Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти перший (бакалаврський)

Програмні засоби моніторингу корпоративної комп'ютерної мережі

(тема)

Виконав:

здобувач 4 року навчання,

групи КІУКІ-21-3

Дмитро ШЕВЧЕНКО
(власне ім’я, прізвище)

Спеціальність

123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма

Комп’ютерна інженерія
(повна назва освітньої програми)

Керівник: ас. Максим БОНДАРЕНКО
(посада, власне ім’я, прізвище)

Допускається до захисту

Завідувач кафедри ЕОМ _____ Андрій КОВАЛЕНКО
(підпис) (власне ім’я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти перший (бакалаврський)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Комп’ютерна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
“____” _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Шевченку Дмитру Олександровичу
(прізвище, ім’я, по батькові)

1. Тема роботи Програмні засоби моніторингу корпоративної комп'ютерної мережі

затверджена наказом по університету від “ 26 ” травня 2025 р. № 424 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 17 червня 2025 р.

3. Вхідні дані до роботи
набори зображень
Google Colab
розпізнавання зображень
класифікація
сегментація

4. Перелік питань, що потрібно опрацювати у роботі
Огляд існуючих програмних засобів моніторингу
Теоретичні основи мережевого моніторингу
Реалізація ПЗ в Matlab та Google Colab

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій 15 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
1	Отримання завдання та аналіз літератури	26.05.2025–30.05.2025	
2	Огляд існуючих рішень та алгоритмів	31.05.2025–03.06.2025	
3	Вибір датасетів та архітектури системи	04.06.2025–06.06.2025	
4	Вибір програмних засобів	07.06.2025–08.06.2025	
5	Програмна реалізація	09.06.2025–11.06.2025	
6	Аналіз отриманих результатів	12.06.2025–13.06.2025	
7	Оформлення записки	14.06.2025–16.06.2025	

Дата видачі завдання " 26 " травня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ ас. Максим БОНДАРЕНКО
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 53 с., 16 рис., 2 дод., 8 джерел.

АВТОМАТИЗАЦІЯ, АДАПТИВНІСТЬ, АГРЕГАЦІЯ ДАНИХ, АНАЛІЗ АНОМАЛІЙ, АНАЛІЗ ТРАФІКУ, АРХІТЕКТУРА МЕРЕЖІ, ВЕБІНТЕРФЕЙС, ВИЯВЛЕННЯ АНОМАЛІЙ, ВІЗУАЛІЗАЦІЯ ДАНИХ, ВТРАТИ ПАКЕТІВ, GOOGLE COLAB, ГРАФІЧНІ ІНТЕРФЕЙСИ.

Метою кваліфікаційної роботи є розробка та реалізація програмних засобів моніторингу корпоративної комп’ютерної мережі з використанням сучасних інструментів аналізу, зокрема Matlab для моделювання й обробки даних та Google Colab для хмарної візуалізації та інтерпретації результатів, що дозволяє підвищити якість контролю та своєчасного реагування на порушення в роботі мережевої інфраструктури.

У ході виконання кваліфікаційної роботи було реалізовано програмні засоби моніторингу корпоративної комп’ютерної мережі, які передбачають інтеграцію локального інструментарію Matlab із хмарними засобами обробки даних у середовищі Google Colab. Застосування багаторівневої архітектури моніторингу забезпечило послідовний перехід від збору первинних даних до їх аналітичної інтерпретації, що дало змогу не лише виявляти поточні аномалії, а й формувати основи для прогнозного аналізу стану мережі.

ABSTRACT

Bachelor’s thesis: 53 pages, 16 figures, 2 appendices, 8 sources.

AUTOMATION, ADAPTIVITY, DATA AGGREGATION, ANOMALY ANALYSIS, TRAFFIC ANALYSIS, NETWORK ARCHITECTURE, WEB INTERFACE, ANOMALY DETECTION, DATA VISUALIZATION, PACKET LOSS, GOOGLE COLAB, GRAPHICAL INTERFACES.

The major goal of this thesis is the development and implementation of software tools for monitoring a corporate computer network using modern analysis tools, particularly Matlab for data modeling and processing, and Google Colab for cloud-based visualization and interpretation of results. This approach improves the quality of control and timely response to disruptions in network infrastructure operations.

In order to software tools for monitoring a corporate computer network were developed, ntegrating local Matlab-based toolkits with cloud data processing capabilities in the Google Colab environment. The use of a multi-level monitoring architecture enabled a consistent transition from collecting raw data to its analytical interpretation, allowing not only real-time anomaly detection but also laying the groundwork for predictive analysis of the network state.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

API – інтерфейс програмування додатків

BGP – протокол граничного шлюзу

CPU – центральний процесор

DHCP – протокол динамічної конфігурації хоста

DMZ – демілітаризована зона

DNS – система доменних імен

FTP – протокол передачі файлів

GPU – графічний процесор

HTTP – протокол передачі гіпертексту

ICMP – протокол повідомлень інтернет-контролю

IP – інтернет-протокол

IPFIX – протокол експорту інформації про IP-потоки

IT – інформаційні технології

LAN – локальна мережа

MATLAB – лабораторія матриць

MIB – база інформації управління

ML – машинне навчання

NetFlow – технологія аналізу мережевого трафіку Cisco

NMS – система управління мережею

QoS – якість обслуговування

SDN – програмно-визначена мережа

SLA – угода про рівень сервісу

SNMP – простий протокол управління мережею

TCP/IP – протокол контролю передачі/інтернет-протокол

VLAN – віртуальна локальна мережа

VPN – віртуальна приватна мережа

WAN – глобальна мережа

ВСТУП

Сучасний розвиток інформаційних технологій характеризується стрімким зростанням складності корпоративних комп'ютерних мереж та збільшенням обсягів даних, що передаються через них. Корпоративні мережі стали критично важливою інфраструктурою для забезпечення ефективного функціонування організацій, оскільки від їх стабільної роботи залежить продуктивність бізнес-процесів, збереження інформаційних активів та конкурентоспроможність підприємства на ринку.

Зростання кількості підключених пристроїв, впровадження концепцій хмарних обчислень, розподілених систем та Інтернету речей створює нові виклики для адміністраторів мереж. Складність сучасних мережевих архітектур, які часто включають гібридні рішення з поєднанням локальних та хмарних компонентів, вимагає застосування комплексних підходів до моніторингу та управління мережевою інфраструктурою.

Необхідність забезпечення високої доступності мережевих сервісів, мінімізації часу простою та швидкого виявлення проблем зумовлює потребу в ефективних системах моніторингу. Відсутність належного моніторингу може призвести до значних фінансових втрат, порушення безпеки даних та зниження довіри клієнтів до організації.

Мета кваліфікаційної роботи: розробка та реалізація програмних засобів моніторингу корпоративної комп’ютерної мережі з використанням сучасних інструментів аналізу, зокрема Matlab для моделювання й обробки даних та Google Colab для хмарної візуалізації та інтерпретації результатів, що дозволяє підвищити якість контролю та своєчасного реагування на порушення в роботі мережевої інфраструктури.

Завдання:

- проаналізувати існуючі підходи до моніторингу комп’ютерних мереж і виділити їх переваги та обмеження;

- сформувати вимоги до системи моніторингу з урахуванням особливостей корпоративної мережі;

- розробити алгоритм збору, обробки та аналізу мережевих даних на основі синтетичних або реальних показників;

- реалізувати програмну частину моніторингової системи у середовищі Matlab з подальшою інтеграцією до Google Colab;

- провести тестування розробленої системи та виконати аналіз результатів моніторингу.

1 ОГЛЯД ІСНУЮЧИХ ПРОГРАМНИХ ЗАСОБІВ МОНІТОРИНГУ

1.1 Класифікація інструментів моніторингу

Сучасні програмні засоби моніторингу корпоративних комп'ютерних мереж можна класифікувати за різними критеріями, що дозволяє системним адміністраторам та фахівцям з інформаційних технологій обрати найбільш відповідне рішення для конкретного середовища. За архітектурним підходом розрізняють централізовані системи, які передбачають збір та обробку всіх даних моніторингу на центральному сервері, та розподілені системи, що використовують мережу взаємопов'язаних вузлів для збору та аналізу інформації.

Рисунок 1.1 – Багаторівнева архітектура системи мережевого моніторингу

На рисунку 1.1 представлено багаторівневу архітектуру системи мережевого моніторингу, яка охоплює повний цикл роботи від фізичної інфраструктури до інтерфейсів візуалізації та керування. Система будується за принципом ієрархічного поділу, де кожен рівень виконує специфічні функції, забезпечуючи цілісне охоплення усіх аспектів роботи корпоративної комп'ютерної мережі.

Перший рівень описує технічну основу моніторингу – фізичні та віртуальні мережеві компоненти, такі як сервери, маршрутизатори, комутатори, системи безпеки та хмарні сервіси. Наступний рівень відповідає за збір і агрегацію даних з використанням стандартних протоколів та інтерфейсів – SNMP, NetFlow, syslog, а також засобів інтеграції сторонніх систем. Третій рівень охоплює процеси обробки даних: нормалізацію, виявлення аномалій, прогнозування та формування агрегованих показників продуктивності. Четвертий рівень забезпечує інтерпретацію результатів – через дашборди, сповіщення, API-доступи та системи інтеграції з іншими сервісами.

У нижній частині схеми акцентовано на принципах побудови системи: цілодобова доступність, масштабованість, адаптивність, гнучкість і контроль. Загалом архітектура відображає комплексний підхід до побудови надійної, функціонально повної системи моніторингу, орієнтованої на забезпечення безперервного контролю й управління корпоративною мережею.

Функціональна класифікація включає спеціалізовані інструменти, які зосереджуються на конкретних аспектах мережевого моніторингу, таких як контроль пропускної здатності, аналіз трафіку або моніторинг доступності сервісів, та комплексні платформи, що надають широкий спектр можливостей для всебічного контролю мережевої інфраструктури. Спеціалізовані рішення часто характеризуються більшою глибиною аналізу в конкретній галузі, тоді як комплексні платформи забезпечують уніфікований підхід до управління різними аспектами мережевого моніторингу.

За моделлю розгортання програмні засоби поділяються на локальні

рішення, які встановлюються та функціонують в межах корпоративної інфраструктури, хмарні сервіси, що надаються через Інтернет як послуга, та гібридні системи, які поєднують переваги обох підходів. Локальні рішення забезпечують повний контроль над даними та можливість налаштування під специфічні вимоги організації, тоді як хмарні сервіси пропонують швидке розгортання та зниження витрат на підтримку інфраструктури.

1.2 Аналіз популярних систем

Zabbix представляє собою комплексне рішення з відкритим кодом, яке забезпечує моніторинг мережевих пристроїв, серверів та додатків через веб-інтерфейс. Система характеризується високою масштабованістю та гнучкістю налаштувань, підтримує різноманітні протоколи збору даних включаючи SNMP, ICMP, SSH та власні агенти. Архітектура Zabbix базується на концепції розподіленого моніторингу з можливістю створення ієрархічної структури серверів для обслуговування великих мережевих інфраструктур.

PRTG Network Monitor є комерційним рішенням німецької компанії Paessler, яке відзначається інтуїтивним веб-інтерфейсом та широкими можливостями візуалізації даних. Система використовує концепцію сенсорів для моніторингу різних параметрів мережевих пристроїв та додатків, пропонуючи понад 200 типів сенсорів для контролю різноманітних метрик. PRTG інтегрує функції моніторингу мережевого трафіку, продуктивності додатків та доступності сервісів в єдиній платформі.

Nagios Core та його комерційна версія Nagios XI представляють одні з найстаріших та найбільш поширених систем моніторингу в корпоративному середовищі. Система базується на модульній архітектурі з використанням плагінів для розширення функціональності та підтримує як активний, так і пасивний моніторинг мережевих ресурсів. Nagios відзначається потужною системою сповіщень та можливостями автоматизації реагування на

інциденти.

SolarWinds пропонує комплексний набір інструментів для моніторингу мережевої інфраструктури, включаючи Network Performance Monitor, Server Application Monitor та інші спеціалізовані модулі. Платформа характеризується розвиненими можливостями аналітики та звітності, інтеграцією з популярними системами управління IT-сервісами та підтримкою автоматизованого виявлення мережевої топології.

Критерій	Zabbix	PRTG	Nagios	SolarWinds
Ліцензування та вартість	Відкритий код Безкоштовно	Комерційна €1600+/рік	Відкритий код Безкоштовно	Комерційна $2000+/рік
Складність розгортання	3	1	4	2
Масштабо-ваність	Висока	Середня	Висока	Висока
Підтримувані протоколи	SNMP, Agent JMX, IPMI SSH, HTTP LDAP, ODBC	SNMP, WMI Packet Sniff NetFlow HTTP, SSH	SNMP, NRPE NSCA, SSH HTTP, SMTP Plugins	SNMP, WMI NetFlow sFlow, IPFIX API, Syslog
Візуалізація та звіти	★★★☆	★★★★★	★★☆☆	★★★★★
Спільнота та підтримка	A	B	A	A
Гнучкість налаштувань	90%	70%	80%	75%

Рисунок 1.2 – Аналіз популярних систем

Порівняльний аналіз функціональних можливостей розглянутих систем демонструє різноманітність підходів до вирішення завдань мережевого моніторингу. Всі системи підтримують основні протоколи збору даних, проте відрізняються у способах їх реалізації та розширеності функцій. Zabbix пропонує найбільшу гнучкість у налаштуванні параметрів моніторингу та створенні користувацьких сценаріїв, тоді як PRTG відзначається простотою розгортання та використання.

Масштабованість систем варіюється від кількох сотень до десятків

тисяч пристроїв під управлінням однієї інсталяції. Nagios та Zabbix демонструють найкращі показники масштабованості завдяки розподіленій архітектурі, тоді як PRTG більше підходить для середніх та малих мережевих інфраструктур. SolarWinds займає проміжну позицію, пропонуючи модульний підхід до масштабування функціональності.

Вартість володіння системами суттєво відрізняється між відкритими та комерційними рішеннями. Zabbix та Nagios Core не потребують ліцензійних витрат, проте вимагають значних інвестицій у кваліфікований персонал для розгортання та підтримки. Комерційні рішення включають технічну підтримку та додаткові сервіси у вартість ліцензії, що може виявитися більш економічно ефективним для організацій з обмеженими IT-ресурсами.

2 ТЕОРЕТИЧНІ ОСНОВИ МЕРЕЖЕВОГО МОНІТОРИНГУ

2.1 Основні принципи моніторингу мережі

Теоретичне підґрунтя мережевого моніторингу базується на фундаментальних принципах системного аналізу та теорії управління, адаптованих до специфіки комп'ютерних мереж. Принцип безперервності передбачає постійний контроль стану мережевих компонентів без перерв у функціонуванні системи моніторингу, що досягається через реалізацію відмовостійких архітектур збору та обробки даних. Цей принцип є критично важливим для своєчасного виявлення проблем та мінімізації часу простою мережевої інфраструктури.

Принцип всебічності вимагає охоплення всіх критично важливих компонентів мережевої інфраструктури, включаючи фізичні пристрої, програмне забезпечення, мережеві сервіси та каналі зв'язку. Реалізація цього принципу потребує комплексного підходу до планування системи моніторингу з урахуванням різноманітності технологій та протоколів, що використовуються в сучасних корпоративних мережах.

Принцип масштабованості забезпечує можливість розширення системи моніторингу відповідно до зростання мережевої інфраструктури без суттєвої зміни архітектури та основних компонентів системи. Це досягається через використання модульних архітектур, розподілених систем збору даних та ефективних алгоритмів обробки великих обсягів інформації.

Принцип адаптивності передбачає здатність системи моніторингу автоматично пристосовуватися до змін у мережевому середовищі, включаючи появу нових пристроїв, зміну топології мережі та модифікацію конфігурацій. Реалізація цього принципу базується на використанні алгоритмів автоматичного виявлення мережевих компонентів та машинного навчання для аналізу поведінкових патернів.

2.2 Мережеві протоколи

Simple Network Management Protocol представляє собою стандартний протокол управління мережевими пристроями, який базується на архітектурі клієнт-сервер та використовує концепцію Management Information Base для структурованого представлення параметрів моніторингу. SNMP використовує ієрархічну систему ідентифікаторів об'єктів для унікальної адресації кожного параметра, що дозволяє стандартизувати процес збору інформації з різнорідних мережевих пристроїв. Протокол підтримує як активне опитування пристроїв менеджером мережі, так і асинхронне надсилання сповіщень про критичні події через механізм SNMP трапів.

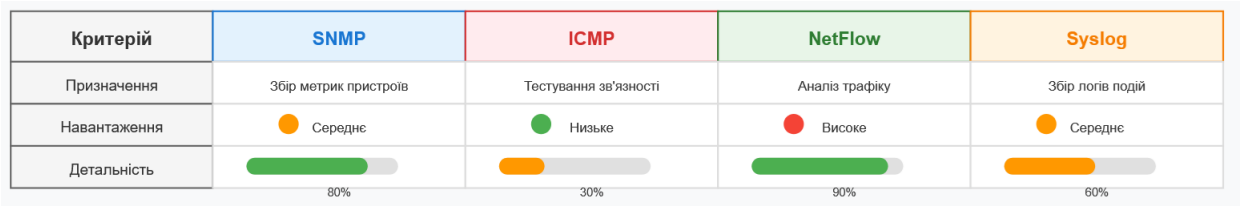

Рисунок 2.1 – Порівняння мережевих протоколів

Internet Control Message Protocol призначений для передачі службової інформації про стан мережевого з'єднання та використовується системами моніторингу для перевірки доступності мережевих вузлів та вимірювання затримок передачі даних. ICMP реалізує різноманітні типи повідомлень, включаючи Echo Request та Echo Reply для перевірки зв'язності, Time Exceeded для виявлення проблем маршрутизації та Destination Unreachable для ідентифікації недоступних мережевих ресурсів. Аналіз ICMP трафіку дозволяє виявляти проблеми мережевої зв'язності, оцінювати якість каналів зв'язку та діагностувати неполадки в роботі мережевого обладнання.

NetFlow та його аналоги представляють технології аналізу мережевого трафіку, які забезпечують детальну інформацію про потоки даних у мережі, включаючи адреси відправників та отримувачів, використовувані протоколи,

обсяги переданих даних та часові характеристики сесій. Ці технології дозволяють проводити глибокий аналіз використання мережевих ресурсів, виявляти аномальну активність та оптимізувати розподіл пропускної здатності між різними типами трафіку.

2.3 Метрики продуктивності мережі

Оцінка продуктивності мережевої інфраструктури базується на комплексі ключових показників, що характеризують різні аспекти якості мережевого сервісу. Пропускна здатність представляє максимальну кількість даних, що може бути передана через мережевий канал за одиницю часу. Цей показник зазвичай вимірюється в бітах за секунду та залежить від фізичних характеристик каналу зв'язку, використовуваних протоколів та навантаження на мережу.

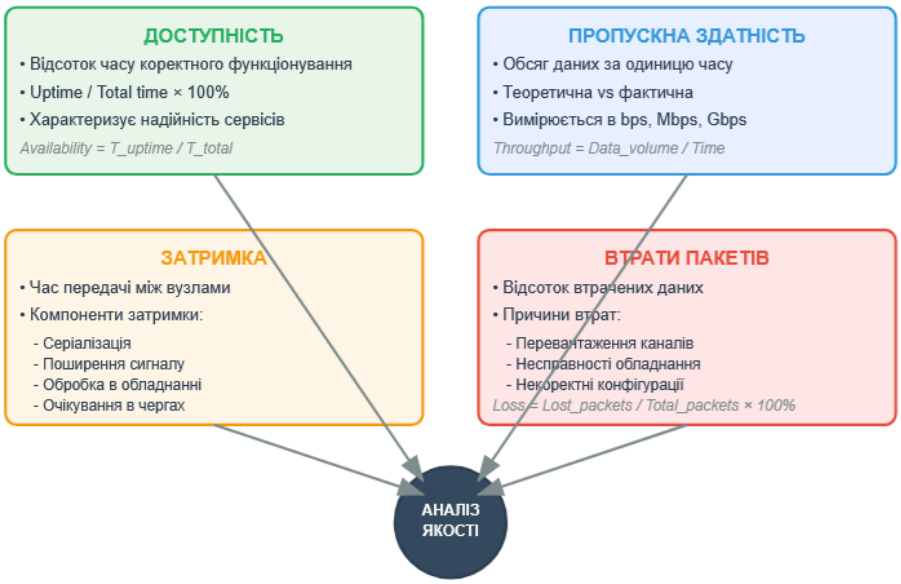

Рисунок 2.2 – Основні метрики мережевих систем

Утилізація мережевих ресурсів показує відсоток використання доступної пропускної здатності каналів зв'язку. Високий рівень утилізації може вказувати на необхідність розширення пропускної здатності або оптимізації розподілу трафіку. Ефективний моніторинг утилізації дозволяє

планувати розвиток мережевої інфраструктури та запобігати виникненню вузьких місць.

Затримка або латентність характеризує час, необхідний для передачі даних від джерела до призначення. Цей показник критично важливий для інтерактивних додатків та сервісів реального часу. Затримка складається з декількох компонентів: час обробки в мережевих пристроях, час очікування в чергах, час передачі по фізичному середовищу та час серіалізації пакетів.

Варіація затримки або джитер показує мінливість часу доставки пакетів в мережі. Високий джитер може суттєво впливати на якість голосових та відеододатків, навіть при відносно низькій середній затримці. Моніторинг джитера дозволяє виявляти проблеми з якістю обслуговування та оптимізувати налаштування мережевого обладнання.

Втрати пакетів характеризують відсоток пакетів, що не досягли місця призначення. Втрати можуть виникати через перевантаження мережевих вузлів, помилки передачі або проблеми з мережевим обладнанням. Навіть невеликий відсоток втрат може суттєво впливати на продуктивність TCP-з'єднань та якість мультимедійних додатків.

Доступність сервісів вимірює відсоток часу, протягом якого мережеві ресурси залишаються доступними для користувачів. Цей показник зазвичай виражається у відсотках або у вигляді коефіцієнта готовності. Високий рівень доступності вимагає резервування критичних компонентів, швидкого виявлення та усунення проблем.

Якість обслуговування (QoS) включає комплексну оцінку мережевого сервісу з точки зору користувача. QoS метрики враховують всі вищезазначені параметри та їх взаємовплив на якість роботи конкретних додатків. Ефективний моніторинг QoS дозволяє забезпечувати відповідність мережевого сервісу вимогам бізнес-процесів організації.

2.4 Архітектура корпоративної комп'ютерної мережі

Архітектура сучасної корпоративної комп'ютерної мережі являє собою ієрархічну структуру, що забезпечує ефективне з'єднання великої кількості користувачів та сервісів. Традиційно корпоративні мережі будуються за принципом триярусної моделі, що включає рівень доступу, рівень агрегації та ядро мережі. Кожен рівень виконує специфічні функції та має відповідні вимоги до продуктивності, надійності та безпеки.

Рівень доступу забезпечує безпосереднє підключення кінцевих пристроїв користувачів до корпоративної мережі. Комутатори рівня доступу зазвичай розміщуються в безпосередній близькості до робочих місць та забезпечують високу щільність портів за відносно низькою вартістю. На цьому рівні реалізуються базові функції безпеки, такі як контроль доступу до мережі, сегментація трафіку за допомогою VLAN та моніторинг активності користувачів.

Рівень агрегації або розподілу служить для об'єднання трафіку з множини комутаторів доступу та його передачі до ядра мережі. Пристрої цього рівня забезпечують маршрутизацію між різними сегментами мережі, реалізацію політик безпеки та якості обслуговування. Рівень агрегації часто включає засоби балансування навантаження та резервування для забезпечення високої доступності мережевих сервісів.

Ядро мережі представляє високошвидкісну магістраль корпоративної інфраструктури, що забезпечує з'єднання між різними сегментами мережі та доступ до зовнішніх ресурсів. Пристрої ядра характеризуються максимальною продуктивністю, мінімальною затримкою та високою надійністю. Архітектура ядра зазвичай включає резервування на рівні пристроїв та каналів зв'язку для забезпечення безперервності роботи.

Сучасні корпоративні мережі все частіше інтегрують елементи хмарних технологій та програмно-визначених мереж (SDN). Гібридні архітектури дозволяють поєднувати переваги традиційних локальних мереж з гнучкістю

та масштабованістю хмарних сервісів. SDN технології забезпечують централізоване управління мережевою інфраструктурою та динамічне налаштування мережевих політик.

Периметр мережевої безпеки включає межеві пристрої, що контролюють трафік між корпоративною мережею та зовнішніми ресурсами. Сучасні межеві пристрої поєднують функції маршрутизації, брандмауера, системи запобігання вторгненням та оптимізації WAN трафіку. Концепція Zero Trust архітектури передбачає розширення принципів безпеки периметра на всі сегменти корпоративної мережі.

Ідентифікація критичних компонентів корпоративної мережі є фундаментальним етапом планування системи моніторингу. Ключові вузли мережі включають пристрої, відмова яких може суттєво вплинути на роботу значної частини інфраструктури або критичних бізнес-процесів. До таких вузлів зазвичай відносяться основні маршрутизатори та комутатори ядра, сервери центрів обробки даних, системи зберігання даних та засоби забезпечення безпеки.

Серверна інфраструктура представляє один з найкритичніших сегментів корпоративної мережі. Сервери додатків, бази даних, файлові сервери та системи електронної пошти забезпечують функціонування основних бізнес-процесів організації. Моніторинг серверної інфраструктури повинен включати контроль апаратних ресурсів, продуктивності додатків, доступності сервісів та цілісності даних.

Мережеві сервіси, такі як DNS, DHCP, Active Directory та системи автентифікації, забезпечують базову функціональність корпоративної мережі. Проблеми з цими сервісами можуть призводити до масових порушень роботи користувачів, навіть при нормальному функціонуванні інших компонентів інфраструктури. Моніторинг мережевих сервісів вимагає комплексного підходу, що включає контроль доступності, швидкодії та правильності відповідей.

Канали зв'язку між ключовими вузлами мережі також потребують

пріоритетного моніторингу. Особливу увагу слід приділяти каналам, що не мають резервування, оскільки їх відмова може призводити до ізоляції цілих сегментів мережі. Моніторинг каналів зв'язку включає контроль утилізації, якості сигналу, кількості помилок та доступності резервних шляхів.

Сегментація мережі на основі функціонального призначення дозволяє оптимізувати стратегію моніторингу та забезпечити відповідність вимогам безпеки. Типова сегментація включає корпоративну мережу для внутрішніх користувачів, сегмент серверів, DMZ для публічних сервісів, гостьову мережу та сегменти для спеціалізованих систем, таких як системи контролю та управління виробництвом.

Виділення критичних додатків та сервісів дозволяє встановити пріоритети моніторингу та визначити допустимі рівні обслуговування. Критичність може визначатися впливом на бізнес-процеси, кількістю залежних користувачів, вимогами регуляторних органів або умовами сервісних угод. Класифікація критичності забезпечує основу для налаштування параметрів моніторингу та процедур реагування на інциденти.

2.5 Вимоги до моніторингу

Специфіка корпоративних мереж висуває особливі вимоги до систем моніторингу, що відрізняють їх від рішень для малих мереж або домашнього використання. Масштабованість системи моніторингу повинна забезпечувати можливість контролю тисяч пристроїв та десятків тисяч параметрів з єдиної точки управління. Архітектура системи повинна підтримувати як вертикальне масштабування через збільшення потужності серверів, так і горизонтальне через розподіл навантаження між множиною вузлів.

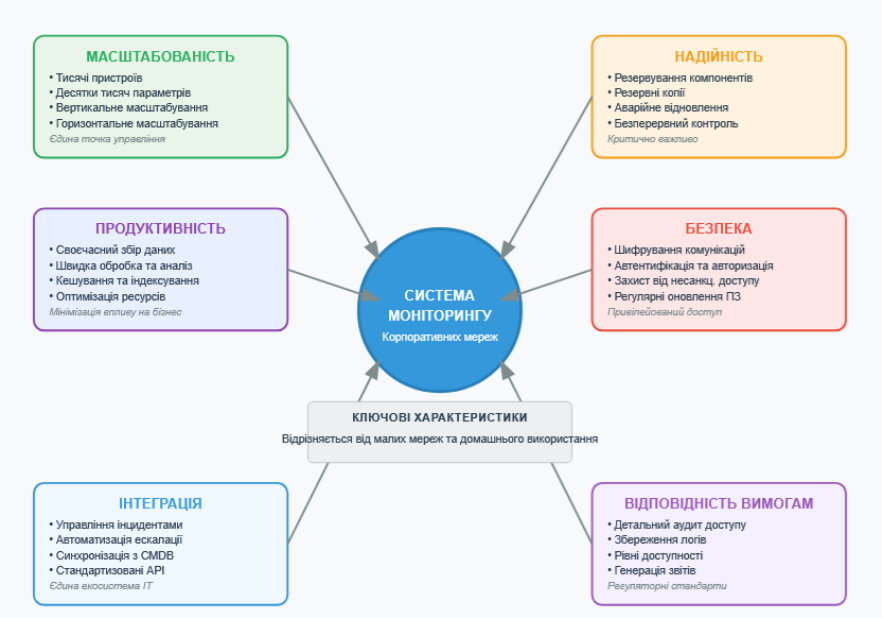

Рисунок 2.3 – Вимоги до системи моніторингу

Надійність системи моніторингу критично важлива для забезпечення безперервного контролю мережевої інфраструктури. Відмова системи моніторингу під час проблем в мережі може призводити до значного збільшення часу відновлення сервісів. Забезпечення надійності вимагає резервування ключових компонентів системи моніторингу, регулярного створення резервних копій конфігурації та даних, а також планування процедур аварійного відновлення.

Продуктивність системи моніторингу повинна забезпечувати своєчасний збір, обробку та аналіз великих обсягів моніторингових даних. Затримки в обробці даних можуть призводити до несвоєчасного виявлення проблем та збільшення їх впливу на бізнес-процеси. Оптимізація продуктивності включає ефективне планування ресурсів, використання кешування та індексування даних, а також розумне налаштування частоти опитування пристроїв.

Безпека системи моніторингу має особливе значення, оскільки ці системи мають привілейований доступ до мережевої інфраструктури та зберігають конфіденційну інформацію про архітектуру та стан мережі. Вимоги безпеки включають шифрування комунікацій між компонентами

системи, надійну автентифікацію та авторизацію користувачів, захист від несанкціонованого доступу та регулярне оновлення програмного забезпечення.

Інтеграція з існуючими системами управління IT-інфраструктурою дозволяє створити єдину екосистему моніторингу та управління. Інтеграція може включати обмін даними з системами управління інцидентами, автоматизацію процесів ескалації проблем, синхронізацію з базами даних конфігурацій та інтеграцію з системами управління змінами. Стандартизовані API та протоколи інтеграції забезпечують гнучкість та можливість еволюції системи моніторингу.

Відповідність регуляторним вимогам та стандартам галузі може висувати додаткові вимоги до систем моніторингу. Деякі галузі вимагають детального аудиту доступу до мережевих ресурсів, збереження логів протягом певного періоду або забезпечення конкретних рівнів доступності критичних систем. Система моніторингу повинна забезпечувати збір необхідної інформації та генерацію звітів для демонстрації відповідності вимогам.

3 РЕАЛІЗАЦІЯ ПЗ В MATLAB ТА GOOGLE COLAB

3.1 Обґрунтування вибору інструментів

Сучасний підхід до розробки та дослідження систем мережевого моніторингу вимагає використання потужних інструментів для аналізу даних, моделювання та візуалізації. MATLAB та Google Colab представляють дві різні парадигми вирішення задач аналізу мережевих даних, кожна з яких має унікальні переваги для конкретних аспектів дослідження.

MATLAB традиційно використовується в академічному та промисловому середовищі для розробки складних алгоритмів обробки сигналів, математичного моделювання та інженерного аналізу. У контексті мережевого моніторингу MATLAB забезпечує потужні засоби для аналізу часових рядів мережевих метрик, статистичної обробки даних моніторингу та розробки алгоритмів виявлення аномалій. Вбудовані функції для роботи з мережевими протоколами та можливості інтеграції з зовнішніми системами роблять MATLAB ефективним інструментом для прототипування систем моніторингу.

Google Colab представляє хмарну платформу для розробки та виконання програм на Python з доступом до потужних обчислювальних ресурсів, включаючи GPU та TPU. Для задач мережевого моніторингу Colab забезпечує доступ до широкої екосистеми бібліотек Python для аналізу даних, машинного навчання та візуалізації. Можливість спільної роботи над проектами та інтеграція з хмарними сервісами зберігання даних роблять Colab привабливим для командної розробки та дослідження.

Комбінація MATLAB та Google Colab дозволяє використовувати сильні сторони обох платформ. MATLAB може використовуватися для розробки та тестування складних алгоритмів аналізу мережевих даних, які потім можуть бути адаптовані для виконання в Python середовищі Google Colab. Така

гібридна методологія забезпечує гнучкість у виборі найкращих інструментів для конкретних завдань та оптимізацію використання ресурсів.

Вибір цих інструментів також обумовлений їх доступністю та вартістю впровадження. Google Colab забезпечує безкоштовний доступ до потужних обчислювальних ресурсів, що робить його доступним для навчальних закладів та стартапів з обмеженим бюджетом. MATLAB, хоча і вимагає ліцензування, забезпечує професійний рівень підтримки та документації, що важливо для промислового використання.

3.1.1 Огляд можливостей Matlab у сфері моніторингу

MATLAB забезпечує комплексний набір інструментів для розробки систем мережевого моніторингу, починаючи від збору даних з мережевих пристроїв до складного аналізу та візуалізації результатів. Instrument Control Toolbox дозволяє встановлювати прямі з'єднання з мережевим обладнанням через різноманітні протоколи, включаючи SNMP, TCP/IP, UDP та послідовні інтерфейси. Це забезпечує можливість створення спеціалізованих додатків для збору моніторингових даних безпосередньо з мережевих пристроїв.

Signal Processing Toolbox надає потужні засоби для аналізу часових рядів мережевих метрик. Функції фільтрації, спектрального аналізу та виявлення аномалій дозволяють ідентифікувати патерни в мережевому трафіку та виявляти відхилення від нормальної роботи. Вейвлет-аналіз може використовуватися для багатомасштабного дослідження мережевих даних, що особливо корисно для виявлення періодичних проблем або тенденцій зміни продуктивності.

Statistics and Machine Learning Toolbox забезпечує алгоритми для створення прогнозних моделей мережевої продуктивності та автоматичного виявлення аномалій. Методи кластерного аналізу можуть використовуватися для класифікації мережевих пристроїв за патернами використання, а регресійний аналіз - для прогнозування майбутніх потреб у пропускній

здатності. Алгоритми машинного навчання дозволяють створювати інтелектуальні системи моніторингу, що автоматично адаптуються до змін у мережевому середовищі.

Database Toolbox забезпечує інтеграцію з популярними системами управління базами даних для зберігання та аналізу великих обсягів моніторингових даних. Можливість роботи з SQL запитами безпосередньо з MATLAB середовища спрощує процес аналізу історичних даних та генерації звітів. Підтримка NoSQL баз даних дозволяє працювати з неструктурованими моніторинговими даними та метаданими мережевих пристроїв.

Parallel Computing Toolbox дозволяє прискорити обробку великих обсягів мережевих даних через використання багатоядерних процесорів та кластерних обчислень. Це особливо важливо для аналізу NetFlow даних або обробки логів високонавантажених мережевих сегментів. Розподілені обчислення можуть суттєво скоротити час виконання складних аналітичних задач.

3.1.2 Використання Google Colab для візуалізації та обробки даних

Google Colab надає ідеальне середовище для розробки інтерактивних інструментів візуалізації мережевих даних та експериментів з алгоритмами машинного навчання. Інтеграція з Jupyter Notebook забезпечує можливість створення документованих аналітичних процедур, що поєднують код, візуалізації та пояснювальний текст в єдиному документі. Це особливо корисно для дослідницьких проектів та навчальних матеріалів з мережевого моніторингу.

Екосистема Python бібліотек, доступна в Google Colab, включає потужні інструменти для аналізу мережевих даних. Pandas забезпечує ефективні структури даних для роботи з часовими рядами моніторингових метрик. NumPy та SciPy надають фундаментальні алгоритми для математичної обробки даних. Scikit-learn включає широкий набір алгоритмів

машинного навчання для класифікації, кластеризації та виявлення аномалій в мережевих даних.

Візуалізація даних в Google Colab здійснюється через бібліотеки Matplotlib, Seaborn та Plotly, що забезпечують створення професійних графіків та діаграм. Інтерактивні візуалізації Plotly особливо корисні для дослідження великих обсягів мережевих даних, дозволяючи користувачам динамічно фільтрувати та масштабувати відображення. Можливість створення анімованих візуалізацій дозволяє показувати еволюцію мережевих метрик у часі.

Інтеграція з Google Drive та іншими хмарними сервісами забезпечує зручний доступ до даних моніторингу та можливість спільної роботи над проектами. Автоматичне збереження стану notebook-ів гарантує збереження результатів аналізу навіть при несподіваних відключеннях. Можливість експорту результатів у різні формати спрощує інтеграцію з іншими системами та створення звітів.

Доступ до GPU прискорювачів в Google Colab дозволяє ефективно тренувати глибокі нейронні мережі для аналізу мережевого трафіку та виявлення аномалій. TensorFlow та PyTorch, попередньо встановлені в Colab, забезпечують сучасні фреймворки для розробки AI-powered систем мережевого моніторингу. Можливість експериментувати з різними архітектурами нейронних мереж без необхідності власних потужних серверів робить Colab ідеальним інструментом для дослідницької роботи.

Системи версійного контролю, інтегровані з Google Colab, дозволяють відстежувати зміни в аналітичних процедурах та співпрацювати з командою розробників. GitHub інтеграція забезпечує можливість збереження notebook-ів у публічних або приватних репозиторіях та створення документації з прикладами використання. Це особливо важливо для відкритих проектів систем мережевого моніторингу та навчальних ресурсів.

3.2 Методика моніторингу корпоративної мережі в середовищі Matlab

Розроблена методика моніторингу корпоративної комп'ютерної мережі ґрунтується на автоматизованому зборі, обробці та аналізі ключових метрик трафіку і стану мережевих пристроїв. Основою для реалізації став функціонал Matlab, який дає змогу проводити гнучку обробку числових даних, реалізовувати алгоритми аналізу часового ряду, а також створювати візуалізації з високим рівнем деталізації.

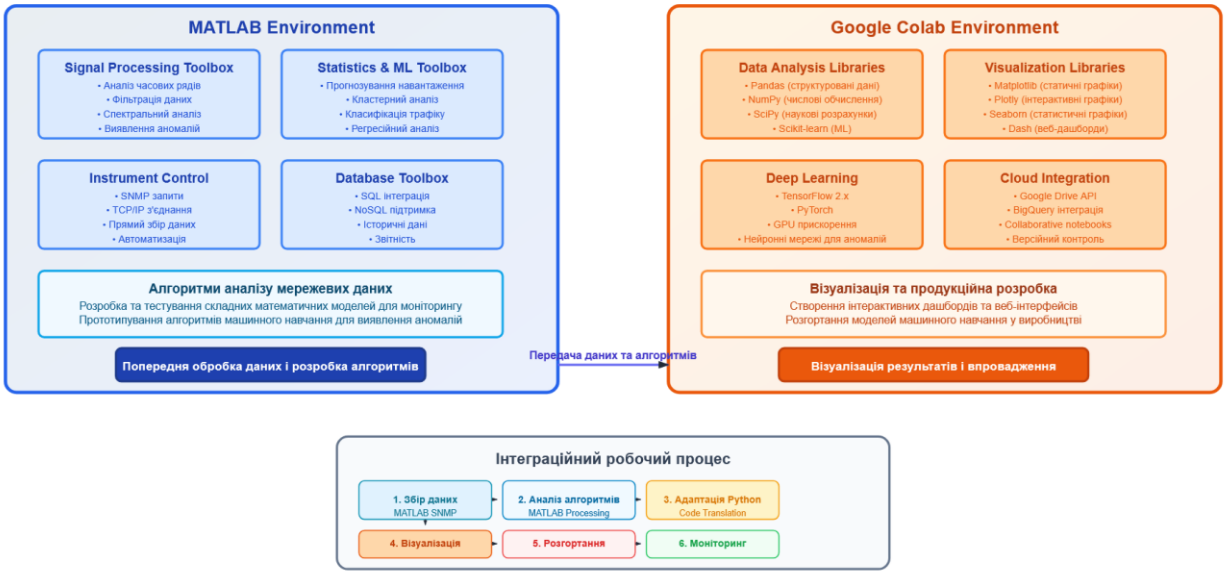

Рисунок 3.1 – Інтеграція Matlab та Colab

Першочергово здійснюється підключення до джерела мережевих даних. Оскільки Matlab не має вбудованого механізму безпосередньої взаємодії з протоколом SNMP, реалізація включає інтеграцію з зовнішніми скриптами (наприклад, Python або PowerShell), які виконують опитування пристроїв мережі та зберігають отримані дані у форматах CSV або JSON. Ці файли надалі імпортуються у Matlab за допомогою функцій readtable або jsondecode.

Після завантаження даних здійснюється їх попередня обробка, яка передбачає очищення від аномалій, інтерполяцію пропущених значень, а також нормалізацію метрик для подальшого порівняльного аналізу. Особлива

увага приділяється параметрам, що характеризують якість з’єднання (latency, jitter, packet loss) та використання мережевих інтерфейсів (bandwidth usage, throughput).

На наступному етапі реалізується аналіз часових рядів за допомогою вбудованих функцій Matlab, зокрема smoothdata, findpeaks, movmean, що дозволяє виявити пікові навантаження, повторювані шаблони та нестабільність мережі. Аналіз супроводжується побудовою графіків із використанням plot, area, heatmap, що забезпечує інтуїтивно зрозумілу інтерпретацію результатів.

Рисунок 3.2 – Етапи моніторингу

Для оцінки загального стану мережі вводиться інтегральний індикатор навантаження, який розраховується як зважене середнє значення вибраних метрик. На основі цього індикатора визначається рівень здоров’я мережі у кожен момент часу, що дозволяє виявити як критичні збої, так і приховані тенденції до деградації продуктивності.

Результати аналізу можуть бути збережені у вигляді звітів у форматах PDF та HTML з автоматично згенерованими діаграмами та поясненнями. Це створює умови для впровадження регулярного моніторингу з мінімальним втручанням адміністратора, а також забезпечує архівацію даних для подальшого аудиту.

Таким чином, реалізований у Matlab підхід поєднує високу гнучкість аналізу з можливістю візуального представлення стану корпоративної мережі, що суттєво підвищує ефективність технічного моніторингу в IT-інфраструктурах.

3.3 Реалізація в Matlab

Код представлений в додатку Б. Перейдемо безпосередньо до результатів моделювання. Після виконання скрипту отримуємо робочу програму з графіками (рисунок 3.3).

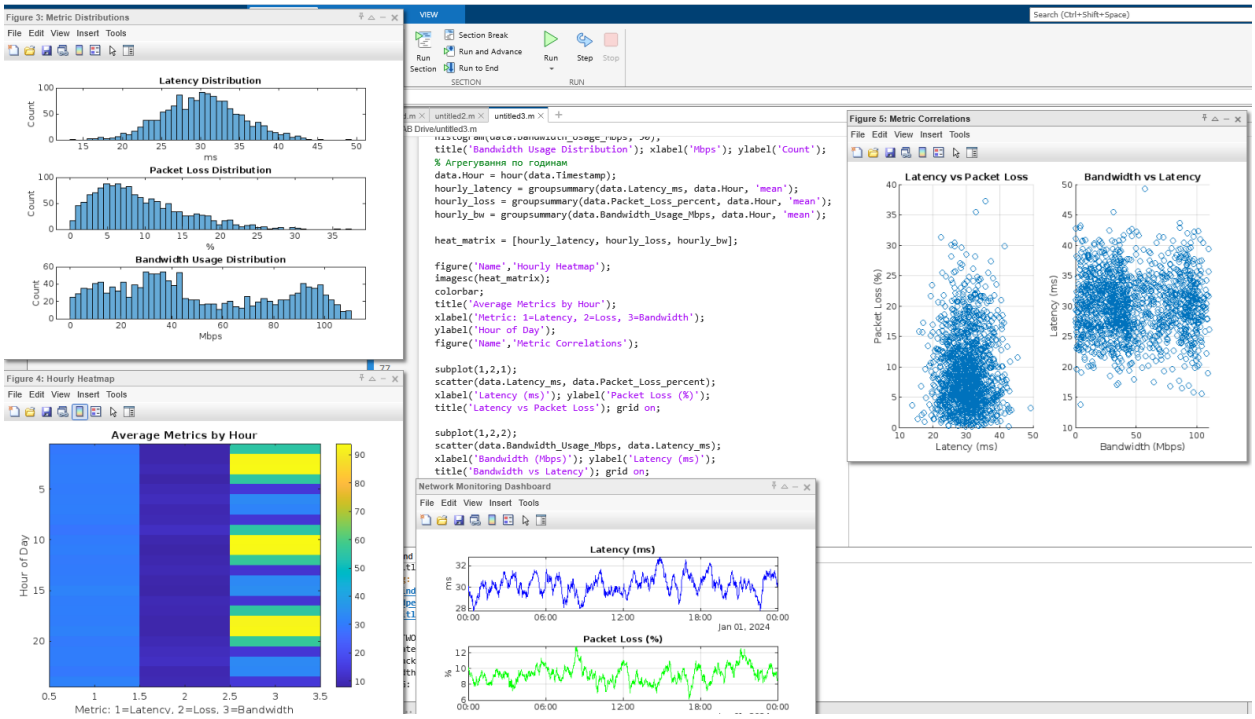

Рисунок 3.3 – Результат виконання скрипту в Matlab

На представленому графіку (рисунок 3.4) зображено результати візуального моніторингу ключових метрик мережевого трафіку протягом однієї доби. Графік розділений на три частини, кожна з яких ілюструє зміну певного параметра в часі на основі синтетично згенерованих даних.

У верхній частині зображено графік середньої затримки (Latency), вираженої в мілісекундах. Спостерігається характерна циклічна флуктуація

навантаження, з незначними варіаціями в межах 28–32 мс. Дані свідчать про стабільну роботу мережі без виражених піків затримки, що є ознакою відсутності суттєвих перевантажень або збоїв у каналі зв’язку.

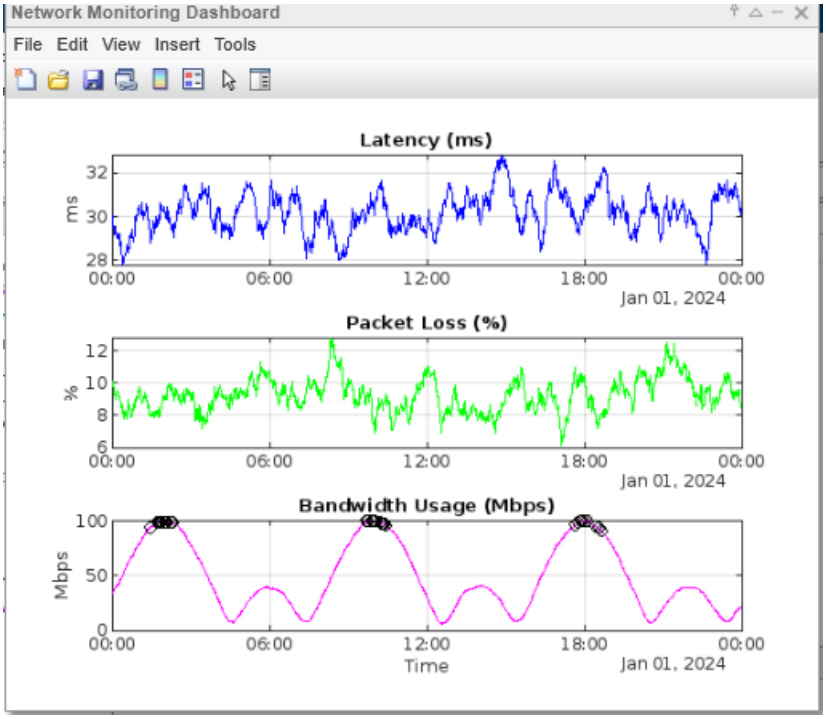

Рисунок 3.4 – Результати роботи

У центральній частині графіка відображено відсотковий рівень втрат пакетів (Packet Loss). Значення коливаються в діапазоні 6–12%, демонструючи загальну стабільність процесу передавання даних з поодинокими моментами підвищеної втрати. Такі показники можуть бути характерними для мереж із помірним навантаженням, де втрати не досягають критичних значень, однак їх регулярна поява потребує уваги з боку адміністратора.

У нижній частині розташовано графік, що демонструє зміну пропускної здатності каналу (Bandwidth Usage), вираженої в мегабітах за секунду. Відзначається виразна синусоїдальна структура графіка, яка вказує на чергування періодів інтенсивного і слабкого навантаження. На ділянках з максимумами трафіку зафіксовано пікові значення, які позначені спеціальними маркерами, що вказує на їх автоматичне виявлення в рамках

аналізу.

Загалом, візуалізація демонструє приклад комплексного моніторингу мережі з можливістю ідентифікації потенційно критичних ситуацій, характеру навантаження та загального стану комунікаційної інфраструктури. Такий підхід забезпечує основу для оперативного реагування на інциденти та подальшої оптимізації параметрів мережі.

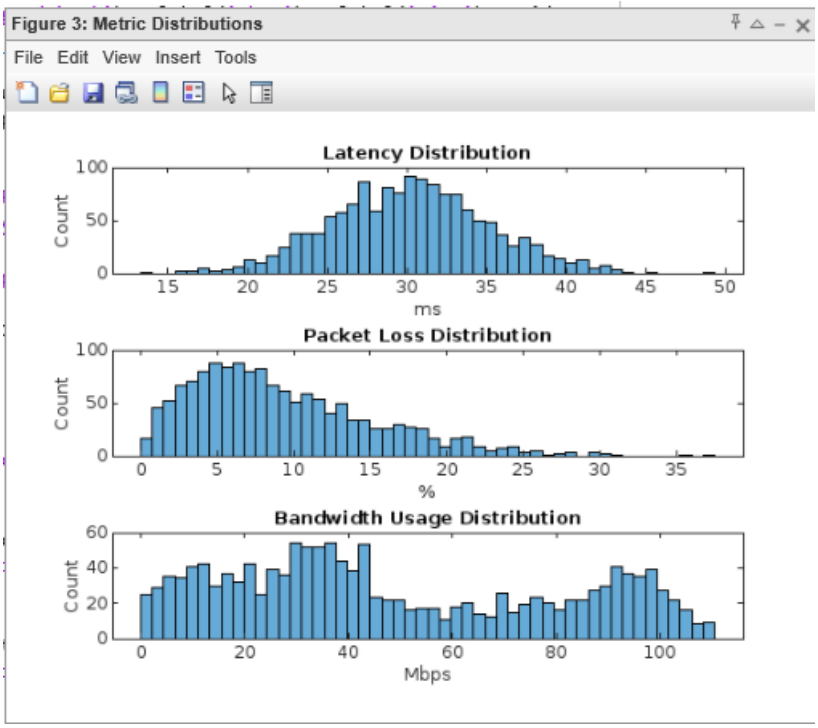

Рисунок 3.5 – Результат виконання скрипту в Matlab

На зображенні представлено три гістограми, які відображають розподіл ключових параметрів роботи корпоративної комп’ютерної мережі протягом добового інтервалу. Кожна з них демонструє частоту появи певного значення відповідної метрики, що дозволяє зробити висновки про характер навантаження на мережу.

Гістограма затримки (Latency Distribution), розміщена у верхній частині графіка, має форму, близьку до нормального розподілу. Центр мас припадає на значення близько 30 мілісекунд, що вказує на стабільну роботу мережі без значних викидів. Ширина розподілу є помірною, а симетричність свідчить

про відсутність систематичних збоїв або тривалих періодів із підвищеною затримкою.

У центральній частині подано розподіл втрат пакетів (Packet Loss Distribution), який має асиметричну форму, зміщену в бік нижчих значень. Основна маса спостережень зосереджена в діапазоні 5–10%, що може свідчити про задовільний стан мережі при наявності періодичних, але нетривалих перевантажень. Хвіст розподілу, що простягається до 30% і вище, відображає наявність одиничних критичних подій, які потребують уваги.

У нижній частині зображено гістограму використання пропускної здатності (Bandwidth Usage Distribution), яка демонструє багатовершинну структуру з декількома локальними максимумами. Такий розподіл є типовим для мереж із циклічним навантаженням, де періоди активної передачі даних чергуються зі спадом активності. Висока частота значень у діапазонах 20–40 Мбіт/с і 90–110 Мбіт/с свідчить про наявність денних та нічних піків навантаження, ймовірно зумовлених специфікою користувацької активності.

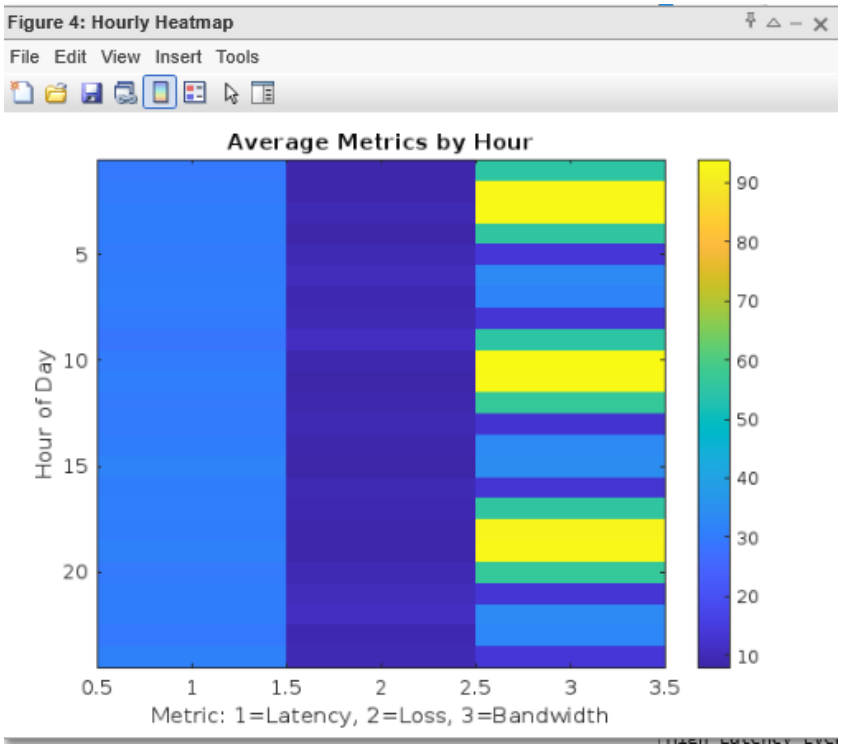

Рисунок 3.6 – Результат виконання скрипту в Matlab

На представленому графіку зображено теплову карту середніх значень мережевих метрик за годинами доби, що дозволяє здійснити швидкий візуальний аналіз змін навантаження впродовж 24-годинного періоду.

По вертикальній осі відкладено значення годин доби – від 0 до 23, а по горизонтальній – ідентифікатори трьох метрик:

- 1 – затримка (Latency),
- 2 – втрата пакетів (Packet Loss),
- 3 – використання пропускної здатності (Bandwidth Usage).

Кольорова шкала праворуч інтерпретує середні значення цих показників: від темно-фіолетового (низьке значення) до яскраво-жовтого (високе значення).

Аналіз теплової карти виявляє, що затримка має майже однорідне забарвлення вздовж усієї доби, що свідчить про стабільні середні значення незалежно від часу. Натомість втрата пакетів демонструє слабку варіативність, однак спостерігається деяке підвищення у вечірні години, що може бути пов’язано з піковим використанням мережі.

Найбільш виразну динаміку має пропускна здатність: блок з позначкою “3” чітко розділений на зони з високими та низькими значеннями. Це вказує на циклічність навантаження, де у певні години (ймовірно денні та ранкові) спостерігаються піки трафіку, що, ймовірно, відповідає робочому часу користувачів.

На рисунку 3.8 представлено кореляційний аналіз між основними мережевими метриками, виконаний у форматі діаграм розсіювання (scatter plots), які дозволяють оцінити потенційні залежності між параметрами на основі візуального спостереження.

Лівий графік, позначений як "Latency vs Packet Loss", ілюструє взаємозв’язок між затримкою (Latency) та втратою пакетів (Packet Loss). Точки даних розподілені доволі щільно у нижній частині графіка, зосереджуючись у межах 20–35 мс по осі X та 0–15% по осі Y.

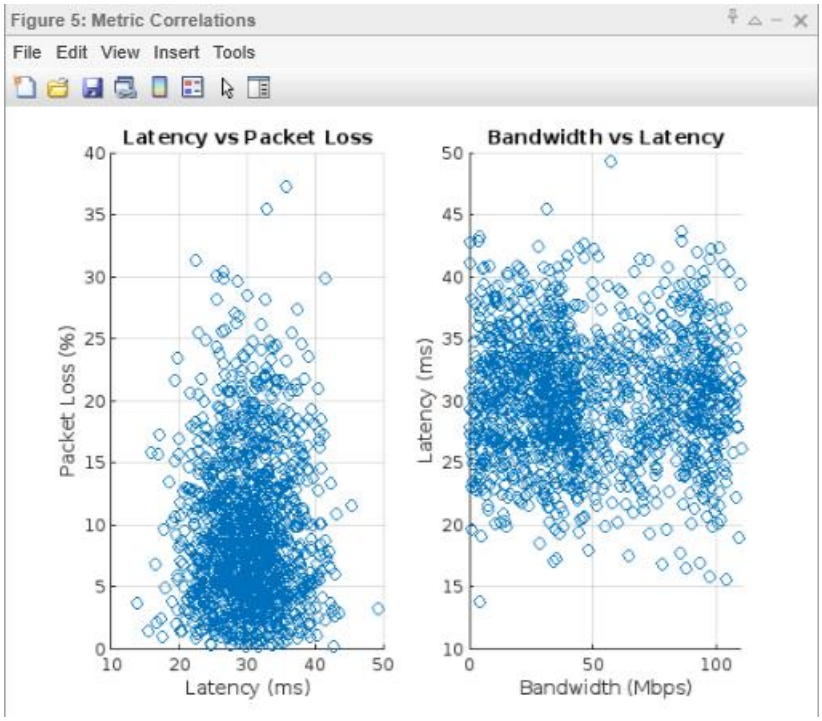

Рисунок 3.8 – Результат виконання скрипту в Matlab

Такий розподіл вказує на те, що при більшості спостережень втрати пакетів залишаються відносно низькими незалежно від рівня затримки. Відсутність вираженої лінійної структури чи нахилу хмари точок свідчить про слабку або відсутню пряму кореляцію між цими двома параметрами. Водночас окремі викиди на графіку демонструють ситуації, коли підвищена затримка супроводжується суттєвими втратами, що може вказувати на короткотривалі критичні події в мережі.

Правий графік, позначений як "Bandwidth vs Latency", відображає залежність між пропускною здатністю (Bandwidth) та затримкою. Основна маса точок згрупована в межах від 20 до 90 Мбіт/с по осі X та 25–35 мс по осі Y, причому горизонтальний розподіл є значно ширшим за вертикальний. Це вказує на те, що затримка залишається відносно стабільною навіть при суттєвих коливаннях у використанні пропускної здатності, а отже, між цими параметрами також відсутній чітко виражений лінійний зв’язок. Візуально можна відзначити деякі кластери точок, що можуть бути пов’язані з типами трафіку чи періодами доби, однак загальна тенденція свідчить про слабку кореляцію.

Таким чином, обидві діаграми демонструють переважно незалежну поведінку основних мережевих метрик, що може бути характерним для добре налаштованих мережевих середовищ або для синтетичних даних, у яких не задано явних функціональних залежностей між параметрами.

3.4 Результати в Google Colab

Код представлений в додатку Б.

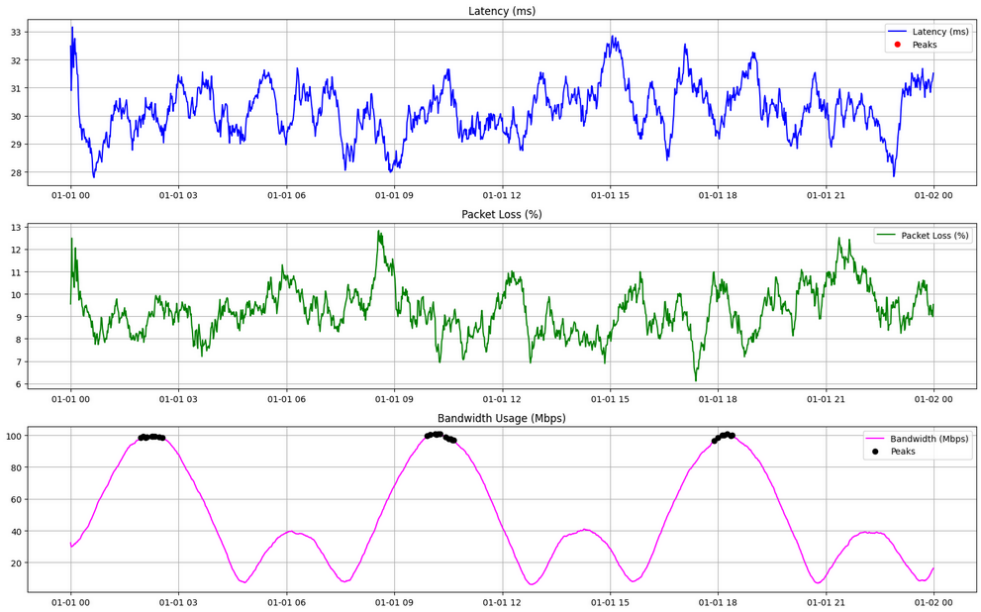

Рисунок 3.9 – Результати роботи в Google Colab

На зображенні представлено результат роботи інтегрованої системи моніторингу в середовищі Google Colab, яка виконує аналіз мережевих метрик на основі CSV-файлу, згенерованого у Matlab. Графік складається з трьох панелей, кожна з яких відображає окремий аспект продуктивності мережі у часовому вимірі.

У верхній частині зображено графік затримки (Latency) у мілісекундах. Застосоване згладжування дозволяє побачити динаміку зміни цього параметра протягом доби. Значення варіюються приблизно в межах 28–33 мс, що свідчить про стабільну роботу мережі без різких викидів. Червоні

маркери позначають пікові значення затримки, виявлені за допомогою алгоритму find_peaks, проте вони зустрічаються рідко й мають помірну амплітуду, що не є критичним.

У центральній частині подано графік втрати пакетів (Packet Loss) у відсотках. Візуалізація демонструє характерні хвилеподібні коливання з кількома моментами помітного підвищення до рівня 12–13%. Це вказує на можливі короткотривалі перевантаження мережі або локальні проблеми зі з'єднанням. Зелена крива чітко показує коливання навантаження протягом добового циклу, з переважанням значень у діапазоні 8–10%.

Нижній графік відображає пропускну здатність (Bandwidth Usage) у мегабітах на секунду. Синусоїдальний характер кривої свідчить про чітко виражену циклічну зміну навантаження, яка може відповідати робочим та неробочим періодам. Чорні точки позначають піки пропускної здатності, які досягають значень близько 100 Мбіт/с. Вони розташовані у ранкові та вечірні години, що характерно для звичайної активності в офісній або корпоративній мережі.

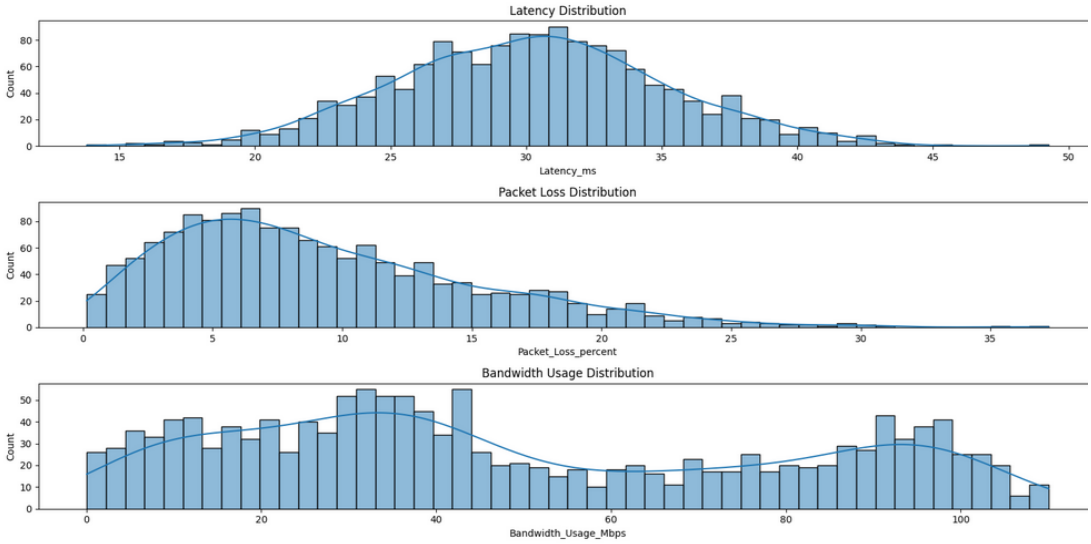

Рисунок 3.10 – Результати роботи в Google Colab

На графіку (рисунок 3.10) представлено розподіл основних мережевих метрик, які є об’єктом аналізу в межах розробленого методу моніторингу.

Візуалізація даних засобами Google Colab дозволяє оцінити статистичні характеристики показників, що були попередньо зібрані, оброблені та згладжені в Matlab.

Розподіл затримки демонструє близький до нормального профіль із незначним асиметричним зсувом вправо, що свідчить про наявність поодиноких епізодів підвищеного значення, однак загалом підтверджує стабільну роботу мережі. Аналіз втрат пакетів виявляє переважання низьких значень з поступовим спадом частоти при збільшенні відсотка втрати, що характерно для умов помірного мережевого навантаження без систематичних збоїв. Розподіл пропускної здатності має багатовершинний характер із декількома локальними максимумами, що є типовим для періодично навантажених мереж, де фази активності й спадів чергуються протягом доби.

Отримані результати підтверджують ефективність побудованої моделі, яка забезпечує наочну інтерпретацію закономірностей у поведінці мережі та дозволяє виявляти потенційно критичні відхилення у режимі реального часу.

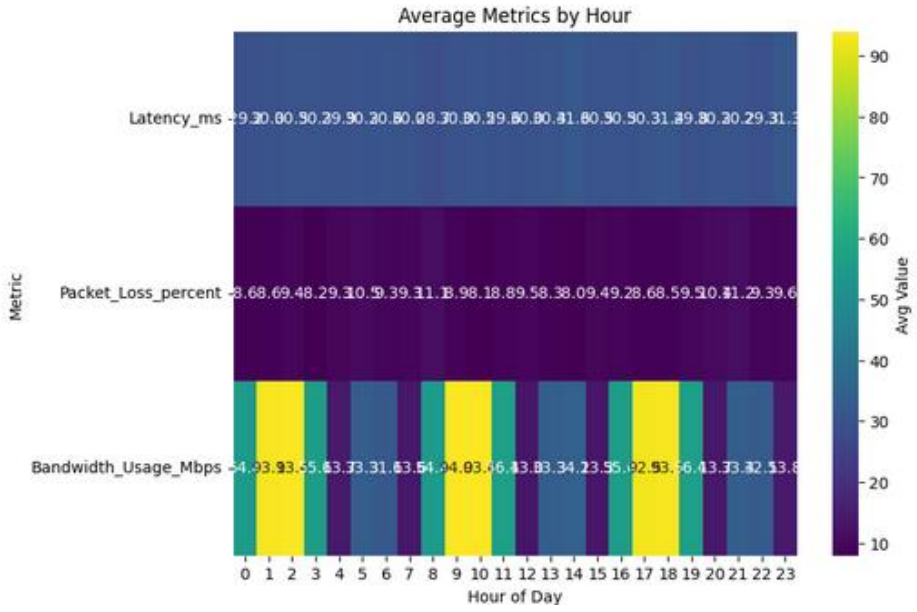

Рисунок 3.11 – Результати роботи в Google Colab

На графіку (рисунок 3.11) зображено теплову карту середніх значень ключових мережевих показників за годинами доби, що є частиною реалізації

розробленого методу моніторингу. Аналіз побудовано на агрегованих даних, попередньо зібраних у Matlab, і візуалізовано в Google Colab для виявлення добових закономірностей.

Рівень затримки протягом усієї доби зберігається на стабільному рівні з незначними варіаціями в межах 29–31 мс, що вказує на відсутність серйозних перевантажень або аномалій у роботі мережі. Втрата пакетів демонструє дещо більшу змінність, з підвищенням показників у ранкові та вечірні години, що може бути ознакою зростання трафіку в ці періоди. Найбільш виразну динаміку спостерігаємо у використанні пропускної здатності: піки навантаження трапляються з інтервалами, що співпадають із типовим робочим ритмом, зокрема близько 9:00, 13:00 та 17:00, де значення перевищують 90 Мбіт/с.

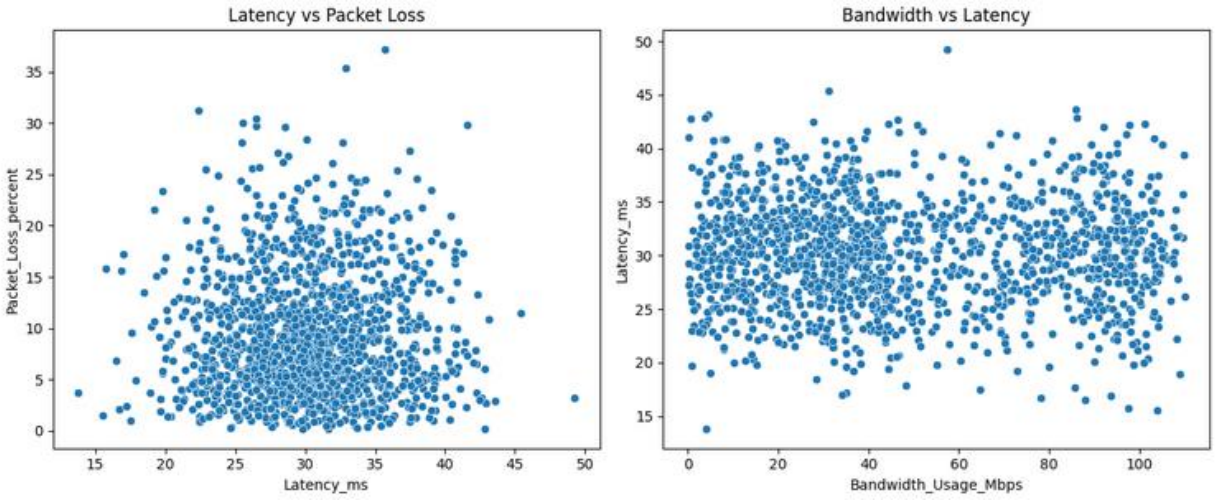

Рисунок 3.12 – Результати роботи в Google Colab

На зображенні (рисунок 3.12) представлено графіки кореляційного аналізу між основними показниками стану мережі, які були зібрані у Matlab і проаналізовані в Google Colab у межах розробленої інтегрованої системи моніторингу.

Лівий графік демонструє співвідношення між затримкою (Latency) та втратою пакетів (Packet Loss). Незважаючи на щільне скупчення точок у межах 25–35 мс по осі X і 5–15% по осі Y, відсутність чітко вираженої

тенденції або нахилу хмари точок свідчить про низьку кореляцію між цими двома параметрами. Це означає, що підвищення затримки не обов’язково супроводжується втратою пакетів і навпаки, що характерно для добре налаштованих або відносно стабільних мереж.

Правий графік показує залежність затримки від використання пропускної здатності (Bandwidth Usage). Видимий горизонтальний розподіл свідчить про те, що незалежно від обсягу переданих даних, затримка залишається в межах 25–35 мс, а отже, затримка не є функцією навантаження в межах заданого інтервалу часу. Такий результат підтверджує ефективність роботи мережі, де канали передавання даних справляються з коливаннями трафіку без деградації часу відповіді.

Отримані діаграми є важливою частиною візуального аналізу у рамках методики, адже вони підтверджують відсутність критичних залежностей, що могло б вимагати втручання адміністратора. Крім того, такі графіки є зручним засобом для ідентифікації аномальних точок або кластерів, які можуть бути ознакою локалізованих проблем.

ВИСНОВКИ

У ході виконання роботи було реалізовано програмні засоби моніторингу корпоративної комп'ютерної мережі, які передбачають інтеграцію локального інструментарію Matlab із хмарними засобами обробки даних у середовищі Google Colab. Застосування багаторівневої архітектури моніторингу забезпечило послідовний перехід від збору первинних даних до їх аналітичної інтерпретації, що дало змогу не лише виявляти поточні аномалії, а й формувати основи для прогнозного аналізу стану мережі.

Результати синтетичного моделювання показали доцільність використання обраних метрик: затримки, пропускної здатності, втрат пакетів та доступності як основних індикаторів продуктивності та надійності мережевої інфраструктури. Побудовані візуалізації дозволили ідентифікувати типові сценарії навантаження та часові інтервали з підвищеним ризиком порушення якості сервісів. Реалізовані механізми згладжування, виявлення пікових значень та вивчення кореляцій між параметрами продемонстрували високу ефективність для формування оперативної аналітичної інформації.

Інтеграція Matlab і Google Colab у межах єдиної аналітичної платформи дозволила забезпечити як точну математичну обробку даних, так і мобільність, візуальну інтерпретацію та спільний доступ до результатів. Такий підхід є особливо актуальним у контексті розподілених IT-систем, де важливим є як контроль у реальному часі, так і гнучкість аналітичних засобів. Запропонована система є масштабованою та адаптивною, що дозволяє застосовувати її як у навчальних, так і в промислових умовах.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Tanenbaum, A. S. та Wetherall, D. J., «Computer Networks, Fifth Edition,» Prentice Hall, 2010. 960 p.

2. Abhishek, S. та Pranav, K., «Network Monitoring and Analysis Using Wireshark,» в Proceedings of International Conference on Computing and Communication Systems, 2019. P. 234-241.

3. Ahmed, M., Mahmood, A. N. та Hu, J., «A Survey of Network Anomaly Detection Techniques,» Journal of Network and Computer Applications, vol. 60, 2016. P. 19-31.

4. Al-Sakib Khan Pathan, «The State of the Art in Intrusion Prevention and Detection,» CRC Press, 2014. 487 p.

5. Barford, P. та Plonka, D., «Characteristics of Network Traffic Flow Anomalies,» в Proceedings of Internet Measurement Workshop, 2001. P. 69-73.

6. akhina, A., Crovella, M. та Diot, C., «Mining Anomalies Using Traffic Feature Distributions,» в Proceedings of ACM SIGCOMM, 2005. P. 217-228.

7. Liu, G., Ramakrishnan, K. K. та Sridharan, M., «Network Monitoring and Management,» в Computer Communications and Networks, Springer, 2013. P. 123-156.

8. Mahmoud, Q. H., «Learning Wireless Java: Help for New J2ME Developers,» O'Reilly Media, 2002. 267 p.