілених мереж із застосуванням хмарних сервісів
керівник проєкту (роботи) к. т. н., доцент, КИРИЧЕК Галина Григорівна
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)
затверджені наказом вищого навчального закладу від "18" жовтня 2024 року № 149
2. Строк подання студентом проєкту (роботи) 10 грудня 2024 року
3. Вихідні дані до проєкту (роботи) Система управління інфраструктурою розподілених мереж із застосуванням хмарних сервісів. Моделі розподілених мереж, хмарні сервіси. Prometheus, Grafana. Система моніторингу.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз розподілених мереж та їх управління. Хмарні технології в управлінні розподіленими мережами. Реалізація в GNS3 методів моніторингу та автоматизації. Моделювання та порівняння підходів до управління мережею.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-4	КИРИЧЕК Г. Г., доцент		
нормоконтроль	ЩЕРБАК Н.В., ст. викл.		

7. Дата видачі завдання 05.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Огляд літературних джерел за темою роботи	10.10.2024 р.	
2	Аналіз розподілених мереж та їх управління	25.10.2024 р.	
3	Методи управління інфраструктурою розподілених мереж	05.11.2024 р	
4	Хмарні технології в управлінні розподіленими мережами	12.11.2024 р.	
5	Реалізація в GNS3 методів моніторингу та автоматизації	18.11.2024 р.	
6	Моделювання та порівняння підходів до управління мережею	25.11.2024 р.	
7	Оформлення отриманих результатів у ПЗ	30.11.2024 р.	
8	Проходження нормоконтролю	05.12.2024 р.	
9	Оформлення додаткового матеріалу	10.12.2024 р.	

Студент _____ **Руслан ЦЕЛУЙКО**
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ **Галина КИРИЧЕК**
(підпис) (ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

ПЗ: 70 с., 21 рис., 15 табл., 21 джерел

AWS AUTO SCALING, AZURE LOAD BALANCER, PROMETHEUS, GRAFANA, РОЗПОДІЛЕНІ МЕРЕЖІ, ХМАРНІ СЕРВІСИ, ПРИВАТНА ХМАРА, ПУБЛІЧНА ХМАРА, ГІБРИДНА ХМАРА

Мета роботи – впровадження хмарних сервісів для управління інфраструктурою розподілених мереж та їх дослідження, аналіз їх продуктивності, безпеки та масштабованості.

Об’єктом є процес управління інфраструктурою розподілених мереж з інтеграцією хмарних технологій.

Предметом є моделі, методи та інструменти автоматизації, моніторингу, централізованого управління і забезпечення продуктивності системи управління розподіленими мережами.

Програмне забезпечення: Graphical Network Simulator 3, AWS Auto Scaling, Microsoft Visio 2010. Хмарні сервіси: Amazon Web Services, Microsoft Azure, Google Cloud Platform. Системи моніторингу: Grafana, Prometheus.

У роботі описано методи моделювання та управління мережами, реалізацію структурної схеми системи, порівняння приватних, публічних та гібридних хмар, їх переваги і недоліки. Виконано моделювання системи управління розподіленою мережею з верифікацією роботи в різних сценаріях навантаження. Результати досліджень демонструють ефективність застосування хмарних технологій для підвищення продуктивності, безпеки та надійності розподілених мереж.

Результати роботи можуть бути використані для модернізації мережевої інфраструктури підприємств з метою підвищення ефективності управління та зменшення операційних витрат.

ABSTRACT

Explanatory note to the master’s work: 70 p, 21 figures, 15 tables, 21 sources

AWS AUTO SCALING, AZURE LOAD BALANCER, PROMETHEUS, GRAFANA, DISTRIBUTED NETWORKS, CLOUD SERVICES, NETWORK MANAGEMENT, PRIVATE CLOUD, PUBLIC CLOUD, HYBRID CLOUD

The purpose of the work is the implementation of cloud services for managing the infrastructure of distributed networks and their research, analysis of their performance, security and scalability.

The object is the process of managing the infrastructure of distributed networks with the integration of cloud technologies.

The subject is models, methods and tools for automation, monitoring, centralised management and performance assurance of the distributed network management system.

Software: Graphical Network Simulator 3, AWS Auto Scaling, Microsoft Visio 2010. Cloud services: Amazon Web Services, Microsoft Azure, Google Cloud Platform. Monitoring systems: Grafana, Prometheus.

The paper describes the methods of modelling and managing networks, the implementation of the system's structural scheme, the comparison of private, public and hybrid clouds, their advantages and disadvantages. The modelling of the distributed network management system with verification of its operation in different load scenarios is carried out. The research results demonstrate the effectiveness of cloud technologies for improving the performance, security and reliability of distributed networks.

The results of the work can be used to modernise the network infrastructure of enterprises in order to improve management efficiency and reduce operating costs.

ЗМІСТ

ВСТУП

У сучасному світі розвиток технологій, зокрема мережевих рішень, є невід'ємною складовою ефективного функціонування будь-якої організації чи підприємства. Розподілені мережі стають все більш популярними завдяки зростанню обсягів даних та необхідності забезпечення безперебійного доступу до ресурсів з різних географічних локацій. Водночас управління інфраструктурою таких мереж стає дедалі складнішим завданням, що потребує автоматизації та гнучкості.

Хмарні технології пропонують ефективні рішення для управління інфраструктурою розподілених мереж, забезпечуючи централізований контроль, моніторинг та масштабованість. Вони дозволяють значно знизити витрати на підтримку інфраструктури та забезпечують підвищену гнучкість у розгортанні нових послуг.

Метою даної роботи є дослідження системи управління інфраструктурою розподілених мереж із застосуванням хмарних сервісів. Для досягнення цієї мети проведемо аналіз існуючих методів і засобів управління розподіленими мережами, а також порівняння хмарних рішень, що застосовуються у таких системах. Результатом роботи є створення рекомендацій щодо впровадження ефективних хмарних рішень для управління розподіленими мережами.

Наукова новизна роботи полягає у комплексному підході до вивчення та впровадження хмарних сервісів для управління розподіленими мережами, що дозволяє підвищити ефективність та надійність мережевої інфраструктури, знизити операційні витрати та оптимізувати ресурси. Практична цінність роботи полягає у тому, що її результати можуть бути використані при реалізації нових та модернізації існуючих мережевих систем з метою забезпечення їх стабільної та ефективної роботи в умовах зростаючих потреб сучасного бізнесу.

1 АНАЛІЗ РОЗПОДІЛЕНИХ МЕРЕЖ ТА ЇХ УПРАВЛІННЯ

1.1 Поняття та класифікація розподілених мереж

Розподілені мережі є важливою частиною сучасної інфраструктури, оскільки вони дозволяють організаціям забезпечити надійний доступ до ресурсів незалежно від географічного розташування користувачів або вузлів. Поняття розподіленої мережі охоплює систему об'єднаних між собою комп'ютерів або інших пристроїв, які можуть бути розташовані у різних місцях, але при цьому функціонувати як єдина структура для обробки і обміну даними [1].

Ключовою ознакою розподілених мереж є те, що вони не мають єдиного централізованого вузла або сервера, який би контролював усі інші елементи системи. Натомість ресурси мережі розподілені між кількома незалежними пристроями, кожен з яких може виконувати певні функції мережі. Це робить розподілені мережі більш стійкими до збоїв і поломок одного окремого вузла, оскільки інші вузли можуть продовжувати роботу без перерви.

Основні типи розподілених мереж включають:

– локальні обчислювальні мережі (LAN) – мережі, що об’єднують пристрої, які знаходяться на невеликій відстані один від одного, зазвичай у межах однієї будівлі чи комплексу будівель. Локальні мережі зазвичай мають високу швидкість передачі даних та використовуються для з'єднання комп'ютерів, серверів, принтерів та інших пристроїв у межах організації [2];

– глобальні обчислювальні мережі (WAN) – це мережі, що охоплюють великі географічні відстані і з'єднують локальні мережі у різних регіонах або країнах. Глобальні мережі використовуються для передачі даних на великі відстані за допомогою таких технологій, як супутникові канали, оптоволоконні лінії або інші види зв'язку;

– хмарні мережі (Cloud Networks) – це сучасні розподілені мережі, побудовані на основі хмарних технологій. У таких мережах інфраструктура,

платформи та програмне забезпечення розміщені на віддалених серверах і доступні користувачам через Інтернет. Хмарні мережі дозволяють масштабувати ресурси в реальному часі залежно від потреб бізнесу, знижуючи при цьому витрати на підтримку фізичної інфраструктури (рис. 1.1);

– гібридні мережі (Hybrid Networks) – це поєднання різних типів мережевої інфраструктури, які включають локальні, глобальні та хмарні мережі. Гібридні рішення часто використовуються для підвищення гнучкості мережі та забезпечення кращої масштабованості ресурсів, комбінуючи переваги різних технологій (рис. 1.2) [3].

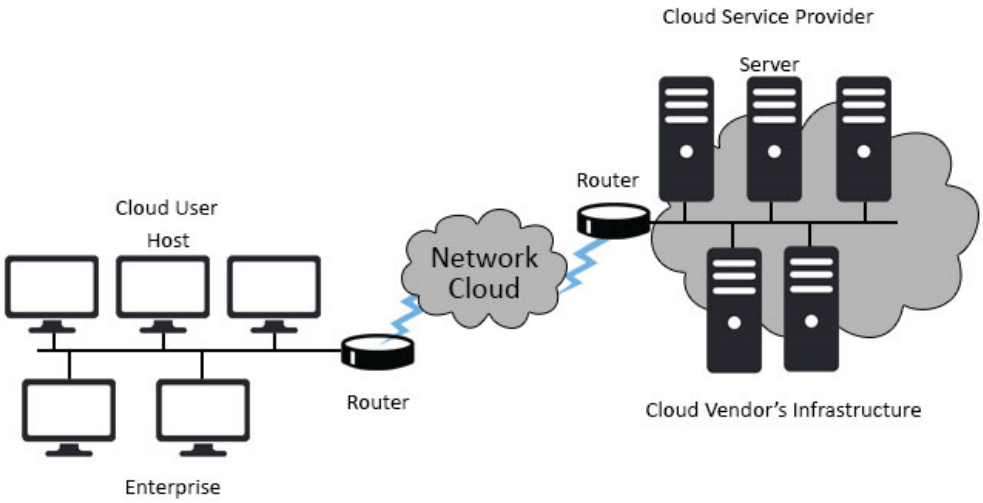

Рисунок 1.1 – Хмарні мережі

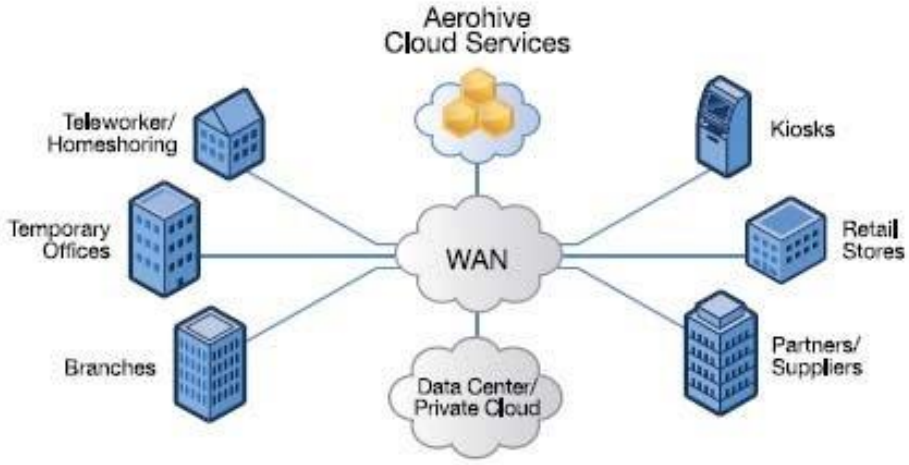

Рисунок 1.2 – Гібридні мережі

Розподілені мережі можна класифікувати за різними критеріями, наприклад, за типом архітектури, за призначенням.

За типом архітектури:

– клієнт-серверні мережі – передбачають наявність серверів, які виконують ключові функції (зберігання даних, обчислення), і клієнтів, що отримують доступ до цих ресурсів. Хоча сервери в таких мережах є важливими вузлами, вони можуть бути дубльовані для забезпечення відмово стійкості;

– пірингові мережі (P2P) – усі вузли рівноправні й можуть виконувати як функції клієнтів, так і серверів. Такі мережі популярні для обміну файлами або децентралізованих обчислень.

За призначенням:

– корпоративні мережі – забезпечують зв’язок між підрозділами компанії, дозволяючи оптимізувати обмін даними, організовувати віддалений доступ співробітників і підтримувати єдиний інформаційний простір;

– публічні мережі – доступні широкому загалу, наприклад, мережі провайдерів Інтернету або публічні точки Wi-Fi;

– спеціалізовані мережі – створюються для вузького кола завдань, таких як управління виробничими процесами, транспортними системами або системами безпеки.

Завдяки своїй різноманітності та масштабованості, розподілені мережі мають широкий спектр застосувань – від локальних офісів і корпоративних середовищ до глобальних комунікаційних систем. Їхнє постійне вдосконалення сприяє створенню нових моделей взаємодії, підвищенню ефективності бізнесу та розвитку сучасного суспільства.

1.2 Методи управління інфраструктурою розподілених мереж

Управління інфраструктурою розподілених мереж є ключовим завданням для забезпечення стабільної та ефективної роботи мережі. З розвитком технологій з’являються нові підходи до адміністрування та моніторингу розподілених систем, що дозволяють не лише підвищити надійність роботи, але й автоматизувати процеси підтримки та обслуговування інфраструктури.

Традиційні методи управління розподіленими мережами зосереджені на централізованому адмініструванні з використанням спеціалізованих апаратних та програмних рішень. Основними функціями традиційного управління є моніторинг, конфігурація обладнання та забезпечення безпеки. Проте, традиційні методи мають обмежену масштабованість і високу вартість обслуговування фізичної інфраструктури, що є значним викликом для великих підприємств із розподіленими ресурсами.

Сучасні автоматизовані системи управління спрощують адміністрування мережевих ресурсів через автоматизацію рутинних процесів. Такі системи забезпечують автоматичне налаштування пристроїв, інтеграцію з інструментами моніторингу та оркестрацію мережевих процесів, що підвищує ефективність управління. Однак автоматизовані рішення вимагають значних початкових інвестицій і складного налаштування.

Хмарні сервіси, як-от AWS, Microsoft Azure та Google Cloud Platform, пропонують гнучкі та масштабовані рішення для управління інфраструктурою мереж, дозволяючи централізовано адмініструвати мережеві ресурси незалежно від їх географічного розташування. Такі рішення є економічними, проте залежність від хмарного провайдера та ризики з безпекою даних є значними факторами, що можуть вплинути на їх вибір [8].

Методи управління на основі політик дозволяють автоматизувати контроль за мережевими ресурсами, використовуючи заздалегідь визначені правила (політики). Це значно спрощує адміністрування та знижує ризики помилок,

викликаних людським фактором, але потребує детального налаштування [14].

Порівняння методів управління інфраструктурою розподілених мереж представлено в таблиці 1.1.

Таблиця 1.1 – Порівняння методів управління інфраструктурою розподілених мереж

Метод управління	Переваги	Недоліки	Приклади
Традиційні методи	Висока надійність фізичної інфраструктури	Висока вартість обслуговування, обмежена масштабованість	Фізичні сервери, мережеві комутатори
Автоматизовані системи	Автоматизація рутинних завдань, ефективне управління великими мережами	Значні початкові інвестиції, складність налаштувань	Cisco DNA Center, SolarWinds
Хмарні сервіси	Гнучкість, масштабованість, зниження витрат на фізичну інфраструктуру	Залежність від хмарного провайдера, питання безпеки даних	AWS, Microsoft Azure, Google Cloud Platform
Методи на основі політик	Спрощення адміністрування, автоматичне застосування правил	Необхідність детального налаштування політик, складність у великих системах	Policy-Based Management системи, такі як VMware NSX, Juniper Contrail

Методи управління інфраструктурою розподілених мереж варіюються залежно від потреб організації. Традиційні методи забезпечують стабільність, але їх масштабованість обмежена. Автоматизовані системи спрощують адміністрування, проте потребують значних інвестицій. Хмарні рішення є більш гнучкими та масштабованими, але залежність від хмарних провайдерів вимагає додаткових заходів безпеки. Управління на основі політик дозволяє ефективно контролювати доступ та безпеку, проте потребує детального налаштування для роботи у великих мережах [7].

1.3 Переваги та виклики використання розподілених мереж

Розподілені мережі стали невід’ємною частиною сучасного світу завдяки своїй здатності забезпечувати високу надійність, гнучкість і масштабованість. Проте їх використання супроводжується певними викликами, які організаціям необхідно враховувати.

Переваги розподілених мереж:

– висока надійність і відмовостійкість – Завдяки розподіленій природі мережі, відмова одного або кількох вузлів не призводить до повного виходу з ладу системи. Це особливо важливо для критичних інфраструктур, таких як банківські системи або мережі охорони здоров'я;

– масштабованість – Розподілені мережі дозволяють легко додавати нові вузли, підвищуючи обчислювальні ресурси або розширюючи географічне покриття. Ця властивість робить їх придатними для організацій, що активно розвиваються;

– гнучкість у виборі технологій – Розподілена мережа може включати різні типи інфраструктури: локальні мережі, хмарні сервіси, мобільні пристрої тощо. Це дозволяє організаціям використовувати найбільш підходящі технології для кожного окремого випадку;

– економічна ефективність – Використання хмарних сервісів у розподілених мережах дозволяє значно знижувати витрати на придбання, обслуговування та модернізацію фізичної інфраструктури [8].

Виклики розподілених мереж:

– ускладнення управління – Розподілені мережі потребують ефективних систем управління, щоб забезпечити злагоджену роботу різних компонентів. Це може вимагати значних зусиль для налаштування та моніторингу;

– проблеми з безпекою – Розподілені мережі є більш вразливими до кіберзагроз, оскільки включають багато точок доступу. Захист даних у таких

мережах вимагає впровадження складних рішень, таких як шифрування, багатофакторна автентифікація та виявлення аномалій;

– залежність від мережевої інфраструктури – Ефективність розподілених мереж залежить від якості зв’язку між вузлами. Проблеми з пропускною здатністю або надійністю мережевих каналів можуть вплинути на продуктивність системи;

– високі початкові витрати – Незважаючи на економію у довгостроковій перспективі, розподілені мережі можуть вимагати значних інвестицій на етапі впровадження, особливо для автоматизації управління [5].

З огляду на постійне зростання обсягів даних і потребу в більшій продуктивності, розподілені мережі залишаються ключовим напрямком розвитку. До перспективних технологій належать:

– 5G-мережі, які забезпечують низьку затримку і високу пропускну здатність;

– технології edge computing, що дозволяють обробляти дані ближче до джерела їх створення;

– автономні мережі, які використовують штучний інтелект для автоматизації процесів управління та моніторингу.

Штучний інтелект (AI) та машинне навчання (ML) відкривають нові можливості для управління розподіленими мережами. Наприклад, AI дозволяє автоматизувати процеси моніторингу та діагностики мереж, прогнозувати потенційні збої та виявляти аномалії у реальному часі. ML-алгоритми допомагають оптимізувати розподіл ресурсів, підвищуючи продуктивність мережі [14].

Таблиця 1.2 показує основні застосування AI у розподілених мережах.

Таблиця 1.2 – Основні застосування AI у розподілених мережах

Застосування AI	Переваги	Приклади
Автоматичний моніторинг	Зниження ручного втручання, швидке виявлення проблем	Cisco AI Endpoint Analytics
Управління трафіком	Оптимізація пропускної здатності	Google Traffic Management
Захист від кібератак	Швидке виявлення загроз	Darktrace AI

Технологія 5G забезпечує значно вищу швидкість передачі даних, низьку затримку та можливість підключення великої кількості пристроїв. Це дозволяє створювати розподілені мережі з високою пропускною здатністю, які можуть підтримувати застосунки на основі Інтернету речей (IoT), таких як розумні міста та автономні транспортні системи [19].

Рисунок 1.3 ілюструє можливості 5G у розподілених мережах.

Рисунок 1.3 – Можливості 5G у розподілених мережах

Хмарні обчислення (Cloud Computing) залишаються основою для багатьох розподілених мереж. Водночас зростає популярність периферійних обчислень, які передбачають обробку даних ближче до місця їхнього створення. Це дозволяє зменшити затримки, підвищити швидкість обробки даних і зменшити навантаження на центральні сервери.

Таблиця 1.3 порівнює хмарні та периферійні обчислення.

Таблиця 1.3 – Хмарні та периферійні обчислення

Параметр	Хмарні обчислення	Периферійні обчислення
Локація обробки даних	Віддалені сервери	Локально, на пристроях
Затримка	Вище	Нижче
Надійність	Залежить від провайдера	Вища при локальному використанні
Масштабованість	Висока	Обмежена

Технології розподілених реєстрів, такі як блокчейн, змінюють підхід до забезпечення безпеки та довіри у розподілених мережах. Блокчейн дозволяє створювати децентралізовані системи, у яких усі транзакції є прозорими й незмінними. Це робить блокчейн привабливим для використання в IoT-мережах, фінансових системах і платформах керування доступом.

Основні переваги блокчейну у розподілених мережах:

– безпека: дані захищені криптографією;

– прозорість: усі транзакції доступні для перегляду;

– стійкість до збоїв: децентралізована архітектура.

Програмно-визначені мережі (SDN) забезпечують централізоване управління мережею через програмні інтерфейси. Це дозволяє швидко адаптувати мережеву інфраструктуру до змін у робочих навантаженнях і вимогах бізнесу. SDN також сприяють підвищенню рівня автоматизації управління мережею.

Розвиток сучасних технологій — таких як AI, 5G, блокчейн, периферійні обчислення та SDN — сприяє підвищенню ефективності управління розподіленими мережами. Вибір конкретних технологій залежить від специфічних потреб організації, її масштабів і доступних ресурсів [12].

Запропоновані напрями розвитку сприятимуть підвищенню ефективності розподілених мереж та їх адаптації до нових викликів.

1.4 Модель системи управління інфраструктурою розподілених мереж

Управління інфраструктурою розподілених мереж із застосуванням хмарних сервісів є сучасним підходом, що забезпечує гнучкість, масштабованість і високу ефективність управління ресурсами. Використання хмарних платформ, таких як Amazon Web Services (AWS), Microsoft Azure, або Google Cloud Platform (GCP), дозволяє централізовано контролювати мережеві ресурси та автоматизувати критично важливі операції в масштабі. Модель системи управління побудована навколо трьох ключових компонентів: хмарних платформ, інструментів моніторингу та мережевих вузлів [6].

Хмарні платформи – це ключовий компонент системи, що забезпечує надання послуг управління інфраструктурою. Завдяки можливості динамічно виділяти та масштабувати ресурси залежно від навантаження, хмарні сервіси забезпечують гнучкість управління розподіленими мережами. Основні функції хмарних платформ включають:

– масштабування: автоматичне збільшення або зменшення ресурсів, що надаються для мережі, залежно від навантаження;

– автоматизоване управління: хмарні сервіси автоматизують більшість процесів, зокрема резервне копіювання, налаштування пристроїв та обробку трафіку;

– безпека: хмарні платформи забезпечують високий рівень безпеки, зокрема шифрування даних, управління політиками безпеки [12].

Інструменти моніторингу – це програмні рішення, які забезпечують контроль за роботою мережевої інфраструктури в режимі реального часу. Вони інтегруються з хмарними сервісами, дозволяючи аналізувати стан вузлів, виявляти збої та проводити аналітику. Найбільш популярні інструменти, які використовуються разом із хмарними платформами, включають:

– prometheus для збору метрик і моніторингу;

– grafana для візуалізації даних;
– nagios для моніторингу стану вузлів та пристроїв [17].

Мережеві вузли – це фізичні або віртуальні сервери, які є основними компонентами інфраструктури. Вони виконують основні функції обробки даних та взаємодії з іншими вузлами через хмарну інфраструктуру. Мережеві вузли можуть бути розміщені в різних географічних точках, але їх управління централізовано здійснюється через хмарні сервіси.

Модель системи управління розподіленими мережами за допомогою хмарних сервісів побудована навколо взаємодії між мережевими вузлами, хмарною платформою та інструментами моніторингу (рис. 1.3). Кожен вузол надсилає свої дані в хмару для обробки та аналізу, а адміністратор має змогу в режимі реального часу спостерігати за станом інфраструктури через інструменти моніторингу [18].

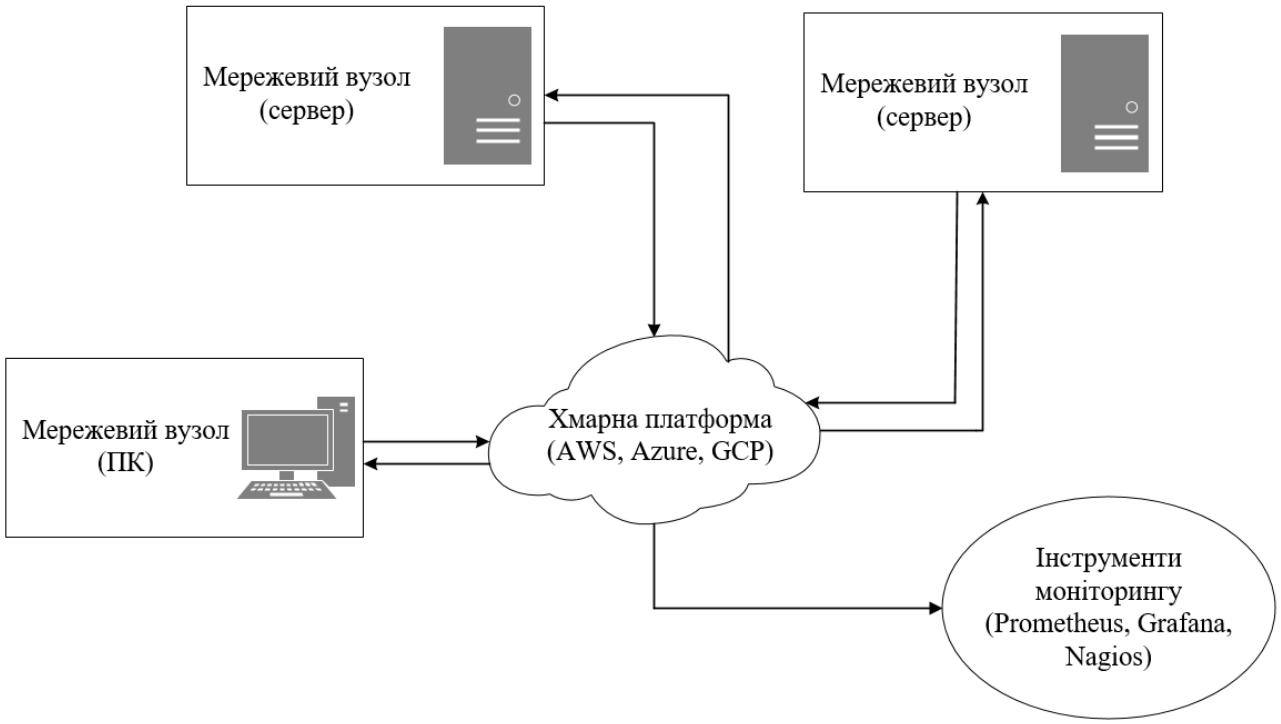

Рисунок 1.3 – Модель системи управління розподіленими мережами за допомогою хмарних сервісів

Взаємодія компонентів:

– відправка даних: мережеві вузли відправляють дані про стан системи (пропускна здатність, помилки, завантаження ресурсів) у хмарну платформу;

– обробка даних: хмарні сервіси аналізують отриману інформацію та приймають рішення про необхідність масштабування ресурсів або запуску резервних процесів;

– моніторинг: інструменти моніторингу в реальному часі збирають та візуалізують дані, надаючи адміністраторам детальний огляд поточного стану мережі та можливі відхилення.

1.5 Постановка завдань проведення досліджень

Впровадження системи управління інфраструктурою розподілених мереж із застосуванням хмарних сервісів вимагає комплексного підходу до вирішення низки завдань, пов'язаних із забезпеченням ефективного управління, безпеки та масштабованості мережі. На основі проведеного аналізу предметної області та характеристик розподілених мереж, визначено ключові задачі, які необхідно вирішити під час виконання цього проєкту:

– проведення аналізу архітектури розподіленої мережі та визначення вимог до хмарних сервісів, які використаються в інтеграції для управління інфраструктурою;

– реалізація моделі управління, що враховує різнорідність мережевих компонентів (сервери, маршрутизатори, кінцеві пристрої) та використання хмарних платформ;

– вибір і впровадження ефективних методів моніторингу та аналізу трафіку в реальному часі, що дозволило забезпечити своєчасне виявлення аномалій у роботі мережі;

– інтеграція хмарних сервісів для автоматизації процесів управління ресурсами мережі та забезпечення можливості централізованого контролю над її елементами;

– реалізація структурної схеми системи управління мережею, що включає опис компонентів мережевої інфраструктури та хмарної платформи, а також їх взаємодію;

– моделювання та верифікація розробленої системи з використанням спеціалізованого програмного забезпечення для симуляції та тестування;

– проведення порівняння альтернативних підходів до впровадження хмарних сервісів у процес управління мережею, зокрема використання приватної та публічної хмари.

Ці завдання охоплюють усі етапи впровадження від аналізу архітектури мережі до впровадження та тестування системи управління. У результаті розроблено функціональну систему управління розподіленою мережею з можливістю інтеграції хмарних сервісів, яка забезпечує надійність, гнучкість та масштабованість мережевої інфраструктури [14].

2 ХМАРНІ ТЕХНОЛОГІЇ В УПРАВЛІННІ РОЗПОДІЛЕНИМИ МЕРЕЖАМИ

2.1 Огляд хмарних рішень для управління мережею

З розвитком сучасних технологій хмарні рішення для управління мережевою інфраструктурою стали одним з основних інструментів для забезпечення ефективності, гнучкості та масштабованості мереж. Хмарні сервіси пропонують централізоване управління та моніторинг мережі, що особливо важливо для розподілених мереж, де обробка даних та управління відбуваються

через численні географічно віддалені точки. Основні хмарні рішення, які використовуються для управління мережами, можна класифікувати за їх функціональністю та типом реалізації [20].

Хмарні рішення для управління мережею включають різноманітні послуги та продукти, які надають як приватні компанії, так і провайдери публічних хмарних платформ. Основні типи хмарних рішень можна розділити на кілька категорій:

– software as a Service (SaaS): Цей підхід передбачає використання програмного забезпечення для управління мережею через хмарну платформу без необхідності інсталяції програмних додатків на локальні сервери. Прикладом є Cisco Meraki, яка надає рішення для централізованого управління мережею через веб-інтерфейс;

– platform as a Service (PaaS): Цей підхід надає розробникам інструменти для створення кастомних додатків управління мережею на основі хмарних платформ. Google Cloud та Amazon Web Services (AWS) надають подібні рішення, які дозволяють інтегрувати мережеве управління у існуючі хмарні архітектури;

– infrastructure as a Service (IaaS): Ця модель забезпечує віртуалізацію інфраструктури, що включає сервери, мережеві пристрої та сховища даних. Прикладом є Microsoft Azure, де користувачі можуть створювати віртуальні приватні мережі (VPN) та керувати інфраструктурою на основі хмарної платформи.

Схема, що показує три рівні сервісів із прикладами. SaaS — на верхньому рівні (Cisco Meraki), PaaS — середній рівень (Google App Engine), IaaS — базовий рівень (Azure Virtual Machines) представлена на рисунку 2.1 [19].

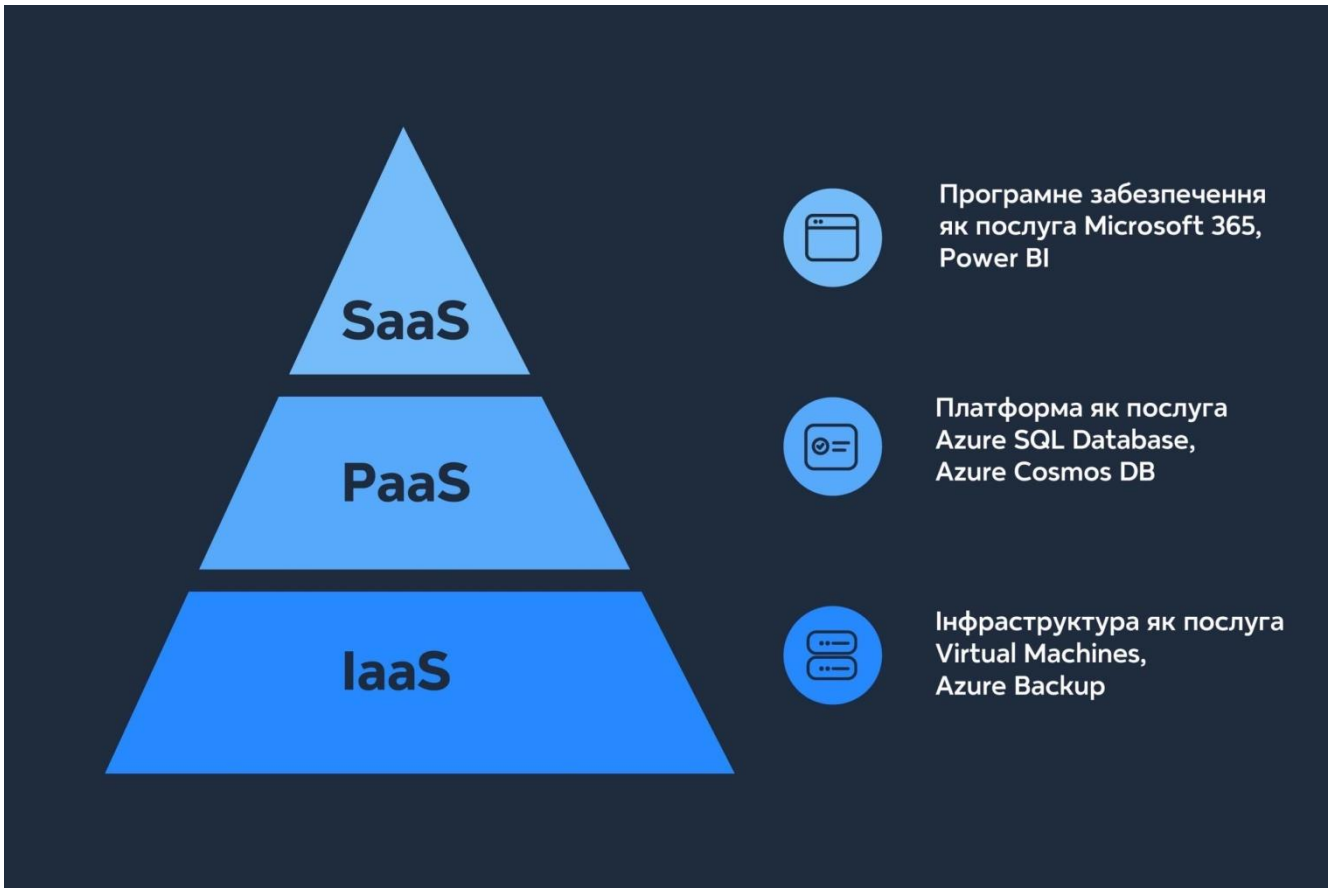

Рисунок 2.1 – Схема класифікації хмарних рішень

Хмарні рішення для управління мережею надають низку функцій, які дозволяють спростити роботу адміністратора та підвищити ефективність мережевих процесів. Основні з них включають:

– централізоване управління: хмарні сервіси надають єдину точку доступу до управління всією мережею, незалежно від її фізичного розташування. Це дозволяє адміністраторам оперативно вносити зміни та контролювати роботу мережі з будь-якої точки світу;

– моніторинг і аналітика: хмарні рішення дозволяють здійснювати моніторинг мережі в реальному часі, надаючи детальні дані про використання ресурсів, пропускну здатність, навантаження на мережу та виявлення аномалій. Наприклад, SolarWinds та Zabbix надають хмарні платформи для мережевого моніторингу;

– автоматизація управління: хмарні платформи дозволяють автоматизувати багато завдань управління, таких як конфігурування нових мережевих пристроїв, балансування навантаження або резервне копіювання даних;

– безпека: хмарні рішення забезпечують високий рівень безпеки через впровадження сучасних механізмів шифрування, управління доступом та двофакторної автентифікації [16].

На рисунку 2.2 показано використання хмарних рішень у різних галузях, де найбільше їх застосування спостерігається в IT і телекомунікаціях, що пояснюється необхідністю забезпечення масштабованості та швидкого розгортання інфраструктури.

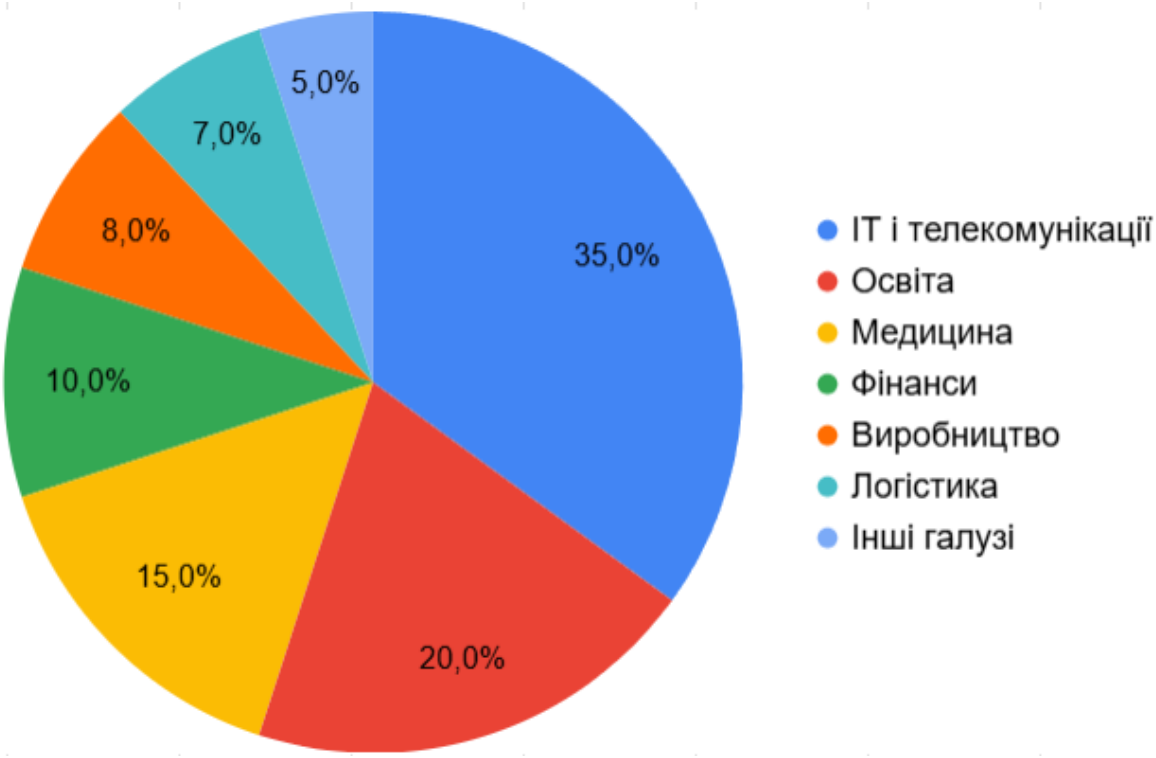

Рисунок 2.2 – Використання хмарних рішень у різних галузях

Згідно з дослідженням Gartner, до 2025 року кількість пристроїв IoT зросте до 75 мільярдів. Це створює великий обсяг даних, які потрібно обробляти, зберігати та аналізувати. Хмарні рішення стають необхідністю для управління

такими даними через їхню здатність до масштабування.

Збільшення обсягу корпоративних даних (Big Data) потребує платформ для аналізу та зберігання. IDC прогнозує, що до 2026 року глобальний обсяг даних зросте до 221 зетабайта. Хмарні сервіси, такі як Google BigQuery або Azure Data Lake, надають інструменти для роботи з такими даними.

Пандемія COVID-19 прискорила перехід багатьох компаній до віддаленої або гібридної роботи. Це зумовило потребу в безпечних і масштабованих рішеннях для управління мережами. Згідно з Statista, до 2024 року 45% компаній використовуватимуть гібридні робочі моделі, що сприяє зростанню попиту на хмарні сервіси, такі як Microsoft Azure Virtual Desktop [18].

Організації все частіше стикаються з регуляторними вимогами щодо захисту даних (наприклад, GDPR у ЄС). Хмарні платформи пропонують інтегровані механізми захисту, такі як шифрування, управління доступом та моніторинг безпеки в реальному часі. Наприклад, Cisco SecureX забезпечує комплексну безпеку для хмарних інфраструктур [7].

Експерти прогнозують, що до 2030 року хмарні рішення стануть стандартом для 90% корпоративних мережевих інфраструктур. Це зумовлено глобальною діджиталізацією та необхідністю забезпечення стійкості мереж під час кризових ситуацій [5].

Таким чином, хмарні рішення є важливим інструментом для ефективного управління мережею, а їх вибір повинен ґрунтуватися на специфічних потребах організації.

2.2 Переваги та недоліки хмарних рішень

Хмарні рішення для управління мережею стали популярним вибором серед компаній та організацій завдяки їх численним перевагам. Однак поряд з очевидними вигодами, ці рішення також мають певні недоліки, які можуть

обмежувати їх використання в деяких сценаріях. У цьому підрозділі розглянемо детально основні переваги та недоліки хмарних рішень у контексті управління мережею.

Переваги:

– гнучкість. Хмарні платформи дозволяють легко адаптувати інфраструктуру до змінних потреб бізнесу. Можна швидко збільшувати або зменшувати ресурси, не потребуючи нових апаратних інвестицій чи складних налаштувань. Це особливо корисно для компаній, які переживають періоди швидкого зростання або мають змінні навантаження;

– масштабованість. Хмарні рішення дозволяють легко масштабувати інфраструктуру у відповідності до поточних вимог. Організації можуть збільшувати потужності, не турбуючись про фізичні обмеження серверів, що забезпечує стійкість мережі під час пікових навантажень;

– економія витрат. Використання хмарних рішень дозволяє знизити витрати на придбання та обслуговування фізичних серверів, а також на зарплату персоналу, що займається їхнім обслуговуванням. Оплата за хмарні послуги здійснюється за фактом використання, що дає можливість зменшити витрати в низькозавантажені періоди;

– централізоване управління. Управління всіма мережевими компонентами здійснюється через єдиний інтерфейс, що спрощує адміністрування великих мережевих інфраструктур. Це також знижує складність інтеграції нових елементів мережі або їхньої зміни;

– інтеграція нових сервісів. Хмарні платформи полегшують додавання нових функцій і сервісів, таких як аналітика, без додаткових інвестицій в інфраструктуру. Це дозволяє компаніям швидко впроваджувати інновації і залишатися конкурентоспроможними.

Недоліки:

– залежність від Інтернет-з'єднання Оскільки всі процеси управління мережею в хмарі відбуваються через Інтернет, якість роботи залежить від

стабільності та швидкості інтернет-з'єднання. У разі перебоїв або низької швидкості з'єднання можливі затримки у роботі мережі та проблеми з доступом до критичних даних;

– проблеми з безпекою Однією з основних проблем використання хмарних рішень є безпека даних. Хоча провайдери хмарних сервісів пропонують різні механізми захисту, включаючи шифрування та аутентифікацію, завжди існує ризик кібератак або втрати даних. Також деякі організації можуть мати обмеження щодо зберігання конфіденційних даних у хмарі через регуляторні вимоги;

– обмеження в адаптації Не всі хмарні рішення можуть повністю відповідати специфічним потребам організації. Наприклад, деякі компанії можуть мати унікальні процеси або вимоги до інфраструктури, які важко налаштувати в межах стандартних хмарних платформ. Це може призводити до необхідності кастомізації або додаткових витрат на інтеграцію;

– потенційна залежність від постачальника (vendor lock-in) Використання певних хмарних платформ може призвести до так званого "vendor lock-in", коли організація стає залежною від одного провайдера послуг і не може легко перенести свої дані або сервіси на іншу платформу. Це обмежує гнучкість компанії у виборі кращих рішень у майбутньому;

– затримки через географічне розташування Оскільки хмарні ресурси можуть бути розташовані у віддалених дата-центрах, передача даних між ними може викликати затримки, особливо якщо мережа розподілена по різних країнах або континентах.

У таблиці 2.1 наведено порівняння переваг і недоліків хмарних рішень за основними критеріями ефективності.

Таблиця 2.1 – Порівняння переваг та недоліків хмарних рішень

Критерій	Переваги	Недоліки
Гнучкість	Легке адаптування до змін бізнесу та зростання навантаження.	Не всі платформи можуть бути адаптовані до унікальних вимог організації.
Масштабованість	Швидке розширення або скорочення ресурсів без інвестицій в обладнання.	Затримки через географічне розташування ресурсів.
Вартість	Оплата за фактичне використання ресурсів, зменшення витрат на обслуговування.	Можливі високі витрати для масштабних і тривалих проєктів.
Централізоване управління	Єдиний інтерфейс управління всією мережею, незалежно від її розташування.	Залежність від Інтернет-з'єднання для доступу до управління.
Безпека	Сучасні механізми шифрування та багатофакторної автентифікації.	Ризик кібератак, регуляторні обмеження на обробку даних у хмарі.

Загалом хмарні рішення надають безліч переваг, що роблять їх привабливими для багатьох організацій, особливо з огляду на їх гнучкість, масштабованість та економічність [11].

2.3 Порівняння хмарних платформ для управління розподіленими мережами

Порівняння хмарних платформ для управління розподіленими мережами є важливим етапом для вибору оптимального рішення, яке відповідає специфічним потребам організації. Вибір хмарної платформи ґрунтується на низці критеріїв, серед яких вартість, функціональність, рівень безпеки, інтеграція з іншими сервісами, масштабованість та продуктивність. У таблиці 2.2 порівняємо найпопулярніші платформи: Amazon Web Services (AWS), Google Cloud Platform (GCP) та Microsoft Azure, з точки зору їхньої придатності для управління інфраструктурою розподілених мереж [10].

Таблиця 2.2 – Порівняння хмарних платформ

Критерій	AWS	Google Cloud Platform (GCP)	Microsoft Azure
Масштабованість	Висока, підтримка великих розподілених систем	Висока, ефективна обробка даних	Висока, особливо у поєднанні з локальними системами
Функціональність	Найбільший набір інструментів для розробників	Спеціалізація на обробці даних та AI	Інтеграція з корпоративними рішеннями Microsoft
Інтеграція	Інтеграція з численними сервісами AWS	Тісна інтеграція з AI та аналітичними сервісами Google	Глибока інтеграція з продуктами Microsoft (Windows, Active Directory)
Безпека	Високий рівень безпеки, сертифікації ISO	Високий рівень шифрування даних та AI-рішення	Високий рівень безпеки, відповідність численним стандартам
Вартість	Дорого при великих обсягах трафіку	Прозорі тарифи, нижчі витрати для малого та середнього бізнесу	Високі витрати на ліцензії для великих підприємств
Гнучкість	Висока, адаптивність до будь-яких вимог	Гнучка, особливо для обробки великих обсягів даних	Висока, особливо для гібридних рішень
Користувацький досвід	Складний для новачків, але потужний для досвідчених користувачів	Зручний для обробки даних, простий у використанні	Інтуїтивно зрозумілий для користувачів продуктів Microsoft
Гібридні рішення	Обмежені можливості	Менше можливостей для гібридних рішень	Широкі можливості для гібридних мереж

Після аналізу основних хмарних платформ стає очевидним, що кожна з них має свої переваги та недоліки залежно від конкретних потреб організації. Amazon Web Services (AWS) є лідером ринку завдяки своїй широкій функціональності, гнучкості та надійності, що робить його ідеальним для великих корпорацій та складних інфраструктур. Google Cloud Platform (GCP) вирізняється своєю ефективністю в обробці великих обсягів даних і інтеграцією з рішеннями штучного інтелекту, що робить його привабливим для компаній, орієнтованих на аналітику та обробку даних. Microsoft Azure, у свою чергу, є найкращим вибором для компаній, що вже використовують продукти Microsoft та потребують гібридних рішень для управління як хмарною, так і локальною інфраструктурою [12].

На ринку хмарних рішень три основні платформи — Amazon Web Services (AWS), Google Cloud Platform (GCP) і Microsoft Azure — займають лідерські позиції, пропонуючи широкий набір інструментів і сервісів для управління розподіленими мережами.

Популярність кожної з платформ значною мірою залежить від галузі застосування:

– AWS активно використовується у сфері електронної комерції, стрімінгових сервісів і фінансових технологій завдяки своїй надійності та масштабованості;

– GCP часто обирають для проєктів, пов’язаних із великими даними, аналітикою та штучним інтелектом;

– Azure є фаворитом серед корпоративних користувачів, які вже інтегрували свої системи з продуктами Microsoft.

На рисунку 2.3 показано розподіл популярності хмарних платформ за відсотковою часткою використання в різних галузях.

Рисунок 2.3 – Розподіл популярності хмарних платформ серед різних галузей

Загалом, вибір платформи для управління розподіленими мережами залежить від вимог щодо масштабованості, рівня безпеки, вартості та інтеграції з іншими сервісами. Платформи пропонують широкий набір інструментів, однак оптимальним рішенням є те, що максимально відповідає конкретним задачам бізнесу та технічним потребам мережі [14].

2.4 Інтеграція хмарних рішень з існуючою інфраструктурою

Інтеграція хмарних платформ із наявною інфраструктурою підприємств є одним із ключових аспектів впровадження сучасних технологій. Вона забезпечує ефективність управління мережею, спрощує адміністрування та сприяє підвищенню продуктивності за рахунок оптимального використання ресурсів. Цей процес включає як технічні, так і організаційні заходи для поєднання локальних і хмарних ресурсів.

Інтеграція хмарних рішень із наявною інфраструктурою може здійснюватися за кількома моделями, кожна з яких має свої особливості, переваги та недоліки. Обрання оптимальної моделі залежить від специфічних потреб організації, доступного бюджету та рівня критичності даних. Розглянемо детальніше кожну модель.

Гібридна модель інтеграції об’єднує переваги приватних і публічних хмарних рішень. Вона передбачає, що конфіденційні дані та критичні бізнес-процеси залишаються в межах приватної інфраструктури, тоді як публічна хмара використовується для масштабованих обчислень або тимчасових завдань.

Переваги:

– забезпечує високий рівень безпеки для чутливих даних;

– гнучкість: можна використовувати ресурси публічної хмари у разі пікових навантажень;

– підтримка сучасних сервісів, таких як аналітика або AI, які часто доступні в публічних хмарах.

Недоліки:

– складність інтеграції двох різних середовищ;

– високі витрати на підтримку приватної хмари.

Банк використовує приватну хмару для зберігання даних клієнтів і публічну хмару для аналізу транзакцій у реальному часі.

Повна міграція в хмару передбачає перенесення всієї інфраструктури до публічної хмари. Він ідеально підходить для стартапів або компаній, які не мають ресурсів для підтримки локальної інфраструктури.

Переваги:

– висока масштабованість та адаптивність до змін навантаження;

– низькі витрати на початкове розгортання;

– швидкий доступ до передових технологій.

Недоліки:

– залежність від постачальника хмарних послуг;

– ризики безпеки та конфіденційності даних.

Netflix використовує Amazon Web Services (AWS) для повної підтримки своєї стрімінгової платформи, що дозволяє швидко масштабувати сервери під час пікових навантажень.

Локальна інтеграція з використанням хмарних функцій – у цьому випадку вся основна інфраструктура залишається локальною, а хмарні сервіси використовуються для додаткових функцій, таких як резервне копіювання, обробка великих даних або тестування нових додатків.

Переваги:

– максимальний контроль над основними даними та процесами;

– можливість використовувати хмарні сервіси тільки за потреби;

– зниження витрат на хмарні обчислення.

Недоліки:

– обмежені можливості масштабування;

– високі витрати на підтримку локальної інфраструктури.

Медіакомпанія зберігає весь відеоконтент на локальних серверах, але використовує Google Cloud для створення резервних копій та обробки відео.

Таблиця 2.3 демонструє порівняння основних моделей інтеграції за ключовими критеріями.

Таблиця 2.3 – Порівняння моделей інтеграції хмарних рішень

Критерій	Гібридна модель	Повна міграція в хмару	Локальна інтеграція з хмарою
Безпека	Висока, дані залишаються у приватній інфраструктурі.	Залежить від постачальника.	Максимальний контроль над даними.
Масштабованість	Висока, за рахунок публічної хмари.	Дуже висока, обмежень немає.	Обмежена локальними ресурсами.
Вартість	Висока (підтримка двох середовищ).	Відносно низька, особливо для стартапів.	Висока через витрати на локальну інфраструктуру.
Гнучкість	Дуже висока.	Висока, але залежність від хмарного провайдера.	Помірна, локальні ресурси потребують оновлення.
Складність впровадження	Висока, інтеграція приватної та публічної хмари.	Низька, повна передача відповідальності провайдеру.	Середня, потребує налаштування інтеграцій.
Основні галузі	Банківська сфера, державні установи.	Стартапи, медіа, електронна комерція.	Інженерія, виробництво, освіта.
Приклади використання	NASA, банківські установи.	Netflix, Dropbox.	Медіакомпанії, локальні освітні установи.

Залежно від потреб організацій, різні моделі інтеграції хмарних рішень мають різну популярність у галузях, що використовують хмарні сервіси. Аналіз ринку показує, що кожна модель має свою нішу і використовується для вирішення певних задач.

Загальні тенденції популярності:

– гібридна модель є найпоширенішою серед середніх і великих організацій. Згідно з дослідженням Gartner (2024), 82% компаній у сфері фінансів та державного сектору обирають гібридну модель через високий рівень безпеки даних;

– повна міграція в хмару найбільш популярна серед стартапів і компаній, які потребують швидкого масштабування. Зокрема, близько 65% технологічних стартапів у 2023 році здійснили повну міграцію до публічних хмар (згідно з даними Statista);

– локальна інтеграція з використанням хмарних функцій використовується організаціями, які прагнуть зберегти контроль над основними ресурсами, але використовують хмари для специфічних задач. Це особливо актуально для галузей, таких як виробництво або освіта, де інфраструктура тісно пов’язана з локальними системами.

Згідно з дослідженнями, популярність різних моделей інтеграції хмарних рішень змінюється в залежності від галузі. На рисунку 2.4 показано відсотковий розподіл популярності моделей інтеграції за галузями, де фінансовий сектор найчастіше використовує гібридну модель, а стартапи обирають повну міграцію в хмару через потребу в масштабованості.

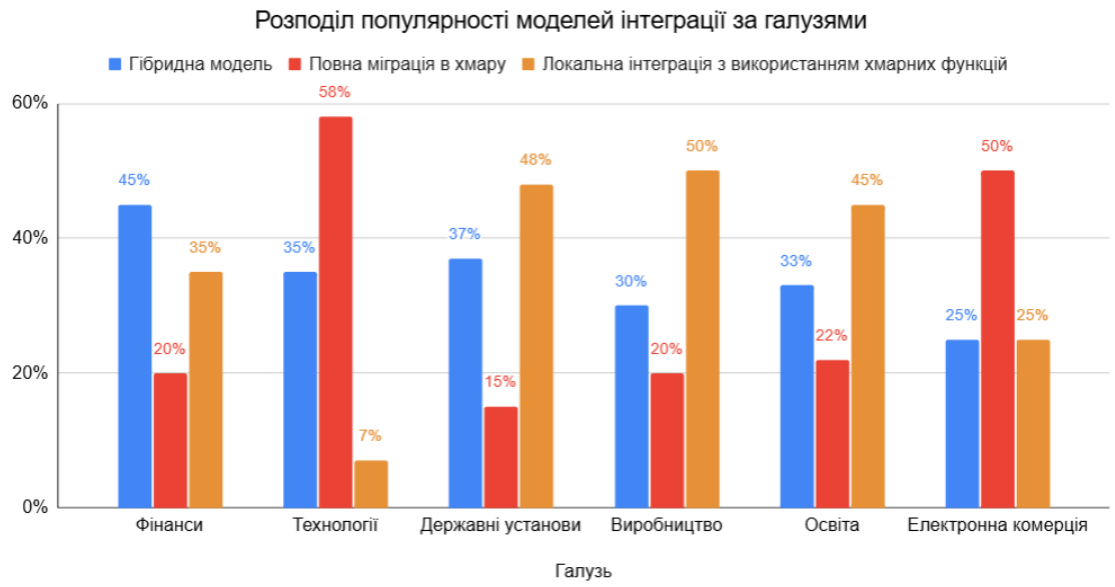

Рисунок 2.4 – Розподіл популярності моделей інтеграції за галузями

Популярність гібридних рішень для управління інфраструктурою розподілених мереж зростає з кожним роком. Завдяки своїй здатності поєднувати приватні та публічні хмари, ця модель забезпечує безпечне зберігання конфіденційних даних і гнучкість для масштабування обчислювальних потужностей у публічних хмарах. Вона особливо популярна серед фінансових організацій та державних установ, де важливо зберігати контроль над даними, одночасно маючи можливість масштабувати ресурси при змінному навантаженні.

На рисунку 2.5 показано динаміку зростання популярності гібридних рішень у період з 2020 по 2024 роки.

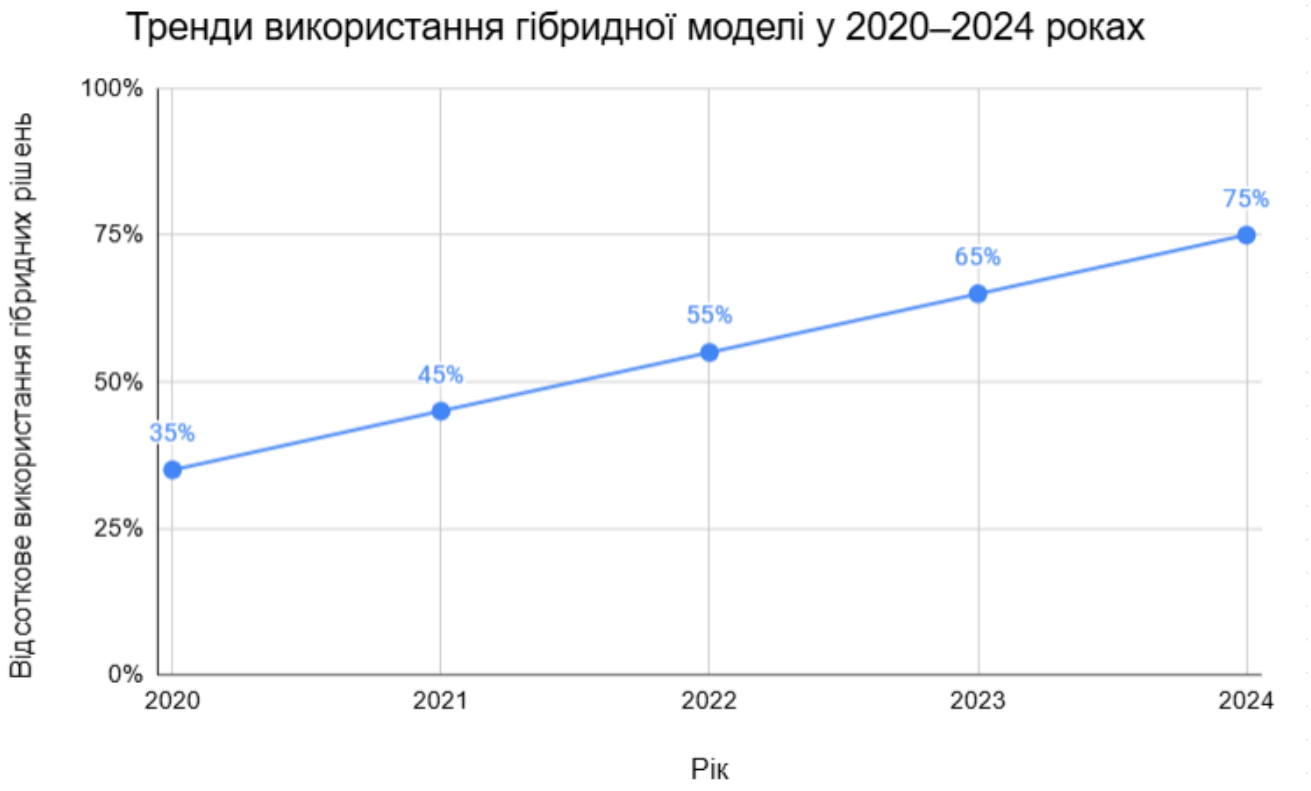

Рисунок 2.5 – Тренди використання гібридної моделі у 2020–2024 роках

Цей графік демонструє динаміку зростання популярності гібридних рішень у різних галузях, яка поступово збільшується з кожним роком через їхню гнучкість та можливості оптимального використання ресурсів.

Основні етапи інтеграції:

– аналіз інфраструктури: оцінка поточного стану мережі, визначення потреб у масштабуванні та функціональності;

– вибір хмарної платформи: базується на вимогах до безпеки, продуктивності, вартості та інтеграції з наявними системами;

– підготовка до міграції: розробка плану переходу, створення резервних копій даних і підготовка тестового середовища;

– впровадження: налаштування хмарних сервісів, інтеграція з локальними ресурсами та тестування системи;

– моніторинг та оптимізація: постійний моніторинг продуктивності та адаптація конфігурацій до змін у навантаженні.

Виклики інтеграції:

– сумісність: складнощі у поєднанні старих систем з новими хмарними технологіями;

– безпека: ризики при передачі даних до хмари та забезпечення їх захисту;

– затримки у передачі даних: особливо актуально для географічно розподілених систем;

– кадрова підготовка: необхідність навчання персоналу для роботи з новими інструментами.

Переваги інтеграції:

– гнучкість: можливість адаптації до зміни навантажень;

– економічність: зменшення витрат на підтримку фізичної інфраструктури;

– масштабованість: швидке розширення або зменшення ресурсів відповідно до потреб.

Компанія Coca-Cola інтегрувала хмарну платформу Microsoft Azure зі своїми локальними системами, що дозволило автоматизувати обробку даних продажів у реальному часі та покращити процес логістики [21].

3 РЕАЛІЗАЦІЯ В GNS3 МЕТОДІВ МОНІТОРИНГУ ТА АВТОМАТИЗАЦІЇ

Ефективне управління розподіленою мережею вимагає створення інфраструктури, яка забезпечує централізований контроль, надійний моніторинг і автоматизацію управління. Для моделювання такої системи використовується середовище GNS3, де реалізовано управління інфраструктурою розподілених мереж із застосуванням хмарних сервісів, а моніторинг здійснюється через Prometheus і Grafana, встановлені на віртуальному сервері Ubuntu [20].

3.1 Реалізація схеми управління мережею в GNS3

Для моделювання розподіленої мережі в GNS3 реалізовано інтегровану схему управління інфраструктурою з використанням хмарних технологій і систем моніторингу. Схема має такі ключові компоненти:

– центральний сервер на базі Ubuntu 20.04, на якому встановлені Prometheus та Grafana. Основна роль сервера полягає в зборі та аналізі метрик із мережевих пристроїв. Сервер підключено до внутрішньої мережі через комутатор з використанням статичної IP-адреси (192.168.1.10/24). Це забезпечує доступ до нього як з боку клієнтів, так і з боку мережевого адміністратора для конфігурації та моніторингу;

– комутатор, що виступає центральним вузлом локальної мережі, з'єднуючи клієнтські пристрої, сервер і маршрутизатор. Забезпечує швидке комутування даних між усіма підключеними пристроями у межах однієї підмережі 192.168.1.0/24;

– маршрутизатор, який виконує функцію з'єднання між внутрішньою мережею та зовнішньою хмарною інфраструктурою через компонент GNS3 Cloud.

Забезпечує маршрутизацію трафіку від клієнтських пристроїв і сервера Ubuntu до Інтернету або інших частин хмарної інфраструктури. Використовує статичну IP-адресу для внутрішнього інтерфейсу (192.168.1.1/24) і автоматично отримує IP-адресу для зовнішнього інтерфейсу від GNS3 Cloud;

– клієнтські пристрої, підключені до маршрутизатора через комутатор, що забезпечує зв’язок з хмарною інфраструктурою. У топології передбачені декілька клієнтських вузлів, які можуть бути представлені віртуальними машинами або емуляторами. Кожен клієнтський пристрій отримує статичну IP-адресу з підмережі 192.168.1.0/24 (наприклад, 192.168.1.20, 192.168.1.21 тощо);

– хмарна компонента реалізована як зовнішній інтерфейс через GNS3 Cloud для підключення до Інтернету або зовнішніх сервісів. Дозволяє підключати маршрутизатор до хмарної інфраструктури для використання зовнішніх API, завантаження оновлень або інтеграції з сервісами хмарного моніторингу.

Схема моделі розподіленої мережі в GNS3, включаючи моніторингову платформу, хмарну інфраструктуру та клієнтські пристрої представлена на рисунку 3.1.

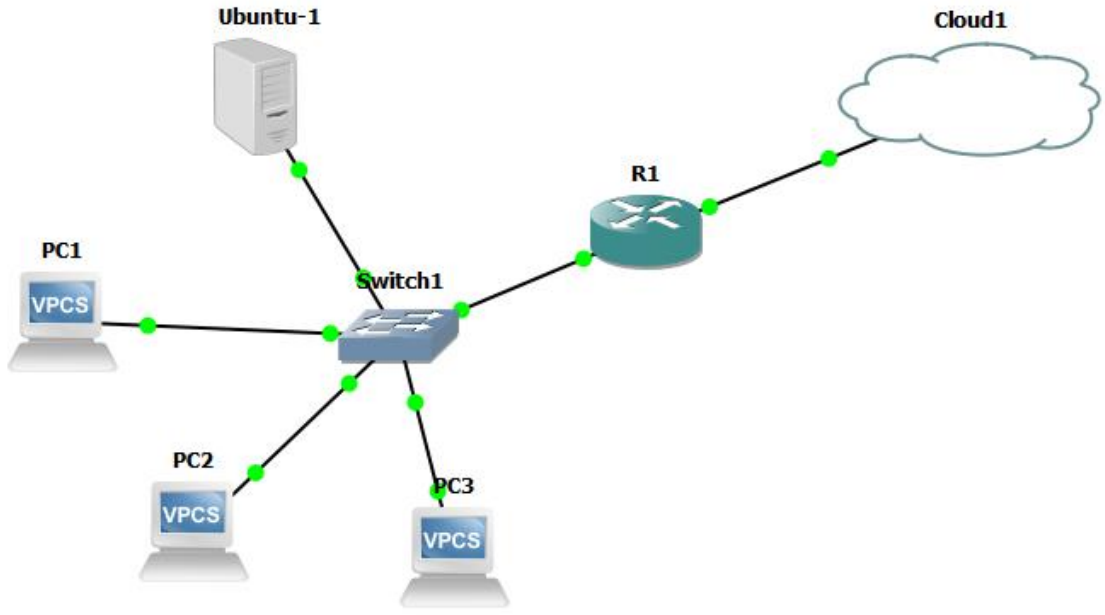

Рисунок 3.1 – Схема моделі розподіленої мережі в GNS3.

Для реалізації описаної схеми в середовищі GNS3 виконано наступні кроки.

Спершу налаштовано центральний сервер Ubuntu-1. Для цього було призначено статичну IP-адресу шляхом редагування конфігураційного файлу /etc/netplan/01-netcfg.yaml, де зазначено параметри мережі (лістинг 3.1):

Лістинг 3.1 – Файл 01-netcfg.yaml з параметрами мережі

```
network:
  version: 2
  renderer: networkd
  ethernets:
    ens3:
      addresses:
        - 192.168.1.10/24
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

Після редагування конфігурації виконано команду sudo netplan apply, щоб застосувати зміни. Далі, для збору й аналізу метрик, на сервер було встановлено Prometheus і Grafana за допомогою команд:

sudo apt update

sudo apt install prometheus

sudo add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"

sudo apt update

sudo apt install grafana

sudo systemctl start grafana-server

На наступному етапі підключено та налаштовано комутатор, до якого приєднано центральний сервер, клієнтські пристрої й маршрутизатор. Перевірено коректність з'єднань між пристроями через пінг.

Таблиця 3.1 відображає налаштування IP-адрес і підключень для ключових пристроїв у схемі.

Таблиця 3.1 – Налаштування IP-адрес і підключень

Пристрій	Інтерфейс	IP-адреса	Призначення
Сервер Ubuntu	eth0	192.168.1.10	Моніторинг (Prometheus, Grafana)
Маршрутизатор	GigabitEthernet0	192.168.1.1	Внутрішній інтерфейс
Клієнти	Ethernet0	192.168.1.20, 192.168.1.21, 192.168.1.22	Користувацький пристрій
GNS3 Cloud	NAT	Автоматично	Інтернет-з'єднання

Далі налаштовано маршрутизатор R1. Внутрішньому інтерфейсу маршрутизатора присвоєно IP-адресу 192.168.1.1/24, використовуючи наступні команди:

```
R1#conf t
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

Для зовнішнього інтерфейсу маршрутизатора, підключеного до компонента GNS3 Cloud, налаштовано автоматичне отримання IP-адреси за допомогою DHCP:

```
R1#conf t
R1(config)#interface GigabitEthernet1/0
R1(config-if)#ip address dhcp
R1(config-if)#no shutdown
```

Крім цього, налаштовано NAT для забезпечення маршрутизації трафіку між внутрішньою мережею та хмарною інфраструктурою:

```
R1(config)#ip nat inside source list 1 interface GigabitEthernet1/0 overload
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip nat inside
R1(config-if)#interface GigabitEthernet1/0
R1(config-if)#ip nat outside
```

Додано маршрут за замовчуванням через команду:

R1(config)#ip route 0.0.0.0 0.0.0.0 dhcp

Кожному клієнтському пристрою вручну призначено статичні IP-адреси в підмережі 192.168.1.0/24. Наприклад, для одного з пристроїв встановлено адресу 192.168.1.20/24, маску підмережі й шлюз за замовчуванням — 192.168.1.1. Після цього перевірено доступність сервера (192.168.1.10) і маршрутизатора (192.168.1.1) за допомогою пінгу.

Хмарну компоненту реалізовано через GNS3 Cloud, яка з'єднана з маршрутизатором через зовнішній інтерфейс. Це дозволило перевірити доступ до Інтернету, наприклад, через виконання команди ping 8.8.8.8 із сервера (рис. 3.2) або клієнтських пристроїв (рис.3.3).

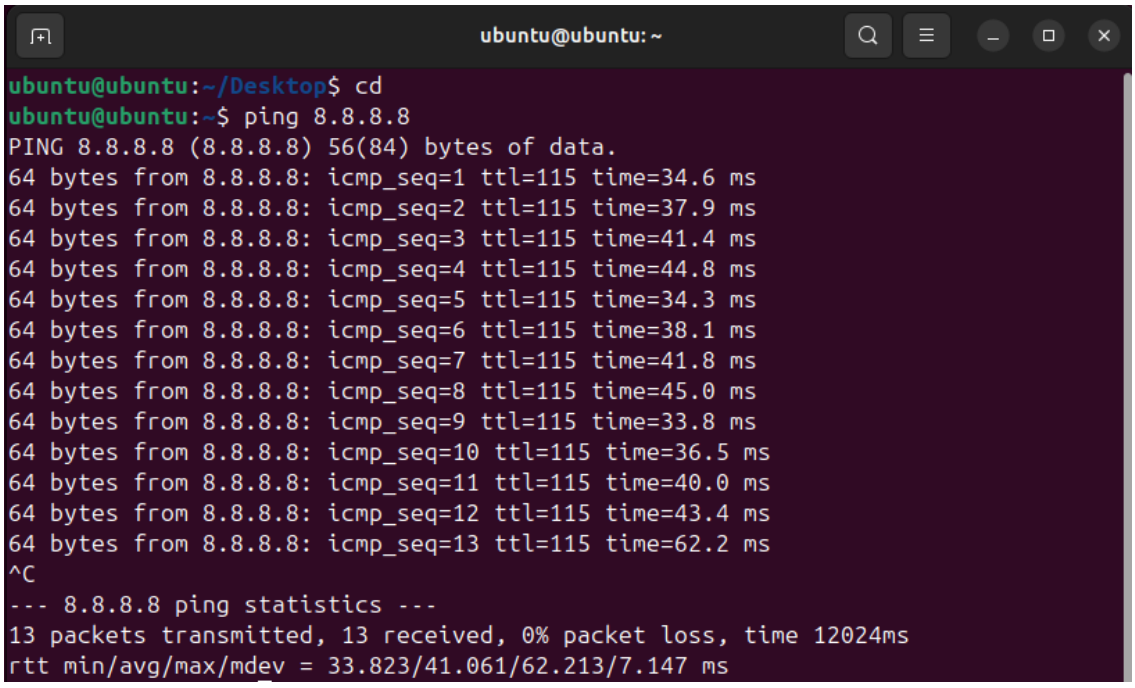

Рисунок 3.2 – Доступ до Інтернету із сервера

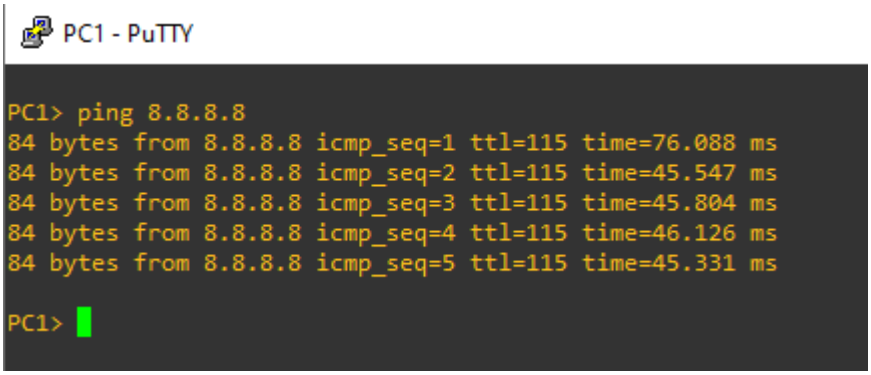

Рисунок 3.3 – Доступ до Інтернету із PC1

На завершальному етапі проведено тестування мережі. Перевірено коректність з'єднань між усіма пристроями в локальній мережі.

Реалізація цієї моделі дозволяє забезпечити інтеграцію локальної мережі з хмарними технологіями, створюючи надійний інструмент для централізованого моніторингу та управління мережею.

3.2 Моніторинг за допомогою Prometheus та Grafana

Реалізація ефективного моніторингу та аналізу трафіку є важливою складовою управління розподіленою мережею. Вона забезпечує прозорість процесів передачі даних, виявлення аномалій та оперативну реакцію на збої чи зовнішні атаки. Основними завданнями моніторингу є збирання актуальних даних, їхній аналіз у режимі реального часу та інтеграція цих даних з існуючими системами управління інфраструктурою [8].

Моніторинг трафіку у реальному часі має на меті досягнення таких результатів:

– підвищення доступності мережі: своєчасне виявлення проблемних вузлів або сегментів для мінімізації простоїв;

– поліпшення продуктивності: аналіз даних про затримку, пропускну здатність та стан ресурсів для усунення вузьких місць у мережі;

– забезпечення безпеки: виявлення аномалій, які можуть свідчити про кіберзагрози або неправомірні дії;

– оптимізація використання ресурсів: контроль за завантаженням серверів, мережевих пристроїв та пропускною здатністю каналів.

Моніторинг мережі є ключовим елементом для забезпечення стабільності та ефективності функціонування розподіленої мережі. Для досягнення цих цілей використовуються різні інструменти, які відрізняються функціональністю, можливостями інтеграції та масштабованістю [13].

На ринку існує велика кількість рішень для моніторингу мереж, серед яких найбільш популярними є Prometheus, Grafana, AWS CloudWatch та Azure Monitor. Кожен із цих інструментів має свої переваги та особливості:

– Prometheus: спеціалізується на збиранні та зберіганні часових рядів метрик, таких як пропускна здатність і затримка. Цей інструмент відзначається високою масштабованістю і підтримує інтеграцію з численними додатками та сервісами;

– Grafana: забезпечує ефективну візуалізацію даних у вигляді графіків, таблиць і панелей, що дозволяє швидко оцінювати стан мережі;

– AWS CloudWatch: надає засоби моніторингу ресурсів AWS, дозволяючи налаштовувати автоматичні сповіщення, масштабування та аналіз стану вузлів;

– Azure Monitor: є аналогом CloudWatch для середовища Microsoft Azure, пропонуючи широкі можливості для відстеження продуктивності ресурсів.

У цій моделі для реалізації моніторингу використано систему Prometheus для збору метрик і Grafana для візуалізації зібраних даних у реальному часі.

Prometheus було встановлено на сервер Ubuntu 20.04, який виступає центральним вузлом для збирання даних. Конфігураційний файл /etc/prometheus/prometheus.yml було оновлено для збору метрик з мережевих

пристроїв через SNMP-експортер:

Лістинг 3.2 – Конфігураційний файл /etc/prometheus/prometheus.yml

```
scrape_configs:
  - job_name: 'network_devices'
    static_configs:
      - targets: ['192.168.1.1:9162', '192.168.1.20:9162']
```

У цій конфігурації:

– job_name визначає ім'я задачі для збору даних;

– targets включає IP-адреси пристроїв, з яких збираються метрики (маршрутизатор та клієнтські пристрої).

Для збору даних з мережевих пристроїв було налаштовано SNMP-експортер, який встановлюється командою:

sudo apt install snmp snmpd snmp-mibs-downloader

Далі в конфігураційному файлі /etc/snmp/snmpd.conf налаштовано спільноту для збирання SNMP-метрик:

rocommunity public 192.168.1.0/24

Grafana налаштовано для використання Prometheus як джерела даних. У веб-інтерфейсі Grafana виконується додавання нового джерела даних (рис. 3.4):

– вибір типу джерела даних: Prometheus;

– введення URL сервера Prometheus: http://192.168.1.10:9090;

– збереження налаштувань і тестування підключення.

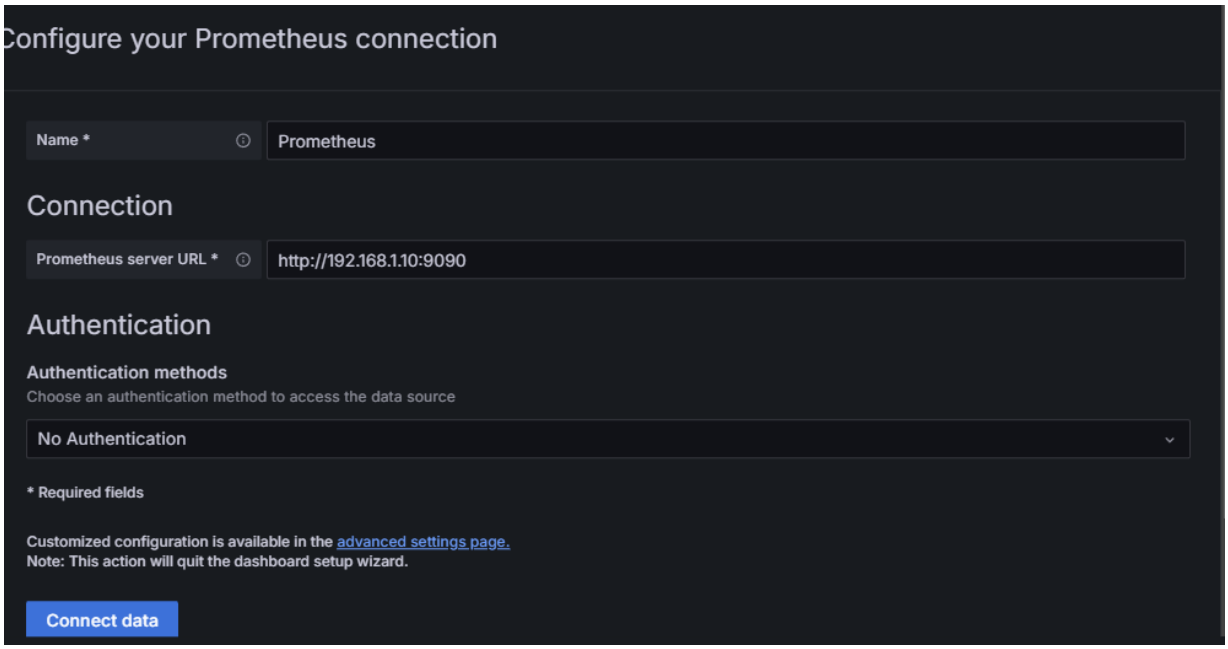

Рисунок 3.4 – Додавання нового джерела даних у веб-інтерфейсі Grafana

Дані, зібрані Prometheus, відображаються на інтерактивних панелях у Grafana, що дозволяє мережевим адміністраторам здійснювати моніторинг у реальному часі [19].

На рисунку 3.5 представлено схему інтеграції, починаючи зі збору даних з пристроїв через SNMP і завершуючи візуалізацією цих даних на панелях Grafana.

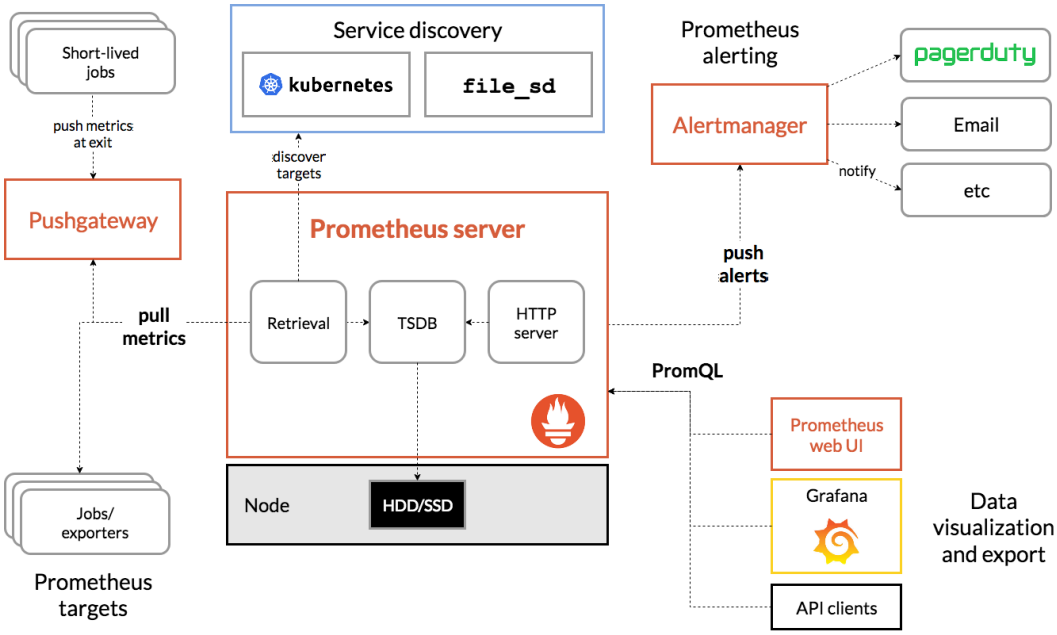

Рисунок 3.5 – Інтеграція інструментів моніторингу з хмарною інфраструктурою

У таблиці 3.2 наведено інформацію про основні параметри налаштування компонентів моніторингу.

Таблиця 3.2 – Основні параметри налаштування компонентів моніторингу

Компонент	Параметр	Значення	Призначення
Prometheus	IP-адреса сервера	192.168.1.10	Центральний вузол збору даних
Grafana	Порт	3000	Інтерфейс візуалізації
SNMP-експортер	Порт	9162	Збір SNMP-метрик
SNMP-спільнота	Тип	public	Доступ до даних у мережі

З розвитком технологій моніторинг стає дедалі більш автоматизованим. Серед сучасних трендів можна виділити:

– використання штучного інтелекту (ШІ): аналіз даних для прогнозування можливих збоїв або виявлення прихованих загроз;

– інтеграція з DevOps: постійний моніторинг як частина циклу розробки та розгортання;

– використання гібридних рішень: поєднання локальних і хмарних систем для забезпечення максимальної гнучкості.

Завдяки цим трендам системи моніторингу стають більш ефективними та надійними, що дозволяє компаніям забезпечувати стабільність своїх мереж навіть у складних умовах.

3.3 Автоматизація управління

Автоматизація управління мережею є важливою складовою сучасних інфраструктур, особливо в умовах розподілених мереж. Вона дозволяє оптимізувати процеси розподілу навантаження, додавання нових вузлів та забезпечення надійності роботи всієї системи. Для досягнення цього у системі

моніторингу Prometheus налаштовано тригерні правила, які автоматично реагують на зміну стану мережі.

Для забезпечення ефективності роботи мережі використовуються балансувальники навантаження. Вони рівномірно розподіляють запити між доступними вузлами, враховуючи їх поточний стан. У разі перевищення встановлених порогових значень ресурси масштабуються автоматично.

Тригерні правила в Prometheus Alertmanager дозволяють виконувати такі дії:

– автоматичне додавання нових вузлів у мережу за підвищення навантаження;

– перенаправлення запитів на вузли з меншою завантаженістю;

– повідомлення адміністратора про критичні станції.

Тригерні правила у Prometheus налаштовуються в конфігураційному файлі alert.rules.yml (лістинг 3.2).

Лістинг 3.2 – Тригерні правила у Prometheus Alertmanager

```
groups:
  - name: scaling_rules
    rules:
      - alert: HighCPUUtilization
        expr: avg(node_cpu_seconds_total) > 70
        for: 2m
        labels:
          severity: warning
        annotations:
          summary: "Високе завантаження CPU"
          description:  "Середній  рівень  використання  CPU
перевищив 70%. Додати новий вузол."

      - alert: HighMemoryUtilization
        expr:          avg(node_memory_Active_bytes          /
node_memory_MemTotal_bytes) > 0.8
        for: 2m
        labels:
          severity: critical
        annotations:
          summary: "Високе використання пам'яті"
          description:  "Рівень  використання  пам'яті  перевищив
80%. Перерозподілити запити."
```

У цих правилах:

– highCPUUtilization тригер активується, якщо середнє завантаження CPU перевищує 70% протягом 2 хвилин;

– highMemoryUtilization тригер активується, якщо використання пам'яті перевищує 80%.

У таблиці 3.3 наведено основні параметри налаштувань тригерів масштабування.

Таблиця 3.3 – Основні параметри налаштувань тригерів масштабування

Параметр	Значення	Опис
CPU Utilization	> 70%	Додається новий вузол
Memory Utilization	> 80%	Перерозподіл запитів
Response Time	> 200 ms	Перевірка вузлів на наявність затримок
Disk Usage	> 85%	Виконується очищення тимчасових файлів

AWS Auto Scaling автоматично змінює кількість активних серверів залежно від поточного навантаження на систему. Цей інструмент інтегрується з іншими сервісами AWS, такими як Elastic Load Balancer (ELB), для ефективного балансування навантаження між серверами.

Auto Scaling дозволяє автоматично збільшувати або зменшувати кількість серверів залежно від навантаження, що забезпечує стабільність роботи мережі при пікових навантаженнях. Наприклад, за умови перевищення використання CPU на 70%, система додає нові сервери для обробки запитів.

Основні параметри налаштування Auto Scaling наведені в таблиці 3.4.

Таблиця 3.4 – Основні параметри налаштування Auto Scaling

Параметр	Значення	Опис
Кількість мінімальних вузлів	2	Початкова кількість серверів
Тригер масштабування	CPU Utilization > 70%	Додає сервери при високому навантаженні
Кількість максимальних вузлів	10	Максимальна кількість серверів

На рисунку 3.6 наведено схему процесу автоматичного масштабування мережі. Вона демонструє взаємодію між компонентами Prometheus, Alertmanager та балансувальниками.

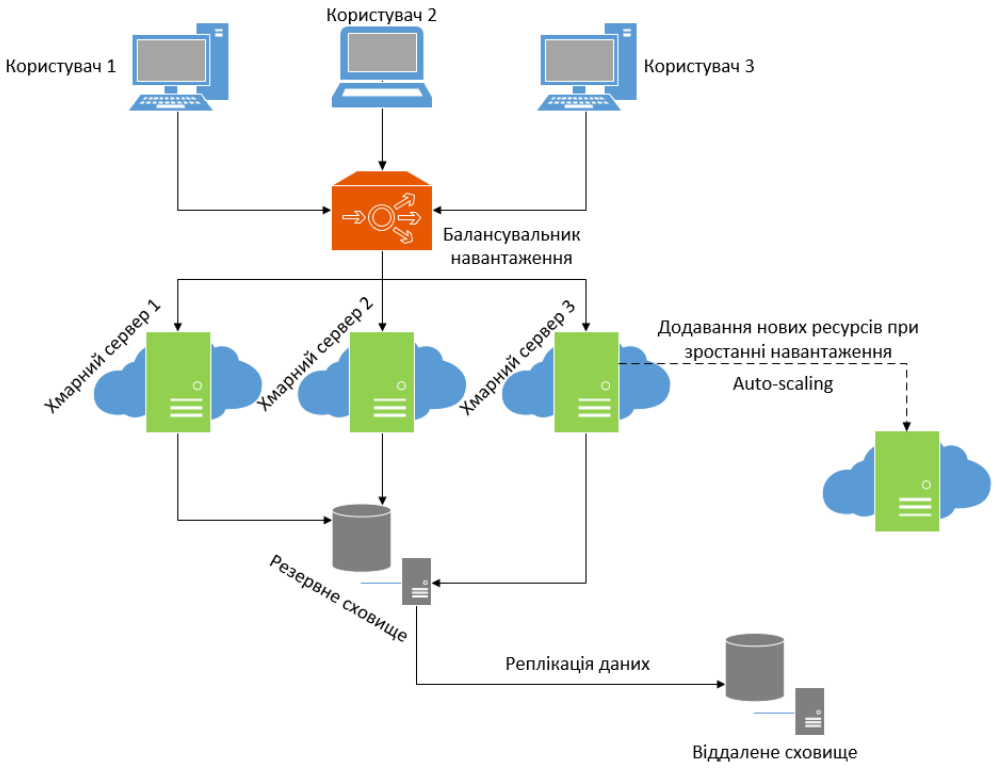

Рисунок 3.6 – Процес автоматичного масштабування мережі за допомогою тригерів Prometheus та балансування запитів.

Для балансування запитів використовується HAProxy. Конфігурація включає автоматичне додавання нових вузлів у пул при досягненні тригерних порогів. Основні параметри конфігурації HAProxy наведені в лістингу 3.3.

Лістинг 3.2 – Тригерні правила у Prometheus

```
frontend http_front
   bind *:80
   default_backend servers

backend servers
   balance roundrobin
   server node1 192.168.1.20:80 check
   server node2 192.168.1.21:80 check
```

Для кращого розуміння автоматизації наведено таблицю 3.5, яка відображає ефективність масштабування:

Таблиця 3.5 – Ефективність масштабування

Стан мережі	Дія	Результат
Завантаження CPU > 70%	Додавання нового вузла	Зниження навантаження на 30%
Затримка > 200 ms	Балансування запитів	Зменшення часу відповіді до 100 ms
Використання пам'яті > 80%	Перерозподіл запитів	Рівномірне використання ресурсів

Графік на рисунку 3.7 показує динаміку зміни навантаження після додавання нового вузла.

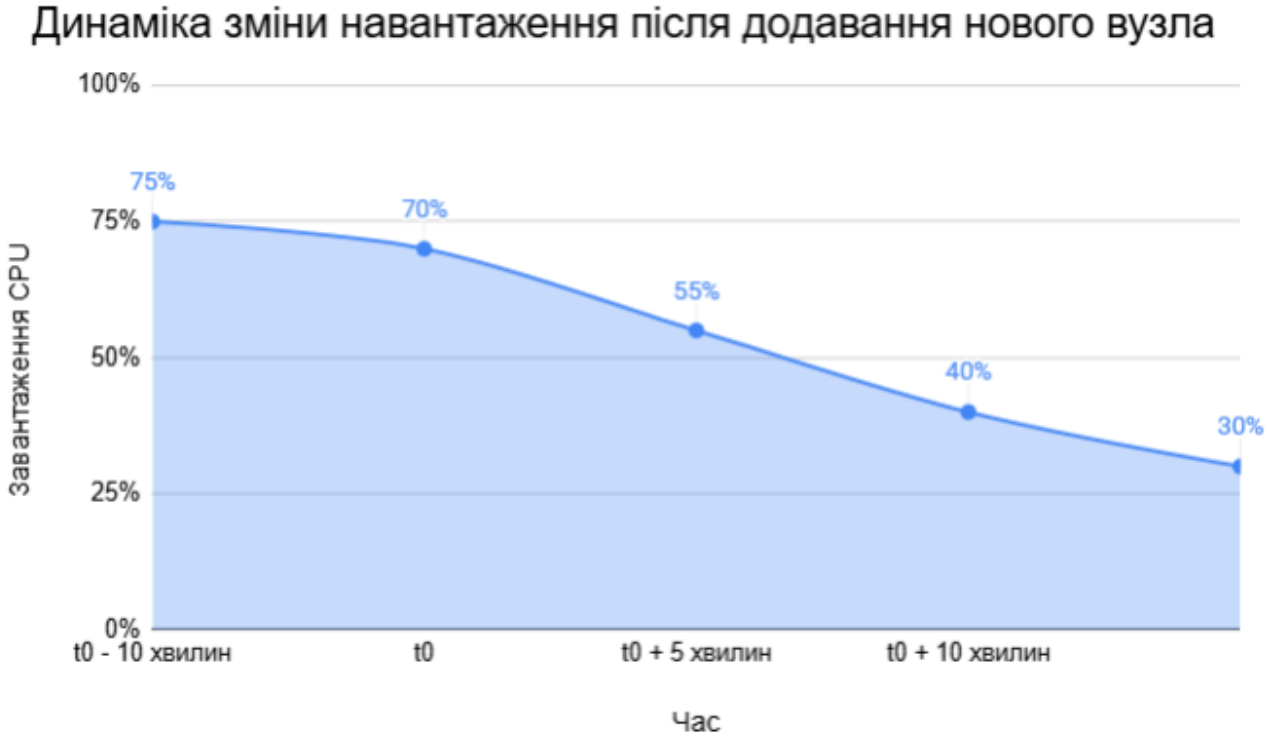

Рисунок 3.7 – Динаміка зміни навантаження після додавання нового вузла

На графіку можна побачити навантаження CPU:

– до події (t0 - 10 хвилин): Навантаження CPU поступово зростає (наприклад, 75%);

– на момент події (t0): Навантаження стабільно на рівні 70%;

– після події: Навантаження починає знижуватися (наприклад, 55% через 5 хвилин і 40% через 10 хвилин).

Автоматизація процесів дозволяє:

– скоротити час реагування на критичні ситуації;

– знизити ймовірність перевантаження мережі;

– підвищити ефективність використання ресурсів.

Інтеграція автоматизації з моніторингом забезпечує прозорість і керованість розподіленої мережі, що є важливим для сучасних інфраструктур.

Використання GNS3 для моделювання розподілених мереж із інтегрованими системами моніторингу (Prometheus, Grafana) та автоматизації забезпечує:

– реалістичне тестування;

– аналіз продуктивності мережі в реальному часі;

– гнучке масштабування мережевої інфраструктури.

Таке рішення демонструє потенціал сучасних хмарних технологій у поєднанні з відкритими моніторинговими системами для забезпечення стабільності й продуктивності мереж.

3.4 Централізоване управління інфраструктурою мережі за допомогою хмарних сервісів

Централізоване управління інфраструктурою мережі є ключовим елементом сучасних розподілених систем, оскільки воно забезпечує спрощений контроль доступу, підвищену безпеку та зменшує ризик помилок у адмініструванні.

Завдяки хмарним сервісам, таким як AWS IAM (Identity and Access Management) та Azure Active Directory, можна централізувати управління правами доступу, автоматизувати процеси налаштування політик безпеки та зменшити витрати на підтримку мережі [1].

Централізоване управління має такі переваги:

– єдина точка управління доступом: усі права доступу налаштовуються та контролюються з однієї платформи, що знижує складність адміністрування та забезпечує узгодженість політик безпеки;

– підвищення рівня безпеки: централізоване управління дозволяє швидко реагувати на загрози, наприклад, шляхом скасування доступу користувачів, які більше не мають повноважень;

– автоматизація управління ролями: система дозволяє створювати ролі з чітко визначеними правами доступу для різних груп користувачів. Наприклад, адміністраторам можна надати доступ до всіх ресурсів, тоді як кінцевим користувачам — лише до тих, які їм потрібні для роботи;

– спрощення відповідності регуляторним вимогам: завдяки централізованому моніторингу та звітності компанії можуть легко виконувати вимоги стандартів безпеки, таких як GDPR або ISO 27001.

AWS IAM дозволяє централізовано керувати доступом до ресурсів в екосистемі Amazon Web Services. Цей інструмент надає можливість створювати ролі та політики доступу, які визначають дії, дозволені для конкретних користувачів або груп [8].

Можливості IAM:

– налаштування детальних політик доступу на основі ролей;

– підтримка багатоетапної автентифікації (Multi-Factor Authentication, MFA);

– відстеження дій користувачів через систему логів (AWS CloudTrail).

Azure Active Directory (AAD) є рішенням від Microsoft, яке забезпечує централізоване управління користувачами та правами доступу до ресурсів у

середовищі Azure.

Ключові функції AAD:

– інтеграція з іншими сервісами Microsoft (Office 365, Dynamics 365);

– автоматизація створення та управління групами користувачів;

– захист доступу до ресурсів через Conditional Access (умовний доступ).

Google Cloud IAM забезпечує централізоване управління доступом до ресурсів у Google Cloud Platform. Інструмент дозволяє створювати ролі на основі політик безпеки, а також інтегрувати доступ з корпоративними системами.

Особливості:

– гнучке налаштування політик доступу;

– інтеграція з Google Workspace для управління доступом до документів та додатків;

– детальний аудит дій користувачів.

Налаштування ролей, які визначають права доступу для різних користувачів, допомагає автоматизувати та спростити адміністрування. Основні ролі можуть включати:

– адміністратор: має повний доступ до всіх ресурсів мережі, включаючи їх налаштування, моніторинг і управління;

– оператор: відповідає за моніторинг стану мережі, виконує базові налаштування вузлів;

– користувач: має обмежений доступ лише до кінцевих ресурсів, необхідних для виконання його завдань.

Опис ролей доступу в системі IAM представлений в таблиці 3.6.

Таблиця 3.6 – Опис ролей доступу в системі IAM

Роль	Доступні дії	Опис
Адміністратор	Повний доступ до налаштувань мережі	Управління ресурсами та доступом
Оператор	Моніторинг та базова конфігурація вузлів	Оперативне управління мережею
Користувач	Доступ до кінцевих ресурсів	Локальний доступ до ресурсів

Для забезпечення безпеки централізованого управління необхідно реалізувати такі заходи:

– шифрування даних під час передачі та зберігання: використовуються протоколи HTTPS для передачі даних, а також механізми шифрування (AES-256) для їхнього зберігання;

– політики контролю доступу: визначаються правила, які обмежують доступ до ресурсів лише авторизованим користувачам або групам;

– багатоетапна автентифікація: використання MFA значно підвищує рівень безпеки, додаючи додатковий рівень перевірки під час входу в систему.

Рисунок 3.8 демонструє схему централізованого контролю доступу, яка ілюструє рольове розподілення прав доступу до різних ресурсів у хмарному середовищі. Користувачі поділяються на три групи: адміністратори, оператори та кінцеві користувачі. Адміністратори мають повний доступ до налаштувань мережі, оператори відповідають за моніторинг і базові налаштування, а кінцеві користувачі можуть лише отримувати доступ до конкретних сервісів, таких як бази даних або файлові сховища [17].

Рисунок 3.8 – Схема централізованого контролю доступу

Централізоване управління також передбачає інтеграцію з системами моніторингу, такими як AWS CloudWatch або Azure Monitor, для відстеження дій користувачів, аналізу безпеки та створення звітів [19].

Інструменти централізованого управління дозволяють ефективно організувати роботу розподілених мереж, забезпечуючи високу доступність, захищеність даних та мінімізацію ризиків несанкціонованого доступу.

4 МОДЕЛЮВАННЯ ТА ПОРІВНЯННЯ ПІДХОДІВ ДО УПРАВЛІННЯ МЕРЕЖЕЮ

Сучасні розподілені мережі характеризуються складною структурою, високим рівнем динаміки та значним навантаженням, що ставить перед організаціями завдання забезпечення ефективного управління та стабільної роботи інфраструктури. Одним із найперспективніших підходів до вирішення цих завдань є інтеграція хмарних сервісів, які надають можливість гнучкого масштабування, автоматизації процесів і підвищення рівня надійності мережі.

У цьому розділі виконано моделювання роботи системи управління розподіленою мережею з використанням хмарних сервісів. Мета полягає у перевірці її продуктивності, стабільності та відмовостійкості в різних сценаріях навантаження. Також здійснено аналіз різних підходів до впровадження хмарних сервісів – приватних, публічних та гібридних, з урахуванням їх особливостей, переваг і недоліків.

Результати моделювання та порівняльний аналіз дозволяють обґрунтувати вибір оптимального підходу для впровадження хмарних сервісів у розподілену мережеву інфраструктуру, виходячи з потреб конкретної організації.

4.1 Реалізація структурної схеми системи управління мережею

Система управління розподіленою мережею є важливим інструментом для підтримання стабільності, ефективності та безпеки мережевої інфраструктури. Така система спрямована на інтеграцію всіх компонентів мережі в єдиний процес управління, що забезпечує централізований контроль, автоматизацію дій, гнучке масштабування та постійний моніторинг. Успішна реалізація цієї системи дозволяє організаціям адаптуватися до змін у навантаженні, швидко реагувати на проблеми та оптимізувати використання ресурсів [15].

Основні функції системи управління:

– централізоване управління: єдиний інтерфейс управління дозволяє координувати роботу всіх компонентів мережі — від серверів і маршрутизаторів до клієнтських вузлів. Це знижує ймовірність помилок, пов’язаних із децентралізованим адмініструванням, і спрощує управління великими розподіленими мережами. Приклад: адміністратор може через єдину панель керувати політиками безпеки, призначати права доступу та налаштовувати маршрутизацію;

– автоматизація дій: автоматизація забезпечує виконання рутинних завдань, таких як резервування даних, моніторинг метрик продуктивності, реагування на перевищення навантаження, без участі людини. Наприклад, за умови високого навантаження система автоматично додає нові сервери через механізм Auto Scaling [14];

– моніторинг і діагностика: постійний моніторинг забезпечує збір і аналіз даних про стан мережі, що дозволяє своєчасно виявляти та усувати несправності. Сучасні інструменти моніторингу інтегруються з хмарними сервісами, такими як Prometheus і Grafana, для аналізу в реальному часі;

– гнучке масштабування: система управління дозволяє адаптувати інфраструктуру до змін у навантаженні. Наприклад, у пікові години система може

додати ресурси, а в періоди низької активності — скоротити їх кількість для зменшення витрат.

Основні компоненти системи

– мережеві вузли – до мережевих вузлів належать сервери, маршрутизатори та комутатори, які забезпечують передачу, маршрутизацію та зберігання даних. Ці вузли є основою для забезпечення роботи мережевої інфраструктури. Сервери обробляють запити клієнтів, зберігають дані та забезпечують роботу додатків. Маршрутизатори відповідають за передачу даних між сегментами мережі, використовуючи оптимальні маршрути. Комутатори з'єднують кінцеві вузли та сервери, забезпечуючи швидку передачу даних у локальних сегментах;

– системи моніторингу – системи моніторингу, такі як Nagios, Zabbix, AWS CloudWatch або Azure Monitor, відповідають за постійний збір даних про стан мережі, зокрема про затримки, пропускну здатність і стан вузлів. Вони дозволяють виявляти аномалії та приймати проактивні рішення для усунення проблем;

– хмарна платформа – інтеграція з хмарними платформами (AWS, Microsoft Azure або Google Cloud) забезпечує гнучке масштабування ресурсів, обробку даних і високу доступність сервісів. Хмара також дозволяє автоматизувати процеси резервного копіювання та відновлення даних;

– клієнтські вузли – клієнтські вузли — це пристрої кінцевих користувачів (комп'ютери, смартфони, IoT-пристрої), які отримують доступ до ресурсів мережі через різні канали зв’язку.

Схема зв’язків між компонентами системи управління показує, як окремі елементи взаємодіють для забезпечення стабільності та продуктивності мережі:

– мережеві вузли передають дані до хмарної платформи;

– хмарна платформа обробляє запити, виконує масштабування ресурсів і забезпечує резервне копіювання даних;

– системи моніторингу збирають дані про стан вузлів і відправляють їх до аналітичного модуля для оцінки продуктивності;

– клієнтські вузли взаємодіють із хмарою через маршрутизатори та комутатори, отримуючи доступ до необхідних ресурсів.

В таблиці 4.1 показано елементи структурної схеми системи управління мережею та їх роль у системі.

Таблиця 4.1 – Елементи структурної схеми системи управління мережею

Елемент	Роль у системі
Мережеві вузли	Забезпечують обробку даних, маршрутизацію та зберігання.
Система моніторингу	Відстежують стан мережі, збирають метрики продуктивності та виявляють аномалії.
Хмарна платформа	Надає інфраструктуру для обчислень, зберігання даних і автоматизації процесів.
Клієнтські вузли	Отримують доступ до сервісів через мережу.

На рисунку 4.1 зображено структурну схему системи управління мережею. Вона включає всі основні компоненти, а також демонструє їхні зв’язки та взаємодію.

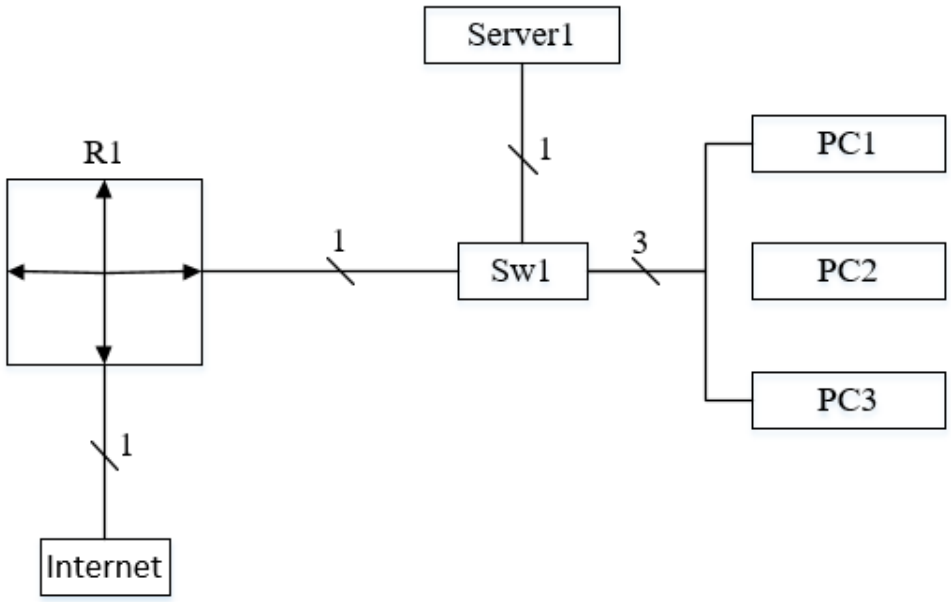

Рисунок 4.1: Структурна схема системи управління мережею

Схема, представлена на рисунку, демонструє базову архітектуру локальної мережі з інтеграцією ключових елементів для моніторингу, управління та розширення мережі.

Компоненти мережі:

– маршрутизатор R1 забезпечує підключення до глобальної мережі Інтернет і здійснює маршрутизацію даних між локальною мережею та зовнішніми підключеннями;

– комутатор Sw1 виконує функцію об'єднання кількох клієнтських пристроїв у локальній мережі, з'єднуючи сервер, клієнтські пристрої (PC1, PC2, PC3) та маршрутизатор;

– сервер Server1 відповідає за моніторинг і управління мережею, забезпечуючи роботу систем, таких як Prometheus і Grafana. Він збирає дані з мережевих пристроїв для аналізу стану мережі;

– клієнтські пристрої PC1, PC2, PC3 використовують ресурси мережі та взаємодіють із сервером через комутатор;

– інтернет-з'єднання надає доступ до зовнішніх ресурсів і забезпечує інтеграцію з хмарними платформами.

Розширена схема системи управління дозволяє забезпечити стабільність, продуктивність і безпеку мережі навіть у складних сценаріях роботи. Ця модель також є основою для впровадження додаткових функцій, таких як автоматизація управління ресурсами та розподіл навантаження.

4.2 Моделювання та верифікація системи управління мережею

Оцінювання функціональних можливостей системи управління розподіленою мережею, її продуктивність і стабільність за різних умов навантаження. Для цього було створено тестове середовище, проведено

моделювання роботи системи в різних сценаріях та здійснено аналіз ключових показників ефективності.

Для моделювання використовувалося симуляційне програмне забезпечення Mininet, яке дозволяє створювати віртуальні мережі з необхідними характеристиками. У створеному середовищі було змодельовано мережу, що складалася з 10 вузлів, 3 балансувальників навантаження та інтеграції з приватною хмарною інфраструктурою. Для збору даних моніторингу використовувалося програмне забезпечення, яке забезпечило реєстрацію показників продуктивності та стабільності роботи системи в реальному часі.

Середовище тестування моделювало інфраструктуру корпоративної мережі, де окремі вузли виконували роль клієнтських пристроїв, а балансувальники навантаження забезпечували рівномірний розподіл трафіку між доступними ресурсами. Приватна хмара використовувалася для забезпечення гнучкого масштабування та автоматизації процесів управління [6].

На рисунку 4.2 представлена структурна схема тестового середовища моделювання, яка демонструє ключові компоненти мережі, включаючи вузли, балансувальники навантаження та інтеграцію з приватною хмарою.

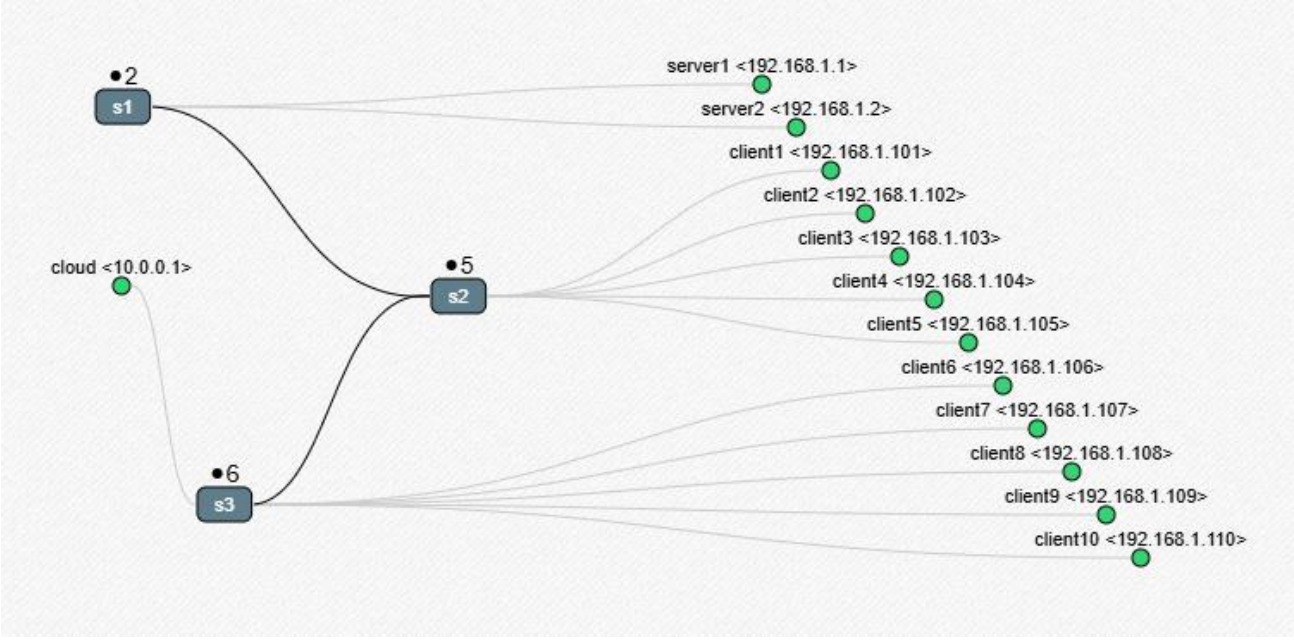

Рисунок 4.2. Схема тестового середовища моделювання

Було розроблено три основних сценарії для тестування системи:

– нормальне навантаження – у цьому сценарії моделювалося одночасне підключення 100 користувачів, що генерували типовий трафік. Цей сценарій дозволяв оцінити базові показники роботи системи, такі як затримка, пропускна здатність і стабільність;

– пікове навантаження – цей сценарій моделював одночасне підключення 1000 користувачів із підвищеними затримками на маршрутизацію. Його мета – оцінити, наскільки ефективно система справляється з екстремальними умовами роботи та чи забезпечується стабільність у таких умовах;

– відмова вузла. – у третьому сценарії емулювалася відмова одного з ключових мережевих комутаторів, що дозволило перевірити здатність системи до відмовостійкості та ефективність балансувальників навантаження в умовах аварійних ситуацій.

Результати показали, що при збільшенні кількості користувачів до 1000 затримка зросла до 100 мс, однак система зберігала функціональність навіть у пікових умовах.

На рисунку 4.3 показано залежність часу відгуку системи від кількості активних користувачів, що дозволяє оцінити її продуктивність при різних сценаріях навантаження.

Рисунок 4.3. Графік залежності часу відгуку системи від кількості активних користувачів

Ключовими метриками для оцінки ефективності системи були: затримка, пропускна здатність, час відгуку, втрати пакетів та стабільність роботи.

Результати моделювання вказують на високу ефективність системи в нормальному режимі роботи. Час відгуку становив у середньому 20 мс, а втрати пакетів не перевищували 0.5%. У пікових умовах затримка зросла до 100 мс, але мережа залишалася функціональною, забезпечуючи доступність основних сервісів. Під час моделювання відмови вузла спостерігалося швидке перерозподілення трафіку між доступними ресурсами, що дозволило уникнути простоїв.

Результати тестування продуктивності за різними сценаріями, яка містить такі дані: середній час відгуку, затримка, пропускна здатність, втрати пакетів і стабільність системи наводяться в таблиці 4.2.

Таблиця 4.2 – Результати тестування продуктивності за різними сценаріями

Сценарій	Середній час відгуку (мс)	Середня затримка (мс)	Пропускна здатність (Мбіт/с)	Втрати пакетів (%)	Стабільність роботи системи
Нормальне навантаження	20	15	950	0.5	Висока. Система працює стабільно.
Пікове навантаження	100	85	700	1.8	Задовільна. Система функціонує.
Відмова вузла	50	35	850	1.0	Висока. Швидке відновлення.

Моделювання підтвердило, що запропонована система управління розподіленою мережею є ефективною та відмовостійкою. Інтеграція хмарних сервісів забезпечує високий рівень продуктивності навіть за екстремальних умов, що робить цей підхід перспективним для широкого впровадження в корпоративних мережах.

4.3 Порівняння підходів до впровадження хмарних сервісів

Ефективність управління розподіленою мережею значною мірою залежить від вибору хмарної моделі. Розглянуто три основні підходи: приватна хмара, публічна хмара та гібридна хмара. Проведено їх аналіз з точки зору безпеки, масштабованості, продуктивності та вартості, що дозволяє оцінити доцільність кожного підходу в залежності від потреб організації.

Приватна хмара передбачає створення власної інфраструктури для зберігання та обробки даних у межах закритого середовища, доступ до якого мають лише уповноважені особи організації.

Основні характеристики приватної хмари:

– безпека: найвищий рівень безпеки, оскільки всі дані залишаються у

межах внутрішньої інфраструктури організації. Це мінімізує ризик несанкціонованого доступу;

– продуктивність: забезпечується стабільність продуктивності завдяки повному контролю над інфраструктурою. Організація може оптимізувати систему під свої потреби;

– вартість: значні інвестиції у впровадження, підтримку апаратного забезпечення, програмного забезпечення та технічного обслуговування;

– масштабованість: обмежена через потребу в додаткових ресурсах, які потребують закупівлі та інтеграції.

Переваги приватної хмари:

– повний контроль над ресурсами та налаштуваннями;

– відповідність регуляторним вимогам, що є критичним для фінансових установ, урядових організацій та медичних установ;

– висока захищеність даних завдяки ізоляції від зовнішніх користувачів.

Недоліки:

– висока вартість реалізації та підтримки;

– потреба у власній команді для управління інфраструктурою.

Приклад використання приватної хмари: фінансові установи, які зберігають конфіденційні дані клієнтів і дотримуються суворих нормативних вимог.

Публічна хмара надає організаціям доступ до обчислювальних ресурсів через сторонніх провайдерів, таких як AWS, Microsoft Azure або Google Cloud Platform.

Основні характеристики публічної хмари:

– безпека: середній рівень безпеки, оскільки дані зберігаються у провайдера. Залежність від їхньої політики безпеки може бути ризиком для конфіденційних даних;

– продуктивність: стабільність продуктивності залежить від налаштувань хмари, але загалом підтримується високий рівень доступності;

– вартість: низька вартість старту через відсутність потреби у власному

обладнанні. Оплата залежить від використаних ресурсів;

– масштабованість: максимальна масштабованість завдяки необмеженим ресурсам провайдера.

Переваги публічної хмари:

– швидке впровадження без необхідності великих початкових витрат;

– гнучкість у використанні ресурсів: організація сплачує лише за фактично використані потужності;

– можливість швидкого масштабування під час пікових навантажень.

Недоліки:

– ризики конфіденційності даних через залежність від сторонніх провайдерів;

– обмежений контроль над інфраструктурою.

Приклад використання публічної хмари: стартапи, які потребують швидкого запуску та масштабування за обмеженого бюджету.

Гібридна хмара об'єднує можливості приватної та публічної хмар, дозволяючи організаціям використовувати переваги обох моделей.

Основні характеристики гібридної хмари:

– безпека: поєднує високий рівень безпеки приватної хмари для конфіденційних даних із гнучкістю публічної хмари для менш критичних задач;

– продуктивність: баланс між продуктивністю приватної хмари та гнучкістю публічної;

– вартість: середній рівень витрат, оскільки потребує інтеграції обох середовищ;

– масштабованість: переваги масштабованості публічної хмари для обчислювальних задач із високим навантаженням.

Переваги гібридної хмари:

– гнучкість у розподілі задач між приватною та публічною інфраструктурою;

– забезпечення високого рівня безпеки для конфіденційних даних;

– можливість використання публічної хмари для тестування або розробки нових продуктів.

Недоліки:

– висока складність впровадження та інтеграції;

– залежність від підтримки кількох платформ.

Приклад використання гібридної хмари: підприємства, які працюють із великими масивами даних, що включають як конфіденційну, так і публічну інформацію.

Для об’єктивного оцінювання кожного підходу було виділено чотири основні критерії:

– безпека: приватна хмара забезпечує максимальний рівень безпеки завдяки ізоляції ресурсів, тоді як у публічній хмарі безпека залежить від політики провайдера. Гібридна хмара поєднує ці можливості, забезпечуючи баланс;

– продуктивність: приватна хмара пропонує стабільну продуктивність, у той час як публічна та гібридна хмари можуть залежати від умов провайдера та інтеграції;

– вартість: приватна хмара є найдорожчою через високі витрати на підтримку інфраструктури. Публічна хмара є економічним варіантом. Гібридна хмара має середні витрати через складність впровадження;

– масштабованість: найкращі результати показує публічна та гібридна хмари, що дозволяють легко масштабувати інфраструктуру.

Аналіз критеріїв безпеки, продуктивності, вартості та масштабованості для кожного підходу наведено в таблиці 4.3.

Таблиця 4.3 – Порівняльна характеристика хмарних підходів

Критерій	Приватна хмара	Публічна хмара	Гібридна хмара
Безпека	Висока	Низька	Середня
Продуктивність	Висока	Середня	Середня
Вартість	Висока	Низька	Середня
Масштабованість	Низька	Висока	Висока

Рекомендації:

– приватна хмара рекомендується для організацій із суворими вимогами до безпеки, таких як фінансові установи або державні підприємства;

– публічна хмара підходить для стартапів або компаній, які потребують швидкого масштабування;

– гібридна хмара є оптимальним варіантом для компаній, які потребують гнучкості та безпеки одночасно, але мають ресурси для інтеграції.

На рисунку 4.4 наведено візуальне порівняння переваг і недоліків кожного підходу, що допомагає вибрати найкраще рішення залежно від потреб організації.

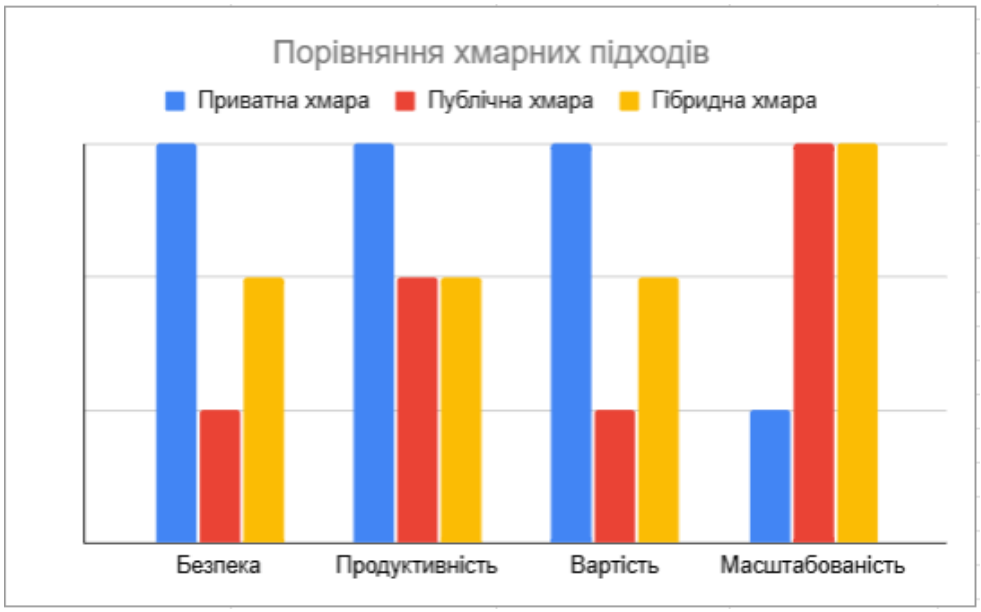

Рисунок 4.4 – Діаграма порівняння приватної, публічної та гібридної хмар

Порівняння підходів до впровадження хмарних сервісів для управління мережею свідчить, що вибір оптимальної моделі залежить від конкретних потреб організації, її ресурсів та вимог до безпеки, масштабованості, продуктивності і вартості.

Загалом, правильний вибір хмарного підходу дозволяє оптимізувати витрати, забезпечити необхідний рівень безпеки та створити гнучку інфраструктуру, здатну відповідати сучасним викликам бізнесу та технологій.

ВИСНОВКИ

Проведена магістерська робота підтверджує ефективність застосування хмарних сервісів для управління інфраструктурою розподілених мереж. У процесі роботи виконано аналіз сучасних методів управління розподіленими мережами, розглянуто основні особливості приватних, публічних і гібридних хмар, а також проведено моделювання системи управління в середовищі GNS3.

Особливу увагу приділено інтеграції систем моніторингу Prometheus і Grafana, які продемонстрували здатність виявляти аномалії в роботі мережі та надавати адміністраторам інформацію в реальному часі. Це значно підвищує продуктивність і знижує ризики збоїв у розподілених інфраструктурах.

Досліджено можливості застосування хмарних сервісів для управління інфраструктурою розподілених мереж, з акцентом на їхню гнучкість, масштабованість та економічну доцільність.

Результати порівняння хмарних платформ показали, що AWS є найбільш універсальною для широкого спектра завдань, тоді як Microsoft Azure має переваги в інтеграції з корпоративними середовищами, а GCP пропонує потужні інструменти для роботи з великими даними та AI.

Виконане моделювання довело переваги гібридної моделі для інтеграції локальної інфраструктури з хмарними сервісами. Це рішення забезпечує високу безпеку критичних даних і гнучкість масштабування ресурсів у пікові періоди.

На основі виконаного дослідження рекомендовано впроваджувати системи управління інфраструктурою розподілених мереж із використанням хмарних сервісів у корпоративних середовищах для підвищення ефективності, продуктивності та зменшення витрат. Результати роботи можуть бути корисними для модернізації існуючих мережевих інфраструктур і створення нових.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Alzakholi O., Haij L. M., Shukur H. M. Comparison among cloud technologies and cloud performance. Jastt. 2020. Vol. 1, no. 1. P. 40–47. URL: https://doi.org/10.38094/jastt1219 (date of access: 28.09.2024).

2. Borra P. A survey of google cloud platform (GCP): features, services, and applications. International journal of advanced research in science, communication and technology. 2024. Vol. 4, no. 3. P. 191–199. URL: https://doi.org/10.48175/IJARSCT-18922 (date of access: 05.10.2024).

3. Borra P. A survey of google cloud platform (GCP): features, services, and applications. International journal of advanced research in science, communication and technology. 2024. Vol. 4, no. 3. P. 191–199.

4. Borst S., Gupta V., Walid A. Distributed caching algorithms for content distribution networks. Proceedings IEEE INFOCOM. 2010. P. 1–9. URL: https://doi.org/10.1109/INFCOM.2010.5461964 (date of access: 01.10.2024).

5. Ekanayake J., Gunarathne T., Qiu J. Cloud technologies for bioinformatics applications. IEEE transactions on parallel and distributed systems. 2010. Vol. 22, no. 6. P. 998–1011. URL: https://doi.org/10.1109/TPDS.2010.178 (date of access: 24.09.2024).

6. Johnson K., Carr J., Day M. The measured performance of content distribution networks. Computer communications. 2001. Vol. 24, no. 2. P. 202–206. URL: https://doi.org/10.1016/S0140-3664(00)00315-7 (date of access: 30.09.2024).

7. Kewate N., Raut A., Dubekar M. A review on AWS - cloud computing technology. International journal for research in applied science & engineering technology. 2022. Vol. 10, no. 1. P. 258–263. URL: https://doi.org/10.22214/ijraset.2022.39802 (date of access: 09.10.2024).

8. Kyriaki E. A.-P., Iasonas N. K.-L., Pavlos S. G. Distributed and decentralized voltage control of smart distribution networks: models, methods, and future

research. IEEE transactions on smart grid. 2017. Vol. 8, no. 6. P. 2999–3008. URL: https://doi.org/10.1109/TSG.2017.2679238 (date of access: 27.09.2024).

9. Luong N. C., Wang P., Niyato D. Resource management in cloud networking using economic analysis and pricing models: a survey. IEEE communications surveys & tutorials. 2017. Vol. 19, no. 2. P. 954–1001. URL: https://doi.org/10.1109/COMST.2017.2647981 (date of access: 25.09.2024).

10. Madhuri T., Sowjanya P. Microsoft azure v/s amazon AWS cloud services: a comparative study. International journal of innovative research in science, engineering and technology. 2016. Vol. 5, no. 3. P. 3904–3908. URL: https://doi.org/10.15680/IJIRSET.2016.0503098 (date of access: 07.10.2024).

11. Mekki T., Jabri I., Rachedi A. Vehicular cloud networks: challenges, architectures, and future directions. Vehicular communications. 2017. No. 9. P. 268–280. URL: https://doi.org/10.1016/j.vehcom.2016.11.009 (date of access: 09.10.2024).

12. Nonde L., El-Gorashi T. E., Elmirghani J. M. Energy efficient virtual network embedding for cloud networks. Journal of lightwave technology. 2014. Vol. 33, no. 9. P. 1828–1849. URL: https://doi.org/10.1109/JLT.2014.2380777 (date of access: 20.09.2024).

13. Serrano N., Gallardo G., Hernantes J. Infrastructure as a service and cloud technologies. IEEE software. 2015. Vol. 32, no. 2. P. 30–36. URL: https://doi.org/10.1109/MS.2015.43 (date of access: 08.10.2024).

14. Singh T. The effect of Amazon Web Services (AWS) on Cloud-Computing. International journal of engineering research & technology. 2021. Vol. 10, no. 11. P. 480–482.

15. Slone J. P. Local area network handbook, sixth edition. Auerbach Publishers, Incorporated, 2020.

16. Yang Q., Barria J. A., Green T. C. Communication infrastructures for distributed control of power distribution networks. IEEE transactions on industrial informatics. 2011. Vol. 7, no. 2. P. 316–327. URL: https://doi.org/10.1109/TII.2011.2123903 (date of access: 04.10.2024).

17. Zhang F., Cao J., Li K. Multi-objective scheduling of many tasks in cloud platforms. Future generation computer systems. 2014. Vol. 37. P. 309–320. URL: https://doi.org/10.1016/j.future.2013.09.006 (date of access: 15.10.2024).

18. Белозьоров С. Ю. Безпека інформації в телекомунікаційних мережах з використанням хмарних сервісів. Радіоелектроніка та молодь у XXI столітті : матеріали 27-го Міжнар. молодіж. форуму, 10–12 травня 2023 р. – Харків : ХНУРЕ, 2023. – Т. 4. – С. 88–89.

19. Соловйов Р. Дослідження та програмна реалізація системи розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі. Збірник праць молодих науковців ЦНТУ. Кропивницький, 2023. Вип. 13. С. 360-372.

20. Третяк В.Ф., Пашнєва А.А. Оптимізація структури сховища даних у вузлах інфокомунікаційної мережі хмарного середовища. Системи управління, навігації та зв’язку. Збірник наукових праць. Полтава: ПНТУ. 2017. Т. 4 (44). С. 122-128. URL: https://journals.nupp.edu.ua/sunz/article/view/390 (дата звернення: 06.10.2024).

21. Целуйко Р., Тягунова М., Киричек Г. Оптимізація роботи комп’ютерної мережі. Технологія-2024 : Матеріали XXVII міжнар. науково-техн. конф., м. Київ, 24 трав. 2024 р. Київ, 2023. С. 182–183.