Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

Система моніторингу мережного трафіку для виявлення перевантажень і аномалій у роботі мереж
Назва теми

Рівень вищої освіти *перший (бакалаврський)*

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Шифр КвРКІ 22030.22.01.54 ПЗ

Виконав здобувач IV курсу, група КІ2-22-1		Підпис	Владислав КАШТАН Ініціали, прізвище
Керівник	доктор філософії Науковий ступінь, учене звання	Підпис	Сергій СВИСТУН Ініціали, прізвище
Нормоконтролер	канд. фіз.-мат. наук, доц. Науковий ступінь, учене звання	Підпис	Тетяна КИСІЛЬ Ініціали, прізвище
		Підпис	Ольга ПАВЛОВА Ініціали, прізвище

До захисту допускаю:
завідувач кафедри КІІС
«01» червня 2026 р.
дата

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Рівень вищої освіти перший (бакалаврський)

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ
Завідувачка кафедри КІІС
_____ Ольга ПАВЛОВА

" 10 " 01 2026 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Каштану Владиславу В'ячеславовичу
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Система моніторингу мережного трафіку для виявлення перевантажень і аномалій у роботі мереж
Керівник проекту (роботи) Свистун Сергій Олегович, доктор філософії.
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання
Затверджена наказом ректора університету від 20.01.2026 р. № 7
2. Термін подання здобувачем роботи на кафедру 01.06.2026 р.
3. Вихідні дані до роботи Завдання на кваліфікаційну роботу
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз предметної області та постановка задачі моніторингу мережного трафіку
Проєктування системи моніторингу мережного трафіку
Реалізація системи моніторингу мережного трафіку та аналіз результатів
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Архітектура системи
Види систем моніторингу мережевого трафіку
Результати роботи системи

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийн

7. Дата видачі завдання «_10_»_____01_____2026 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітк
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	10.01.2026	виконан
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2026	виконан
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	01.03.2026	виконан
4	Робота над розділом 2 – вибір компонентів та проєктування системи моніторингу мережного трафіку	01.04.2026	виконан
5	Робота над розділом 3 – реалізація системи моніторингу мережного трафіку та аналіз результатів	29.04.2026	виконан
6	Оформлення пояснювальної записки згідно вимог	25.05.2026	виконан
7	Попередній захист ВКР	26.05.2026	виконан
8	Захист ВКР на засіданні ЕК	Червень 2026 року	

Здобувач _____ Владислав КАШТАН
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Сергій СВИСТУН
Підпис Ім'я, ПРІЗВИЩЕ

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 22030.22.01.54 ПЗ	Пояснювальна записка	63		
			Графічні матеріали			
2		КвРКІ 22030.22.01.54 Е8	Архітектура системи	1		
3		КвРКІ 22030.22.01.54 Е8	Види систем моніторингу мережного трафіку	1		
4		КвРКІ 22030.22.01.54 Е8	Результати роботи системи	1		

Зм	Арк	№ докум	Підпис	Дата	КвРКІ 22030.22.01.54 ВП		
Розробив		Каштан			Відомість проекту	Літера	Аркуш	Аркушів
Перевір.		Свистун				У	1	1
Н. контр.		Кисіль				ХНУ, КІ2-22-1		
Затв.		Павлова						

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система моніторингу мережного трафіку для виявлення перевантажень і аномалій у роботі мереж».

Автор роботи: Владислав КАШТАН

Керівник роботи: Сергій СВИСТУН

Пояснювальна записка: 63 с., 15 рис., 9 табл., 3 дод., 49 джерел.

Графічна частина: 3 креслення.

АНОМАЛІЇ, МЕРЕЖНИЙ ТРАФІК, ПЕРЕВАНТАЖЕННЯ, РОЗПОДІЛЕНА АРХІТЕКТУРА, СИСТЕМА МОНІТОРИНГУ, МОНІТОРИНГ, ПРОТОКОЛИ ВЗАЄМОДІЇ.

Кваліфікаційна робота бакалавра присвячена розробці та дослідженню системи моніторингу мережного трафіку для виявлення перевантажень та аномалій у роботі комп'ютерних мереж. Актуальність теми зумовлена зростанням обсягів мережевого трафіку, ускладненням структури сучасних інформаційних систем та необхідністю забезпечення стабільної, надійної і безпечної роботи мережевої інфраструктури. Сучасні мережі функціонують в умовах високого навантаження та постійних змін, що потребує використання ефективних засобів моніторингу, здатних здійснювати безперервний збір, обробку та аналіз мережних даних у режимі реального часу. Використання сучасних підходів до аналізу мережного трафіку, зокрема статистичних, порогових та потокових методів, дозволяє своєчасно виявляти перевантаження, аномалії та потенційні загрози у роботі мережі.

Метою даної бакалаврської роботи є виявлення перевантажень та аномалій у роботі мереж шляхом розробка системи моніторингу мережного трафіку.

Підпис здобувача

30.05.2026

Дата

ЗМІСТ

ВСТУП

Актуальність дослідження. Сучасний розвиток інформаційних технологій супроводжується стрімким зростанням обсягів передавання даних у комп'ютерних мережах. Розширення мережевої інфраструктури, збільшення кількості користувачів та сервісів, а також підвищення вимог до якості обслуговування зумовлюють необхідність забезпечення стабільної, надійної та безпечної роботи мереж. У цих умовах особливого значення набуває моніторинг мережного трафіку як інструмент контролю стану мережі.

Однією з основних проблем сучасних мереж є виникнення перевантажень та аномалій у мережному трафіку. Перевантаження призводять до зниження продуктивності мережі, збільшення затримок та втрат пакетів, що негативно впливає на якість надання послуг. Аномалії можуть бути викликані як технічними причинами, так і навмисними діями, зокрема мережевими атаками або несанкціонованим доступом до ресурсів.

Своєчасне виявлення таких явищ є важливим завданням для забезпечення ефективного функціонування мережі. Для цього використовуються системи моніторингу, які дозволяють здійснювати збір, обробку та аналіз мережного трафіку. Однак існуючі рішення не завжди забезпечують необхідний рівень швидкодії, точності або масштабованості, що обумовлює актуальність розробки нових підходів до побудови таких систем.

Метою даної бакалаврської роботи є виявлення перевантажень та аномалій у роботі мереж шляхом розробка системи моніторингу мережного трафіку для виявлення.

Для досягнення поставленої мети необхідно вирішити такі задачі:

– проаналізувати сучасний стан та особливості функціонування комп'ютерних мереж;

– дослідити існуючі методи та засоби моніторингу мережного трафіку;

– визначити основні причини виникнення перевантажень та аномалій;

– розглянути методи їх виявлення;

– розробити структуру системи моніторингу мережного трафіку;

– реалізувати програмну систему моніторингу;

– провести тестування та оцінку ефективності розробленого рішення.

Об’єктом дослідження є процеси передачі та обробки даних у комп’ютерних мережах.

Предметом дослідження є методи та засоби моніторингу мережного трафіку для виявлення перевантажень та аномалій.

Практичне значення роботи полягає у можливості використання розробленої системи для контролю стану мережі, своєчасного виявлення проблем та підвищення ефективності її функціонування.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ МОНІТОРИНГУ МЕРЕЖНОГО ТРАФІКУ

1.1 Аналіз сучасного стану мережевих технологій

Сучасний розвиток інформаційних технологій безпосередньо пов’язаний із стрімкою еволюцією комп’ютерних мереж, які стали фундаментом цифрового суспільства. Упродовж останніх десятиліть мережеві технології зазнали суттєвих змін, що обумовлено зростанням обсягів переданих даних, появою нових сервісів та підвищенням вимог до якості обслуговування. Сьогодні комп’ютерні мережі використовуються для забезпечення функціонування критично важливих систем, включаючи банківські сервіси, телекомунікації, хмарні обчислення та інтернет речей.

Однією з ключових характеристик сучасних мереж є їх висока пропускна здатність. Завдяки впровадженню оптичних каналів зв’язку та сучасних протоколів передачі даних стало можливим забезпечення швидкостей на рівні гігабітів і навіть терабітів на секунду. Проте разом із цим зростає і навантаження на мережеву інфраструктуру, що створює нові виклики для її ефективного функціонування.

Важливою тенденцією розвитку є перехід до хмарних технологій. Хмарні сервіси дозволяють зберігати та обробляти великі обсяги даних на віддалених серверах, що значно зменшує вимоги до локальних ресурсів користувачів. Водночас це призводить до суттєвого збільшення мережного трафіку, оскільки значна частина операцій переноситься у мережеве середовище. У таких умовах стабільність мережі стає критично важливою.

Ще одним важливим напрямком розвитку є віртуалізація мережевих ресурсів. Використання технологій віртуалізації дозволяє створювати віртуальні мережі, сервери та інші компоненти інфраструктури, що підвищує гнучкість і масштабованість систем. Проте це також ускладнює процес моніторингу, оскільки фізична інфраструктура вже не відображає реальної

логічної структури мережі.

Значний вплив на розвиток мереж має концепція інтернету речей (IoT), яка передбачає підключення великої кількості пристроїв до мережі. Це можуть бути сенсори, побутова техніка, промислове обладнання тощо. Кількість таких пристроїв постійно зростає, що призводить до появи великої кількості малих за обсягом, але частих мережевих запитів. У результаті формується новий тип трафіку, який потребує спеціалізованих методів аналізу.

Не менш важливою є тенденція зростання мобільного трафіку. Завдяки розвитку технологій 4G та 5G користувачі отримали можливість швидкого доступу до мережі з мобільних пристроїв. Це призвело до значного збільшення обсягів потокового відео, онлайн-ігор та інших ресурсомістких сервісів. Мобільний трафік характеризується високою динамічністю та нерівномірністю, що ускладнює його прогнозування.

У таблиці 1.1 наведено основні тенденції розвитку мережевих технологій та їх вплив на мережний трафік.

Таблиця 1.1 – Основні тенденції розвитку мережевих технологій

Тенденція	Характеристика	Вплив на трафік
Хмарні технології	Обробка даних на віддалених серверах	Збільшення обсягу трафіку
Віртуалізація	Створення віртуальних ресурсів	Ускладнення моніторингу
IoT	Велика кількість пристроїв	Зростання кількості запитів
5G	Високошвидкісний мобільний інтернет	Збільшення потокового трафіку
Дата-центри	Централізація обробки даних	Високе навантаження на мережу

Окрему увагу слід приділити розвитку дата-центрів, які є ядром сучасної мережевої інфраструктури (рисунок 1.1).

Рисунок 1.1 – Структура сучасної мережевої архітектури

Саме в дата-центрах зосереджені основні обчислювальні ресурси та системи зберігання даних. Вони обслуговують мільйони користувачів одночасно, що створює значні навантаження на мережу. Для забезпечення ефективної роботи таких систем необхідно використовувати високопродуктивні мережеві рішення та сучасні засоби моніторингу.

Зростання складності мережевих систем обумовлює необхідність використання нових підходів до управління трафіком. Традиційні методи вже не забезпечують достатньої ефективності, особливо в умовах великих обсягів даних та високих швидкостей передачі.

Аналіз сучасного стану мережевих технологій дозволяє зробити висновок, що мережі стають більш складними, динамічними та навантаженими. Це, у свою чергу, підвищує вимоги до систем моніторингу, які повинні забезпечувати обробку великих обсягів даних у реальному часі, виявлення перевантажень та аномалій, а також підтримку стабільної роботи мережі.

Продовжуючи аналіз сучасних мережевих технологій, слід відзначити важливу роль програмно-визначених мереж (SDN, Software-Defined Networking). Даний підхід передбачає відокремлення площини керування мережею від площини передачі даних, що дозволяє централізовано управляти всією мережею. Використання SDN значно підвищує гнучкість мережевої

інфраструктури, дозволяє швидко змінювати конфігурацію та оптимізувати маршрутизацію трафіку. Водночас це створює нові виклики для систем моніторингу, оскільки необхідно враховувати не лише фізичні, але й логічні зміни в мережі.

Ще одним перспективним напрямком є використання технологій NFV (Network Functions Virtualization), які дозволяють реалізовувати мережеві функції у вигляді програмного забезпечення. Це означає, що такі компоненти, як маршрутизатори, брандмауери та балансувальники навантаження, можуть працювати на звичайних серверах без використання спеціалізованого обладнання. З одного боку, це знижує витрати на інфраструктуру, а з іншого боку ускладнює процес контролю та аналізу трафіку, оскільки функції мережі стають розподіленими та динамічними.

Важливим аспектом сучасних мереж є забезпечення якості обслуговування (QoS, Quality of Service). QoS передбачає пріоритезацію трафіку залежно від типу сервісу. Наприклад, голосовий та відеотрафік потребують мінімальних затримок, тоді як передача файлів може виконуватися з менш суворими вимогами. Для реалізації QoS використовуються різні механізми, такі як черги, обмеження пропускної здатності та маркування пакетів. Однак реалізація цих механізмів потребує постійного моніторингу стану мережі.

Слід також зазначити, що сучасні мережі активно використовують механізми балансування навантаження. Балансувальники дозволяють рівномірно розподіляти трафік між серверами, що підвищує продуктивність та відмовостійкість системи. Проте неправильна конфігурація або перевантаження окремих вузлів може призвести до виникнення вузьких місць, які складно виявити без спеціалізованих засобів моніторингу.

Окрему увагу необхідно приділити питанням безпеки мереж. З розвитком технологій зростає і кількість кіберзагроз, таких як DDoS-атаки, перехоплення даних, несанкціонований доступ та інші види атак. Сучасні мережі повинні

мати вбудовані механізми захисту, включаючи системи виявлення вторгнень, шифрування даних та автентифікацію користувачів. У цьому контексті моніторинг мережного трафіку стає важливим інструментом для виявлення підозрілої активності.

Крім того, варто враховувати вплив технологій великих даних (Big Data) на мережеву інфраструктуру. Обробка великих обсягів інформації потребує передачі значних потоків даних між вузлами, що створює додаткове навантаження на мережу. Для ефективної роботи таких систем необхідно забезпечити високу пропускну здатність та мінімальні затримки.

Вплив сучасних мережевих технлогій на системи моніторингу представлені в таблиці 1.2.

Таблиця 1.2 – Вплив сучасних мережевих технлогій на системи моніторингу

Технологія	Основна особливість	Вимоги до моніторингу
SDN	Централізоване управління	Аналіз логічної структури мережі
NFV	Віртуалізація функцій	Моніторинг віртуальних компонентів
QoS	Пріоритезація трафіку	Контроль затримок і втрат
IoT	Велика кількість пристроїв	Обробка великої кількості подій
Big Data	Великі обсяги даних	Висока продуктивність системи

Отже, проведений аналіз підтверджує, що розвиток мережевих технологій безпосередньо впливає на складність задач моніторингу та вимагає використання нових підходів і методів для забезпечення ефективної роботи мережевих систем.

1.2 Аналіз існуючих систем моніторингу мережного трафіку

У сучасних комп’ютерних мережах моніторинг трафіку є невід’ємною складовою забезпечення їх стабільного функціонування. Існує значна кількість програмних та апаратних рішень, призначених для аналізу мережевої активності, контролю навантаження, а також виявлення аномалій і потенційних загроз. Кожна з таких систем має свої особливості, переваги та обмеження, що обумовлює необхідність їх детального аналізу.

Системи моніторингу мережного трафіку можна класифікувати за різними критеріями, зокрема за рівнем аналізу, функціональним призначенням та способом обробки даних. Найбільш поширеним є поділ на системи загального моніторингу, системи глибокого аналізу трафіку та системи виявлення вторгнень.

Системи загального моніторингу призначені для контролю стану мережевої інфраструктури в цілому. Вони забезпечують збір статистичних даних про використання ресурсів, завантаження каналів зв’язку, доступність мережевих вузлів та інші параметри. Такі системи дозволяють адміністраторам отримувати загальне уявлення про стан мережі та своєчасно реагувати на відхилення. Основною їх перевагою є простота використання та можливість інтеграції з різними мережевими пристроями. Проте вони зазвичай не забезпечують детального аналізу трафіку, що обмежує їх застосування для виявлення складних аномалій.

Іншою важливою групою є системи глибокого аналізу трафіку, які здійснюють детальне дослідження мережевих пакетів. Вони дозволяють аналізувати вміст пакетів, визначати типи протоколів, виявляти підозрілі шаблони та досліджувати поведінку користувачів.

Такі системи широко використовуються для діагностики проблем у мережі та аналізу її продуктивності. Водночас їх використання пов’язане з високими вимогами до обчислювальних ресурсів, оскільки обробка великої

кількості пакетів у реальному часі є складним завданням.

Окрему категорію становлять системи виявлення та запобігання вторгненням (IDS/IPS). Вони призначені для забезпечення безпеки мережі шляхом аналізу трафіку на наявність ознак атак. Такі системи можуть працювати як на основі сигнатурного аналізу, так і з використанням поведінкових моделей. Перевагою є можливість автоматичного реагування на загрози, однак їх ефективність значною мірою залежить від актуальності бази сигнатур та налаштувань системи.

У таблиці 1.3 наведено узагальнену класифікацію систем моніторингу мережного трафіку.

Таблиця 1.3 – Класифікація систем моніторингу мережного трафіку

Тип системи	Призначення	Переваги	Недоліки
Загальний моніторинг	Контроль стану мережі	Простота, наочність	Низька деталізація
Аналіз трафіку	Детальний аналіз пакетів	Висока точність	Високе навантаження
IDS/IPS	Виявлення атак	Безпека	Потреба в налаштуванні

Серед сучасних систем моніторингу слід виділити як комерційні, так і відкриті рішення. Комерційні системи, як правило, мають широкий функціонал, технічну підтримку та зручний інтерфейс, однак їх використання пов’язане з високими фінансовими витратами. Відкриті рішення є більш доступними, але потребують додаткових зусиль для налаштування та підтримки.

Важливою характеристикою сучасних систем є використання потокових технологій аналізу, таких як NetFlow, sFlow або IPFIX. Ці технології дозволяють отримувати агреговану інформацію про мережеві потоки без необхідності аналізу кожного окремого пакета. Це значно зменшує

навантаження на систему та дозволяє масштабувати рішення для великих мереж. Однак такий підхід має обмежену деталізацію і не дозволяє аналізувати вміст трафіку.

Ще одним напрямком розвитку є використання розподілених систем моніторингу. У таких системах збір даних здійснюється на різних вузлах мережі, після чого інформація передається до центрального сервера для обробки. Це дозволяє підвищити надійність та масштабованість системи, але ускладнює її архітектуру.

На рисунку 1.2 представлено узагальнену архітектуру системи моніторингу мережного трафіку.

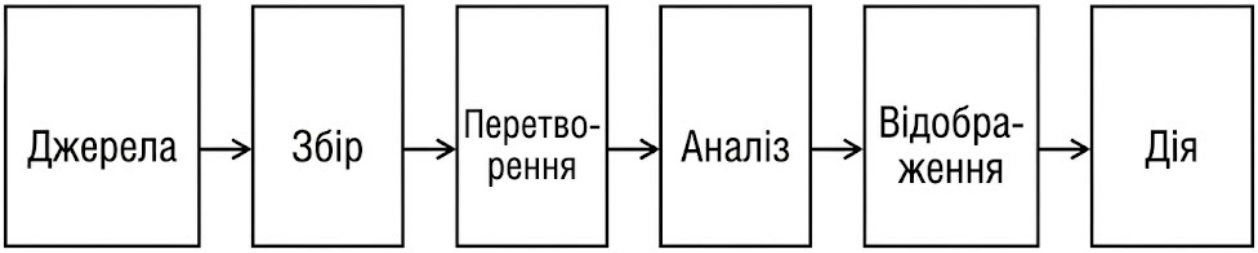


Рисунок 1.2 – Архітектура системи моніторингу

Аналіз існуючих систем показує, що жодна з них не є універсальною. Вибір конкретного рішення залежить від вимог до системи, масштабів мережі та поставлених задач. У більшості випадків використовується комбінований підхід, який поєднує кілька методів моніторингу.

Серед основних проблем існуючих систем слід виділити складність обробки великих обсягів даних, обмежену швидкість реагування на аномалії та необхідність ручного налаштування. Крім того, багато систем не здатні ефективно працювати в умовах динамічних змін мережевої інфраструктури.

Таким чином, проведений аналіз показує, що існуючі системи моніторингу мають як значні переваги, так і певні недоліки. Це обумовлює необхідність розробки нових підходів до моніторингу мережного трафіку, які б

поєднували високу точність, швидкодію та адаптивність до змін у мережі.

1.3 Аномалії в мережному трафіку та методи їх виявлення

У сучасних комп'ютерних мережах однією з ключових задач забезпечення їх стабільної та безпечної роботи є своєчасне виявлення аномалій у мережному трафіку. Аномалії являють собою відхилення від нормальної поведінки мережі, які можуть свідчити про наявність збоїв, перевантажень або несанкціонованої активності. Виявлення таких відхилень є складним завданням через різноманітність мережевих процесів та динамічний характер трафіку.

Під аномалією в мережному трафіку розуміють будь-яку подію або сукупність подій, які суттєво відрізняються від типової моделі функціонування мережі. Це можуть бути як короткочасні сплески навантаження, так і тривалі зміни у структурі трафіку. Важливою особливістю аномалій є те, що вони не завжди мають явно виражені ознаки, що ускладнює їх виявлення.

Аномалії в мережі можуть виникати з різних причин, серед яких можна виділити:

- технічні збої обладнання;
- помилки конфігурації мережевих пристроїв;
- перевантаження каналів зв'язку;
- дії користувачів;
- зовнішні кіберзагрози.

У загальному випадку аномалії поділяються на декілька основних типів: точкові, контекстні та колективні. Точкові аномалії характеризуються одиничними відхиленнями від нормальних значень параметрів. Контекстні аномалії залежать від умов, у яких відбувається подія, наприклад, збільшення трафіку у нічний час може розглядатися як підозріле. Колективні аномалії являють собою сукупність подій, які разом формують нетипову поведінку.

У таблиці 1.4 наведено класифікацію аномалій у мережному трафіку.

Таблиця 1.5 – Класифікація аномалій мережного трафіку

Тип аномалії	Характеристика	Приклад
Точкова	Одиничне відхилення	Різкий стрибок трафіку
Контекстна	Залежить від умов	Активність у нетиповий час
Колективна	Група подій	DDoS-атака

Одним із основних інструментів виявлення аномалій є системи виявлення вторгнень (IDS, Intrusion Detection Systems). Такі системи аналізують мережевий трафік з метою виявлення підозрілої активності та потенційних загроз. IDS можуть бути мережевими (NIDS), які контролюють трафік у мережі, та хостовими (HIDS), які аналізують події на окремих пристроях.

Принцип роботи IDS базується на аналізі мережевих пакетів або потоків даних. У процесі роботи система порівнює отримані дані з певними правилами або моделями нормальної поведінки. У разі виявлення відхилень формується повідомлення про можливу загрозу.

Існують два основні підходи до виявлення аномалій у IDS: сигнатурний та аномалійний.

Сигнатурний підхід передбачає використання бази відомих шаблонів атак. Кожна сигнатура описує характерні ознаки певної загрози, наприклад, специфічну послідовність пакетів або особливості заголовків. Основною перевагою цього методу є висока точність виявлення відомих атак та низька кількість хибних спрацювань. Проте він не дозволяє виявляти нові або модифіковані загрози.

Аномалійний підхід базується на визначенні нормальної поведінки мережі та виявленні відхилень від неї. Для цього використовуються статистичні методи, які аналізують такі параметри, як інтенсивність трафіку, розподіл пакетів та час передачі. Перевагою є можливість виявлення невідомих атак, однак цей метод може генерувати більшу кількість хибних спрацювань.

На рисунку 1.3 представлено принцип роботи системи IDS.

Рисунок 1.3 – Принцип роботи системи IDS

Для виявлення аномалій також широко застосовуються порогові методи. Вони передбачають встановлення граничних значень для певних параметрів, наприклад, обсягу трафіку або кількості запитів. Якщо значення перевищує встановлений поріг, система генерує сигнал про можливу аномалію. Такий підхід є простим у реалізації, але потребує правильного налаштування порогів.

Важливу роль у виявленні аномалій відіграє аналіз мережевих потоків. Використання технологій NetFlow або подібних дозволяє отримувати агреговану інформацію про трафік, включаючи джерело, призначення, обсяг та

тривалість з’єднання. Це дає змогу швидко виявляти підозрілі шаблони, такі як велика кількість з’єднань від одного джерела.

Серед найбільш поширених прикладів аномалій можна виділити:

– DDoS-атаки, які характеризуються різким збільшенням кількості запитів;

– сканування портів, що проявляється у великій кількості спроб підключення;

– спроби підбору паролів (brute force);

– аномальне збільшення вихідного трафіку, що може свідчити про витік даних;

– незвичну активність користувачів.

Серед наведених прикладів аномалій особливе місце займають DDoS-атаки, які є однією з найбільш небезпечних форм порушення роботи мережі. Вони характеризуються різким і значним збільшенням кількості запитів до сервера або мережевого ресурсу, що перевищує його обчислювальні можливості.

У результаті цього сервер або мережевий вузол не може обробляти легітимні запити користувачів, що призводить до відмови в обслуговуванні. Особливістю таких атак є їх розподілений характер, оскільки запити надходять одночасно з великої кількості пристроїв, які часто є частиною бот-мереж. Це ускладнює процес виявлення джерела атаки та її нейтралізації.

У мережному трафіку DDoS-атаки проявляються у вигляді різкого зростання кількості пакетів, збільшення навантаження на канал зв’язку та зниження швидкості обробки запитів.

Іншою поширеною формою аномальної активності є сканування портів, яке використовується зловмисниками для дослідження мережевої інфраструктури. Процес сканування полягає у перевірці доступності портів на віддаленому вузлі з метою виявлення відкритих сервісів, які можуть містити вразливості.

У більшості випадків сканування здійснюється автоматизованими програмами, які за короткий час генерують велику кількість запитів до різних портів. У мережному трафіку це проявляється у вигляді великої кількості коротких з’єднань, які не завершуються повноцінною передачею даних. Виявлення такої активності є важливим етапом запобігання подальшим атакам, оскільки сканування часто передує спробам несанкціонованого доступу.

До аномалій також належать спроби підбору паролів, відомі як brute force атаки. Вони полягають у багаторазовому введенні різних комбінацій облікових даних з метою отримання доступу до системи. Такі атаки можуть бути спрямовані на різні сервіси, включаючи веб-додатки, віддалений доступ та електронну пошту.

У мережному трафіку brute force атаки проявляються у вигляді великої кількості запитів на автентифікацію за короткий проміжок часу. Це створює додаткове навантаження на сервери та може призводити до їх часткового або повного перевантаження. Крім того, у разі успішного підбору пароля зловмисник отримує можливість виконувати дії від імені користувача, що становить серйозну загрозу безпеці.

Ще одним важливим типом аномалії є різке збільшення вихідного трафіку, яке може свідчити про витік інформації або компрометацію системи. У нормальних умовах обсяг вихідного трафіку має відносно стабільний характер і залежить від типу діяльності користувачів.

Проте у випадку зараження комп’ютера шкідливим програмним забезпеченням або несанкціонованого доступу може спостерігатися значне зростання передачі даних на зовнішні ресурси. Це може бути пов’язано з передачею конфіденційної інформації, резервних копій або інших даних, які не повинні покидати межі мережі. Така поведінка є одним із ключових індикаторів компрометації системи та потребує негайного реагування.

Окрему категорію становить незвична активність користувачів, яка може проявлятися у зміні типових моделей їх поведінки. Наприклад, користувач

може здійснювати вхід у систему в нетиповий час, використовувати незвичні сервіси або виконувати операції, які раніше не були характерними. У деяких випадках це може бути пов’язано зі зміною умов роботи, проте часто такі відхилення свідчать про компрометацію облікового запису або внутрішні загрози. Аналіз поведінки користувачів дозволяє виявляти такі аномалії та своєчасно реагувати на них.

Крім наведених прикладів, до аномалій також можна віднести різкі зміни у структурі мережного трафіку, наприклад, зміну співвідношення між різними типами протоколів або збільшення кількості помилок передачі. Такі зміни можуть свідчити про технічні проблеми в мережі або спроби впливу на її роботу. Виявлення подібних відхилень потребує постійного моніторингу та аналізу статистичних показників.

Різні типи аномалій мають свої характерні ознаки та причини виникнення, однак усі вони впливають на стабільність та безпеку мережі. Їх своєчасне виявлення дозволяє запобігти серйозним наслідкам, включаючи втрату даних, зниження продуктивності та порушення роботи сервісів. Саме тому системи моніторингу мережного трафіку повинні забезпечувати не лише збір інформації, але й ефективний аналіз з метою виявлення таких відхилень.

У таблиці 1.6 наведено приклади типових мережевих атак та їх ознаки.

Таблиця 1.6 – Приклади типових мережевих атак

Тип атаки	Ознаки
DDoS	Велика кількість запитів
Port scanning	Часті підключення до різних портів
Brute force	Повторні спроби авторизації
Data exfiltration	Різке збільшення вихідного трафіку

Таким чином, виявлення аномалій у мережному трафіку є складним, але необхідним завданням для забезпечення безпеки та стабільності мережі.

Використання систем IDS, порогових методів та аналізу потоків дозволяє ефективно виявляти підозрілу активність і своєчасно реагувати на загрози. Отримані результати можуть бути використані для подальшої розробки системи моніторингу, яка забезпечить автоматизоване виявлення перевантажень та аномалій у мережі.

1.4 Основні метрики оцінювання стану мережі

Для ефективного моніторингу мережного трафіку та своєчасного виявлення перевантажень і аномалій важливе значення має використання відповідних метрик, які характеризують стан мережі. Саме на основі цих показників здійснюється аналіз ефективності роботи мережевої інфраструктури, а також приймаються рішення щодо її оптимізації.

Однією з основних характеристик є пропускна здатність мережі. Вона визначає максимальний обсяг даних, який може бути переданий через мережу за одиницю часу. Пропускна здатність залежить від типу каналу зв’язку, використовуваного обладнання та протоколів передачі даних.

У реальних умовах ефективна пропускна здатність часто є меншою за теоретичну через вплив різних факторів, таких як затримки, втрати пакетів та перевантаження.

Іншою важливою метрикою є затримка передачі даних (latency). Вона визначає час, необхідний для передачі пакета від джерела до отримувача. Затримка включає час обробки, передачі та маршрутизації даних.

У сучасних мережах затримка є критично важливим параметром, особливо для сервісів реального часу, таких як відеоконференції або IP-телефонія.

Важливим показником є також варіація затримки, або джиттер (jitter). Вона характеризує нестабільність затримки у часі. Високий рівень джиттера може призводити до погіршення якості передачі мультимедійного контенту,

зокрема виникнення затримок або переривання зв’язку.

Ще однією ключовою метрикою є рівень втрат пакетів. Втрати виникають у випадках, коли мережа не встигає обробити або передати всі пакети. Це може бути пов’язано з перевантаженням, помилками передачі або несправністю обладнання. Високий рівень втрат негативно впливає на якість передачі даних і може призводити до необхідності повторної передачі інформації.

До важливих характеристик також належить інтенсивність трафіку, яка визначає кількість переданих пакетів або байтів за одиницю часу. Аналіз інтенсивності дозволяє виявляти періоди пікового навантаження та оцінювати рівень використання мережевих ресурсів.

У таблиці 1.7 наведено основні метрики мережі та їх характеристики.

Таблиця 1.7 – Основні метрики стану мережі

Метрика	Опис	Вплив на мережу
Пропускна здатність	Максимальна швидкість передачі	Визначає продуктивність
Затримка	Час передачі пакета	Впливає на швидкодію
Джиттер	Коливання затримки	Впливає на якість зв’язку
Втрати пакетів	Кількість втрачених пакетів	Знижує надійність
Інтенсивність трафіку	Обсяг даних за час	Характеризує навантаження

Для оцінювання стану мережі важливо не лише аналізувати окремі метрики, але й враховувати їх взаємозв’язок. Наприклад, збільшення інтенсивності трафіку зазвичай призводить до зростання затримки та втрат пакетів. Тому комплексний аналіз дозволяє більш точно визначити причини виникнення проблем у мережі.

Сучасні системи моніторингу використовують ці метрики для формування аналітичних звітів та візуалізації стану мережі. Це дозволяє

адміністраторам оперативно реагувати на зміни та запобігати виникненню критичних ситуацій.

Таким чином, використання основних метрик є необхідною умовою для ефективного моніторингу мережного трафіку. Вони дозволяють оцінити стан мережі, виявити перевантаження та аномалії, а також забезпечити стабільну роботу інформаційних систем.

1.5 Постановка задачі

На основі проведеного аналізу предметної області, сучасного стану мережевих технологій, існуючих систем моніторингу, а також проблем перевантаження та аномалій у мережному трафіку можна сформулювати основну задачу даного дослідження.

Сучасні комп'ютерні мережі характеризуються високою складністю, значними обсягами переданих даних та динамічністю змін. Це створює суттєві труднощі для забезпечення їх стабільної та безпечної роботи.

Існуючі системи моніторингу не завжди здатні ефективно виявляти перевантаження та аномалії в режимі реального часу, що обумовлює необхідність розробки нових підходів до аналізу мережного трафіку.

Для досягнення поставленої мети необхідно вирішити такі наступні задачі.

1. Провести аналіз сучасного стану мережевих технологій та особливостей мережного трафіку, а також дослідити існуючі методи та засоби моніторингу мереж.
2. Проаналізувати причини виникнення перевантажень та аномалій та визначити вимоги до системи моніторингу.
3. Розробити структурну та функціональну схеми системи.
4. Реалізувати програмний модуль моніторингу мережного трафіку та провести тестування системи та оцінити її ефективність.

1.6 Висновки до першого розділу

У межах розділу 1 було проведено комплексний аналіз предметної області моніторингу мережного трафіку. Розглянуто сучасний стан розвитку мережевих технологій, визначено основні тенденції їх розвитку, а також проаналізовано особливості функціонування сучасних комп'ютерних мереж.

Особливу увагу було приділено проблемам перевантаження мережі та виникнення аномалій у мережному трафіку. Встановлено, що ці явища є одними з основних факторів, які негативно впливають на стабільність та ефективність роботи мережевих систем. Розглянуто основні причини їх виникнення, а також наслідки, до яких вони можуть призводити.

У ході аналізу існуючих систем моніторингу мережного трафіку було виявлено їх основні переваги та недоліки. Зокрема, встановлено, що більшість сучасних рішень або не забезпечують достатньої деталізації аналізу, або потребують значних обчислювальних ресурсів. Крім того, багато систем мають обмежені можливості щодо виявлення нових або складних аномалій.

Також було розглянуто основні типи аномалій у мережному трафіку, включаючи DDoS-атаки, сканування портів, спроби підбору паролів, витік даних та незвичну активність користувачів. Визначено їх характерні ознаки та вплив на роботу мережі.

На основі проведеного аналізу обґрунтовано необхідність розробки системи моніторингу мережного трафіку, яка буде здатна ефективно виявляти перевантаження та аномалії, забезпечуючи при цьому достатню швидкодію та точність.

2 ПРОЄКТУВАННЯ СИСТЕМИ МОНІТОРИНГУ МЕРЕЖНОГО ТРАФІКУ

2.1 Основні підходи до моніторингу мережного трафіку

Моніторинг мережного трафіку є одним із ключових процесів забезпечення стабільної та безпечної роботи комп'ютерних мереж. Його основною метою є безперервне спостереження за станом мережевих потоків, виявлення відхилень від нормальної поведінки, а також своєчасне реагування на можливі проблеми, такі як перевантаження або аномальна активність. У сучасних інформаційних системах моніторинг виконує не лише діагностичну, але й превентивну функцію, дозволяючи запобігати критичним збоям у роботі мережевої інфраструктури.

Існує кілька базових підходів до організації моніторингу мережного трафіку, які відрізняються способом збору та рівнем деталізації даних. До основних належать пасивний моніторинг, активний моніторинг та потоковий (flow-based) моніторинг. Кожен із цих підходів має свою сферу застосування та використовується залежно від вимог до системи.

Пасивний моніторинг ґрунтується на аналізі реального мережного трафіку без впливу на його передачу. У цьому випадку система моніторингу отримує копії пакетів або статистичну інформацію з мережевих пристроїв (наприклад, маршрутизаторів або комутаторів) і виконує їх подальший аналіз. Основною перевагою такого підходу є те, що він не створює додаткового навантаження на мережу та дозволяє отримувати об'єктивні дані про її стан у реальному часі.

Однак пасивний моніторинг має і певні недоліки. Насамперед це великі обсяги даних, які необхідно обробляти. У високонавантажених мережах кількість пакетів може бути настільки великою, що їх повний аналіз у реальному часі стає складним або навіть неможливим без використання потужних обчислювальних ресурсів. Крім того, пасивний моніторинг не завжди

дозволяє точно визначити причину проблеми, оскільки він лише фіксує факт її виникнення.

Активний моніторинг передбачає інший підхід, при якому система спеціально генерує тестовий трафік для оцінки параметрів мережі. Це можуть бути ICMP-запити (наприклад, ping), тестові HTTP-з'єднання або інші типи контрольованих запитів. На основі результатів таких перевірок визначаються ключові характеристики мережі, зокрема затримка, доступність вузлів та пропускна здатність каналів.

Перевагою активного моніторингу є можливість отримання контрольованих і повторюваних результатів, що дозволяє більш точно оцінювати стан мережі. Водночас цей підхід має суттєвий недолік, він створює додатковий трафік, який може впливати на загальне навантаження мережі, особливо у великих системах або при частому виконанні перевірок.

Потоковий моніторинг (flow-based monitoring) є одним із найбільш поширених сучасних підходів. Його суть полягає в аналізі не окремих пакетів, а агрегованих потоків даних. Потік визначається як сукупність пакетів, що мають спільні параметри, такі як IP-адреса джерела та призначення, порти, протокол та інші характеристики.

Використання потокового підходу дозволяє значно зменшити обсяг даних, які необхідно обробляти, що робить його більш ефективним для великих мереж. Крім того, flow-based моніторинг забезпечує достатній рівень деталізації для виявлення перевантажень і аномалій, не перевантажуючи систему надмірною інформацією.

Окремо слід зазначити комбіновані підходи, які поєднують переваги різних методів. Наприклад, у багатьох сучасних системах використовується потоковий моніторинг для загального аналізу стану мережі, а пакетний аналіз застосовується лише у випадках виявлення підозрілої активності. Такий підхід дозволяє досягти балансу між точністю аналізу та ефективністю використання ресурсів.

У практичних системах моніторингу також важливу роль відіграє вибір рівня збору даних. Моніторинг може здійснюватися на рівні мережевих пристроїв, серверів або кінцевих вузлів. Кожен із цих рівнів надає різну інформацію про стан мережі. Наприклад, мережеві пристрої дозволяють отримати загальну картину трафіку, тоді як кінцеві вузли показують більш детальну інформацію про конкретні процеси та застосунки.

На вибір підходу до моніторингу також впливають такі фактори, як масштаб мережі, вимоги до швидкодії системи, необхідний рівень деталізації та доступні обчислювальні ресурси. У великих корпоративних мережах зазвичай застосовуються розподілені системи моніторингу, які дозволяють обробляти дані на декількох вузлах одночасно.

Отже, вибір підходу до моніторингу мережного трафіку є компромісом між точністю, продуктивністю та складністю реалізації системи. У більшості сучасних рішень використовується комбінація кількох підходів, що дозволяє забезпечити ефективний контроль стану мережі та своєчасне виявлення проблем.

2.2 Методи збору даних про мережний трафік

Збір даних про мережний трафік є одним із найважливіших етапів побудови системи моніторингу. Саме від якості та повноти отриманої інформації залежить точність подальшого аналізу, виявлення перевантажень та аномалій, а також ефективність усієї системи в цілому. У сучасних комп’ютерних мережах застосовується декілька основних методів збору даних, кожен із яких має свої особливості, переваги та обмеження.

Найбільш детальним методом є захоплення пакетів (packet capture). Даний підхід передбачає перехоплення кожного мережевого пакета, який проходить через мережевий інтерфейс, із подальшим аналізом його заголовків та, за необхідності, вмісту. Для реалізації такого підходу часто

використовуються спеціальні бібліотеки та інструменти, такі як libpcap або WinPcap.

Перевагою packet capture є максимальна деталізація даних. Система отримує повну інформацію про мережевий обмін, включаючи IP-адреси, порти, типи протоколів, розміри пакетів та часові характеристики. Це дозволяє проводити глибокий аналіз трафіку та виявляти складні аномалії, які неможливо визначити на рівні агрегованих даних.

Водночас основним недоліком цього підходу є високе навантаження на обчислювальні ресурси. У високошвидкісних мережах кількість пакетів може досягати мільйонів за секунду, що ускладнює їх повний аналіз у режимі реального часу. Крім того, зберігання повного набору пакетів потребує значного обсягу пам’яті.

Іншим поширеним методом збору даних є використання потокових технологій, таких як NetFlow, sFlow або IPFIX. На відміну від пакетного аналізу, дані методи базуються на зборі інформації про мережеві потоки, а не окремі пакети.

Потік у цьому контексті визначається як сукупність пакетів, що мають спільні атрибути, зокрема IP-адресу джерела та призначення, порти, протокол та інші параметри. NetFlow, наприклад, збирає інформацію про кількість переданих байтів, кількість пакетів, тривалість з’єднання та інші статистичні характеристики.

Перевагою потокового підходу є значне зменшення обсягу даних, які необхідно обробляти. Це дозволяє використовувати його у великих корпоративних мережах та дата-центрах, де повний пакетний аналіз є недоцільним через високе навантаження. Крім того, flow-based підхід добре підходить для виявлення перевантажень та загальних аномалій трафіку.

Однак потокові технології мають обмеження у деталізації. Оскільки вони не зберігають вміст окремих пакетів, це ускладнює виявлення деяких типів атак, які потребують глибокого аналізу payload. Таким чином, NetFlow і подібні

технології більше орієнтовані на статистичний аналіз, ніж на глибоку перевірку даних.

У таблиці 2.1 наведено порівняння основних методів збору даних про мережний трафік.

Таблиця 2.1 – Порівняння методів збору мережного трафіку

Метод	Рівень деталізації	Навантаження	Область застосування
Packet capture	Дуже високий	Високе	Аналіз атак, форензика
NetFlow / sFlow	Середній	Низьке	Моніторинг навантаження
Логи пристроїв	Низький–середній	Низьке	Діагностика проблем
Endpoint agents	Високий	Середнє	Аналіз поведінки користувачів

Ще одним методом збору інформації є аналіз логів мережевого обладнання. Багато маршрутизаторів, комутаторів та серверів ведуть журнали подій, у яких фіксуються різні аспекти роботи системи, включаючи інформацію про з’єднання, помилки, перевантаження та зміни конфігурації.

Логування дозволяє отримати додатковий контекст щодо стану мережі та є важливим джерелом інформації для діагностики проблем. Проте дані з логів зазвичай є менш структурованими та потребують додаткової обробки перед аналізом.

Окремо слід виділити метод збору даних на рівні кінцевих пристроїв. У цьому випадку спеціальне програмне забезпечення встановлюється безпосередньо на сервери або робочі станції і збирає інформацію про мережеву активність конкретного вузла. Це дозволяє отримати детальну картину поведінки користувачів та процесів, однак потребує встановлення агентів на кожному пристрої.

2.3 Методи аналізу мережного трафіку, виявлення перевантажень та аномалій

Важливо зазначити, що у сучасних системах моніторингу рідко використовується лише один метод збору даних. Найчастіше застосовується комбінований підхід, який дозволяє поєднати переваги різних технологій. Наприклад, NetFlow може використовуватися для постійного моніторингу стану мережі, тоді як packet capture активується лише при виявленні підозрілої активності.

Також важливим аспектом є місце збору даних у мережній архітектурі. Дані можуть збиратися на рівні магістральних каналів, на периферійних маршрутизаторах або безпосередньо на серверах. Вибір точки збору впливає на повноту інформації та навантаження на систему.

Аналіз мережного трафіку є ключовим етапом у процесі моніторингу комп’ютерних мереж, оскільки саме на цьому етапі здійснюється інтерпретація зібраних даних та формування висновків щодо стану мережної інфраструктури. Основною метою аналізу є виявлення відхилень від нормальної поведінки, визначення перевантажень, а також ідентифікація можливих аномалій або загроз.

У сучасних системах моніторингу застосовується кілька основних підходів до аналізу мережного трафіку, які можуть використовуватися як окремо, так і в комплексі. До таких підходів належать статистичний аналіз, порогові методи, сигнатурний аналіз та аналіз потоків даних.

Статистичний аналіз базується на обробці числових характеристик мережного трафіку, таких як середнє значення, дисперсія, стандартне відхилення та інші статистичні показники. Даний підхід дозволяє формувати уявлення про нормальну поведінку мережі та виявляти відхилення від неї.

Одним із основних принципів статистичного аналізу є побудова базової моделі нормального стану мережі. Така модель формується на основі

історичних даних і використовується як еталон для подальшого порівняння. Якщо поточні значення суттєво відхиляються від базової моделі, система може фіксувати це як потенційну аномалію.

Перевагою статистичного підходу є його універсальність та можливість застосування до різних типів трафіку. Водночас він вимагає наявності достатнього обсягу історичних даних для побудови коректної моделі.

Порогові методи є одним із найпростіших способів виявлення аномалій та перевантажень. Їх суть полягає у визначенні граничних значень для певних параметрів мережі, таких як кількість пакетів, обсяг трафіку, затримка або кількість з’єднань.

Якщо значення контрольованого параметра перевищує встановлений поріг, система генерує попередження або сигнал тривоги. Наприклад, перевищення допустимого рівня навантаження на канал зв’язку може свідчити про початок перевантаження.

Основною перевагою порогових методів є їх простота реалізації та низькі вимоги до обчислювальних ресурсів. Однак їх недоліком є необхідність точного налаштування порогових значень, оскільки занадто низькі або високі пороги можуть призводити до хибних спрацювань або пропуску реальних проблем.

Метод виявлення атак та аномалій базується на використанні бази сигнатур, які містять характерні ознаки певних шкідливих дій.

У процесі аналізу мережевий трафік порівнюється з відомими сигнатурами. Якщо виявляється збіг, система фіксує інцидент. Такий підхід широко використовується в системах виявлення вторгнень (IDS).

Перевагою сигнатурного аналізу є висока точність виявлення відомих атак та низький рівень хибних спрацювань. Недоліком є нездатність виявляти нові або модифіковані атаки, сигнатури яких ще не додані до бази.

Аналіз потоків є одним із найбільш ефективних підходів для оцінки стану мережі. Він базується на розгляді сукупності пакетів як єдиного потоку, що

дозволяє значно зменшити обсяг оброблюваних даних.

Потоки аналізуються за такими параметрами, як тривалість з’єднання, кількість переданих байтів, кількість пакетів та частота з’єднань. Це дозволяє виявляти аномальні патерни поведінки, наприклад, різке збільшення кількості коротких з’єднань або незвично великий обсяг вихідного трафіку.

Перевантаження мережі виникає у випадках, коли обсяг переданих даних перевищує пропускну здатність мережевих каналів або обчислювальних ресурсів вузлів. Це призводить до збільшення затримок, втрат пакетів та зниження загальної продуктивності системи.

Основними методами виявлення перевантажень є:

- аналіз інтенсивності трафіку;
- моніторинг затримок;
- аналіз втрат пакетів;
- контроль завантаження каналів зв’язку.

Аналіз інтенсивності трафіку дозволяє виявляти пікові навантаження, які можуть свідчити про наближення або настання перевантаження. Моніторинг затримок є особливо важливим для сервісів реального часу, де навіть незначне збільшення latency може призвести до суттєвого погіршення якості обслуговування.

Втрати пакетів є ще одним критичним показником. Їх збільшення зазвичай свідчить про перевантаження мережевих пристроїв або каналів зв’язку.

Виявлення аномалій є складнішою задачею порівняно з виявленням перевантажень, оскільки аномалії можуть мати різну природу та не завжди проявляються у вигляді явних перевищень параметрів.

Аномалії можуть бути викликані як технічними причинами, так і навмисними діями, такими як атаки або несанкціонований доступ. Основними методами їх виявлення є поєднання статистичного аналізу, порогових методів та сигнатурного аналізу.

Особливу роль відіграє аналіз поведінки трафіку в часі. Наприклад, різкі зміни у кількості з’єднань або незвичні шаблони активності можуть свідчити про наявність аномалій.

У сучасних системах моніторингу рідко використовується лише один метод аналізу. Найбільш ефективним є комбінований підхід, який поєднує різні методи для підвищення точності та надійності.

Наприклад:

- порогові методи використовуються для швидкого виявлення критичних перевантажень;
- статистичний аналіз застосовується для довгострокового оцінювання стану мережі;
- сигнатурний аналіз використовується для виявлення відомих атак;
- аналіз потоків дозволяє оцінювати загальну поведінку трафіку.

Такий підхід дозволяє зменшити кількість хибних спрацювань та підвищити ефективність роботи системи моніторингу.

2.4 Архітектура системи моніторингу мережного трафіку

Архітектура системи моніторингу мережного трафіку визначає принцип організації компонентів системи, їх взаємодію та порядок обробки інформаційних потоків. Від правильно побудованої архітектури залежить ефективність виявлення перевантажень і аномалій, швидкодія системи, а також її масштабованість і надійність.

У загальному випадку система моніторингу мережного трафіку складається з кількох основних функціональних рівнів: рівня збору даних, рівня обробки та аналізу, рівня зберігання інформації та рівня представлення результатів користувачу. Така багаторівнева структура дозволяє розділити функції системи та забезпечити її модульність.

Архітектура системи моніторингу мережного трафіку представлена на

рисунку 2.1.

Рисунок 2.1 – Архітектура системи моніторингу мережного трафіку

Рівень збору даних є початковим етапом архітектури системи

моніторингу. На цьому рівні здійснюється отримання інформації про мережевий трафік із різних джерел. Це можуть бути мережеві інтерфейси серверів, маршрутизатори, комутатори або спеціальні агенти, встановлені на кінцевих пристроях.

Збір даних може здійснюватися за допомогою різних методів, таких як packet capture або потокові технології (NetFlow, sFlow). Вибір конкретного методу залежить від вимог до деталізації та продуктивності системи. На цьому етапі важливо забезпечити мінімальний вплив на роботу мережі, оскільки надмірне навантаження може погіршити її продуктивність.

Після збору даних виконується їх попередня обробка. Цей етап включає фільтрацію, нормалізацію та агрегацію інформації. Фільтрація дозволяє відсіяти зайві або нерелевантні дані, тоді як нормалізація забезпечує приведення інформації до єдиного формату.

Агрегація даних полягає в об’єднанні окремих пакетів у потоки або групи за певними критеріями, такими як IP-адреси, порти або часові інтервали. Це дозволяє значно зменшити обсяг інформації, що надалі підлягає аналізу.

Попередня обробка є важливим етапом, оскільки вона безпосередньо впливає на продуктивність всієї системи.

Рівень аналізу є центральним елементом архітектури системи моніторингу. Саме на цьому етапі здійснюється виявлення перевантажень та аномалій у мережному трафіку.

На рівні аналізу застосовуються різні методи, зокрема статистичний аналіз, порогові методи та сигнатурний аналіз. Статистичні методи дозволяють оцінювати нормальний стан мережі та виявляти відхилення. Порогові методи забезпечують швидке реагування на перевищення критичних значень. Сигнатурний аналіз використовується для виявлення відомих типів атак та аномалій.

У більш складних системах також може застосовуватися кореляційний аналіз, який дозволяє встановлювати взаємозв’язки між різними подіями в

мережі та виявляти складні сценарії атак або збоїв.

Рівень зберігання відповідає за накопичення та організацію даних, отриманих у процесі моніторингу. У якості сховищ можуть використовуватися реляційні бази даних, NoSQL-рішення або спеціалізовані системи зберігання часових рядів.

Зберігання даних дозволяє виконувати ретроспективний аналіз, будувати графіки змін параметрів мережі та формувати звіти. Крім того, історичні дані використовуються для побудови базових моделей нормальної поведінки мережі.

Важливою вимогою до рівня зберігання є забезпечення швидкого доступу до даних, оскільки система моніторингу часто працює в режимі, наближеному до реального часу.

Рівень представлення відповідає за взаємодію з користувачем. На цьому рівні результати аналізу відображаються у зручному для сприйняття вигляді. Це можуть бути графіки, таблиці, діаграми або текстові повідомлення про інциденти.

Інтерфейс користувача повинен забезпечувати оперативне отримання інформації про стан мережі, а також можливість перегляду історичних даних. У сучасних системах часто використовується веб-інтерфейс, що дозволяє доступ до системи з будь-якого пристрою.

У практиці побудови систем моніторингу мережного трафіку виділяють два основні типи архітектур: централізовану та розподілену. Вибір між цими підходами визначається масштабом мережі, вимогами до продуктивності, надійності та можливостями обробки великих обсягів даних.

Централізована архітектура передбачає організацію системи, у якій усі дані про мережний трафік збираються та передаються на один центральний сервер. Саме на цьому сервері виконується їх зберігання, обробка та аналіз. Такий підхід є найбільш простим з точки зору реалізації, оскільки всі функціональні компоненти системи зосереджені в одному місці. Це спрощує

розгортання, налаштування та адміністрування системи моніторингу.

Однією з основних переваг централізованої архітектури є цілісність даних та зручність їх обробки. Оскільки вся інформація знаходиться в одному сховищі, значно спрощується виконання аналітичних операцій, побудова звітів та візуалізація стану мережі. Крім того, централізований підхід дозволяє легше реалізувати механізми контролю доступу та забезпечити єдину політику безпеки (рисунок 2.2).

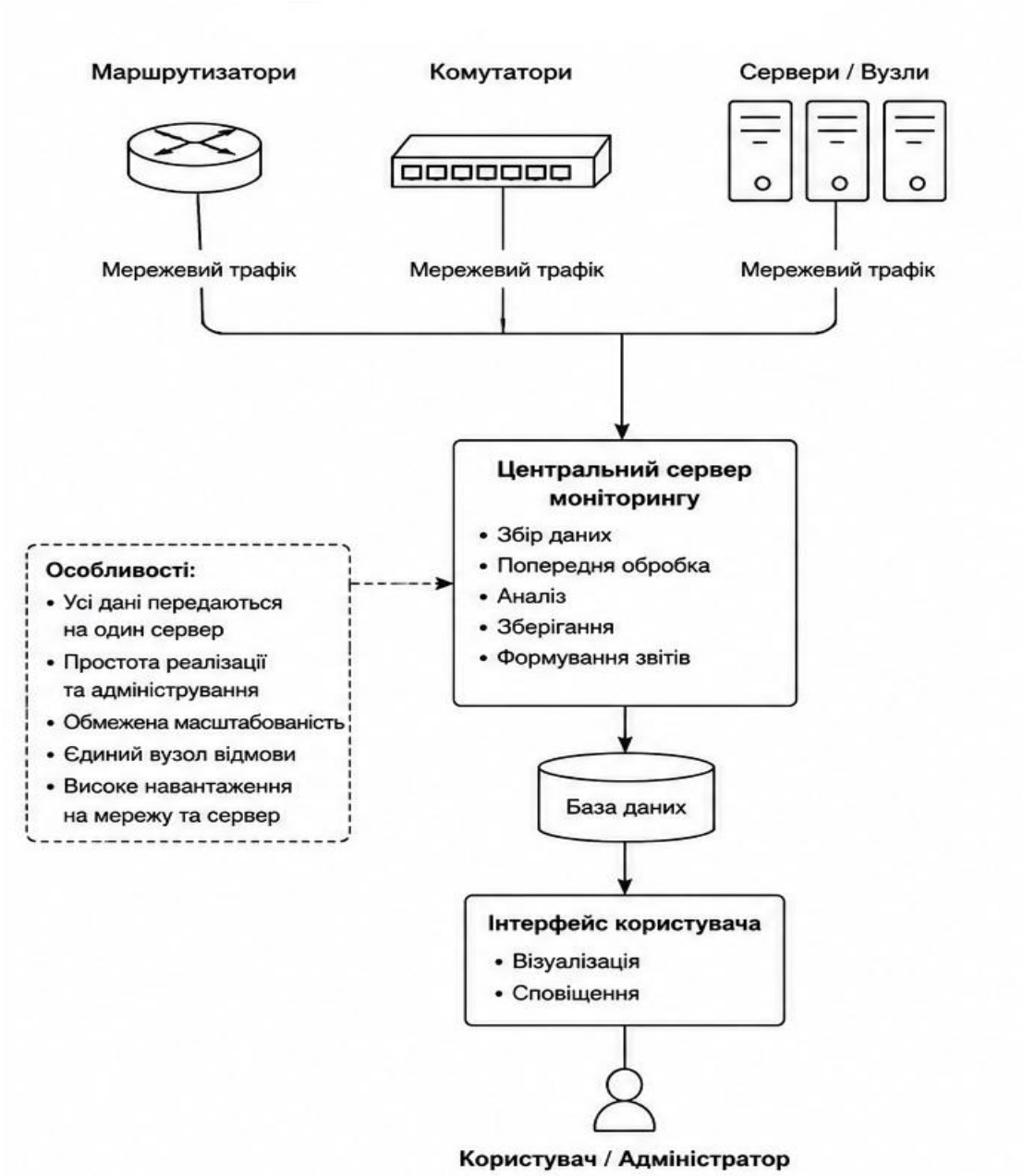


Рисунок 2.2 – Централізована архітектура

Проте централізована архітектура має і суттєві недоліки. Основним із них є обмежена масштабованість. У разі зростання обсягу трафіку центральний сервер може не справлятися з обробкою даних, що призводить до зниження продуктивності системи. Також існує ризик виникнення так званого «вузького місця», коли продуктивність усієї системи обмежується можливостями одного вузла.

Ще одним важливим недоліком є низька відмовостійкість. У випадку виходу з ладу центрального сервера вся система моніторингу може стати недоступною, що унеможливлює контроль стану мережі. Крім того, передача великого обсягу даних до центрального вузла може створювати додаткове навантаження на мережу.

На відміну від централізованої, розподілена архітектура передбачає використання декількох вузлів, які виконують функції збору та попередньої обробки даних (рисунок 2.3). У такій системі кожен вузол відповідає за певний сегмент мережі або частину трафіку. Зібрані дані можуть частково оброблятися на локальному рівні, після чого передаватися до центрального сервера або системи агрегації.

Основною перевагою розподіленої архітектури є висока масштабованість. У разі збільшення навантаження можна додавати нові вузли, що дозволяє рівномірно розподіляти обробку даних. Це робить систему більш гнучкою та придатною для використання у великих мережах.

Ще однією важливою перевагою є підвищена надійність. Відмова одного з вузлів не призводить до повної втрати працездатності системи, оскільки інші вузли продовжують функціонувати. Таким чином забезпечується відмовостійкість та безперервність моніторингу.

Крім того, розподілена архітектура дозволяє зменшити обсяг переданих даних у мережі. Завдяки попередній обробці інформації на локальних вузлах передається лише агрегована або релевантна інформація, що знижує навантаження на канали зв’язку.

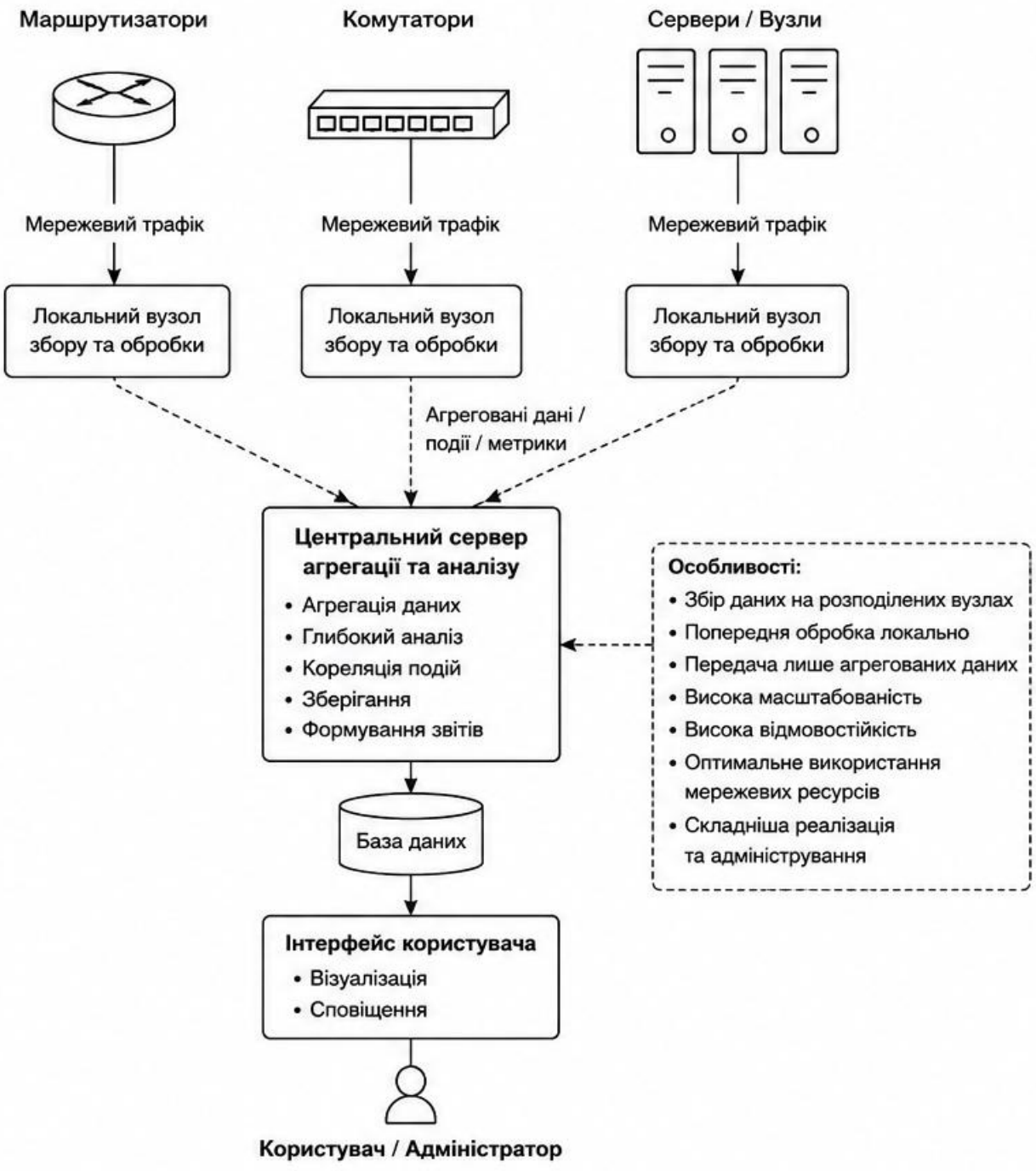


Рисунок 2.4 – Розподілена архітектура

Водночас розподілені системи є більш складними у реалізації та налаштуванні. Необхідно забезпечити синхронізацію даних між вузлами, організувати механізми обміну інформацією та узгодження результатів аналізу. Крім того, ускладнюється адміністрування системи, оскільки потрібно керувати

великою кількістю компонентів.

У практичних реалізаціях часто використовується комбінований підхід, який поєднує елементи централізованої та розподіленої архітектур. У таких системах збір та попередня обробка даних здійснюється на розподілених вузлах, тоді як централізований сервер виконує функції агрегації, аналізу та представлення результатів.

2.5 Потоки даних у системі моніторингу

Робота системи моніторингу може бути представлена у вигляді потоків даних, які проходять через всі рівні архітектури. Спочатку дані збираються з мережевих пристроїв, після чого проходять етап попередньої обробки. Далі вони надходять до аналітичного модуля, де виконується їх інтерпретація.

У разі виявлення аномалій або перевантажень формується відповідне повідомлення, яке передається на рівень представлення. Таким чином забезпечується безперервний цикл моніторингу.

На початковому етапі відбувається збір даних із мережевих пристроїв, таких як маршрутизатори, комутатори, сервери та кінцеві вузли. Дані можуть надходити у вигляді окремих пакетів, потоків або статистичних показників. Важливою особливістю цього етапу є забезпечення безперервності збору інформації, оскільки навіть короткочасна втрата даних може призвести до некоректних висновків щодо стану мережі.

Після збору дані надходять до модуля попередньої обробки, де виконується їх фільтрація, нормалізація та агрегація. Фільтрація дозволяє відокремити релевантну інформацію від зайвої, наприклад, виключити службовий або нецікавий для аналізу трафік. Нормалізація забезпечує приведення даних до єдиного формату, що є необхідним для подальшої обробки. Агрегація дозволяє об’єднувати дані за певними ознаками, зменшуючи їх обсяг і спрощуючи аналіз.

Наступним етапом є передача підготовлених даних до аналітичного

модуля. Саме тут виконується основна обробка інформації, яка включає виявлення перевантажень, аналіз поведінки трафіку та ідентифікацію аномалій. У цьому модулі застосовуються різні методи аналізу, такі як статистичні, порогові та сигнатурні підходи. Результатом роботи аналітичного модуля є формування висновків щодо поточного стану мережі.

У разі виявлення відхилень від нормальної роботи, таких як перевантаження каналів зв’язку або аномальна активність, система формує відповідні повідомлення або сигнали тривоги. Ці повідомлення передаються до рівня представлення, де вони відображаються у вигляді сповіщень, графіків або звітів. Це дозволяє адміністраторам мережі оперативно реагувати на проблеми та вживати необхідних заходів.

Паралельно з процесом аналізу дані можуть зберігатися у базі даних для подальшого використання. Збережена інформація дозволяє виконувати ретроспективний аналіз, будувати тренди зміни параметрів мережі та вдосконалювати алгоритми моніторингу. Крім того, історичні дані можуть використовуватися для формування базових моделей нормальної поведінки мережі.

Важливою особливістю потоків даних у системі моніторингу є їх циклічний характер. Після завершення одного циклу обробки система продовжує отримувати нові дані, забезпечуючи безперервний контроль стану мережі. Це дозволяє своєчасно виявляти навіть короткочасні аномалії та реагувати на них.

Також слід враховувати, що в умовах високонавантажених мереж потоки даних можуть бути дуже інтенсивними. У таких випадках важливо забезпечити оптимізацію процесів обробки, зокрема шляхом використання паралельних обчислень або розподілених систем. Це дозволяє уникнути перевантаження системи моніторингу та забезпечити її стабільну роботу.

Таким чином, організація потоків даних є ключовим аспектом функціонування системи моніторингу мережного трафіку. Від правильного

проєктування цих потоків залежить ефективність збору, обробки та аналізу інформації, а також здатність системи своєчасно виявляти перевантаження та аномалії у роботі мережі.

2.6 Висновки до другого розділу

У межах розділу 2 було проведено детальний аналіз методів та засобів моніторингу мережного трафіку. Розглянуто основні підходи до організації моніторингу, зокрема пасивний, активний та потоковий, що дозволило визначити їх особливості, переваги та обмеження.

Проаналізовано сучасні методи збору даних про мережний трафік, включаючи захоплення пакетів, використання потокових технологій та аналіз журналів мережевих пристроїв. Встановлено, що найбільш ефективним є комбінований підхід, який забезпечує баланс між деталізацією інформації та навантаженням на систему.

Особливу увагу приділено методам аналізу мережного трафіку, виявлення перевантажень та аномалій. Розглянуто статистичні, порогові та сигнатурні методи, а також їх поєднання для підвищення точності виявлення відхилень. Визначено, що комплексне використання цих методів дозволяє забезпечити більш надійний контроль стану мережі.

У ході дослідження було розглянуто архітектурні особливості систем моніторингу, зокрема централізовану та розподілену моделі. Встановлено, що централізована архітектура є простішою у реалізації, однак має обмеження щодо масштабованості та надійності, тоді як розподілена забезпечує кращу продуктивність і відмовостійкість у великих мережах.

3 РЕАЛІЗАЦІЯ СИСТЕМИ МОНІТОРИНГУ МЕРЕЖНОГО ТРАФІКУ ТА АНАЛІЗ РЕЗУЛЬТАТІВ

3.1 Вибір середовища та інструментів реалізації

Практична реалізація системи моніторингу мережного трафіку для виявлення перевантажень та аномалій вимагає використання програмних засобів, здатних забезпечити обробку великих обсягів даних у режимі, близькому до реального часу, а також гнучкість для подальшого розширення функціональних можливостей. Вибір інструментів здійснювався з урахуванням критеріїв продуктивності, доступності бібліотек для аналізу мережевого трафіку, простоти інтеграції компонентів і підтримки сучасних методів аналізу даних. Вибір програмних засобів для реалізації системи моніторингу мережного трафіку є критично важливим етапом, оскільки саме від нього залежить продуктивність системи, точність аналізу, масштабованість та зручність подальшого використання. При виборі технологій враховувалися такі критерії: швидкодія, можливість роботи в режимі реального часу, наявність бібліотек для аналізу мережевого трафіку, простота розробки та підтримки, а також можливість інтеграції з іншими системами.

У якості основної мови програмування було обрано Python. Дане рішення обумовлено тим, що Python є однією з найбільш популярних мов для обробки даних та мережевого аналізу. До його переваг можна віднести простий синтаксис, що дозволяє швидко реалізовувати складні алгоритми, а також наявність великої кількості бібліотек для роботи з мережею та аналізу даних. Крім того, Python підтримує багатоплатформеність і має активну спільноту розробників, що спрощує пошук рішень і підтримку системи.

Водночас Python має і певні недоліки. Основним з них є відносно низька швидкодія порівняно з компільованими мовами, такими як C або C++. Це може бути критичним при обробці дуже великих обсягів трафіку. Проте для задач моніторингу в локальних або середніх мережах продуктивність Python є

достатньою, особливо з урахуванням можливості оптимізації коду та використання ефективних бібліотек.

Для реалізації окремих підсистем використано такі бібліотеки:

– Scapy для перехоплення та аналізу мережевих пакетів;
– PyShark як альтернатива для глибшого аналізу протоколів;
– Pandas для обробки табличних даних і формування часових рядів;
– NumPy для виконання математичних операцій;
– Matplotlib та Plotly для побудови графіків і візуалізації;
– SQLite для збереження історичних даних.

Застосування SQLite пояснюється простотою інтеграції, відсутністю необхідності в окремому сервері баз даних і достатньою продуктивністю для задач локального моніторингу.

У разі масштабування системи передбачено можливість переходу на PostgreSQL.

Для захоплення мережевого трафіку було обрано бібліотеку Scapy. Вона забезпечує гнучкий доступ до пакетів на різних рівнях мережевої моделі та дозволяє виконувати їх детальний аналіз. Основною перевагою Scapy є універсальність: вона підтримує широкий спектр протоколів і дозволяє не лише аналізувати, але й генерувати мережеві пакети. Це особливо важливо при тестуванні системи.

До недоліків Scapy можна віднести порівняно нижчу продуктивність у порівнянні з більш спеціалізованими інструментами, такими як libpcap або DPDK. Крім того, при обробці великого потоку пакетів можливе перевантаження процесора. Незважаючи на це, Scapy є оптимальним вибором для навчальних і дослідницьких систем завдяки своїй простоті та функціональності.

Альтернативним інструментом є PyShark, який базується на можливостях Wireshark. Його перевагою є більш глибокий аналіз протоколів і зручність роботи з уже структурованими даними. Проте PyShark залежить від зовнішніх

компонентів і має більші накладні витрати, що робить його менш придатним для високопродуктивних систем у реальному часі.

Для обробки та аналізу даних було використано бібліотеки Pandas і NumPy. Pandas дозволяє ефективно працювати з табличними даними, виконувати групування, агрегацію та фільтрацію. Це значно спрощує реалізацію алгоритмів аналізу трафіку. NumPy, у свою чергу, забезпечує швидкі математичні обчислення та роботу з масивами даних.

Перевагами Pandas є висока продуктивність при роботі з великими наборами даних і зручність використання. Недоліком є значне споживання пам’яті, що може стати обмеженням при обробці великих потоків даних у реальному часі. NumPy є дуже ефективним, проте потребує певного рівня підготовки для правильного використання.

Для збереження даних було обрано SQLite. Основною перевагою цієї системи є її простота: вона не потребує встановлення окремого сервера та легко інтегрується у програму. SQLite забезпечує достатню швидкість роботи для локальних систем моніторингу та дозволяє зберігати історичні дані для подальшого аналізу.

Недоліком SQLite є обмежена масштабованість. Вона не підходить для систем із великою кількістю одночасних користувачів або дуже великим обсягом даних. У таких випадках доцільно використовувати більш потужні системи керування базами даних, наприклад PostgreSQL.

Для візуалізації даних було використано бібліотеки Matplotlib та Plotly. Matplotlib є стандартним інструментом для побудови графіків у Python і забезпечує широкі можливості налаштування. Plotly дозволяє створювати інтерактивні графіки, що значно підвищує зручність аналізу даних.

Перевагою Matplotlib є стабільність і гнучкість, проте її інтерфейс є менш інтуїтивним. Plotly, навпаки, забезпечує сучасний вигляд графіків і інтерактивність, але має більші вимоги до ресурсів.

Таким чином, обраний стек технологій є збалансованим рішенням, яке

забезпечує достатню продуктивність, гнучкість і зручність розробки. Незважаючи на наявність певних недоліків, кожен компонент відповідає поставленим задачам, а їх поєднання дозволяє створити ефективну систему моніторингу мережного трафіку.

3.2 Реалізація модуля збору та первинної обробки мережевого трафіку

Ключовим етапом функціонування розробленої системи моніторингу є збір мережевого трафіку, оскільки саме на цьому етапі формується первинний набір даних, від якого залежить точність подальшого аналізу та ефективність виявлення аномалій. Для реалізації даного процесу розроблено спеціалізований модуль захоплення пакетів, який працює в режимі реального часу та здійснює перехоплення даних безпосередньо з мережевого інтерфейсу. З

агальна схема збору мережевого трафіка наведена на рисунку 3.1.

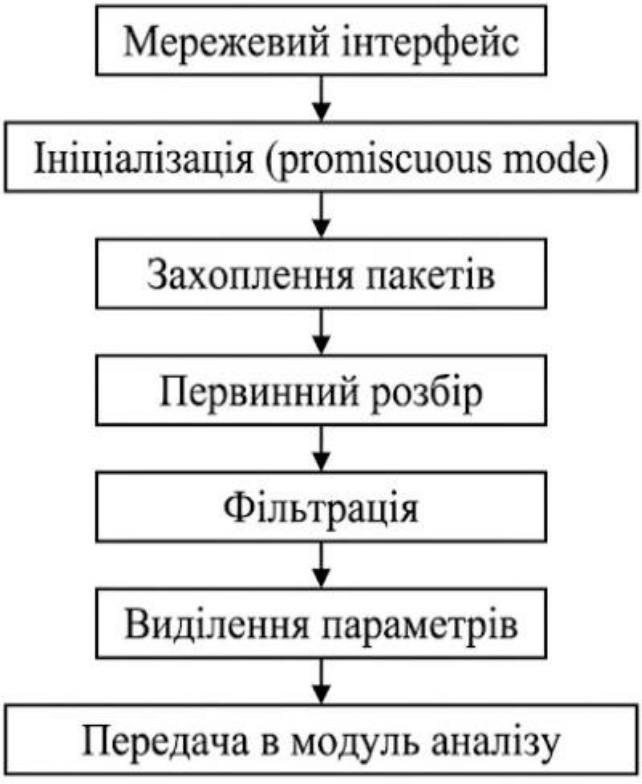


Рисунок 3.1 – Загальна схема збору мережевого трафіка

Режим реального часу означає, що обробка пакетів виконується одразу після їх надходження, без значних затримок. Це є критично важливим для систем моніторингу, оскільки дозволяє оперативно реагувати на перевантаження мережі або виникнення аномальних ситуацій, таких як різке зростання трафіку чи підозріла активність з боку окремих вузлів.

Процес збору мережевого трафіку складається з кількох послідовних етапів, які утворюють єдиний конвеєр обробки даних. На першому етапі здійснюється ініціалізація мережевого інтерфейсу. Система визначає доступні інтерфейси (наприклад, Ethernet або Wi-Fi), після чого обирається той, через який проходить основний трафік. Для забезпечення повного доступу до пакетів інтерфейс переводиться в так званий «promiscuous mode», що дозволяє перехоплювати всі пакети, незалежно від їх адресації.

Після ініціалізації починається безпосереднє захоплення пакетів. На цьому етапі система отримує потік сирих (raw) даних, які містять як корисну інформацію, так і службові заголовки різних рівнів моделі OSI. Кожен пакет проходить первинний розбір, у ході якого виділяються заголовки канального, мережевого та транспортного рівнів.

Наступним важливим етапом функціонування системи є фільтрація мережевого трафіку, яка відіграє ключову роль у забезпеченні ефективності та продуктивності всієї системи моніторингу. У реальних мережах обсяг переданих даних є надзвичайно великим, і значна частина мережевих пакетів не несе корисної інформації для задач аналізу або є службовою. До таких пакетів належать ARP-запити, широкомовні (broadcast) повідомлення, пакети протоколів керування мережею, а також інші допоміжні типи трафіку, що забезпечують функціонування мережевої інфраструктури, але не відображають реальну поведінку користувачів або прикладних сервісів.

Якщо не застосовувати механізми фільтрації, система буде змушена обробляти весь потік пакетів без винятку, що призведе до значного перевантаження обчислювальних ресурсів. У результаті може спостерігатися

зниження швидкодії, збільшення затримок обробки та навіть втрата частини пакетів. Крім того, надлишкові дані ускладнюють процес аналізу, оскільки знижують співвідношення корисної інформації до загального обсягу даних.

Фільтрація трафіку реалізується шляхом застосування набору правил, які визначають, які пакети підлягають обробці, а які відкидаються. Дані правила можуть базуватися на різних критеріях. Одним із основних є тип протоколу. Наприклад, система може аналізувати лише IP-трафік, ігноруючи пакети канального рівня, які не містять інформації, необхідної для виявлення аномалій у мережевому навантаженні.

Іншим важливим критерієм є IP-адреса джерела або призначення. Це дозволяє обмежити аналіз певними сегментами мережі або окремими вузлами. Наприклад, можна виключити локальні службові адреси або, навпаки, зосередитися лише на зовнішньому трафіку. Також широко застосовується фільтрація за портами, що дає змогу виділяти конкретні сервіси, такі як HTTP, HTTPS або FTP, і аналізувати лише відповідні типи з’єднань.

Додатково може використовуватися фільтрація за розміром пакета. Наприклад, надто малі пакети можуть бути характерними для службових повідомлень або атак типу flooding, тоді як великі пакети можуть свідчити про передачу значних обсягів даних. Аналіз таких характеристик дозволяє підвищити точність виявлення аномалій.

Ще одним критерієм є напрямок передачі трафіку, тобто вхідний або вихідний. Це дає змогу окремо аналізувати трафік, що надходить у мережу, та трафік, який її залишає. Такий підхід є особливо корисним для виявлення витоку даних або несанкціонованої активності.

Важливо зазначити, що процес фільтрації повинен бути збалансованим. Надмірно жорсткі правила можуть призвести до втрати важливої інформації, тоді як занадто слабка фільтрація не забезпечить необхідного зниження навантаження. Тому набір правил фільтрації повинен налаштовуватися з урахуванням специфіки мережі та поставлених задач аналізу.

Схема процесу фільтрації мережевого трафіку наведена на рисунку 3.2

Рисунок 3.2 – Детальна схема фільтрації мережевого трафіка

Алгоритм фільтрації мережевого трафіку реалізує послідовну перевірку кожного пакета за заданими критеріями (рисунок 3.3).

```
function filter_packet(packet):
    # Перевірка, чи є пакет IP
    if not is_ip(packet):
        return DROP
    # Перевірка протоколу
    protocol = get_protocol(packet)
    if protocol not in [TCP, UDP, ICMP]:
        return DROP
    # Перевірка IP-адрес
    src_ip = get_source_ip(packet)
    dst_ip = get_destination_ip(packet)
```

Рисунок 3.3 – Псевдокод алгоритму фільтрації мережевого трафіку

```
if not is_allowed_ip(src_ip, dst_ip):
    return DROP
# Перевірка портів
src_port = get_source_port(packet)
dst_port = get_destination_port(packet)
if not is_allowed_port(src_port, dst_port):
    return DROP
# Перевірка розміру пакета
size = get_packet_size(packet)
if size < MIN_SIZE or size > MAX_SIZE:
    return DROP
# Якщо всі перевірки пройдені
return ACCEPT
```

Кінець рисунку 3.3

Структура обробки мережевого пакета є одним із ключових етапів функціонування системи моніторингу мережного трафіку, оскільки саме на цьому етапі відбувається перетворення сирих даних у структуровану інформацію, придатну для подальшого аналізу (рисунок 3.4).

Рисунок 3.4 – Структура обробки мережевого пакета

Після захоплення та первинної фільтрації мережевий пакет надходить у модуль обробки, де виконується його детальний розбір відповідно до рівнів мережевої моделі.

Мережевий пакет являє собою послідовність байтів, що містить заголовки різних рівнів (канального, мережевого та транспортного), а також корисне навантаження. На першому етапі обробки здійснюється декодування пакета, під час якого відбувається аналіз його структури та виділення заголовків. Зокрема, визначаються поля Ethernet-заголовка (MAC-адреси), IP-заголовка (IP-адреси, TTL, тип протоколу) та транспортного рівня (порти, службові прапори). Це дозволяє інтерпретувати сирі дані у зрозумілому для системи вигляді.

Після декодування виконується виділення ключових параметрів, які використовуються для подальшого аналізу. До таких параметрів належать IP-адреса джерела та призначення, тип транспортного протоколу (TCP, UDP, ICMP), номери портів, розмір пакета та часові характеристики, зокрема мітка часу отримання. Зазначені параметри формують основу для побудови статистичних моделей і виявлення аномалій у мережевому трафіку.

Наступним етапом є нормалізація даних. Оскільки пакети можуть мати різну структуру та надходити з різних джерел, необхідно привести їх до єдиного формату. Це включає уніфікацію запису IP-адрес, перетворення часових міток у стандартний формат, приведення назв протоколів до єдиного вигляду, а також обробку можливих відсутніх або некоректних значень. Нормалізація забезпечує коректність подальших обчислень і спрощує обробку великих обсягів даних.

Після нормалізації формується структурований запис, який представляє собою набір параметрів пакета у вигляді об’єкта або рядка таблиці. Такий запис може бути використаний для збереження в базі даних або передачі до модуля аналізу. Формування структурованого представлення дозволяє перейти від низькорівневого аналізу окремих пакетів до високорівневого аналізу мережевої активності.

Важливим етапом є перевірка коректності отриманих даних. На цьому етапі перевіряється правильність IP-адрес, допустимість значень портів, відповідність розміру пакета встановленим межам, а також цілісність даних. У разі виявлення помилок або аномальних значень пакет може бути відкинутий або позначений як підозрілий.

Завершальним етапом є передача оброблених даних до наступного модуля системи, зокрема модуля агрегації або аналізу. Передача може здійснюватися через буфер або чергу повідомлень, що дозволяє реалізувати асинхронну обробку та підвищити загальну продуктивність системи. Такий підхід забезпечує безперервність збору даних навіть при високому навантаженні.

Таким чином, структура обробки мережевого пакета включає послідовність взаємопов'язаних етапів: декодування, виділення параметрів, нормалізацію, формування структурованого запису, перевірку коректності та передачу даних. Ефективна реалізація цього процесу є критично важливою для забезпечення точності аналізу та стабільності роботи всієї системи моніторингу.

Алгоритм обробки мережевого пакета може бути представлений у вигляді наступного псевдокоду (рисунок 3.5)

```
function process_packet(packet):
    # Декодування пакета
    headers = decode(packet)
    # Перевірка наявності IP-заголовка
    if not has_ip(headers):
        return DROP
    # Виділення основних параметрів
    src_ip = get_source_ip(headers)
    dst_ip = get_destination_ip(headers)
    protocol = get_protocol(headers)
    size = get_packet_size(packet)
    timestamp = get_timestamp()
```

Рисунок 3.5 – Псевдокод алгоритму обробки мережевого пакета

```
# Виділення портів (для TCP/UDP)
    if protocol == TCP or protocol == UDP:
        src_port = get_source_port(headers)
 dst_port = get_destination_port(headers)
    else:
        src_port = NULL
        dst_port = NULL
    # Нормалізація даних
    src_ip = normalize_ip(src_ip)
    dst_ip = normalize_ip(dst_ip)
    protocol = normalize_protocol(protocol)
    # Перевірка коректності
    if not valid_ip(src_ip) or not valid_ip(dst_ip):
        return DROP
    if size <= 0 or size > MAX_PACKET_SIZE:
        return DROP
    # Формування структурованого запису
    record = create_record(
        timestamp,
        src_ip,
        dst_ip,
        protocol,
        src_port,
        dst_port,
        size
    )
    # Передача в модуль аналізу
    send_to_analysis(record)
    return ACCEPT
```

Кінець рисунку 3.5

Наведений алгоритм відображає послідовність дій, що виконуються над кожним пакетом, та демонструє логіку переходу від сирих даних до структурованого представлення, яке використовується для подальшого аналізу мережевого трафіку.

На першому етапі відсіюються пакети, що не належать до IP-протоколу. Далі виконується перевірка транспортного протоколу, що дозволяє обмежити аналіз лише необхідними типами з’єднань. Наступні етапи включають перевірку IP-адрес, портів та розміру пакета. У разі невідповідності хоча б

одному з критеріїв пакет відкидається. Такий підхід дозволяє мінімізувати навантаження на систему та забезпечити ефективну обробку лише релевантного трафіку.

Таким чином, фільтрація мережевого трафіку є необхідним етапом, який дозволяє значно зменшити обсяг оброблюваних даних, підвищити швидкодію системи та забезпечити більш точний і ефективний аналіз мережевої активності. Вона виступає проміжною ланкою між збором даних і їх подальшою обробкою, забезпечуючи підготовку якісного вхідного набору даних для системи виявлення аномалій.

3.3. Реалізація алгоритмів аналізу трафіку та виявлення аномалій

Для забезпечення ефективного виявлення перевантажень і аномалій у роботі мережі в розробленій системі застосовано комбінований підхід, що базується на використанні статистичних методів, порогового аналізу та аналізу динаміки змін трафіку. Такий підхід дозволяє підвищити точність виявлення відхилень і зменшити кількість хибних спрацювань, що є важливим для практичного застосування системи.

Основною ідеєю статистичного підходу є порівняння поточних значень мережевого трафіку з типовими значеннями, які характеризують нормальний стан мережі. Для цього формується модель нормального трафіку на основі історичних даних, отриманих у процесі спостереження за мережею в умовах її стабільної роботи. Такі дані агрегуються за часовими інтервалами та використовуються для обчислення базових статистичних характеристик.

Ключовими параметрами є середнє значення трафіку та стандартне відхилення. Середнє значення відображає типовий рівень навантаження мережі, тоді як стандартне відхилення характеризує допустимі коливання цього навантаження. На основі цих показників визначаються межі нормального функціонування системи. Як правило, використовується інтервал, що

визначається як середнє значення плюс-мінус кілька стандартних відхилень. Значення трафіку, які виходять за ці межі, класифікуються як аномальні.

Такий підхід дозволяє враховувати природні коливання трафіку та адаптуватися до змін у поведінці мережі. Наприклад, у години пік середній рівень трафіку може бути значно вищим, ніж у нічний час, і статистична модель дозволяє коректно це врахувати.

Поряд зі статистичним методом застосовується пороговий аналіз, який передбачає встановлення фіксованих рівнів завантаження мережі. Ці рівні визначаються у відсотках від максимальної пропускної здатності каналу або на основі емпіричних спостережень. У разі перевищення встановлених порогів система генерує відповідні сигнали попередження або критичне повідомлення.

Пороговий підхід є простим у реалізації та забезпечує швидке реагування на перевантаження мережі. Він особливо ефективний у випадках, коли необхідно оперативно виявляти перевищення допустимого рівня навантаження, незалежно від статистичних характеристик.

Рівні завантаження мережі наведені в таблиці 3.1.

Таблиця 3.1 – Рівні завантаження мережі

Завантаження	Стан системи
0–70%	Нормальний
70–90%	Попередження
90–100%	Критичний

Додатково в системі використовується аналіз динаміки змін трафіку, який дозволяє виявляти аномалії, що проявляються у вигляді різких змін інтенсивності трафіку. Навіть якщо абсолютні значення не перевищують встановлених порогів, різкі стрибки або спадання можуть свідчити про підозрілу активність, наприклад, сканування мережі або початок атаки.

Для реалізації такого аналізу використовується оцінка швидкості зміни трафіку між сусідніми часовими інтервалами. Якщо різниця між значеннями перевищує заданий поріг, така ситуація розглядається як потенційна аномалія.

Це дозволяє виявляти короткочасні події, які можуть бути пропущені при використанні лише статичних порогів.

На рисунку 3.6 наведений графік нормального та аномального трафіку.

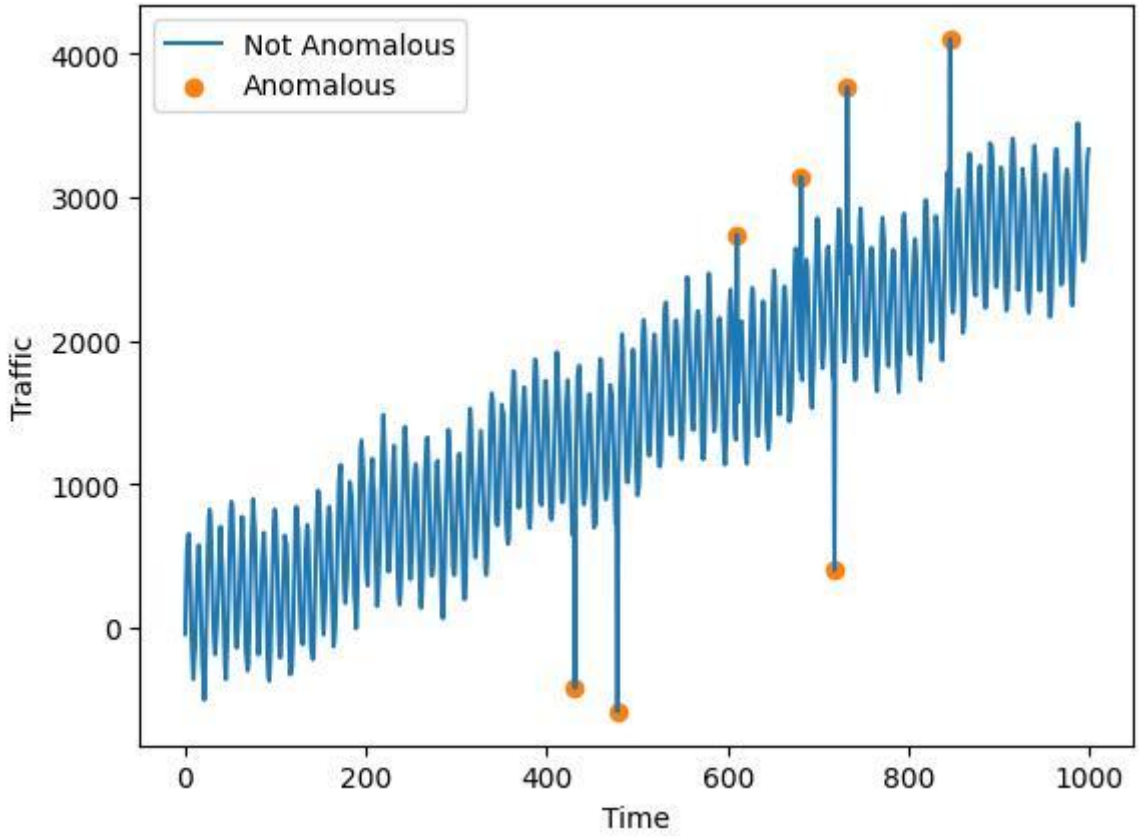


Рисунок 3.6 – Графік нормального та аномального трафіку

На наведеному графіку видно, що нормальний трафік характеризується відносно плавними змінами в межах допустимого діапазону, тоді як аномальний трафік проявляється у вигляді різких піків або провалів. Такі відхилення можуть бути ознаками перевантаження мережі або несанкціонованої активності.

Поєднання статистичних методів, порогового аналізу та аналізу динаміки змін дозволяє створити гнучку та ефективну систему виявлення аномалій. Статистичний підхід забезпечує адаптивність до змін у поведінці мережі, пороговий швидке реагування на перевантаження, а аналіз динаміки забезпечує виявлення короткочасних і різких змін.

3.4 Реалізація підсистеми збереження та візуалізації даних

Одним із ключових компонентів системи моніторингу мережевого трафіку є підсистема збереження та візуалізації даних, яка забезпечує накопичення, структуризацію, довготривале зберігання та наочне представлення інформації про стан мережі. Реалізація даної підсистеми дозволяє не лише здійснювати аналіз у режимі реального часу, але й проводити ретроспективне дослідження мережевої активності, що є важливим для виявлення довгострокових тенденцій і повторюваних аномалій.

Підсистема збереження даних базується на використанні реляційної бази даних, що забезпечує ефективну організацію та доступ до інформації. У якості системи керування базами даних обрано SQLite, що пояснюється її простотою інтеграції, відсутністю необхідності в окремому сервері та достатньою продуктивністю для задач локального моніторингу. SQLite дозволяє зберігати дані у вигляді структурованих таблиць і виконувати швидкий доступ до них за допомогою SQL-запитів.

Основною таблицею бази даних є таблиця журналу трафіку, яка містить записи про кожен оброблений пакет або агрегований інтервал. До основних полів цієї таблиці належать: часовий штамп, IP-адреса джерела, IP-адреса призначення, тип протоколу, номер порту, розмір пакета, а також статус (нормальний або аномальний). Така структура дозволяє зберігати як детальну, так і узагальнену інформацію про мережевий трафік.

Для підвищення ефективності роботи бази даних використовується індексація ключових полів, зокрема часових міток і IP-адрес. Це дозволяє значно прискорити виконання запитів, пов’язаних із пошуком та аналізом даних за певний період часу або для конкретних вузлів мережі. Крім того, застосовується механізм обмеження розміру бази даних шляхом видалення застарілих записів або архівування даних.

Окрім збереження сирих або агрегованих даних, система підтримує

формування похідних показників, які також можуть зберігатися у базі даних. До таких показників належать середні значення трафіку, пікові навантаження, кількість аномалій за певний період та інші статистичні характеристики. Це дозволяє скоротити час обробки при повторному аналізі.

Важливим аспектом є організація запису даних у базу. Для цього використовується буферизація, яка дозволяє накопичувати дані у пам’яті та записувати їх у базу пакетами. Такий підхід зменшує кількість операцій введення-виведення та підвищує загальну продуктивність системи.

Підсистема візуалізації є невід’ємною частиною системи моніторингу, оскільки вона забезпечує зручне та інтуїтивно зрозуміле представлення даних для користувача. Візуалізація дозволяє швидко оцінити стан мережі, виявити аномалії та прийняти відповідні рішення.

Основним способом візуалізації є побудова графіків зміни трафіку в часі (рисунок 3.7). Такі графіки відображають залежність обсягу переданих даних або кількості пакетів від часу. На них можуть бути додатково позначені аномальні ділянки, що дозволяє легко ідентифікувати проблемні моменти.

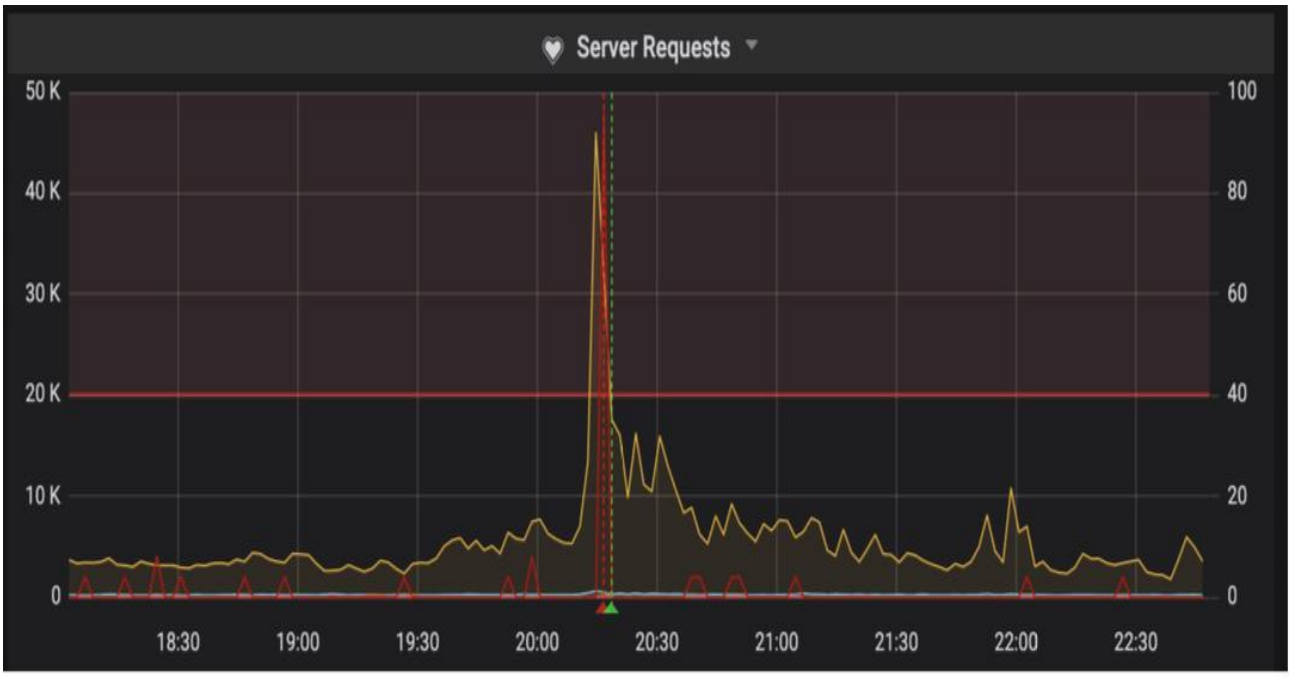


Рисунок 3.7 – Зміни трафіку в часі

3.5 Інтерфейс користувача системи моніторингу трафіку

Інтерфейс користувача є важливою складовою системи моніторингу мережевого трафіку, оскільки саме через нього здійснюється взаємодія адміністратора або аналітика із системою. Основною метою інтерфейсу є забезпечення зручного, інтуїтивно зрозумілого та ефективного доступу до функціональних можливостей підсистеми, включаючи перегляд поточних даних, аналіз статистики та формування звітів.

Головна сторінка інтерфейсу зазвичай містить інформаційну панель (дашборд), на якій у реальному часі відображаються ключові показники мережевого трафіку. До таких показників належать загальний обсяг переданих даних, швидкість передачі, кількість активних з'єднань, а також розподіл трафіку за протоколами або вузлами мережі. Для підвищення наочності ці дані можуть бути представлені у вигляді графіків, діаграм та таблиць, що дозволяє швидко оцінити поточний стан мережі та виявити потенційні проблеми (рисунок 3.8).

Рисунок 3.8 – Головна сторінка інтерфейсу

Важливою функцією підсистеми є можливість генерації звітів. Звіти можуть формуватися за заданий період часу та містити основні статистичні показники, графіки та список виявлених аномалій. Це дозволяє використовувати систему не лише для оперативного моніторингу, але й для документування стану мережі. Користувач може обирати параметри звіту, такі як часовий інтервал, типи даних для аналізу, а також формат представлення результатів.

Звіти можуть включати детальну інформацію про пікові навантаження, підозрілу активність, збої у передачі даних або нестандартну поведінку окремих вузлів. Це особливо важливо для забезпечення інформаційної безпеки, оскільки дозволяє своєчасно реагувати на потенційні загрози, такі як атаки типу DDoS або несанкціонований доступ до ресурсів мережі.

Також передбачено можливість експорту даних у різні формати, такі як CSV або JSON, що дозволяє інтегрувати систему з іншими аналітичними інструментами або використовувати дані для подальших досліджень. Експортовані дані можуть бути використані для побудови власних моделей аналізу, машинного навчання або збереження в зовнішніх системах звітності.

Інтерфейс користувача забезпечує зручні засоби фільтрації та пошуку інформації. Користувач може задавати параметри відбору даних за IP-адресами, портами, протоколами, часовими інтервалами або іншими характеристиками. Це значно спрощує процес аналізу великих обсягів інформації та дозволяє швидко знаходити необхідні дані.

Окрему увагу приділено питанням продуктивності та масштабованості підсистеми. Використання агрегованих даних, індексації та буферизації дозволяє забезпечити стабільну роботу навіть при значному обсязі трафіку. Завдяки цьому система може обробляти великі потоки даних у реальному часі без суттєвих затримок.

Для підвищення продуктивності застосовуються сучасні підходи до обробки даних, зокрема кешування результатів запитів та оптимізація доступу

до бази даних. Це дозволяє зменшити навантаження на сервер та прискорити відображення інформації в інтерфейсі користувача.

Крім того, система може використовувати асинхронну обробку запитів, що забезпечує плавну роботу навіть при великій кількості одночасних користувачів.

У разі необхідності система може бути розширена шляхом переходу на більш потужні системи управління базами даних або використання розподілених рішень. Це дозволяє масштабувати систему відповідно до зростання обсягів трафіку та кількості підключених пристроїв.

Використання хмарних технологій також відкриває можливості для гнучкого масштабування та підвищення надійності системи. Використання хмарних технологій дозволяє системі динамічно змінювати обчислювальні ресурси залежно від поточного навантаження. Це забезпечує ефективне використання інфраструктури та зменшує витрати на утримання власного обладнання. Хмарні платформи надають високий рівень відмовостійкості завдяки розподіленому зберіганню даних та резервному копіюванню. У разі збоїв або перевантажень система може автоматично перемикатися на інші сервери без втрати даних. Крім того, використання хмари спрощує розгортання та оновлення системи, що дозволяє швидше впроваджувати нові функції.

Інтерфейс користувача також може включати систему сповіщень, яка інформує адміністратора про критичні події або перевищення встановлених порогових значень. Сповіщення можуть відображатися безпосередньо в інтерфейсі або надсилатися через електронну пошту чи інші канали зв’язку. Це дозволяє оперативно реагувати на проблеми та мінімізувати їх вплив на роботу мережі.

Для системи моніторингу мережевого трафіку блок виявлених аномалій є ключовим елементом інтерфейсу, який фокусується на оперативному реагуванні, документуванні та подальшому аналізі.

Усі аномалії класифікуються за трьома основними категоріями, першою з

яких є аномалії продуктивності, пов'язані з різким погіршенням якісних показників мережі. До них відносяться сплески затримки, коли раптово зростає час відгуку вище критичного порогу, втрати пакетів із перевищенням допустимого відсотка відхилень на стабільній лінці, а також аномальні падіння пропускної здатності при стабільному навантаженні.

Другою категорією є аномалії безпеки, які вказують на потенційні кібератаки або несанкціоновану активність. Вони включають мережеве сканування у вигляді масових послідовних запитів від однієї IP-адреси до різних портів хоста, потокові аномалії типу DoS чи DDoS зі стрімким нетиповим зростанням кількості пакетів, та ексфільтрацію даних, що характеризується нетипово великим обсягом вихідного трафіку на зовнішні адреси. Третя категорія охоплює системні та структурні аномалії, які свідчать про збої в роботі обладнання або зміну конфігурації, наприклад, появу незвичних для певної підмережі протоколів або фіксацію високої активності передавання великих масивів даних у неробочі нічні години.

На інтерфейсі користувача кожна виявлена аномалія має свій рівень критичності, який у чорно-білій палітрі диференціюється відтінками сірого та графічними маркерами.

Низький рівень позначається світло-сірим кольором і відображає поодинокі відхилення від базової лінії, які не впливають на загальну працездатність системи.

Середній рівень маркується сірим кольором і сигналізує про повторювані відхилення, що потребують уваги адміністратора. Високий рівень виділяється чорним кольором або жирним шрифтом, вказуючи на явні ознаки атаки чи критичного збою, які вимагають негайного втручання.

У табличній частині дашборду компонент списку виявлених аномалій структурує дані для подальшого аналізу та експорту у формати CSV або JSON. Кожен рядок логу містить точний час фіксації події підсистемою, ідентифікатор або IP-адресу джерела аномального трафіку, конкретну назву типу відхилення,

поточне значення метрики в момент аномалії порівняно з нормою, візуальний маркер рівня загрози та поточний статус розслідування події. Безпосередньо на лінійних графіках та гістограмах аномалії відображаються за допомогою методу базової лінії.

Система автоматично аналізує історичні дані завдяки індексації та буферизації трафіку, будує світло-сірий коридор норми, а всі точки, що виходять за його межі, маркує контрастними темними маркерами. Надалі ці дані підсистема акумулює у статистичні показники для звітів, дозволяючи аналізувати динаміку появи відхилень за заданий період часу.

Окрім базових функцій моніторингу та формування звітів, сучасні системи аналізу мережевого трафіку можуть включати ряд додаткових можливостей, що значно підвищують ефективність роботи користувача. Однією з таких можливостей є персоналізація інтерфейсу. Користувач може налаштовувати відображення панелей, обирати необхідні віджети, змінювати структуру дашборду відповідно до власних потреб. Це дозволяє зосередитися лише на тих показниках, які є найбільш важливими у конкретному випадку.

Ще одним важливим аспектом є підтримка ролей та рівнів доступу. У системі можуть бути передбачені різні типи користувачів, наприклад адміністратори, аналітики та звичайні користувачі. Кожна роль має власний набір прав доступу до функцій системи та даних. Це підвищує безпеку та дозволяє ефективно організувати роботу в команді.

Значну роль відіграє інтеграція з іншими системами. Інтерфейс користувача може забезпечувати взаємодію з системами кібербезпеки, системами управління подіями (SIEM), а також іншими мережевими інструментами. Завдяки цьому можна об'єднати дані з різних джерел та отримати більш повну картину стану мережі.

Також варто відзначити можливість візуалізації топології мережі. У вигляді інтерактивної схеми користувач може бачити структуру мережі, взаємозв’язки між вузлами, а також поточний стан кожного елемента. Це

значно спрощує виявлення проблемних ділянок та аналіз інцидентів.

Особливу увагу слід приділити зручності користування (юзабіліті) інтерфейсу. Важливо, щоб інтерфейс був інтуїтивно зрозумілим, мав логічну структуру та швидкий доступ до основних функцій. Використання сучасних принципів UX/UI-дизайну, таких як мінімалізм, адаптивність та чітка візуальна ієрархія, сприяє підвищенню ефективності роботи користувача.

Адаптивність інтерфейсу є ще одним важливим фактором. Система повинна коректно працювати на різних пристроях, таких як персональні комп'ютери, планшети та смартфони. Це дозволяє здійснювати моніторинг мережі у будь-який час і з будь-якого місця, що особливо важливо для адміністраторів.

Крім того, доцільно реалізувати механізми журналювання дій користувачів. Це дозволяє відстежувати, які саме операції виконувалися в системі, що є важливим як з точки зору безпеки, так і для аналізу роботи персоналу. Журнали можуть використовуватися для аудиту та розслідування інцидентів.

Не менш важливою є підтримка автоматизації процесів. Інтерфейс може надавати можливість створення сценаріїв або правил, які автоматично виконуються при настанні певних умов. Наприклад, система може автоматично надсилати сповіщення або блокувати підозрілу активність.

Окремо варто згадати про використання технологій машинного навчання. Інтерфейс може відображати результати інтелектуального аналізу даних, зокрема прогнозування навантаження або виявлення аномалій. Це дозволяє переходити від реактивного до проактивного управління мережею.

Отже, розширення функціональності інтерфейсу користувача дозволяє значно підвищити ефективність системи моніторингу трафіку. Впровадження додаткових можливостей забезпечує більш глибокий аналіз, покращує зручність роботи та сприяє підвищенню рівня безпеки мережевої інфраструктури.

Інтерфейс користувача системи моніторингу трафіку є ключовим елементом, який забезпечує ефективний контроль, аналіз та управління мережевими ресурсами. Його функціональність, зручність використання та продуктивність безпосередньо впливають на здатність системи виконувати свої завдання та забезпечувати стабільну роботу мережі.

3.5 Висновки до третього розділу

У третьому розділі було розглянуто практичні аспекти реалізації системи моніторингу мережевого трафіку, призначеної для виявлення перевантажень і аномалій у роботі мережі. Основну увагу приділено розробці та впровадженню ключових компонентів системи, що забезпечують збір, обробку, аналіз, збереження та візуалізацію даних.

У ході роботи було обґрунтовано вибір інструментальних засобів і середовища реалізації, що дозволило створити ефективну та гнучку програмну систему. Використання сучасних бібліотек і технологій забезпечило можливість обробки мережевого трафіку в режимі реального часу та подальшого аналізу великих обсягів даних.

Реалізовано модуль збору мережевого трафіку, який здійснює перехоплення пакетів, їх фільтрацію та первинну обробку. Особливу увагу приділено структурі обробки пакета, що включає декодування, виділення ключових параметрів, нормалізацію та формування структурованих записів. Це дозволило забезпечити коректність і зручність подальшого аналізу даних.

Також розроблено підсистему збереження та візуалізації даних, яка забезпечує накопичення інформації, її структуризацію та наочне представлення. Використання бази даних і графічних засобів візуалізації дозволяє проводити як оперативний, так і ретроспективний аналіз стану мережі.

ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень було спроектовано та реалізовано систему моніторингу мережного трафіку, що забезпечує виявлення перевантажень та аномалій у роботі мереж.

У межах розділу 1 було проведено комплексний аналіз предметної області моніторингу мережного трафіку. Розглянуто сучасний стан розвитку мережевих технологій, визначено основні тенденції їх розвитку, а також проаналізовано особливості функціонування сучасних комп'ютерних мереж.

Особливу увагу було приділено проблемам перевантаження мережі та виникнення аномалій у мережному трафіку. Встановлено, що ці явища є одними з основних факторів, які негативно впливають на стабільність та ефективність роботи мережевих систем. Розглянуто основні причини їх виникнення, а також наслідки, до яких вони можуть призводити.

У ході аналізу існуючих систем моніторингу мережного трафіку було виявлено їх основні переваги та недоліки. Зокрема, встановлено, що більшість сучасних рішень або не забезпечують достатньої деталізації аналізу, або потребують значних обчислювальних ресурсів. Крім того, багато систем мають обмежені можливості щодо виявлення нових або складних аномалій.

Також було розглянуто основні типи аномалій у мережному трафіку, включаючи DDoS-атаки, сканування портів, спроби підбору паролів, витік даних та незвичну активність користувачів. Визначено їх характерні ознаки та вплив на роботу мережі.

У межах розділу 2 було проведено детальний аналіз методів та засобів моніторингу мережного трафіку. Розглянуто основні підходи до організації моніторингу, зокрема пасивний, активний та потоковий, що дозволило визначити їх особливості, переваги та обмеження.

Проаналізовано сучасні методи збору даних про мережний трафік, включаючи захоплення пакетів, використання потокових технологій та аналіз

журналів мережевих пристроїв. Встановлено, що найбільш ефективним є комбінований підхід, який забезпечує баланс між деталізацією інформації та навантаженням на систему.

Особливу увагу приділено методам аналізу мережного трафіку, виявлення перевантажень та аномалій. Розглянуто статистичні, порогові та сигнатурні методи, а також їх поєднання для підвищення точності виявлення відхилень. Визначено, що комплексне використання цих методів дозволяє забезпечити більш надійний контроль стану мережі.

У ході дослідження було розглянуто архітектурні особливості систем моніторингу, зокрема централізовану та розподілену моделі. Встановлено, що централізована архітектура є простішою у реалізації, однак має обмеження щодо масштабованості та надійності, тоді як розподілена забезпечує кращу продуктивність і відмовостійкість у великих мережах.

У третьому розділі було розглянуто практичні аспекти реалізації системи моніторингу мережевого трафіку, призначеної для виявлення перевантажень і аномалій у роботі мережі. Основну увагу приділено розробці та впровадженню ключових компонентів системи, що забезпечують збір, обробку, аналіз, збереження та візуалізацію даних.

У ході роботи було обґрунтовано вибір інструментальних засобів і середовища реалізації, що дозволило створити ефективну та гнучку програмну систему. Використання сучасних бібліотек і технологій забезпечило можливість обробки мережевого трафіку в режимі реального часу та подальшого аналізу великих обсягів даних.

Реалізовано модуль збору мережевого трафіку, який здійснює перехоплення пакетів, їх фільтрацію та первинну обробку.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Bhuyan M. H., Bhattacharyya D. K., Kalita J. K. Network Traffic Anomaly Detection and Prevention: Concepts, Techniques, and Tools. Cham : Springer, 2017. 263 p. DOI: 10.1007/978-3-319-65188-0.

2. Author Sayantan, Roy Sayantan. A comprehensive Survey on Network Traffic Anomaly Detection using Deep Learning. 2024. 10.13140/RG.2.2.32071.30884.

3. Tsikerdekis M., Waldron S., Emanuelson A. Network Anomaly Detection Using Exponential Random Graph Models and Autoregressive Moving Average. *IEEE Access*. 2021. Vol. 9. P. 132685–132700. DOI: 10.1109/ACCESS.2021.3116575.

4. Кльоц Ю., Петляк Н.. Виявлення аномального трафіку у комп'ютерних мережах. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2022. № 3. С. 65–71.

5. Kapre A., Padmavathi B. Behaviour based botnet detection with traffic analysis and flow interavals using PSO and SVM. *International Conference on Intelligent Computing and Control Systems: Proceedings* (Madurai, India, 15-16 June 2017). Madurai. 2017. P. 718–722.

6. Нічепорук А. О., Нічепорук А. А., Нічепорук Ю. О., Казанцев А. Д. Метод виокремлення фрагментів бот-мереж на основі аналізу мережевого трафіку. *Вісник Хмельницького національного університету. Технічні науки*. 2020. № 2(283). С. 141–149. DOI: 10.31891/2307-5732-2020-283-2-141-149.

7. Laanaoui M. D., Lachgar M., Mohamed H., Hamid H., Villar S. G., Ashraf I. Enhancing urban traffic management through real-time anomaly detection and load balancing. *Ieee Access*. 2024. Vol. 12. Pp. 63683-63700.

8. Сеник А., Пиріг Ю., Шпур О. Дослідження інтелектуального алгоритму моніторингу якості роботи систем масового обслуговування. *Infocommunication technologies and electronic engineering*. 2024.

(4, № 2). С.103-112.

9. Торошанко Я. І., Якимчук Н. М. Статистичні моделі управління телекомунікаційними мережами та методи боротьби з перевантаженнями. *Телекомунікаційні та інформаційні технології*. 2017. №3.

10. Проніна О. І., Рейжевський М. І. Розробка програмного забезпечення генерації мережевого трафіку в комп'ютерних мережах для задач кібербезпеки. *Вісник Приазовського Державного Технічного Університету. Серія: Технічні науки*. 2025. №52. С. 75-82.

11. Стрелковська І., Соловська І., Стрелковська Ю. Детектування трафіку ddos-атак на веб-сервери. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2025. №4. С. 203-210.

12. Srikavin S., Joshika S., Senabadhy Sesan R., Nandhini K., Hema Yazhini J. D., Raj P., Senthilkumar A. (2025, April). Real-Time Traffic Monitoring for Anomaly Detection and Congestion Management. In *International Conference on Business Intelligence and Data Analytics* . 2025. pp. 57-68. Cham: Springer Nature Switzerland.

13. AsSadhan B., Zeb K., Al-Muhtadi J., Alshebeili S. Anomaly detection based on LRD behavior analysis of decomposed control and data planes network traffic using SOSS and FARIMA models. *IEEE Access*. 2017. Vol. *5*. Pp. 13501-13519.

14. Fowdur T. P., Babooram L. Network Traffic Monitoring and Analysis. In *Machine Learning For Network Traffic and Video Quality Analysis: Develop and Deploy Applications Using JavaScript and Node. Js*/ 2024. pp. 51-96. Berkeley, CA: Apress.

15. D'Alconzo A., Drago I., Morichetta A., Mellia M., Casas P. A survey on big data for network traffic monitoring and analysis. *IEEE Transactions on Network and Service Management*. 2019. №*16*(3). Pp. 800-813.

16. Kaur S., Barisal S. K., Maddikayala V. N., Sunil M. P., Gogula S., Vashisht R. Real-Time Internet Congestion Detection Using Passive Flow

Analysis. *J. Internet Serv. Inf. Secur.* 2025. Vol. 15(4).

17. Савченко Я., Левченко С. Аналіз вимог до програмного забезпечення для керування локальними комп'ютерними мережами. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2026. №.1. С. 404-411.

18. Da Silva A. S., Wickboldt J. A., Granville L. Z., Schaeffer-Filho A. (2016, April). ATLANTIC: A framework for anomaly traffic detection, classification, and mitigation in SDN. In *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*. pp. 27-35. IEEE.

19. Carvalho L. F., Fernandes G., Rodrigues J. J., Mendes L. S., Proenca M. L. (2017, May). A novel anomaly detection system to assist network management in SDN environment. In *2017 IEEE international conference on communications (ICC)*. pp. 1-6. IEEE.

20. Raja N. M., Vegad S. An empirical study for the traffic flow rate prediction-based anomaly detection in software-defined networking: a challenging overview. *Social network analysis and mining*. 2023. Vol. 13(1). P. 72.

21. Jafarian T., Masdari M., Ghaffari A., Majidzadeh K. Security anomaly detection in software-defined networking based on a prediction technique. *International Journal of Communication Systems*. 2020. Vol. *33*(14). e4524.

22. Carvalho L. F., Abrão T., de Souza Mendes L., Proença Jr M. L. An ecosystem for anomaly detection and mitigation in software-defined networking. *Expert Systems with Applications*. 2018. Vol. 104. Pp. 121-133.

23. Granby B. R., Askwith B., Marnerides A. K. (2015, November). SDN-PANDA: software-defined network platform for anomaly detection applications. In *2015 IEEE 23rd International Conference on Network Protocols (ICNP)*. 2015. Pp. 463-466. IEEE.

24. Ujjan R. M. A., Pervez Z., Dahal K. (2018, June). Suspicious traffic detection in SDN with collaborative techniques of snort and deep neural networks. In *2018 IEEE 20th International Conference on High Performance Computing and*

Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). pp. 915-920). IEEE.

25. Hirsi A., Audah L., Salh A., Sahar N. M., Ahmed S., Alhartomi M. A. (2024, August). Ddos anomaly detection in software-defined networks: An evaluation of machine learning techniques for traffic classification and prediction. In *2024 International Conference on Future Technologies for Smart Society (ICFTSS)*. pp. 100-105. IEEE.

26. Ranshous S., Shen S., Koutra D., Harenberg S., Faloutsos C., Samatova N. F. Anomaly detection in dynamic networks: a survey. *Wiley Interdisciplinary Reviews: Computational Statistics*. 2015. Vol. 7(3). Pp. 223-247.

27. Bereziński P., Jasiul B., Szpyrka M. An entropy-based network anomaly detection method. *Entropy*. 2015. Vol. 17(4). Pp. 2367-2408.

28. Moustafa N., Slay J. The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. *Information Security Journal: A Global Perspective*. 2016. Vol. 25(1-3). Pp. 18-31.

29. Taylor A., Japkowicz N., Leblanc S. (2015, December). Frequency-based anomaly detection for the automotive CAN bus. In *2015 World Congress on Industrial Control Systems Security (WCICSS)*. 2015. pp. 45-49. IEEE.

30. Goh J., Adepu S., Tan M., Lee Z. S. (2017, January). Anomaly detection in cyber physical systems using recurrent neural networks. In *2017 IEEE 18th international symposium on high assurance systems engineering (HASE)*. pp. 140-145. IEEE.

31. Cook A. A., Mısırlı G., Fan Z. Anomaly detection for IoT time-series data: A survey. *IEEE Internet of Things Journal*. 2019. Vol. *7*(7). Pp. 6481-6494.

32. Inoue J., Yamagata Y., Chen Y., Poskitt C. M., Sun J. (2017, November). Anomaly detection for a water treatment system using unsupervised machine learning. In *2017 IEEE international conference on data mining workshops*

(ICDMW). pp. 1058-1065. IEEE.

33. Hajisalem V., Babaie S. A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection. *Computer Networks*. 2018. Vol. 136. Pp. 37-50.

34. Chen, Z., Yeo, C. K., Lee, B. S., & Lau, C. T. (2018, April). Autoencoder-based network anomaly detection. In *2018 Wireless telecommunications symposium (WTS)* (pp. 1-5). IEEE.

35. Su Y., Zhao Y., Niu C., Liu R., Sun W., Pei D. (2019, July). Robust anomaly detection for multivariate time series through stochastic recurrent neural network. In *Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining*. pp. 2828-2837.

36. Ren H., Xu B., Wang Y., Yi C., Huang C., Kou X., Zhang Q. (2019, July). Time-series anomaly detection service at microsoft. In *Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining* . pp. 3009-3017.

37. Zhou X., Hu Y., Liang W., Ma J., Jin Q. Variational LSTM enhanced anomaly detection for industrial big data. *IEEE Transactions on Industrial Informatics*. 2020. Vol. 17(5). Pp. 3469-3477.

38. Taylor A., Leblanc S., Japkowicz N. (2016, October). Anomaly detection in automobile control network data with long short-term memory networks. In *2016 IEEE international conference on data science and advanced analytics (DSAA)*. pp. 130-139. IEEE.

39. Ameen S. Attack and anomaly detection in iot networks using machine learning techniques: A review. *Asian journal of research in computer science*. 2021.

40. Li Y., Liang W., Xie K., Zhang D., Li K., Xiong N. N. EventMon: Real-time event-based streaming network monitoring data recovery. *IEEE Transactions on Dependable and Secure Computing*. 2024. Vol. 22(3). Pp. 2413-2429.

41. Xu H., Sun Z., Cao Y., Bilal H. RETRACTED ARTICLE: A data-driven approach for intrusion and anomaly detection using automated machine learning for

the Internet of Things. *Soft computing*. 2023. Vol. 27(19). Pp. 14469-14481.

42. Zhao H., Wang Y., Duan J., Huang C., Cao D., Tong Y., .Zhang Q. (2020, November). Multivariate time-series anomaly detection via graph attention network. In *2020 IEEE international conference on data mining (ICDM)*. pp. 841-850. IEEE.

43. Медзатий Д., Марценюк А. Метод моніторингу параметрів комп'ютерної мережі в реальному часі. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2026. № 2. С. 14–23. DOI: 10.31891/2219-9365-2026-86-2.

44. Кирик М., Плесканка Н., Рій А. Дослідження можливостей застосування методу isolation forest для виявлення аномалій у мережевому трафік. *Herald of Khmelnytskyi National University. Technical Sciences*. 2025. №*349*(2). С. 171-177. https://doi.org/10.31891/2307-5732-2025-349-25.

45. Shen L., Li Z., Kwok J. Timeseries anomaly detection using temporal hierarchical one-class network. *Advances in neural information processing systems*. 2020. Vol. 33. Pp. 13016-13026.

46. Lu Q., Xie X., Parlikad A. K., Schooling J. M. Digital twin-enabled anomaly detection for built asset monitoring in operation and maintenance. *Automation in Construction*. 2020. Vol. 118. P. 103277.

47. Ribeiro M., Lazzaretti A. E., Lopes H. S.. A study of deep convolutional auto-encoders for anomaly detection in videos. *Pattern Recognition Letters*. 2018. Vol. 105. Pp. 13-22.

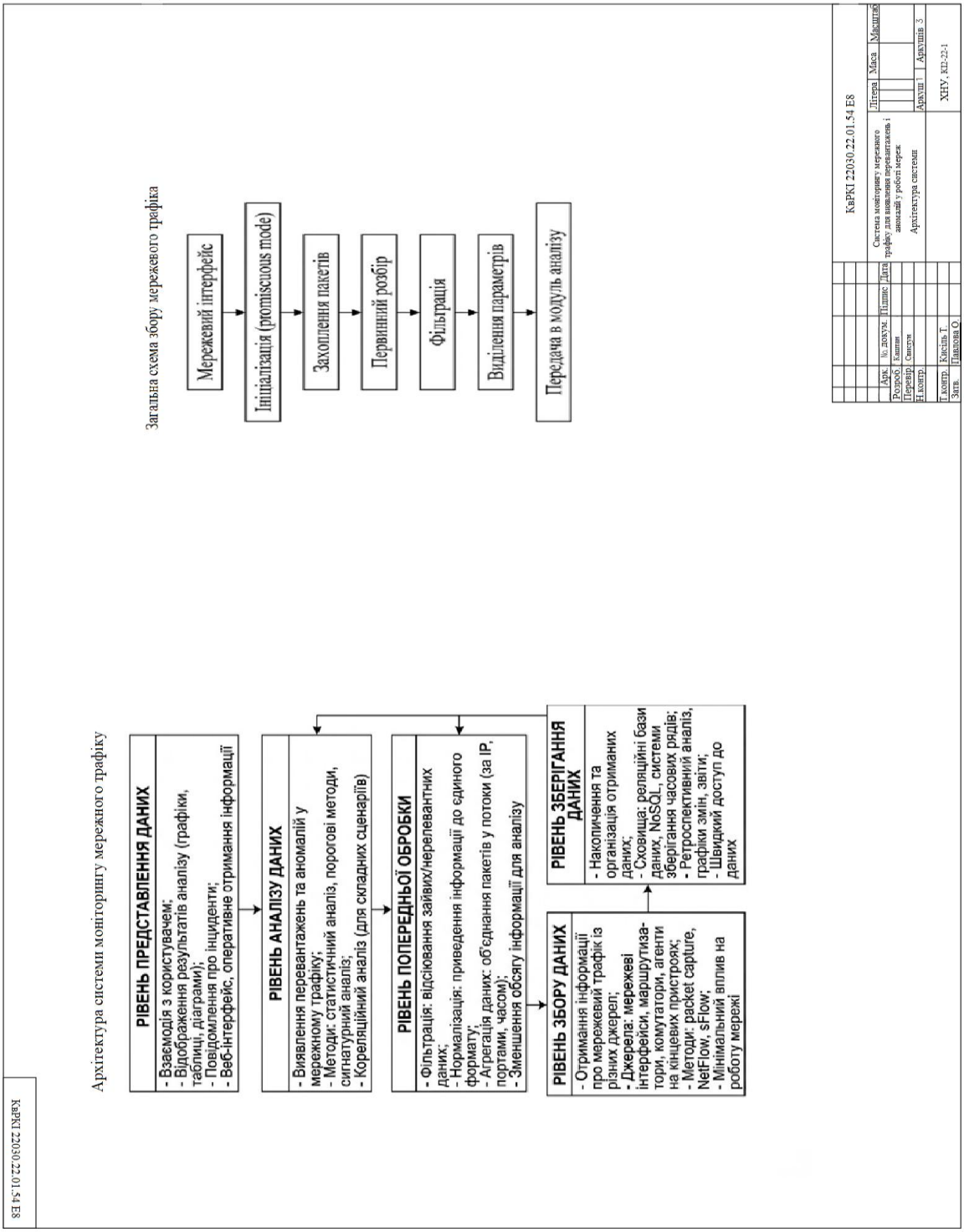
48. Lin S., Clark R., Birke R., Schönborn, S., Trigoni N., Roberts S. (2020, May). Anomaly detection for time series using vae-lstm hybrid model. In *ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2020. Pp. 4322-4326. IEEE.

49. Velan P., Čermák, M., Čeleda P., Draša, M. A survey of methods for encrypted traffic classification and analysis. *International Journal of Network Management*. 2015. Vol. *25*(5). Pp. 355-374.

ДОДАТОК А

(обов’язковий)

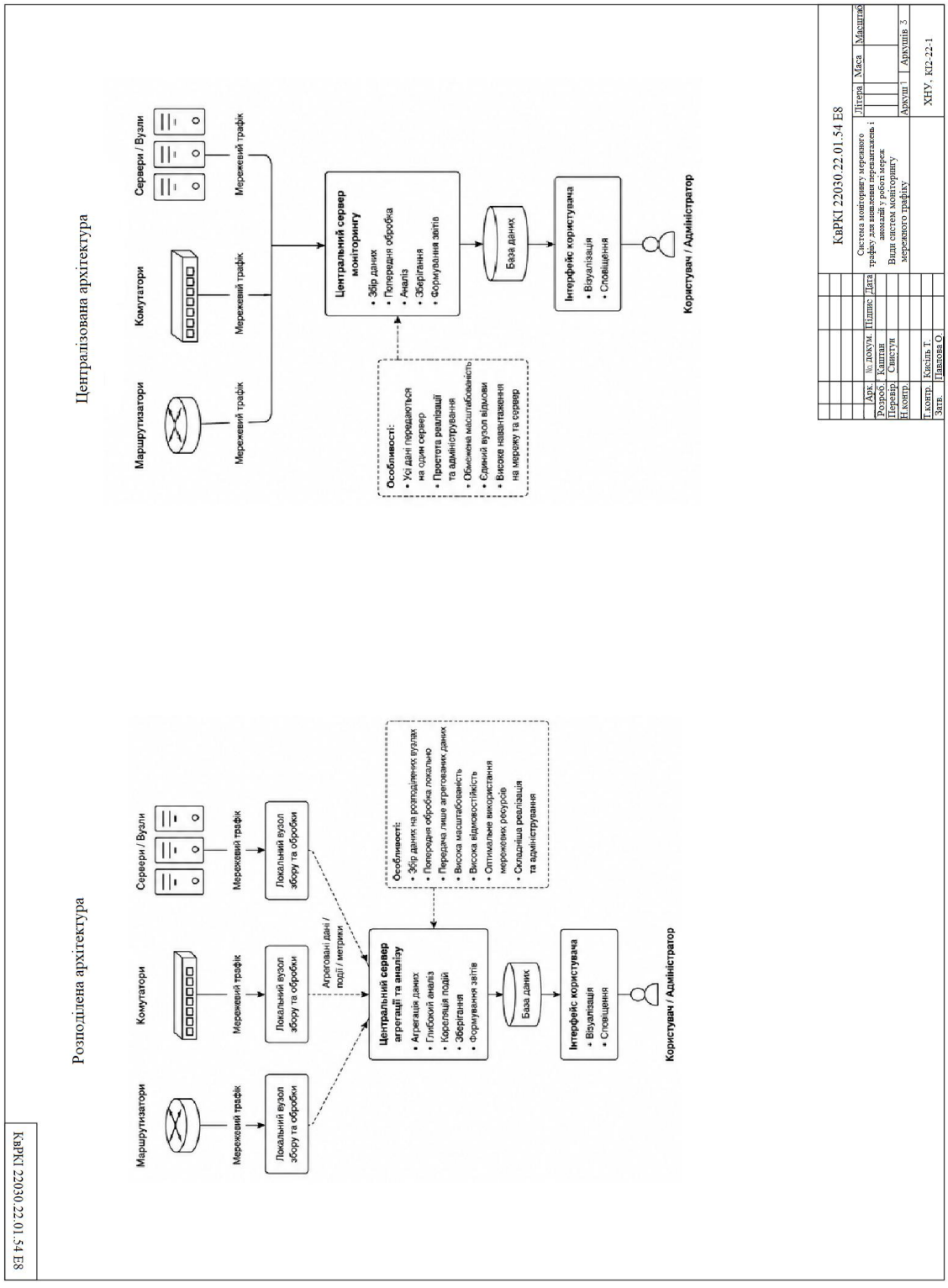
Копія креслення «Архітектура системи»



ДОДАТОК Б

(обов’язковий)

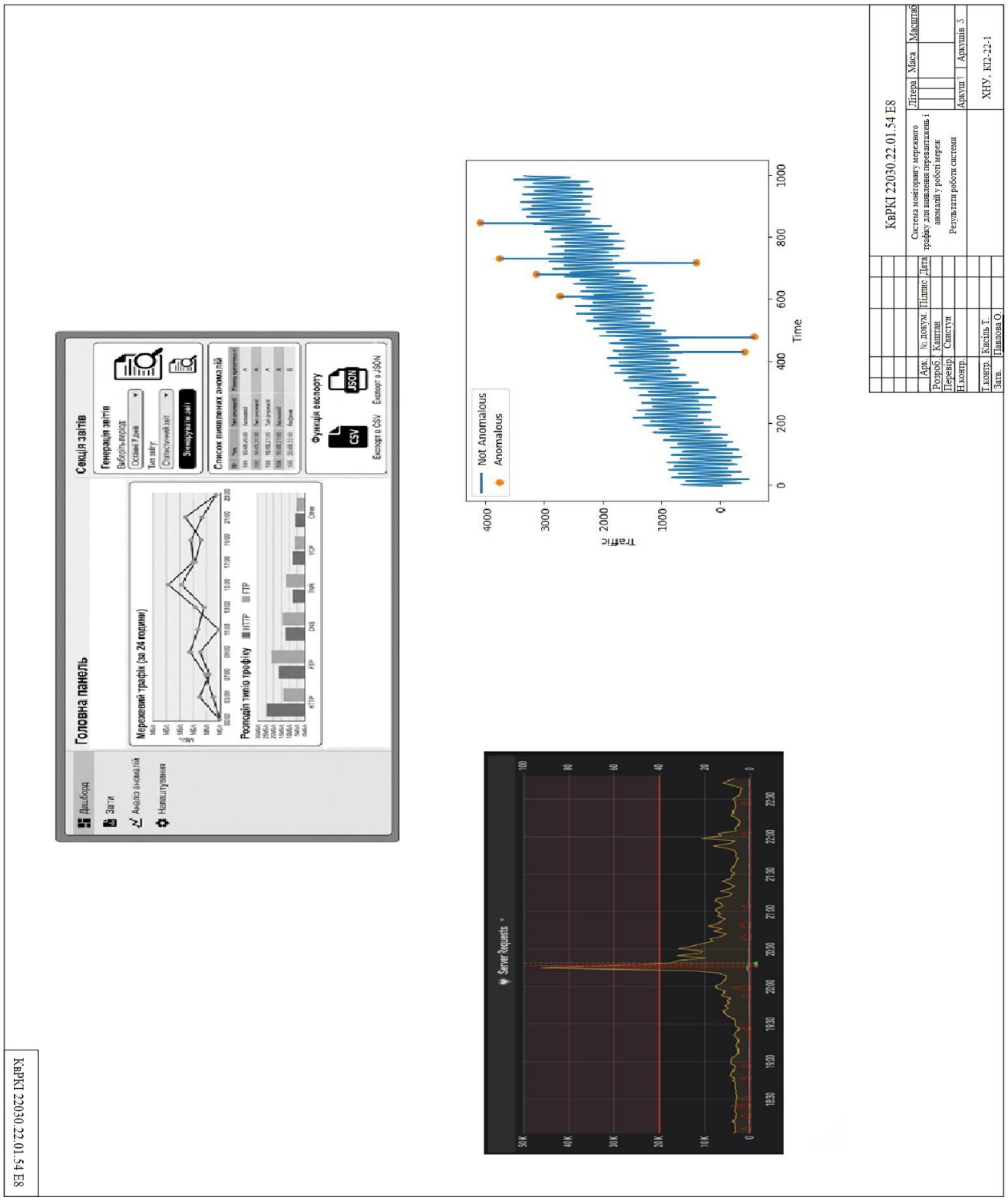
Копія креслення «Види систем моніторингу мережного трафіку»



ДОДАТОК В

(обов’язковий)

Копія креслення «Результати роботи системи»



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Каштан Владислав В'ячеславович

Тема: Система моніторингу мережного трафіку для виявлення перевантажень і аномалій у роботі мереж

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень 3 Кількість сторінок записки 79

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи виявлення перевантажень та аномалій у роботі мереж шляхом розробка системи моніторингу мережного трафіку.

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У межах розділу 1 було проведено комплексний аналіз предметної області моніторингу мережного трафіку. Розглянуто сучасний стан розвитку мережевих технологій, визначено основні тенденції їх розвитку, а також проаналізовано особливості функціонування сучасних комп'ютерних мереж. Особливу увагу було приділено проблемам перевантаження мережі та виникнення аномалій у мережному трафіку. Встановлено, що ці явища є одними з основних факторів, які негативно впливають на стабільність та ефективність роботи мережевих систем. Розглянуто основні причини їх виникнення, а також наслідки, до яких вони можуть призводити.

У межах розділу 2 було проведено детальний аналіз методів та засобів моніторингу мережного трафіку. Розглянуто основні підходи до організації моніторингу, зокрема пасивний, активний та потоковий, що дозволило визначити їх особливості, переваги та обмеження. Проаналізовано сучасні методи збору даних про мережний трафік, включаючи захоплення пакетів, використання потокових технологій та аналіз журналів мережевих пристроїв. Встановлено, що найбільш

ефективним є комбінований підхід, який забезпечує баланс між деталізацією інформації та навантаженням на систему.

У третьому розділі було розглянуто практичні аспекти реалізації системи моніторингу мережевого трафіку, призначеної для виявлення перевантажень і аномалій у роботі мережі. Основну увагу приділено розробці та впровадженню ключових компонентів системи, що забезпечують збір, обробку, аналіз, збереження та візуалізацію даних.

4. Позитивні сторони роботи: практична цінність роботи.

5. Негативні сторони роботи: недостатня увага приділена тестуванню системи на реальних даних.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на належному професійно-технічному рівні.

8. Інші зауваження: _____

9. Оцінка дипломної роботи: задовільно (70/D)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Підченко С.К. д.т.н., проф., завідувач каф. ТМІТ

"15" 06 2026 р. _____ (підпис)

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Владислав КАШТАН

Співавтор:

Назва: Система моніторингу мережного трафіку для виявлення перевантажень і аномалій у роботі мереж

Експерт: Сергій СВИСТУН

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:2.64%

Коефіцієнт подібності 2:0.38%

Мікропробіли: 3

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2026-06-14 10:55:15.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

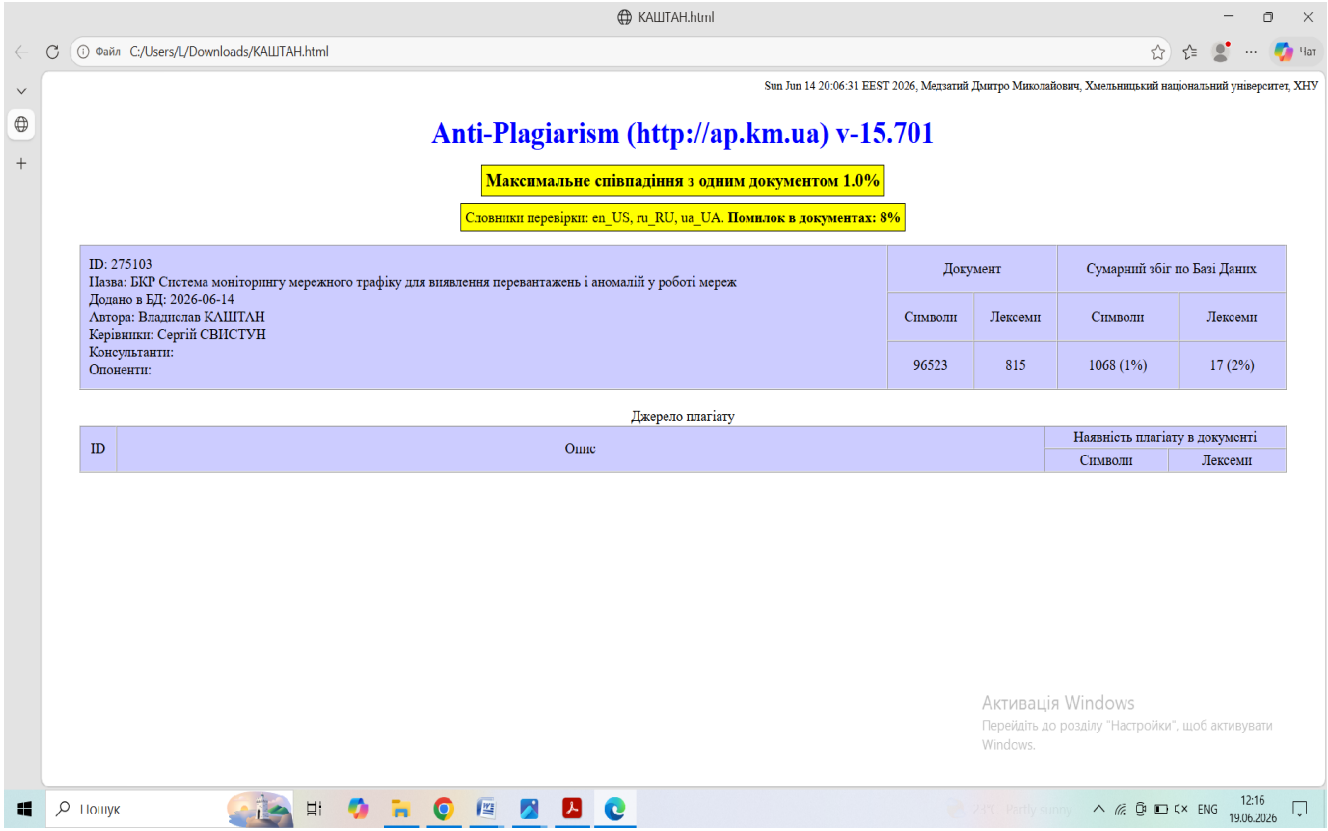
☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2026-06-14 Доцент Андрій Нічепорук

Дата експерт


КАШТАН.html
Файл C:/Users/L/Downloads/КАШТАН.html
Чат
Sun Jun 14 20:06:31 EEST 2026, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ
Anti-Plagiarism (http://ap.km.ua) v-15.701
Максимальне співпадіння з одним документом 1.0%
Словники перевірки: en_US, ru_RU, ua_UA. Помилок в документах: 8%
ID: 275103
Назва: БКР Система моніторингу мережного трафіку для виявлення перевантажень і аномалій у роботі мереж
Додано в БД: 2026-06-14
Автора: Владислав КАШТАН
Керівники: Сергій СВИСТУН
Консультанти:
Опоненти:
Документ
Символи
Лексеми
96523
815
Сумарний збіг по Базі Даних
Символи
Лексеми
1068 (1%)
17 (2%)
Джерело плагіату
ID
Опис
Наявність плагіату в документі
Символи
Лексеми
Активація Windows
Перейдіть до розділу "Настройки", щоб активувати Windows.
Пошук
ENG
12:16
19.06.2026

Зав. кафедри КІС
д-р. філософії Ользі ПАВЛОВІЙ

Владислав КАШТАН
ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ2-22-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений (а). Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а). Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

1 травня 2026 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи Система моніторингу мережного трафіку для виявлення перевантажень і аномалій у роботі мереж
Автор Владислав КАШТАН
Освітня програма Комп'ютерна інженерія та програмування
Рівень вищої освіти перший (бакалаврський)
Спеціальність 123 Комп'ютерна інженерія
Науковий керівник: доктор філософії Сергій СВИСТУН

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту.	відповідає
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована.	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат.	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;

2) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;

3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

4) значна частина знайденого плагіату відноситься до списку використаних джерел

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 2,64%; та системою Anti-Plagiarism складає 1%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

01.06.2026

Завідувач кафедри — Підпис — Ольга ПАВЛОВА (Ім'я, ПРІЗВИЩЕ)

Гарант освітньої програми — Підпис — Андрій НІЧЕПОРУК (Ім'я, ПРІЗВИЩЕ)

Керівник кваліфікаційної роботи — Підпис — Сергій СВИСТУН (Ім'я, ПРІЗВИЩЕ)