Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

Магістр
(назва освітнього ступеня)

на тему: Оптимізація та контроль ефективності функціонування локальної комп'ютерної мережі із застосуванням інтелектуальних методів аналізу трафіку

Виконав: студент(ка) 6 курсу, групи СІм-62
спеціальності 123 «Комп'ютерна інженерія»
(шифр і назва спеціальності)

(підпис) Семанюк В.М (прізвище та ініціали)

Керівник (підпис) Тиш Є.В (прізвище та ініціали)

Нормоконтроль (підпис) Луцик Н.С (прізвище та ініціали)

Завідувач кафедри (підпис) Осухівська Г.М. (прізвище та ініціали)

Рецензент (підпис) Деркач М.В (прізвище та ініціали)

Тернопіль
2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ *Осухівська Г.М.*
(підпис) (прізвище та ініціали)
«17» листопада 2025 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *магістр*
(назва освітнього ступеня)

за спеціальністю *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

студенту *Семанюк Василь Михайлович*
(прізвище, ім'я, по батькові)

1. Тема роботи *Оптимізація та контроль ефективності функціонування локальної комп'ютерної мережі із застосуванням інтелектуальних методів аналізу трафіку*

Керівник роботи *кандидат технічних наук, доцент кафедри КС, Тиш Євгенія Володимирівна*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « *14* » *листопада 2025* року № 4/7-987

2. Термін подання студентом завершеної роботи *16 грудня 2025 р.*

3. Вихідні дані до роботи *принципи формування мережевого трафіку в локальних комп'ютерних мережах, методи та засоби його моніторингу, а також інтелектуальні методи аналізу даних для виявлення аномалій і оптимізації роботи мережі.*

4. Зміст роботи (перелік питань, які потрібно розробити)

Вступ
1 Аналітичний огляд сучасних підходів до оптимізації та моніторингу локальних мереж
2 Теоретичні основи оптимізації мережі та інтелектуального аналізу трафіку
3 Розроблення та дослідження моделі інтелектуального аналізу трафіку для оптимізації ЛКМ
4 Охорона праці та безпека в надзвичайних ситуаціях
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

1. Актуальність і мета дослідження.
2. Завдання, об'єкт і предмет, наукова новизна і практична цінність дослідження.
3. Методи та інструменти моніторингу локальної комп'ютерної мережі.
4. Архітектура системи моніторингу та організація експериментального стенду.
5. Логіка вибору інтелектуального методу оптимізації локальної комп'ютерної мережі.
6. Блок-схема адаптивної інтелектуальної оптимізації локальної комп'ютерної мережі.
7. Результати експериментальних досліджень та їх аналіз.
8. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	*Осухівська Г.М., зав.каф. КС*	*04.12.2025*	
Безпека в надзвичайних ситуаціях	*Стручок В.С., ст. викладач каф. ОХ*	*05.12.2025*	

7. Дата видачі завдання *17.11.2025р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	*Огляд літературних джерел. Постановка завдання на кваліфікаційну роботу.*	*17.11.2025р. – 23.11.2025р.*	*Викон.*
2.	*Формування теоретичних основ для побудови інтелектуальної системи оптимізації локальної комп'ютерної мережі.*	*24.11.2025р. – 02.12.2025р.*	*Викон.*
3.	*Розроблення та дослідження моделі інтелктуального аналізу трафіку*	*03.12.2025р. – 10.12.2025р.*	*Викон.*
4.	*Охорона праці та безпека в надзвичайних ситуаціях*	*04.12.2025р. – 10.12.2025р.*	*Викон.*
5.	*Оформлення пояснювальної записки і графічного матеріалу*	*11.12.2025р. – 19.12.2025р.*	*Викон.*
6.	*Попередній захист кваліфікаційної роботи магістра*	*16.12.2025р.*	*Викон.*
7.	*Захист кваліфікаційної роботи магістра*	*23.12.2025р.*	*Викон.*

Студент _____ *Семанюк В.М*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Тиш Є.В*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Семанюк В.М. Методи оптимізації та контролю ефективності функціонування локальної комп’ютерної мережі із застосуванням інтелектуальних методів аналізу трафіку: робота на здобуття кваліфікаційного ступеня магістра: спец. 123 — комп’ютерна інженерія / наук.кер. Є. В. Тиш. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2025.

Ключові слова: локальна комп’ютерна мережа, оптимізація мережі, аналіз трафіку, машинне навчання, інтелектуальні системи, моніторинг, ефективність.

У роботі розглянуто сучасні підходи до оптимізації та контролю ефективності локальних комп’ютерних мереж із використанням інтелектуальних методів аналізу мережевого трафіку. Проведено аналітичний огляд методів моніторингу, оцінювання продуктивності та виявлення аномалій у трафіку. Розроблено модель аналізу трафіку на основі методів машинного навчання та виконано її практичну реалізацію. Наведено результати експериментальних досліджень, які підтверджують підвищення точності виявлення аномалій та оптимізацію роботи мережі порівняно з традиційними підходами. Сформульовано рекомендації щодо впровадження інтелектуальних методів аналізу трафіку в інфраструктуру локальних комп’ютерних мереж.

ANNOTATION

Semaniuk V.M. Optimization and performance control of a local computer network using intelligent traffic-analysis methods. Master’s Graduation Thesis: speciality 123 — Computer engineering / supervisor Tysh Ie. Ternopil: Ternopil Ivan Puluj National Technical University, 2025.

Keywords: local computer network, network optimization, traffic analysis, machine learning, intelligent systems, monitoring, performance.

The thesis investigates modern approaches to optimizing and controlling the performance of local computer networks using intelligent traffic analysis techniques. An analytical review of network monitoring methods, performance assessment approaches, and anomaly detection techniques is provided. A traffic analysis model based on machine learning algorithms has been developed and practically implemented. Experimental results demonstrate improved accuracy of anomaly detection and enhanced network performance compared to traditional methods. Recommendations for integrating intelligent traffic analysis solutions into local network infrastructures are proposed.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ

DPI (англ. Deep Packet Inspection) глибока інспекція пакетів (пакетний аналіз)

IPFIX (англ. Internet Protocol Flow Information Export) експорт інформації про потоки Інтернет-протоколу

ЛКМ локальна комп’ютерна мережа

LSTM (англ. Long Short-Term Memory) довготривала короткочасна пам'ять (тип нейронної мережі)

ML (англ. Machine Learning) машинне навчання (алгоритми)

NetFlow протокол обліку мережевого трафіку (статистика потоків)

PCAP (англ. Packet Capture) захоплення пакетів

QoS (англ. Quality of Service) якість обслуговування

RNN (англ. Recurrent Neural Network) рекурентна нейронна мережа

SNMP (англ. Simple Network Management Protocol) простий протокол керування мережею

SPAN (англ. Switched Port Analyzer) аналізатор комутованого порту

VLAN (англ. Virtual Local Area Network) віртуальна локальна мережа

ВСТУП

Актуальність роботи. Сучасні локальні комп’ютерні мережі функціонують в умовах постійного зростання обсягів передавання даних, ускладнення структури мережевого трафіку та підвищених вимог до надійності, продуктивності й безпеки. Забезпечення стабільної роботи мережевих сервісів, мінімальних затримок та ефективного використання ресурсів є критично важливим для організацій різного масштабу. Водночас традиційні методи моніторингу та аналізу трафіку не завжди здатні своєчасно реагувати на динамічні зміни мережевого середовища та виявляти приховані аномалії. У зв’язку з цим актуальним є застосування інтелектуальних методів аналізу трафіку, які дозволяють підвищити ефективність контролю та оптимізації функціонування локальних комп’ютерних мереж.

Метою кваліфікаційної роботи є підвищення ефективності функціонування локальної комп’ютерної мережі шляхом застосування інтелектуальних методів аналізу мережевого трафіку та розроблення підходів до оптимізації її роботи.

Завдання кваліфікаційної роботи:

- провести аналітичний огляд сучасних методів моніторингу та оптимізації локальних комп’ютерних мереж;
- дослідити інтелектуальні методи аналізу мережевого трафіку та оцінити їх придатність для підвищення ефективності роботи локальних комп’ютерних мереж;
- розробити модель або алгоритм аналізу трафіку на основі методів машинного навчання;
- реалізувати експериментальну систему або програмний модуль аналізу трафіку;
- провести експериментальне дослідження ефективності запропонованого підходу та порівняти отримані результати з традиційними методами;
- сформулювати практичні рекомендації щодо впровадження інтелектуальних методів оптимізації в локальних комп’ютерних мережах.

Відповідно до поставленої мети та сформульованих завдань визначено об’єкт і предмет дослідження.

Об'єкт дослідження: процеси функціонування локальної комп'ютерної мережі.

Предмет дослідження: методи оптимізації та контролю ефективності функціонування локальної комп'ютерної мережі із застосуванням інтелектуальних методів аналізу мережевого трафіку.

Методи дослідження: У роботі використано методи математичного моделювання комп'ютерних мереж, статистичний та кореляційний аналіз мережевого трафіку, алгоритми машинного навчання для класифікації, кластеризації та виявлення аномалій, а також методи експериментальних досліджень, структурного аналізу та системного підходу для оцінювання ефективності функціонування локальних комп'ютерних мереж.

Наукова новизна дослідження полягає в удосконаленні підходів до аналізу та контролю мережевого трафіку шляхом застосування інтелектуальних методів, що дозволяє підвищити точність виявлення аномалій, оптимізувати використання мережевих ресурсів і підвищити рівень автоматизації управління локальною комп'ютерною мережею.

Практичне значення результатів кваліфікаційної роботи полягає у можливості використання розробленої моделі та програмного модуля в системах моніторингу локальних мереж для своєчасного виявлення перевантажень, прогнозування мережевого трафіку та підвищення ефективності експлуатації мережевого обладнання в організаціях різного профілю.

Публікації. Результати дослідження апробовано у вигляді тез доповідей на науковій конференції «Актуальні задачі сучасних технологій», що відбулася в Тернопільському національному технічному університеті імені Івана Пулюя 11–12 грудня 2025 року [4,5].

Структура роботи. Кваліфікаційна робота складається з вступу, чотирьох розділів, висновків, списку використаних джерел та додатків [2]. Пояснювальна записка доповнена графічними матеріалами, що ілюструють основні результати дослідження.

РОЗДІЛ 1
АНАЛІТИЧНИЙ ОГЛЯД СУЧАСНИХ ПІДХОДІВ ДО ОПТИМІЗАЦІЇ ТА МОНІТОРИНГУ ЛОКАЛЬНИХ МЕРЕЖ

1.1. Архітектура та принципи функціонування ЛКМ

Локальні комп’ютерні мережі (ЛКМ) є фундаментальною складовою інформаційної інфраструктури сучасних організацій. Вони забезпечують обмін даними, доступ до інформаційних ресурсів, централізоване управління та підтримку цифрових сервісів, без яких неможливе ефективне функціонування програмних комплексів, систем телекомунікацій, хмарних рішень чи корпоративних платформ. У період стрімкого зростання обсягів даних та динамічного розвитку мережевих технологій роль локальних мереж істотно зростає, адже саме вони забезпечують передачу трафіку між численними пристроями та сервісами, підтримуючи стабільність і безперервність бізнес-процесів [3].

Функціонування локальних мереж базується на класичних моделях OSI та TCP/IP, які визначають логічну організацію процесу передавання даних. Кожен рівень виконує власну роль:

- фізичний відповідає за трансляцію електричних чи оптичних сигналів;
- канальний за формування кадрів і комутацію;
- мережевий за маршрутизацію пакетів;
- транспортний за керування з’єднаннями і надійністю передавання.

Така багаторівнева організація дозволяє структурувати мережеву взаємодію та забезпечує масштабованість і взаємодію обладнання різних виробників [3].

Архітектура ЛКМ включає комплекс апаратних та програмних компонентів, кожен з яких виконує власну функцію в процесі передавання даних. Центральне місце займають комутатори, що забезпечують комутацію на другому рівні та формують основу фізичного та логічного з’єднання вузлів. Маршрутизатори та комутатори третього рівня забезпечують взаємодію між сегментами мережі, здійснюючи маршрутизацію на основі IP-адресації. У свою чергу, точки доступу Wi-Fi створюють

бездротову інфраструктуру, яка доповнює дротову мережу та дозволяє підключати мобільні та IoT-пристрої. Сервери корпоративних служб, таких як DHCP, DNS чи Active Directory, забезпечують централізоване керування ресурсами та автоматизують обслуговування користувачів. Важливу роль відіграють і кінцеві пристрої робочі станції, IP-телефони, камери відеоспостереження, контролери доступу, які утворюють навантаження та генерують трафік.

Суттєвим елементом архітектури є фізична інфраструктура кабельні системи, комутаційні панелі, шафи та інші компоненти СКС. Саме від якості прокладання кабельних ліній, типів використовуваних матеріалів та структури комутацій залежить пропускна здатність каналів і стабільність передавання даних. Поширеним підходом є використання комбінованих рішень. Мідні канали для робочих станцій та оптоволокно для магістральних ділянок [8].

Топологічна організація локальної мережі також визначає її ефективність і масштабованість. Найбільш поширеною є топологія «зірки», у якій усі пристрої підключаються до центрального комутатора. Для великих корпоративних мереж застосовують ієрархічну трьохрівневу архітектуру Core–Distribution–Access, що забезпечує рівномірний розподіл навантаження, спрощує модернізацію та підвищує відмовостійкість. Бездротові мережі часто реалізують у вигляді mesh-структур, що дозволяють пристроям автоматично формувати оптимальні маршрути, підвищуючи покриття та стійкість до збоїв [9].

Функціонування мережі визначається низкою принципів, які забезпечують її надійність та ефективність. Одним із ключових є механізм адресації й маршрутизації, що дозволяє пакетам даних знаходити шлях між вузлами. Сегментація мережі, яка реалізується за допомогою VLAN чи списків контролю доступу, зменшує широкомовний трафік, підвищує безпеку та забезпечує логічний поділ інфраструктури. Якість обслуговування (QoS) дозволяє керувати пріоритетами трафіку та оптимізувати роботу критично важливих сервісів, таких як VoIP чи відеоконференції. Значну роль відіграють і механізми відмовостійкості та резервування, серед яких STP, LACP або VRRP, які забезпечують безперервність роботи у випадку збою обладнання або каналу зв’язку [8].

Безпека є невід'ємною складовою архітектури ЛКМ. Для захисту мережевої інфраструктури застосовують фільтрацію трафіку, механізми Port Security, 802.1X-автентифікацію, системи виявлення та запобігання вторгненням, а також моніторинг ARP-та DHCP-аномалій. Комплекс цих засобів дозволяє мінімізувати ризики, пов’язані з несанкціонованим доступом, шкідливим трафіком та внутрішніми загрозами [12].

Нарешті, важливою частиною архітектури є системи моніторингу, які забезпечують контроль за станом обладнання та трафіку. Сучасні рішення не лише відстежують навантаження чи доступність пристроїв, а й дозволяють аналізувати структуру трафіку, виявляти аномалії та прогнозувати пікові навантаження [9].

З розвитком корпоративних мереж відбувається поступовий перехід від традиційної статичної архітектури до гнучкіших технологій, таких як SDN, Zero-Trust чи Intent-Based Networking. Вони дозволяють централізовано керувати політиками, автоматизувати конфігурацію та інтегрувати інтелектуальні системи аналізу даних, що є важливим для подальшої оптимізації та підвищення ефективності роботи локальних мереж [18].

1.2. Показники ефективності функціонування локальної мережі

Ефективність функціонування локальної комп’ютерної мережі визначається здатністю забезпечувати стабільне, безперервне та прогнозоване передавання даних між її вузлами. У сучасних умовах, коли обсяги інформаційних потоків постійно зростають, а вимоги до швидкодії мережевої інфраструктури стають дедалі вищими, особливого значення набуває комплексна оцінка її продуктивності. Показники ефективності дають змогу не лише розуміти поточний стан мережі, але й прогнозувати її поведінку в умовах підвищеного навантаження, виявляти «вузькі місця» та ухвалювати рішення щодо оптимізації чи модернізації обладнання [15].

Одним із ключових параметрів є пропускна здатність, яка відображає максимальний обсяг даних, що може бути переданий каналом зв’язку за одиницю часу. Однак цей показник не завжди характеризує реальну продуктивність мережі,

оскільки фактична швидкість передавання залежить від численних факторів: протокольних накладних витрат, стану фізичного середовища, параметрів комутації та кількості активних користувачів. Тому для практичного аналізу використовують показник throughput реальну швидкість передавання даних за певних умов, яка зазвичай є нижчою за теоретичну пропускну здатність [15].

Ще одним важливим параметром, що впливає на якість роботи мережі, є затримка часу, який потрібний для передавання пакета від джерела до одержувача. У критичних застосунках, якості мережевих сервісів реального часу.

До переліку ключових показників ефективності також належать втрати пакетів, які виникають через перевантаження комутаційних вузлів, несправності обладнання або некоректну роботу мережевих протоколів. Невеликі відсотки втрат можуть бути непомітними для звичайних користувачів. Проте в системах, що працюють у реальному часі під час передавання великих обсягів даних вони спричиняють повторні передавання пакетів, зниження пропускної здатності та суттєве погіршення якості сервісу [23].

Важливу роль у визначенні ефективності відіграє рівень завантаження мережевих інтерфейсів. Комутатори та маршрутизатори мають певні апаратні обмеження на швидкість оброблення пакетів. У тому числі перевищення цих параметрів спричиняє виникнення черг, збільшення затримок, втрат і зниження пропускної здатності. Аналіз завантаження інтерфейсів дозволяє своєчасно виявляти тенденції перевантаження та приймати рішення щодо оптимізації або модернізації інфраструктури.

Також не менш значущим є показник доступності мережі. Його оцінюють у відсотках часу, протягом якого мережа або окремі її компоненти перебувають у працездатному стані. Для корпоративних інфраструктур критично важливим вважається рівень доступності 99,5–99,99 %, що передбачає мінімальний час простою. Показник доступності значною мірою залежить від якості апаратного забезпечення, конфігурації резервування, стабільності джерел живлення, а також від ефективності мережевих політик та інструментів моніторингу [19].

Комплексна оцінка ефективності передбачає аналіз усіх зазначених характеристик у взаємозв’язку, оскільки кожна з них окремо не дає повної картини. Наприклад, висока пропускна здатність не гарантує стабільного передавання даних за умов значного джиттера чи затримки, а низький рівень втрат може маскувати сильні коливання затримки або перевантаження інтерфейсів. Тому сучасні системи моніторингу об’єднують дані з різних джерел SNMP, NetFlow, логів сервісів, телеметрії пристроїв і використовують інтегровані метрики для аналізу стану мережі [19].

Таким чином, показники ефективності локальної мережі формують основу для подальшого аналізу продуктивності та оптимізації. Вони дозволяють своєчасно визначити ресурси, які працюють на межі можливостей, виявити проблемні ділянки та підготувати мережу до зростання навантажень. У контексті даної роботи ці показники є критично важливими, оскільки саме на їх основі здійснюється подальший інтелектуальний аналіз трафіку та оцінювання результативності застосованих методів оптимізації.

1.3. Методи моніторингу та контролю стану комп’ютерних мереж

Ефективне функціонування локальної комп’ютерної мережі неможливе без постійного моніторингу її стану, адже сучасні мережі характеризуються динамічністю навантажень, різноманітністю джерел трафіку та високими вимогами до безперебійності роботи. Моніторинг дозволяє своєчасно виявляти проблеми, пов’язані з перевантаженням, збоями обладнання, аномальною активністю чи зниженням продуктивності. Крім того, системи моніторингу відіграють важливу роль у забезпеченні безпеки, адже вони фіксують нетипову поведінку, що може свідчити про атаки або внутрішні порушення [3].

Історично контроль мережі починався з простого спостереження за роботою обладнання, проте з часом ці механізми перетворилися на багаторівневі системи збору та аналізу даних. Одним із найпоширеніших інструментів став протокол SNMP, який забезпечив стандартизований спосіб отримання інформації про стан мережевих

пристроїв. Через SNMP адміністратори отримують доступ до ключових показників завантаження інтерфейсів, кількості помилок, температури обладнання, обсягів переданого трафіку. Цей підхід став основою для перших систем централізованого моніторингу, таких як Zabbix або Nagios, які дозволили автоматизувати процес збору даних та реагування на події [24].

Проте SNMP має певні обмеження: він надає переважно статистичну інформацію про вузли але не містить детальних відомостей про структуру трафіку. Тому розвиток мережевих технологій сприяв появі інструментів потокового аналізу, таких як NetFlow, sFlow чи IPFIX. Ці методи дозволяють не просто фіксувати стан інтерфейсів, а відстежувати кожен мережевий потік: джерело, призначення, протокол, порт, обсяг переданих даних, тривалість сесії. Потоковий моніторинг суттєво розширив можливості контролю, оскільки надав інформацію про реальне завантаження мережі та структуру трафіку, дозволив виявляти аномалії поведінки пристроїв, надмірну активність окремих користувачів чи підозріле використання портів [24].

Ще більш детальний рівень контролю забезпечує пакетний аналіз (Deep Packet Inspection), який дозволяє переглядати структуру кожного мережевого пакета, аналізувати протоколи застосунків і за необхідності, виявляти вторгнення або шкідливу активність. Інструменти на кшталт Wireshark, Zeek або Suricata можуть не лише фіксувати події але й будувати детальні сесійні журнали, які відображають взаємодію між вузлами. Перевагою цього підходу є можливість глибокої діагностики проблем і виявлення складних аномалій, тоді як його недоліком є значне навантаження на систему та ризик генерації великих обсягів даних [15].

З розвитком мережевих технологій компанії почали впроваджувати телеметрію сучасний підхід до збору даних, який передбачає безперервне передавання інформації про стан пристроїв з мінімальною затримкою. На відміну від SNMP, який працює за принципом опитування, телеметрія надсилає дані у режимі реального часу, що дозволяє отримувати значно точнішу й оперативнішу інформацію про зміни у мережі. Телеметрія особливо актуальна в умовах зростання швидкостей та складності

інфраструктури, адже дозволяє своєчасно реагувати на критичні зміни, мінімізувати затримки та покращувати загальну стабільність роботи.

Сучасні системи моніторингу поєднують кілька методів збору даних [24]. Наприклад, платформи Zabbix, Grafana або PRTG здатні одночасно використовувати такі протоколи та методи, як SNMP, NetFlow, пакетний аналіз і телеметрія, об’єднуючи ці дані у візуалізовані панелі стану мережі. Це дозволяє формувати комплексну картину продуктивності та оперативно виявляти проблеми, які можуть призвести до деградації роботи.

Також важливим напрямом моніторингу стало виявлення аномалій, що неможливо реалізувати лише статичними методами. Через це у мережеве адміністрування поступово інтегруються інтелектуальні підходи такі як кластеризація трафіку, машинне навчання, поведінкові моделі користувачів. На відміну від традиційних методів, які працюють на основі порогових значень, ці технології дають змогу визначати нетипові патерни поведінки, що можуть свідчити про технічні проблеми, так і про загрози безпеці [25].

Таким чином, сучасні методи моніторингу та контролю стану мережі еволюціонували від простого збору статистики до комплексних систем аналізу, здатних виявляти аномалії, оцінювати стан потоків трафіку та прогнозувати навантаження. Це робить моніторинг фундаментальною основою подальшого інтелектуального аналізу, що розглядається у наступних підрозділах і є ключовим елементом ефективного управління локальними комп’ютерними мережами.

1.4. Інструменти збору та аналізу мережевого трафіку

Аналіз мережевого трафіку є одним з ключових процесів забезпечення стабільності, ефективності та безпеки локальної комп’ютерної мережі [21]. Якщо методи моніторингу розглянуті у попередньому підрозділі здебільшого спрямовані на отримання загальної інформації про стан мережевих пристроїв та інтерфейсів, то інструменти збору трафіку забезпечують значно глибший рівень контролю. Вони дозволяють досліджувати структуру, об’єм, динаміку та поведінкові характеристики

інформаційних потоків, що є фундаментом для подальшої оптимізації мережі та застосування інтелектуальних методів аналізу.

З розвитком мережевих технологій інструменти збору трафіку еволюціонували від простих пакетних аналізаторів до комплексних систем, які здатні обробляти величезні обсяги даних у режимі реального часу. Вибір конкретного інструмента залежить від поставлених завдань: глибокий аналіз протоколів, виявлення аномалій, оцінювання навантаження, оптимізація роботи сервісів чи забезпечення мережевої безпеки. Саме тому сучасні адміністратори часто використовують не один, а кілька взаємодоповнюючих методів.

Одним із фундаментальних інструментів для аналізу трафіку є пакетні аналізатори одним з яких найвідомішим є Wireshark. Він дозволяє переглядати вміст окремих пакетів, аналізувати протоколи різних рівнів, структуру TCP-сесій, RTP-потоків чи службових повідомлень мережевих пристроїв. Пакетний аналіз є незамінним для діагностики складних мережевих помилок, тестування нових сервісів, детального аналізу продуктивності протоколів чи виявлення підозрілої активності. Попри свою універсальність Wireshark має певні обмеження, такі як значний обсяг даних, необхідність захоплення повних пакетів та високе навантаження на систему при тривалому записі [19].

Для вирішення проблем масштабованості та зменшення обсягу даних використовують системи потокового аналізу, такі як NetFlow, sFlow або IPFIX. На відміну від пакетних аналізаторів, вони не зберігають повний вміст пакетів, а формують агреговану статистику про мережеві потоки. Завдяки цьому адміністратор отримує інформацію про те, які вузли взаємодіють між собою, які сервіси генерують найбільше навантаження, які протоколи домінують у трафіку. Також може виявляти підозрілі потоки, що є характерними для бот-мереж, DDoS-атак або мережевих сканувань. Використання NetFlow стало стандартом у багатьох корпоративних мережах, оскільки цей метод дозволяє зберегти баланс між глибиною аналізу та продуктивністю системи збору даних [18].

Для більш високорівневого аналізу трафіку використовуються спеціалізовані системи, такі як Zeek (раніше Bro). На відміну від класичних IDS/IPS, Zeek не лише

фіксує сигнатури небезпечної активності, а й аналізує поведінкові характеристики трафіку. Він формується у вигляді структурованих журналів, що відображають взаємодію між клієнтами та серверами, HTTP-запити, DNS-резольвінг, SSL-сесії та іншу релевантну інформацію. Завдяки такій структурі Zeek є основою для побудови систем високорівневої аналітики, включно з алгоритмами машинного навчання, які можуть працювати з числовими та категоріальними ознаками трафіку.

Важливу нішу у сфері аналізу трафіку займають системи IDS/IPS, такі як Suricata. Цей інструмент здатний проводити як сигнатурний, так і поведінковий аналіз. Його особливість полягає у високій продуктивності, можливості обробляти багатопотоковий трафік та інтегруватися з потоковими колекторами або SIEM-платформами. Suricata використовується не тільки для виявлення атак, але й для формування розширених метаданих, які є важливою основою для інтелектуального аналізу та побудови прогнозних моделей.

У контексті великих мережевих інфраструктур особливе значення має агрегація, індексація та подальша візуалізація зібраних даних. Саме тут застосовуються рішення на основі Elasticsearch, Logstash та Kibana (ELK Stack) [17]. Вони дозволяють обробляти великі обсяги телеметричних даних, створювати інтерактивні панелі, аналізувати аномальні події та будувати аналітичні моделі. ELK став своєрідним стандартом у сфері зберігання мережевих логів і трафікових метаданих, оскільки забезпечує швидкий доступ до інформації та можливість масштабування у межах сотень чи тисяч вузлів.

Поступовий перехід індустрії мереж до концепцій реального часу стимулював розвиток телеметрії нового підходу, який дедалі активніше замінює традиційний SNMP. На відміну від опитувального методу, телеметрія надсилає дані про стан пристроїв у безперервному потоці. Це дозволяє отримувати значно точнішу інформацію, яка може бути використана для виявлення аномалій у режимі реального часу, прогнозування навантажень або адаптивної зміни мережевих політик.

Сучасні системи аналізу трафіку часто поєднують різні методи збору: пакетний, потоковий, телеметричний та поведінковий. Поєднання цих підходів дозволяє отримати багатовимірну картину роботи мережі та створити умови для застосування

інтелектуальних алгоритмів. Саме інтегроване використання різнорівневих даних стає основою для побудови систем оптимізації, які можуть динамічно адаптуватися до змін у структурі та обсягу трафіку.

Таким чином, інструменти збору та аналізу трафіку є ключовим елементом сучасного мережевого адміністрування. Вони забезпечують фундамент для прийняття рішень, підвищують ефективність роботи мережі, дозволяють виявляти та усувати несправності, а також створюють передумови для впровадження інтелектуальних систем оптимізації, які розглядаються у наступних розділах роботи.

1.5. Проблеми оптимізації та продуктивності сучасних ЛКМ

Постійне зростання обсягів передавання даних, поява ресурсомістких застосунків та збільшення кількості підключених пристроїв створюють нові виклики для локальних комп’ютерних мереж. Традиційні підходи до побудови й обслуговування мережевої інфраструктури вже не здатні повною мірою гарантувати стабільність, масштабованість та високу продуктивність у сучасних умовах. Це зумовлює необхідність перегляду існуючих підходів до оптимізації та розуміння проблем, що найбільшою мірою впливають на ефективність функціонування ЛКМ.

Однією з ключових проблем є нерівномірність розподілу навантаження між сегментами мережі. У корпоративних інфраструктурах часто спостерігається ситуація, коли частина комутаторів або каналів працює на межі своєї пропускної здатності, тоді як інші залишаються практично незавантаженими. Така диспропорція виникає як через особливості структурних підрозділів, так і через технічні чинники відсутність коректної сегментації, неефективні маршрути або неправильне застосування політик QoS. У результаті критично важливі сервіси можуть зазнавати затримок або збоїв, навіть якщо загальні ресурси мережі достатні [9].

Другою суттєвою проблемою є відсутність можливості оперативного визначення та прогнозування пікових станів. Більшість мереж формує навантаження нерівномірно у певні години, дні тижня або навіть у залежності від окремих процесів (резервне копіювання, оновлення систем, аналітичні запити). Якщо така поведінка не

аналізується системно, мережа працює у «реактивному режимі» адміністратор усуває проблеми лише після їх виникнення, що істотно знижує її доступність та призводить до невиправданих витрат часу і ресурсів.

Складність мережевої інфраструктури також сприяє появі проблем пов’язаних із маршрутизацією. Неправильно налаштовані таблиці маршрутів, використання статичних маршрутів у динамічних середовищах, застарілі протоколи або некоректні реалізації балансування навантаження можуть спричиняти неефективні шляхи передавання даних. Це проявляється у вигляді підвищених затримок, втрат пакетів або перевантаження окремих вузлів, які стають «вузькими місцями» інфраструктури.

Особливої уваги заслуговує зростання ролі бездротових технологій [15]. Масове впровадження Wi-Fi 5/6/6E, IoT-пристроїв та мобільних клієнтів створює навантаження, яке часто важко передбачити. Бездротові мережі надзвичайно чутливі до інтерференції, щільності користувачів, фізичних перешкод і зміни радіочастотного оточення. Як наслідок, навіть за наявності високошвидкісного доступу «по повітрю» реальна пропускна здатність та стабільність можуть істотно залежати від факторів, які складно контролювати традиційними методами.

До загальних проблем продуктивності додається й аспект інформаційної безпеки. Сучасні кібератаки дедалі частіше маскуються під звичайний трафік, використовують легітимні порти та протоколи, що ускладнює їх виявлення за допомогою простих механізмів. Аномальна активність, така як нетипові піки трафіку, сканування мережі або підозрілі взаємодії між вузлами, часто залишається непоміченою у традиційних системах моніторингу. Це не лише створює загрозу порушення конфіденційності чи цілісності даних але й впливає на продуктивність. =

Окремим чинником є апаратні обмеження та несумісність обладнання. У мережах, що розвивалися поступово часто зустрічається різнорідне обладнання, яке підтримує різні технології, протоколи та рівні продуктивності. Це ускладнює впровадження сучасних методів оптимізації та створює передумови для додаткових затримок або конфліктів. Наприклад, старі комутатори можуть не підтримувати сучасні функції QoS або телеметрії, а маршрутизатори працювати на межі апаратних можливостей при обробці великої кількості потоків.

Сьогодні мережі дедалі більше переходять до віртуалізованих та розподілених архітектур: SDN, хмарні сервіси, віддалені офіси, VPN-з’єднання. Це збільшує складність взаємодії між мережевими сегментами та висуває нові вимоги до контролю продуктивності. Статичні методи аналізу в таких умовах уже не є ефективними, оскільки вони не враховують динамічний характер з’єднань і зміну патернів трафіку [21].

Усі ці чинники створюють складну картину у якій традиційні засоби оптимізації такі як ручне налаштування маршрутизації, статичні правила QoS або періодичний аналіз логів уже не здатні забезпечити потрібну адаптивність. Мережі потребують інтелектуальних систем, що можуть динамічно аналізувати стан інфраструктури, виявляти закономірності, прогнозувати можливі порушення та автоматично пропонувати або реалізовувати коригувальні дії. Саме застосування інтелектуальних методів аналізу трафіку стає ключовим етапом переходу від реактивного до проактивного управління, що значно підвищує ефективність роботи локальних комп’ютерних мереж.

1.6. Висновки до розділу 1

У першому розділі проведено комплексний аналітичний огляд сучасних підходів до побудови та оптимізації локальних комп’ютерних мереж. Розглянуто їх архітектуру, принципи функціонування, ключові показники ефективності, а також методи моніторингу й аналізу мережевого трафіку. Встановлено, що стабільність і продуктивність локальної мережі безпосередньо залежать від коректної організації інфраструктури, ефективної сегментації, наявності механізмів відмовостійкості та застосування систем моніторингу, здатних обробляти значні обсяги даних у режимі, близькому до реального часу.

Окрему увагу приділено аналізу сучасних методів контролю трафіку від статистичних SNMP-механізмів до потокового аналізу (NetFlow, IPFIX), глибинної інспекції пакетів та телеметрії нового покоління. Показано, що кожен із підходів має власні переваги, проте лише їх поєднання забезпечує повноцінне уявлення про стан

мережі та створює передумови для застосування інтелектуальних алгоритмів кластеризації, виявлення аномалій і прогнозування навантаження [11].

У ході огляду визначено основні проблеми сучасних локальних мереж, зокрема нерівномірний розподіл трафіку, складність масштабування, обмежену точність традиційних методів моніторингу, труднощі виявлення пікових навантажень і вплив кіберзагроз, що маскуються під легітимний трафік. Узагальнення отриманих результатів свідчить, що ефективне управління локальними мережами в сучасних умовах потребує використання інтелектуальних методів аналізу трафіку, які забезпечують адаптивну оптимізацію роботи мережі та формують основу для подальших теоретичних досліджень, представлених у розділі 2.

РОЗДІЛ 2
ТЕОРЕТИЧНІ ОСНОВИ ОПТИМІЗАЦІЇ МЕРЕЖІ ТА ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ТРАФІКУ

2.1. Теоретичні основи оптимізації роботи комп’ютерних мереж

Оптимізація роботи комп’ютерних мереж базується на сукупності теоретичних моделей, які описують процеси передавання даних, структуру трафіку та закономірності взаємодії між вузлами мережевої інфраструктури. Зі зростанням обсягів трафіку і збільшенням кількості пристроїв, підключених до мережі, традиційні методи адміністрування стають недостатніми, що підвищує важливість глибокого теоретичного аналізу. Саме тому оптимізація передбачає не лише поліпшення технічних параметрів пристроїв, а й використання математичних, статистичних та інтелектуальних моделей, які дозволяють прогнозувати навантаження і визначати оптимальні режими роботи мережі [10].

У класичному підході комп’ютерна мережа розглядається як система масового обслуговування (рис 2.1), де мережеві вузли виконують роль обслуговуючих пристроїв, а пакети роль заявок, що надходять до них з певною інтенсивністю. Такий підхід дає змогу оцінити середній час очікування, пропускну здатність та ймовірність перевантаження пристроїв.

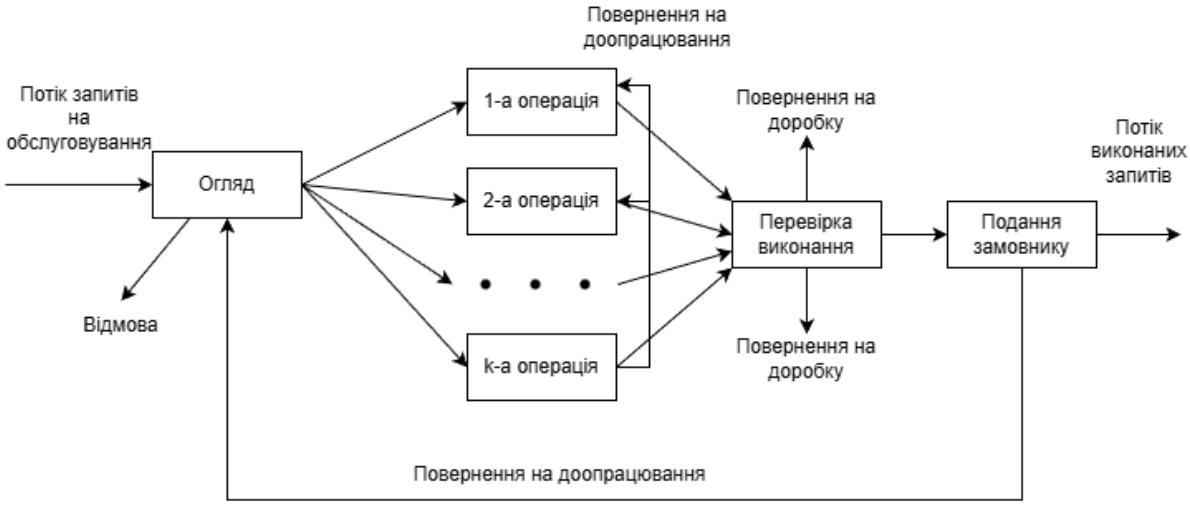

Рис. 2.1. Модель мережевого вузла як системи масового обслуговування

Застосування моделей масового обслуговування дозволяє визначити такі ключові параметри, як інтенсивність потоку λ, швидкість обслуговування μ та коефіцієнт завантаження ρ. Саме величина ρ визначає, наскільки близько система перебуває до режиму перевантаження. Коли ρ наближається до 1, навіть незначне зростання трафіку може спричинити різке збільшення затримки та довжини черг, що негативно впливає на продуктивність мережі [14].

Структура трафіку в реальних мережах має нерівномірний характер, що пов’язано з поведінкою користувачів, бізнес-процесами та особливостями роботи сервісів. Аналіз часових рядів дозволяє описати цю динаміку, оскільки мережеві навантаження часто мають повторювані добові, тижневі або сезонні закономірності.

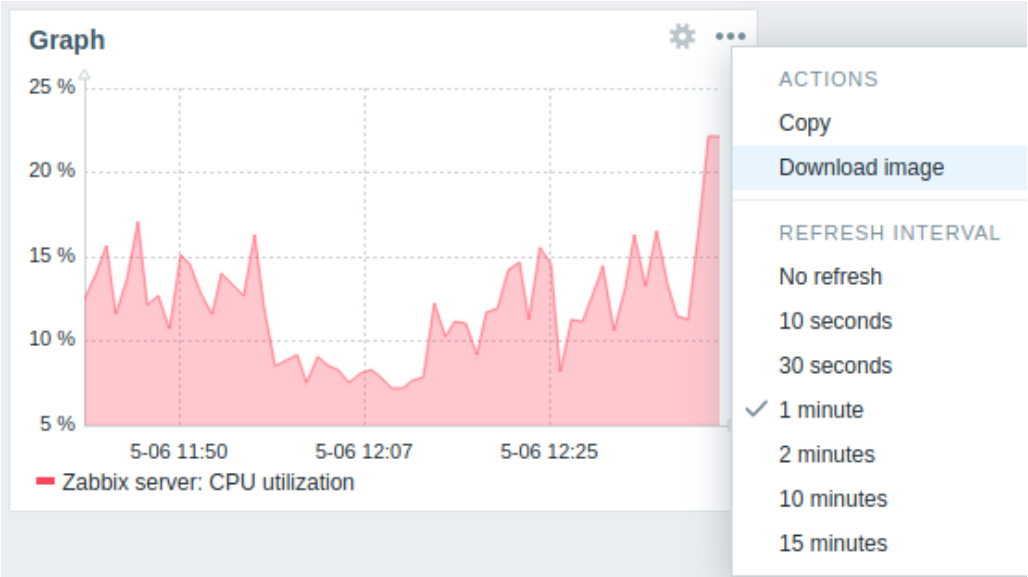

Рис. 2.2 Графік добового навантаження мережевого інтерфейсу

Такі графіки (рис.2.2) дозволяють визначити періоди у які мережа потребує додаткових ресурсів або навпаки моменти, коли її завантаження є мінімальним. Це є базою для подальшого планування пропускної здатності та впровадження адаптивних механізмів розподілу трафіку. Окрім аналізу часових рядів застосовуються й статистичні методи, які дозволяють виявляти тенденції, сплески навантаження або нетипову активність, що може свідчити як про технічні проблеми, так і про можливі загрози безпеці.

Класичні методи оптимізації зосереджені на вдосконаленні маршрутизації, балансуванні навантаження, сегментації мережі та забезпеченні якості обслуговування (QoS). Вони спрямовані на раціональне використання ресурсів і попередження перевантажень у критичних сегментах. Ці підходи ефективні у стабільних і передбачуваних мережах, однак зі зростанням складності інфраструктури їх ефективність зменшується. Сучасні мережеві системи потребують адаптивних рішень здатних реагувати на зміни у реальному часі [11].

У цьому контексті важливого значення набувають інтелектуальні методи оптимізації, що ґрунтуються на принципах машинного навчання та аналізу великих даних. Вони дозволяють автоматично виявляти закономірності у трафіку, класифікувати потоки, визначати аномальну активність та прогнозувати можливі перевантаження.

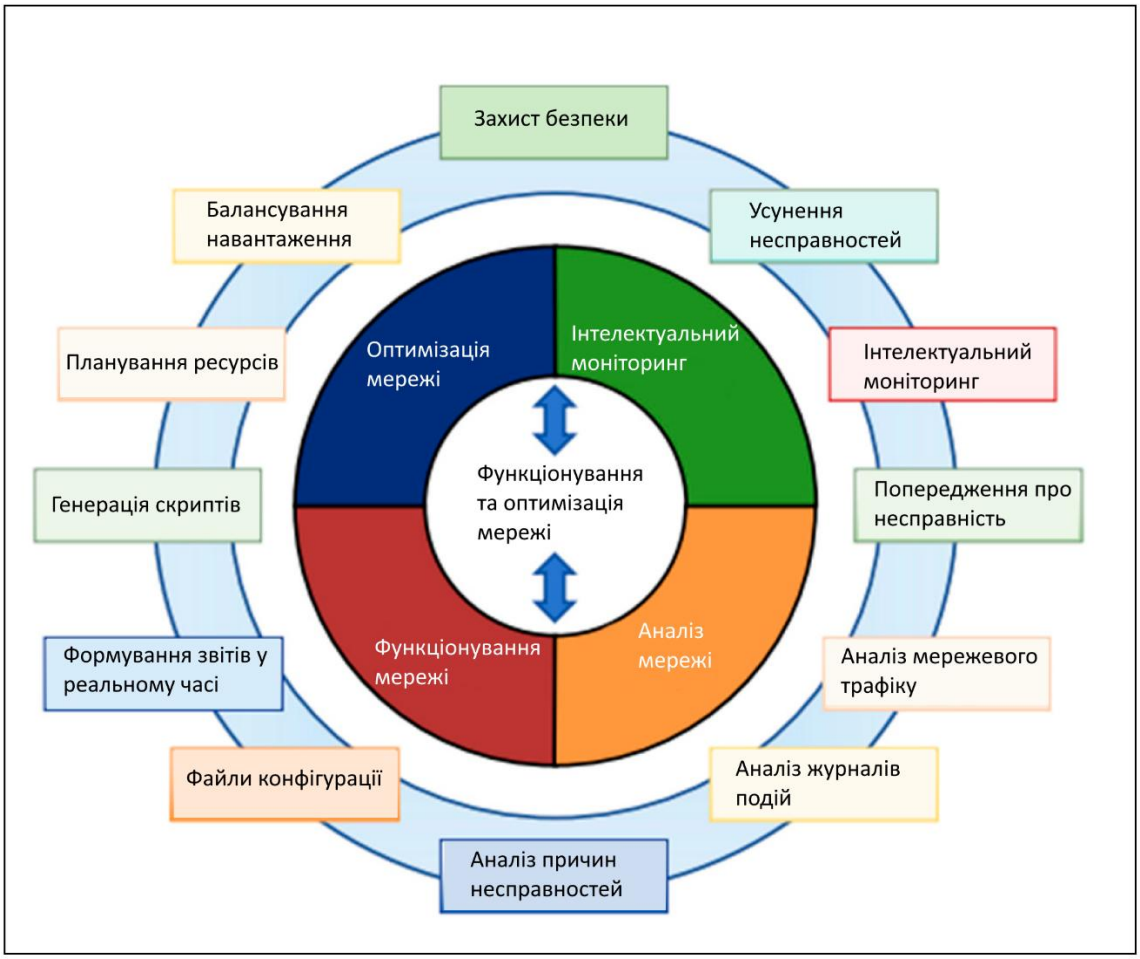

Рис. 2.3 Узагальнена модель інтелектуальної системи оптимізації роботи мережі

Завдяки таким моделям (рис.2.3) стає можливим прогнозування стану мережі та автоматичне виявлення нетипових режимів роботи. На відміну від традиційних підходів, інтелектуальні методи здатні працювати з великими обсягами потокових даних, здійснювати аналіз у реальному часі та зменшувати вплив людського фактора під час прийняття рішень [15].

Узагальнюючи теоретичні основи оптимізації роботи комп'ютерних мереж охоплюють класичні математичні моделі, статистичний аналіз трафіку та сучасні інтелектуальні підходи. Лише їхнє комплексне застосування дозволяє створити стійку до навантажень, ефективну й адаптивну інфраструктуру, здатну забезпечувати високу якість мережевих сервісів у динамічних умовах.

2.2. Інтелектуальні методи аналізу трафіку

Зі зростанням складності комп'ютерних мереж традиційні методи аналізу трафіку такі як ручне опитування пристроїв, статистичний аналіз окремих інтерфейсів або пакетна інспекція поступово перестають забезпечувати необхідний рівень точності та адаптивності. Сучасні мережеві системи формують великі обсяги потокових даних, що характеризуються нерівномірністю, високою варіабельністю та залежністю від контексту роботи користувачів і сервісів. У таких умовах оптимізація мережі неможлива без застосування інтелектуальних методів аналізу, які здатні виявляти приховані закономірності, прогнозувати зміни навантаження та визначати аномальні ситуації у режимі, наближеному до реального часу [10].

На відміну від класичних підходів, інтелектуальні методи аналізу трафіку ґрунтуються на машинному навчанні, статистичних моделях високої складності та алгоритмах пошуку аномалій. Вони дозволяють працювати з великими масивами даних, враховувати багатовимірність потоків і використовувати контекстну інформацію, що недоступна стандартним інструментам. Загальний принцип функціонування таких систем передбачає збір телеметрії, попередню обробку даних, формування ознак, побудову моделей і подальше ухвалення рішень.

Основу роботи інтелектуальних методів становлять алгоритми машинного навчання, які дозволяють розпізнавати типи трафіку, визначати аномальні патерни та прогнозувати поведінку мережі. Найчастіше застосовуються методи класифікації, що дозволяють розмежувати легітимні та підозрілі потоки. Такі моделі навчаються на великій кількості прикладів, що дає змогу виявляти приховані залежності між параметрами трафіку, які не можуть бути помічені класичними методами. Зокрема, дерева рішень та випадкові ліси ефективні у випадках, коли потрібно визначити, які атрибути пакета або потоку найбільше впливають на віднесення його до тієї чи іншої категорії [10].

Окремий напрямок становлять методи кластеризації, які не потребують попередньої розмітки даних. Вони дозволяють групувати трафік на основі схожості характеристик, виявляючи при цьому аномальні групи, що можуть бути пов’язані з нетиповою активністю користувачів або з підозрілими взаємодіями у мережі. Такі методи особливо корисні в умовах, коли структура трафіку змінюється динамічно, а створення чіткої фіксованої моделі є неможливим. Наприклад, алгоритми k-means або DBSCAN дозволяють визначити кластери нормального трафіку й виділити окремі відхилення, що потребують подальшого аналізу.

Для виявлення складних атак, повільних аномалій або поведінкових відхилень широко застосовуються нейронні мережі. Вони забезпечують здатність до апроксимації нелінійних залежностей і можуть працювати з багатовимірними ознаками, включаючи часові параметри, інтенсивність потоків, типи протоколів та інші характеристики. Рекурентні нейронні мережі (RNN) та довготривала пам’ять (LSTM) особливо ефективні при аналізі часових рядів трафіку, оскільки здатні враховувати його еволюцію та прогнозувати майбутні стани. Саме такі моделі використовуються для прогнозування піків навантаження або виявлення повільних DDoS-атак, які непомітні короткочасними вимірюваннями [11].

Важливою частиною інтелектуального аналізу трафіку є виявлення аномалій. На відміну від підходів з використанням порогових значень, інтелектуальні методи здатні враховувати поведінковий контекст мережі. Аномалія визначається не тільки за абсолютними значеннями параметрів але й за їхньою відповідністю типовим

патернам поведінки. Це дозволяє фіксувати як раптові сплески активності так і поступові відхилення, які можуть свідчити про появу нових типів атак або неефективність у функціонуванні певних сегментів. Типові приклади аномалій трафіку різке збільшення кількості SYN-запитів, нетипові з’єднання між сегментами або повільне накопичення неприродного обсягу трафіку добре відображаються у поведінкових моделях, сформованих машинним навчанням [11].

Не менш важливим аспектом є процес формування ознак, який визначає, які саме параметри потоку будуть використані моделлю машинного навчання. Найчастіше до таких ознак належать розмір пакета, тривалість сеансу, кількість переданих байтів, інтервал між пакетами, частота звернень до певних портів, різноманіття використаних протоколів та інші характеристики. Правильно підібрані ознаки визначають ефективність навчання моделі та її здатність розрізняти типи трафіку. Системи потокової аналітики, такі як NetFlow/IPFIX [18], забезпечують базовий набір параметрів, який може бути використаний для формування цих ознак.

Узагальнюючи, інтелектуальні методи аналізу трафіку дозволяють побудувати адаптивні системи, які не тільки визначають поточний стан мережі, а й прогнозують майбутні зміни, формуючи основу для проактивної оптимізації. Використання таких методів у поєднанні зі збором телеметрії та потокових даних дозволяє суттєво підвищити стабільність роботи мережі, забезпечити її безпеку та мінімізувати вплив людського фактора на прийняття рішень.

2.3. Методи машинного навчання для класифікації та виявлення аномалій

Сучасні комп’ютерні мережі генерують величезні потоки трафіку, структура якого характеризується нелінійністю з високою варіабельністю та наявністю прихованих закономірностей. Статичні методи аналізу дедалі частіше виявляються недостатніми для своєчасного виявлення загроз, перевантажень або нетипової поведінки мережевих вузлів. Саме тому методи машинного навчання стали одним з ключових інструментів аналізу трафіку, оскільки дозволяють автоматично

класифікувати пакети або потоки, визначати аномальні відхилення та прогнозувати зміни у навантаженні.

Інтелектуальні алгоритми опрацьовують багатомірні набори характеристик трафіку таких як розмір пакета, інтервал між передаванням, кількість байтів у потоці, частота звернень до певних портів, типи протоколів та інші ознаки. Застосування машинного навчання дає змогу не лише аналізувати окремі параметри, а й визначати складні зв'язки між ними, що забезпечує значно вищу точність класифікації ніж традиційні фільтри або сигнатурні методи. Узагальнена архітектура (рис. 2.4) системи машинного навчання для класифікації трафіку відображає послідовність етапів від збору даних до прийняття рішень [21].

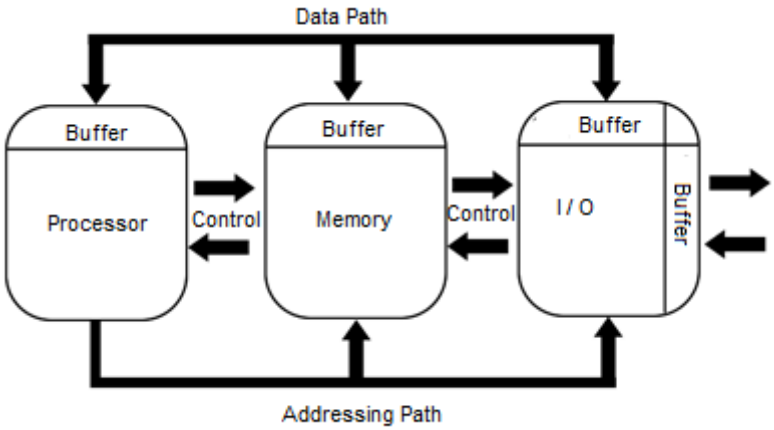

Рис. 2.4 Архітектура інтелектуальної системи аналізу трафіку

Класифікаційні алгоритми машинного навчання виконують важливу роль у мережевих системах, оскільки дозволяють розділяти трафік за протоколами, типами сервісів або рівнем ризику. Для цих завдань найчастіше застосовуються дерева рішень, випадкові ліси, опорні вектори (SVM) та градієнтний бустинг. Їхня перевага полягає у здатності функціонувати зі змішаними типами ознак та враховувати багатофакторні залежності. Завдяки цьому класифікатори можуть точно визначити, чи належить потік до нормального робочого трафіку, чи містить потенційні ознаки сканування портів, DDoS-активності або мережевого вторгнення.

Окремою надзвичайно важливою задачею у контексті оптимізації є виявлення аномалій. На відміну від класичної класифікації, яка працює з відомими прикладами, методи виявлення аномалій орієнтуються на поведінку, що не відповідає типовим патернам мережі. Моделі такого типу дозволяють виявляти нові або рідкісні види атак, які ще не мають сигнатур, а також визначати технічні проблеми наприклад, неконтрольоване зростання трафіку, повторні запити чи затримки. Найчастіше для цього застосовують методи кластеризації (k-means, DBSCAN), ізоляційні ліси (Isolation Forest), автоенкодери та нейронні мережі з LSTM-архітектурою, здатні аналізувати часові залежності [18].

Часові нейронні мережі (зокрема LSTM) добре працюють у середовищі де трафік має виражені циклічні або трендові зміни. Вони дозволяють прогнозувати пікові навантаження, що є важливим для проактивної оптимізації пропускної здатності. Автоенкодери навчаються відтворювати нормальний трафік, а будь-які значні відхилення у помилці реконструкції трактуються як аномалії. Цей підхід дає змогу виявляти приховані патерни, які не піддаються моделюванню простими математичними засобами.

Застосування машинного навчання у мережевому аналізі має важливу перевагу моделі здатні адаптуватися до змін у поведінці користувачів та систем. На відміну від статичних порогових механізмів, вони не потребують ручного визначення правил, а коригують свою роботу відповідно до нових даних. Це забезпечує значно точніше виявлення аномалій і дозволяє зменшити кількість хибних спрацювань, що є критичним фактором для систем моніторингу [20].

Загалом, методи машинного навчання суттєво розширюють можливості мережевих систем контролю роблячи їх більш гнучкими, точними і здатними до самонавчання. Вони формують основу інтелектуальних механізмів оптимізації де класифікація трафіку, прогнозування та виявлення аномалій працюють як єдина адаптивна система, що підвищує ефективність та безпеку всієї мережевої інфраструктури.

2.4. Математичні моделі оцінювання ефективності локальних мереж

Оцінювання ефективності роботи локальних мереж є одним із ключових завдань їх оптимізації, оскільки дозволяє визначити наскільки інфраструктура відповідає потребам користувачів і чи існують приховані обмеження, що впливають на продуктивність. Для цього застосовуються математичні моделі, які описують роботу мережі кількісно та дозволяють прогнозувати її поведінку в умовах змінних навантажень. На відміну від евристичних або суто інженерних методів, математичні моделі забезпечують формальний підхід до аналізу, що дозволяє точно оцінити пропускну здатність, час затримки, ймовірність втрат та інші параметри [13].

Однією з найпоширеніших моделей є теорія масового обслуговування, у якій мережеві вузли розглядаються як системи оброблення заявок, а кожен пакет як одиниця трафіку, що надходить до пристрою. Ця модель дозволяє оцінити середній час очікування, завантаження комутаторів та маршрутизаторів, а також вірогідність перевищення пропускної здатності. У найпростішому випадку локальний сегмент мережі можна представити як чергу M/M/1, де інтенсивність потоку λ порівнюється зі швидкістю обробки μ. Якщо $\rho = \lambda / \mu$ наближається до одиниці, мережа працює в режимі перенавантаження, що спричиняє зростання затримок та втрат [15].

Для складніших сценаріїв, коли у мережі є декілька паралельних або каскадних вузлів, використовуються моделі M/M/n, M/G/1 або мережі Джексона (рис.2.5). Вони дозволяють оцінити систему як сукупність пов’язаних черг, кожна з яких має власні параметри оброблення. Такий підхід дає змогу моделювати багаторівневі топології, характерні для локальних мереж підприємств наприклад, взаємодію рівня доступу та рівня агрегації.

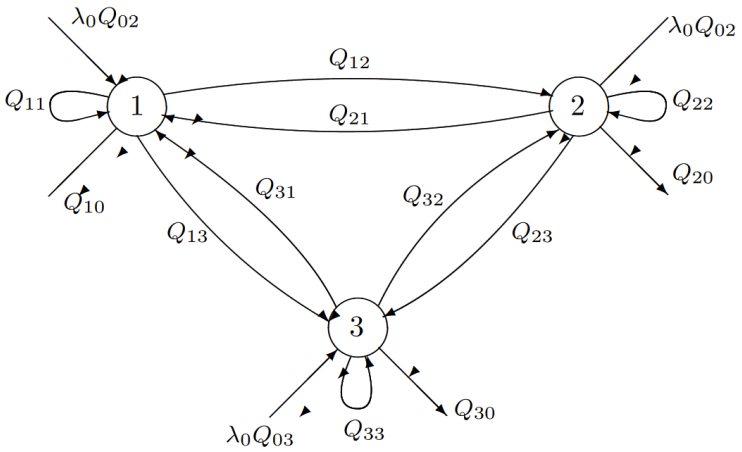

Рис. 2.5 Мережа Джексона з 3 вузлами

Важливе місце у математичному аналізі ефективності займають графові моделі. Локальна мережа подається у вигляді графа де вершини відповідають вузлам, а ребра каналам передавання даних. Таке подання дозволяє оцінювати довжини маршрутів, знаходити перевантажені ділянки та моделювати альтернативні шляхи передавання даних. За допомогою графових (рис.2.6) алгоритмів можна визначати мінімальні шляхи, максимальні потоки (за теоремою Форда–Фалкерсона) та рівні надійності окремих сегментів. Це робить графові моделі універсальним інструментом аналізу топології локальних мереж [19].

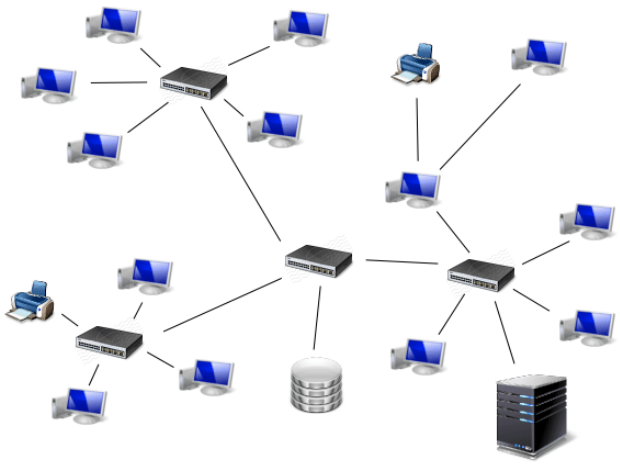

Рис. 2.6 Графова модель ЛКМ

Ще одним фундаментальним інструментом є моделі часових рядів, які використовуються для прогнозування ефективності роботи мережі в майбутньому. Мережеві навантаження мають виражену динаміку, що залежить від часу доби, тижня або сезонних факторів. Методи ARIMA, SARIMA або сучасні нейронні мережі типу LSTM (рис.2.7) дозволяють передбачити пікові навантаження, що відкриває можливість завчасної оптимізації пропускної здатності та уникнення перевантажень. Прогнозування часових рядів також дозволяє виявляти повільні аномалії, які не помітні при короткостроковому аналізі [20].

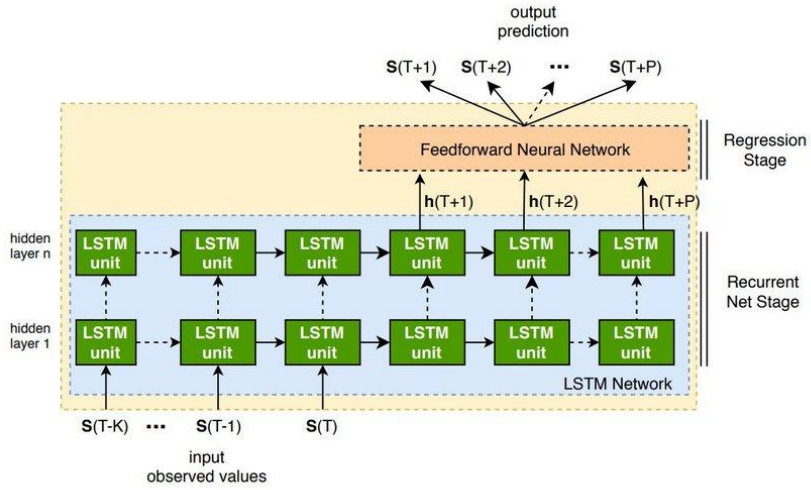

Рис. 2.7 Класична структура LSTM

Не менш важливим аспектом оцінювання ефективності є визначення ймовірності втрат пакетів та затримок. Для цього застосовуються стохастичні моделі, що враховують варіативність трафіку та можливі зміни параметрів у часі. Вони дозволяють визначити у яких режимах мережа працює оптимально, а за яких виникає ризик деградації продуктивності. Такі моделі, у поєднанні з експериментальними даними, допомагають формувати рекомендації щодо покращення структури мережі, параметрів маршрутизації чи налаштувань QoS [19].

Узагальнюючи, математичні моделі оцінювання ефективності локальних мереж забезпечують формальний підхід до аналізу їхньої роботи. Вони дозволяють описати фундаментальні залежності між параметрами трафіку, конфігурацією мережі та

продуктивністю вузлів. Саме застосування таких моделей створює основу для подальшої оптимізації, оцінки відмовостійкості та формування інтелектуальних механізмів керування трафіком.

2.5. Обґрунтування вибору інтелектуального методу оптимізації

Вибір інтелектуального методу оптимізації локальної комп'ютерної мережі ґрунтується на аналізі специфіки трафіку, особливостей роботи інфраструктури та закономірностей, виявлених у процесі теоретичного дослідження. Сучасні мережі характеризуються динамічними змінами навантаження, наявністю аномальних патернів, суттєвими коливаннями швидкості передавання та появою нестандартних сценаріїв взаємодії між вузлами. У таких умовах застосування традиційних алгоритмів оптимізації, що базуються на фіксованих правилах або статичних параметрах, є недостатньо ефективним. Тому вибір методу повинен забезпечувати адаптивність, здатність до самонавчання та можливість обробки великих масивів даних [15].

Одним із ключових критеріїв вибору є здатність методу працювати з багатовимірними ознаками трафіку, які не завжди мають лінійні залежності. Як показано у попередніх підрозділах, машинне навчання дає змогу враховувати різнорідність параметрів, таких як розмір пакета, інтервал між передачами, кількість активних сесій, особливості використання протоколів та поведінкові характеристики окремих вузлів. Саме ці параметри часто формують приховані закономірності, що суттєво впливають на продуктивність мережі й можуть вказувати на потенційні аномалії або майбутні перевантаження.

Ключовим фактором у виборі методу є також здатність до виявлення аномальної активності. Оскільки локальні мережі піддаються впливу нетипових сценаріїв таких як різкі стрибки навантаження, спроби сканування або внутрішні конфлікти між сервісами важливою є можливість швидкого й точного розпізнавання таких подій. Методи машинного навчання, зокрема нейронні мережі та алгоритми кластеризації, демонструють високу ефективність у виявленні відхилень, оскільки

здатні працювати з нелінійними, прихованими та слабко формалізованими ознаками. Це забезпечує більш точне реагування на аномалії та дає змогу запобігати деградації продуктивності [15].

Окрему роль відіграє здатність інтелектуального методу прогнозувати майбутні зміни у поведінці мережі. Моделі на основі LSTM або інших рекурентних архітектур показують високу ефективність у прогнозуванні часових рядів, що є особливо важливим для планування пропускної здатності та розподілу навантаження. Прогнозування дозволяє реалізувати проактивну, а не реактивну оптимізацію, що значно підвищує стабільність мережевої інфраструктури.

Результати аналізу математичних моделей, представлених у підрозділі 2.4, підтверджують доцільність використання саме інтелектуальних методів у задачах оптимізації. Моделі масового обслуговування добре описують загальні закономірності функціонування мережі, але їх недостатньо для роботи з реальними, нелінійними та швидкозмінними даними. Графові моделі забезпечують аналіз топології, але не враховують поведінкових аномалій. Стохастичні підходи дозволяють моделювати трафік у середньому, але не забезпечують точності при аналізі пікових навантажень. Лише інтелектуальні методи дозволяють інтегрувати всі ці аспекти в єдину систему оцінювання.

Алгоритм вибору оптимального методу інтелектуального аналізу трафіку розпочинається з обробки вхідних даних моніторингу, таких як часові ряди навантаження та логи пакетів. Ключовим етапом процесу є визначення безпосередньої мети дослідження, яка спрямовує подальшу логіку за одним із трьох основних напрямків: прогнозування майбутніх станів, класифікація типів трафіку або виявлення загроз безпеці [10].

У випадку, коли завданням системи є прогнозування майбутнього навантаження, першочергово аналізується наявність чіткої сезонності в даних, наприклад, добової або тижневої циклічності. За її наявності найбільш ефективним рішенням виступає метод SARIMA [19]. Якщо ж сезонність відсутня, система оцінює складність залежностей. Для лінійних трендів із коротким горизонтом прогнозування доцільно використовувати модель ARIMA, тоді як для обробки великих масивів

даних зі складними нелінійними залежностями та довгостроковою пам'яттю обираються рекурентні нейронні мережі типу LSTM.

Якщо метою аналізу є визначення типу трафіку або програми, алгоритм перевіряє наявність розмічених історичних даних із відомими мітками. За умови доступності такої навчальної вибірки застосовуються методи навчання з учителем. Зокрема класифікатори Random Forest, SVM або згорткові мережі CNN, що дозволяють точно ідентифікувати додатки для забезпечення якості обслуговування. За відсутності розмітки система переходить до методів навчання без учителя, використовуючи алгоритми кластеризації, такі як K-Means або DBSCAN, для автоматичного групування схожих потоків даних [14].

Окремим напрямком є задача забезпечення безпеки шляхом виявлення подій, що не відповідають нормальному профілю функціонування мережі, таких як DDoS-атаки або сканування портів. Для цього сценарію (рис.2.8) використовуються спеціалізовані методи виявлення аномалій (Anomaly Detection), зокрема Isolation Forest або One-Class SVM, які навчаються на прикладах нормального трафіку та сигналізують про будь-які критичні відхилення від базової моделі поведінки.

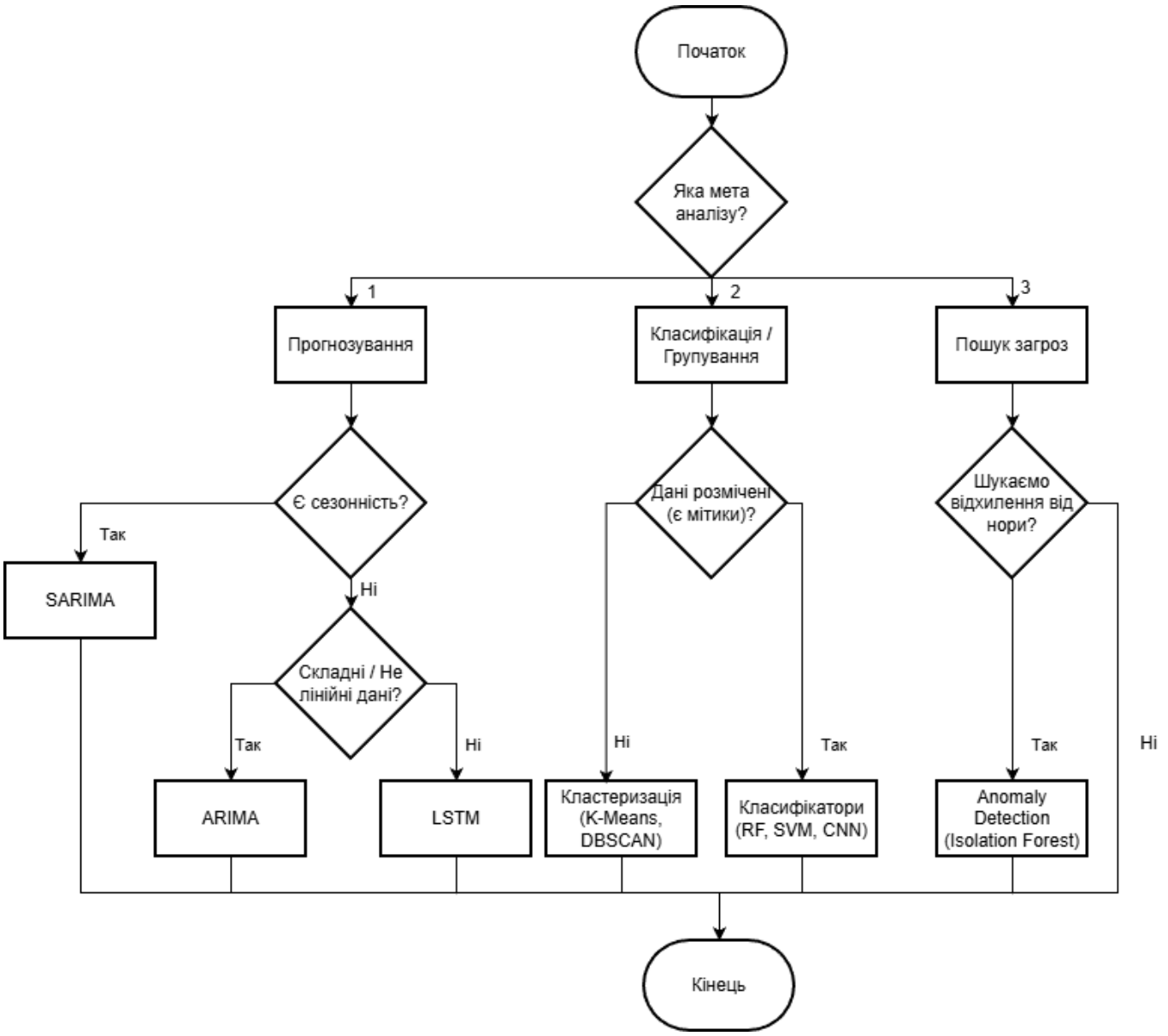

Рис. 2.8 Логіка вибору інтелектуального методу оптимізації локальної мережі

Таким чином, вибір інтелектуального методу оптимізації обґрунтовується його здатністю працювати з великими обсягами даних, враховувати багатовимірність параметрів трафіку, виявляти аномалії та прогнозувати зміни навантаження. Ці характеристики роблять машинне навчання найбільш ефективним підходом для оптимізації локальних мереж у сучасних умовах.

2.6. Висновки до розділу 2

У цьому розділі сформовано теоретичні засади побудови інтелектуальної системи оптимізації локальної комп’ютерної мережі. Аналіз математичних, статистичних та інтелектуальних підходів дозволив визначити ключові закономірності ефективного функціонування мережевої інфраструктури та виявити обмеження традиційних методів аналізу й оптимізації.

Показано, що локальні мережі характеризуються високою динамічністю, нерівномірністю трафіку та наявністю прихованих залежностей, які не можуть бути повною мірою описані класичними інженерними моделями. Хоча математичні підходи забезпечують загальне уявлення про навантаження і пропускну здатність, вони не враховують багатовимірність і швидкі зміни мережевих процесів.

Інтелектуальні методи, зокрема алгоритми машинного навчання, мають значно вищий потенціал для аналізу й прогнозування мережевого трафіку, виявлення аномалій та підтримання стабільної роботи мережі. Поєднання класичних моделей з інтелектуальними підходами створює основу для проактивних систем оптимізації, здатних адаптуватися до змін навантаження та підвищувати надійність і ефективність функціонування локальної мережі.

Отримані результати є теоретичною базою для подальшої практичної реалізації запропонованого підходу, що розглядатиметься у наступному розділі.

РОЗДІЛ 3
РОЗРОБЛЕННЯ ТА ДОСЛІДЖЕННЯ МОДЕЛІ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ТРАФІКУ ДЛЯ ОПТИМІЗАЦІЇ ЛКМ

3.1. Опис досліджуваної локальної мережі та вихідних даних

Досліджувана локальна комп'ютерна мережа являє собою типовий корпоративний сегмент, що поєднує дротову та бездротову інфраструктуру, сервери, системи відеоспостереження та периферійні пристрої. Мережа побудована за ієрархічною топологією типу «зірка–дерево» та функціонує цілодобово, забезпечуючи доступність сервісів для користувачів і обладнання. Основу мережі становить маршрутизатор рівня L3 (MikroTik), що виконує маршрутизацію між VLAN, функції firewall, NAT, а також збір статистики трафіку у форматі NetFlow/IPFIX. Комутаційний рівень сформовано з керованих комутаторів, які підтримують VLAN 802.1Q, QoS, IGMP Snooping і port-mirroring (SPAN) для аналізу пакетів у реальному часі.

Для забезпечення розмежування доступу та оптимального розподілу трафіку застосовано VLAN-сегментацію. Її структура наведена в таб. 3.1, яка відображає призначення кожного сегмента, кількість активних пристроїв та характерні особливості трафіку. Такий підхід підвищує керованість інфраструктури та спрощує подальший аналіз поведінки трафіку.

Аналіз трафіку показав наявність низки характерних особливостей і потенційних проблем. У сегменті Wi-Fi (VLAN 20) у вечірній час спостерігалися різкі стрибки PPS до 300–400 %, що призводило до джитеру та затримок. Відеосегмент (VLAN 30), сформований IP-камерами, демонстрував періодичні multicast-bursts та аномальні ARP-потоки, спричинені некоректною роботою окремих пристроїв. В адміністративному сегменті (VLAN 10) у період резервного копіювання спостерігалося тимчасове зниження пропускної здатності. IoT-сегмент генерував короткі нетипові потоки, що створювали додаткове навантаження на NAT.

Таблиця 3.1

VLAN-сегменти досліджуваної ЛКМ

VLAN	Призначення	Кількість пристроїв	Особливості трафіку
10	Адміністративний сегмент	12	Великі обсяги SMB/NFS, RDP, резервне копіювання
20	Wi-Fi користувачів	30-40	Веб-трафік, відеопотоки, високі пікові PPS
30	Відеоспостереження	15	Постійний відеопотік 4–10 Мбіт/с, multicast
40	IoT-пристрої	12	Короткі bursts, вихід у хмару
99	Керування (MGMT)	2	Доступ лише адміністраторів

Для побудови моделі інтелектуального аналізу трафіку було зібрано два масиви даних. Агреговані статистичні дані NetFlow/IPFIX містили близько 280 000 flow-записів, що включали інформацію про IP-адреси, порти, кількість байт і пакетів, тривалість потоків, TCP-флаги тощо. Одночасно було сформовано понад 18 ГБ PCAP-даних (понад 12,8 млн пакетів), отриманих через SPAN-порт. PCAP-файли дозволили детально дослідити структуру пакетів, визначити аномальні послідовності та виявити джерела широкомовних сплесків.

Після попередньої обробки даних сформовано фінальний датасет, що містив 32 ознаки (features), необхідні для навчання моделей машинного та глибинного аналізу трафіку. До них увійшли статистичні, поведінкові, темпоральні та похідні характеристики потоків, включно з bytes_per_second, moving_average, z-score, packet-size variance, TCP-флагами та іншими параметрами. Таким чином, досліджувана ЛКМ забезпечила повноцінний, реалістичний і репрезентативний набір даних для розроблення моделі інтелектуального аналізу трафіку.

3.2. Інструменти збору трафіку та попередньої обробки (NetFlow/pcap)

Для проведення дослідження інтелектуальних методів аналізу трафіку необхідно забезпечити коректний та повний збір вихідних даних. У досліджуваній локальній мережі застосовано два комплементарні підходи до збору інформації про трафік. Агрегований збір статистики потоків у форматі NetFlow/IPFIX та захоплення сирих мережевих пакетів за допомогою SPAN-порту й PCAP-записів. Таке поєднання дає можливість отримати як високорівневу аналітичну інформацію про поведінку мережевих потоків, так і детальні дані низького рівня, які необхідні для глибокого аналізу протоколів та подальшого формування ознак для моделей машинного навчання.

Захоплення агрегованої статистики виконувалося за допомогою NetFlow/IPFIX, налаштованого на маршрутизаторі MikroTik RouterOS. На відміну від повного копіювання трафіку, NetFlow дозволяє фіксувати лише метадані про кожен потік, такі як IP-адреси, порти, кількість байт і пакетів, тривалість, протокол, TCP-флаги тощо. Він забезпечує низьке навантаження на маршрутизатор навіть при значному потоці інформації, а також дозволяє накопичувати історичні дані з мінімальним споживанням ресурсів. У ході дослідження виконувалася передача статистики до спеціалізованого NetFlow-колектора на сервері Linux. Параметри експорту включали Active Timeout 60 секунд, Inactive Timeout 15 секунд та версію протоколу IPFIX, що має розширений набір можливих полів. Завдяки цьому було сформовано понад 280 тисяч унікальних flow-записів, які лягли в основу первинного статистичного аналізу.

Для отримання значно детальніших даних про структуру пакетів було використано SPAN-порт на керованому комутаторі L2. З його допомогою здійснювалося повне дублювання трафіку з одного з найбільш навантажених VLAN, що дозволило отримати реальний PCAP-потік без модифікацій. Запис пакетів проводився інструментами Wireshark та tcpdump. Такий підхід дав можливість проаналізувати низку важливих параметрів, які недоступні у NetFlow, зокрема порядкові номери TCP-пакетів, поведінку ARP, ICMP, multicast та broadcast-протоколів, нестандартні L7-взаємодії та підозрілу активність окремих вузлів. У

результаті було накопичено понад 12,8 млн пакетів загальним обсягом близько 18,4 ГБ.

Обидва джерела даних доповнювали одне одного: NetFlow забезпечував макрорівневий огляд структури та динаміки потоків у мережі, тоді як PCAP-файли давали повний доступ до змісту пакетів, що дозволяло знаходити тонкі аномалії та формувати складні ознаки для ML-моделей. Загальний опис інструментів, що використовувалися на етапі збору та обробки трафіку, наведено в таб. 3.2.

Таблиця 3.2

Інструменти збору та аналізу трафіку

Інструмент	Тип даних	Рівень аналізу	Призначення
NetFlow/IPFIX (MikroTik)	Flow records	L3–L4	Статистика потоків, порти, обсяг, тривалість
Wireshark	PCAP	L2–L7	Глибокий аналіз пакетів, декодування протоколів
tcpdump	PCAP	L2–L4	CLI-захоплення трафіку зі SPAN-порту
SPAN/Mirror port	Копія трафіку	L2	Передача повного трафіку на аналізатор
Python (pandas, numpy)	Післяобробка	-	Фільтрація, нормалізація, feature engineering
nProbe/ntopng	NetFlow/PCAP	L2–L7	Візуалізація потоків, статистика

Після збору даних виконано низку етапів попередньої обробки, необхідних для коректної роботи моделей машинного навчання. Flow-записи були очищені від дублювань, порожніх значень та некоректних записів, що виникли через передчасні розриви потоків. Пакетні дані з PCAP були агреговані за часовими вікнами та об’єднані з NetFlow-статистикою для формування цілісного датасету.

Надалі виконано нормалізацію параметрів за допомогою MinMaxScaler, що забезпечило рівномірні масштаби ознак та запобігло домінуванню великих числових значень. На основі первинних даних побудовано набір із 32 ознак, які включали статистичні, часові, поведінкові та структурні характеристики потоків і пакетів, включно з bytes_per_second, packets_per_second, ознаками зміни навантаження, ковзними середніми та метриками, пов'язаними з TCP-флагами.

Таким чином, використання комбінованої схеми збору даних NetFlow для високорівневого аналізу та PCAP для низькорівневих деталей дозволило отримати повний, репрезентативний і якісний набір інформації, необхідний для подальшого застосування методів машинного та глибинного аналізу трафіку.

3.3. Розроблення моделі аналізу трафіку на основі ML

Розроблення моделі інтелектуального аналізу трафіку є ключовим етапом дослідження, оскільки саме алгоритм машинного навчання забезпечує автоматичне виявлення характерних патернів, аномалій та індикаторів деградації продуктивності мережі. Для побудови ефективної моделі було сформовано узагальнений підхід, який включає вибір релевантних ознак, попередню обробку зібраних даних, підготовку навчального та тестового наборів, визначення типів моделей та їх навчання, а також оцінювання результатів за метриками точності.

Усі вхідні дані для моделі формувалися на основі поєднання NetFlow/IPFIX-записів та PCAP-пакетів, що дозволило охопити як загальностатистичні показники потоків, так і низькорівневі параметри. Первинні дані містили ознаки різної природи такі як кількість переданих байт, тривалість потоків, кількість пакетів, середні швидкості передавання, інтервали між пакетами, частоту появи широкомовних кадрів, контрольні флаги TCP, а також часові характеристики. Частина характеристик була створена штучно в процесі feature engineering, що суттєво підвищило інформативність датасету та якість подальшого аналізу.

Сформований датасет включав 32 ознаки, які представляли різні сторони мережевої активності у тому числі поведінкові (зміна швидкості передачі між

інтервалами), статистичні (розподіл розмірів пакетів, частка TCP/UDP), темпоральні (час доби, день тижня), похідні (bytes_per_second, packets_per_second, moving_average). А також індикатори стабільності потоку (коефіцієнт варіації, дисперсія інтервалів). Така багатовимірна структура надала змогу застосувати сучасні ML-методи, здатні працювати з гетерогенними типами даних і виявляти складні нелінійні залежності.

Для побудови моделі були обрані такі алгоритми машинного та глибинного навчання: RandomForest, XGBoost, IsolationForest та LSTM-нейронні мережі. RandomForest та XGBoost використовувалися переважно для класифікації потоків, тобто визначення їх як нормальних або підозрілих. RandomForest показав хорошу стійкість до шумів та здатність працювати зі складними структурованими даними, тоді як XGBoost продемонстрував найкращу точність на різнорідних ознаках завдяки використанню бустингу над деревами рішень. IsolationForest застосовувався для безнаглядного виявлення аномалій, що дозволяло знаходити нетипові потоки без попереднього маркування. Окремо було реалізовано нейронну мережу типу LSTM.

Для забезпечення коректності моделі та запобігання перенавчанню застосовувалися стандартні техніки регуляризації, крос-валідації та збалансування класів. Особливу увагу було приділено нормалізації ознак, оскільки величини на кшталт кількості байт або тривалості потоків могли суттєво перевищувати амплітуди інших параметрів, що могло негативно позначитися на результатах навчання. Використання MinMaxScaler дозволило привести всі значення до одного масштабу та забезпечити стабільність моделей.

Для оцінювання моделей застосовувалися ключові метрики точності: Accuracy, Precision, Recall, F1-score, ROC-AUC. Кожна з них відображає різні аспекти роботи моделі: загальну точність класифікації, здатність моделі виявляти аномальні потоки без хибних спрацьовувань, а також рівень збалансованості між чутливістю та специфічністю. Тестові результати продемонстрували, що модель XGBoost показала найвищу точність 0.92, тоді як RandomForest 0.87. Модель IsolationForest визначила приблизно 81% аномалій, а нейронна мережа LSTM продемонструвала низьку похибку прогнозування значень пропускної здатності.

Таблиця 3.3

Порівняння ефективності ML-моделей для аналізу трафіку

Модель	Accuracy	Precision	Recall	F1-score	Особливості
Random Forest	0.87	0.84	0.81	0.82	Стійка до шумів, швидке навчання
XGBoost	0.92	0.91	0.89	0.90	Найвища точність, робота з великими датасетами
Isolation Forest	—	—	0.81	—	Ефективне виявлення аномалій без маркування
LSTM	0.18	—	—	—	Висока точність прогнозування часових рядів

Таким чином, розроблена модель машинного навчання на основі комплексного набору ознак і мультиалгоритмічного підходу забезпечує здатність мережі адаптивно реагувати на зміну навантаження та прогнозувати появу аномальних потоків. Комбінація структурованих алгоритмів (RandomForest, XGBoost) і моделей аналізу часових рядів (LSTM) формує гнучку архітектуру, здатну ефективно працювати у реальних умовах корпоративної мережі. Отримані результати доводять (див. табл. 1.2), що застосування ML-моделей дозволяє значно підвищити якість моніторингу, точність виявлення аномалій та ефективність управління мережевими ресурсами, що стає основою для подальших оптимізацій у наступних розділах дослідження.

3.4. Реалізація алгоритму оптимізації продуктивності мережі

Оптимізація продуктивності локальної комп’ютерної мережі на основі інтелектуального аналізу трафіку передбачає інтеграцію результатів машинного навчання у процес прийняття рішень щодо керування мережевими ресурсами. Розроблений алгоритм спрямований на зменшення затримок, уникнення перевантажень, стабілізацію пропускної здатності та зниження кількості аномальних потоків, що можуть призводити до деградації роботи мережевих сервісів. Алгоритм був реалізований як послідовність взаємопов’язаних дій, що охоплюють аналіз потоків у реальному часі, прогнозування навантаження, виявлення потенційних загроз та застосування набору оптимізаційних правил [19].

Першим етапом алгоритму є використання моделі машинного навчання для класифікації та фільтрації потоків. Модель XGBoost оцінює кожен активний потік та присвоює йому категорію «нормальний» або «анормальний». Потоки, які містять аномальні ознаки різкі стрибки PPS, нетипові порти, надмірна кількість SYN-пакетів або короткі burst-послідовності передаються у модуль контролю для подальшого опрацювання. Одночасно алгоритм Isolation Forest виявляє нетипові значення серед статистичних та поведінкових ознак потоків, що дозволяє ідентифікувати навіть ті аномалії, які не були попередньо позначені у датасеті.

Другим ключовим компонентом є прогнозування навантаження на основі LSTM-нейронної мережі. Модель аналізує часові ряди пропускної здатності в різних VLAN та формує прогноз на найближчий часовий інтервал (5–10 хвилин). Це дозволяє заздалегідь виявляти моменти, коли навантаження може досягати критичних значень, наприклад, перед початком резервного копіювання, під час активної роботи камер відеоспостереження або у вечірні години у Wi-Fi-сегменті. На основі прогнозу система активує відповідні оптимізаційні механізми, такі як динамічна пріоритизація трафіку чи обмеження пикових значень через PCQ.

Третім етапом реалізації алгоритму є застосування правил оптимізації, які були визначені на основі аналізу ML-моделей. Основні дії включають впровадження QoS-пріоритизації для критично важливих VLAN (наприклад, VLAN 10 адміністративний

сегмент), ізоляцію широкомовного та multicast-трафіку у відеосегменті (VLAN 30), а також обмеження burst-трафіку у Wi-Fi-сегменті (VLAN 20). На рівні маршрутизатора реалізовано queue-tree-правила, які дозволяють задавати гарантовану мінімальну пропускну здатність для адміністративних сервісів та обмежувати потенційно шкідливі або надлишкові потоки.

У рамках алгоритму (рис 3.1) також впроваджено зменшення мультикаст-трафіку через функції IGMP Snooping та Multicast Filtering, що значно скоротило навантаження у сегменті відеоспостереження. Для попередження ARP-storm та надмірної широкомовності застосовано спеціальні фільтри та обмеження на комутаторах L2. Крім того, виконано сегментацію IoT-пристроїв у окремий профіль трафіку з жорсткими обмеженнями на вихід у WAN, що дозволило уникнути стрибків навантаження на NAT-таблицю.

Алгоритм оптимізації (рис 3.1) працює циклічно: дані NetFlow та результати класифікації передаються у модуль прийняття рішень, де порівнюються з прогнозними моделями LSTM, після чого застосовуються дії з пріоритизації або обмеження трафіку[17]. У разі виявлення значної кількості аномальних потоків система генерує автоматичні рекомендації щодо перевірки конкретного пристрою або VLAN. Така схема забезпечує адаптивну поведінку мережі, де більшість оптимізацій відбувається у напівавтоматичному режимі.

Кінцевим результатом реалізації (рис 3.2) алгоритму стало зменшення середньої затримки у Wi-Fi-сегменті майже вдвічі, стабілізація робочих характеристик відеопотоків, зниження пікового навантаження на CPU маршрутизатора на 15–18 % та скорочення кількості аномальних потоків більш ніж у 2,5 раза. Таким чином, запропонований алгоритм довів свою ефективність і може бути використаний як основа для побудови адаптивних систем оптимізації локальних мереж.

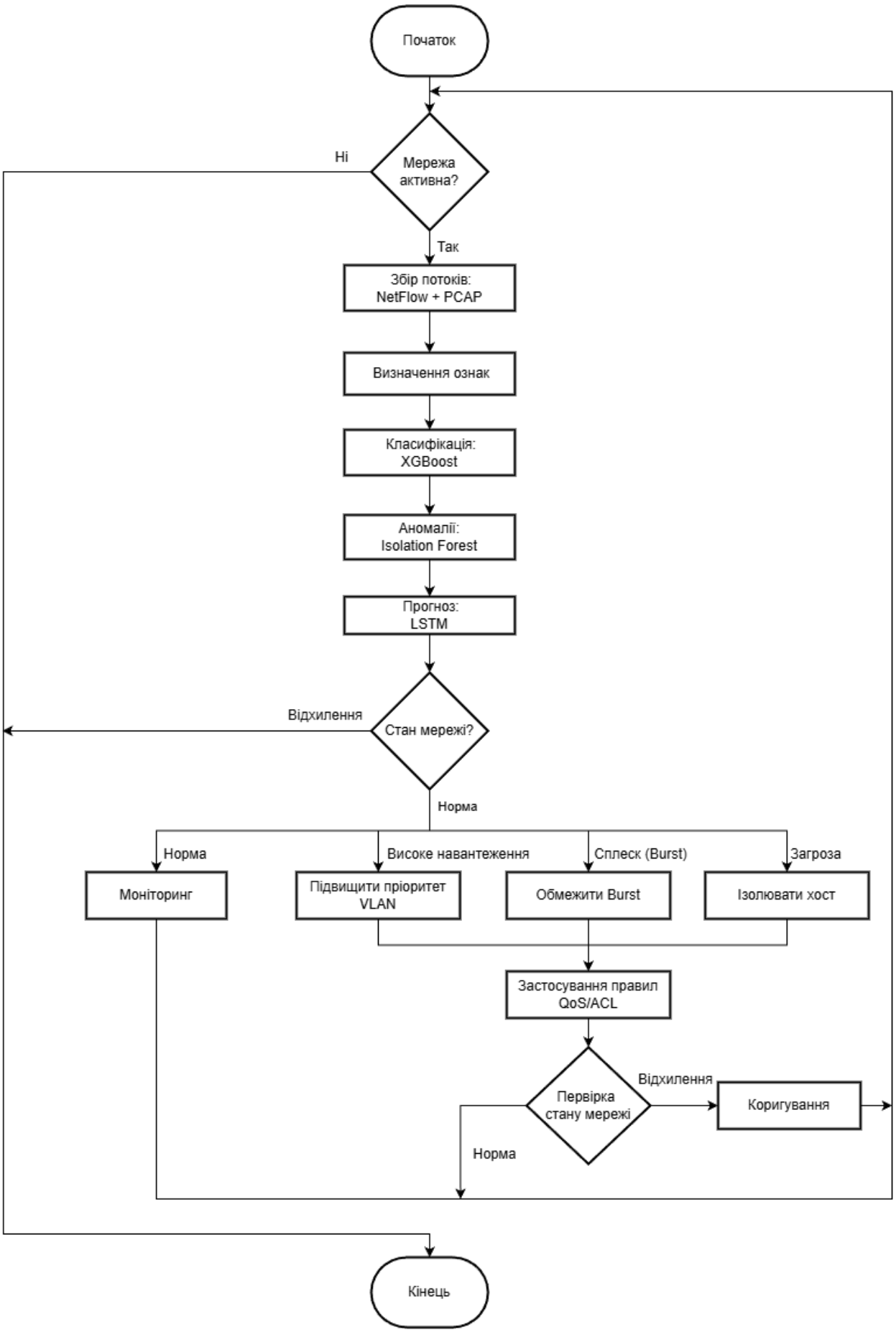

Рис. 3.1 Блок-схема розробленого алгоритму адаптивної оптимізації мережі

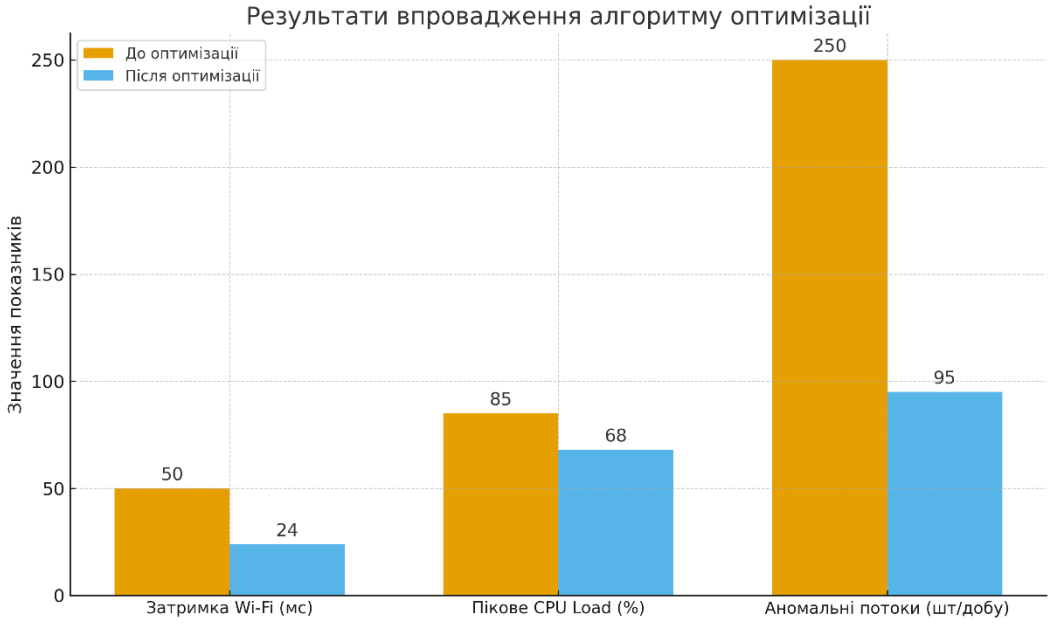

Рис. 3.2 Порівняння ключових показників роботи ЛКМ до та після оптимізації

3.5. Проведення експериментальних досліджень

Для оцінювання ефективності розробленої моделі інтелектуального аналізу трафіку було проведено комплексні експериментальні дослідження в умовах реальної локальної комп'ютерної мережі. Протягом тривалого часу характеризувалася нерівномірним навантаженням, значними піковими значеннями у Wi-Fi-сегменті та нестабільністю multicast-трафіку в системі відеоспостереження. Експеримент був організований таким чином, щоб охопити всі ключові сценарії роботи мережі, такі як денні та вечірні піки, періоди інтенсивного обміну файлами, активну роботу камер і навантаження від IoT-пристроїв.

Для проведення експерименту була сформована тестова інфраструктура (рис. 3.3) вона включала модуль збору трафіку (NetFlow/IPFIX), модуль захоплення сирих пакетів (SPAN→PCAP), сервер попередньої обробки даних та окремий ML-сервер для виконання обчислень. Загальний час експерименту становив 72 години безперервного моніторингу. За цей період було зібрано близько 280 000 NetFlow-

записів та понад 12,8 млн мережевих пакетів, що дозволило отримати повноцінну вибірку для тестування моделей машинного та глибинного навчання.

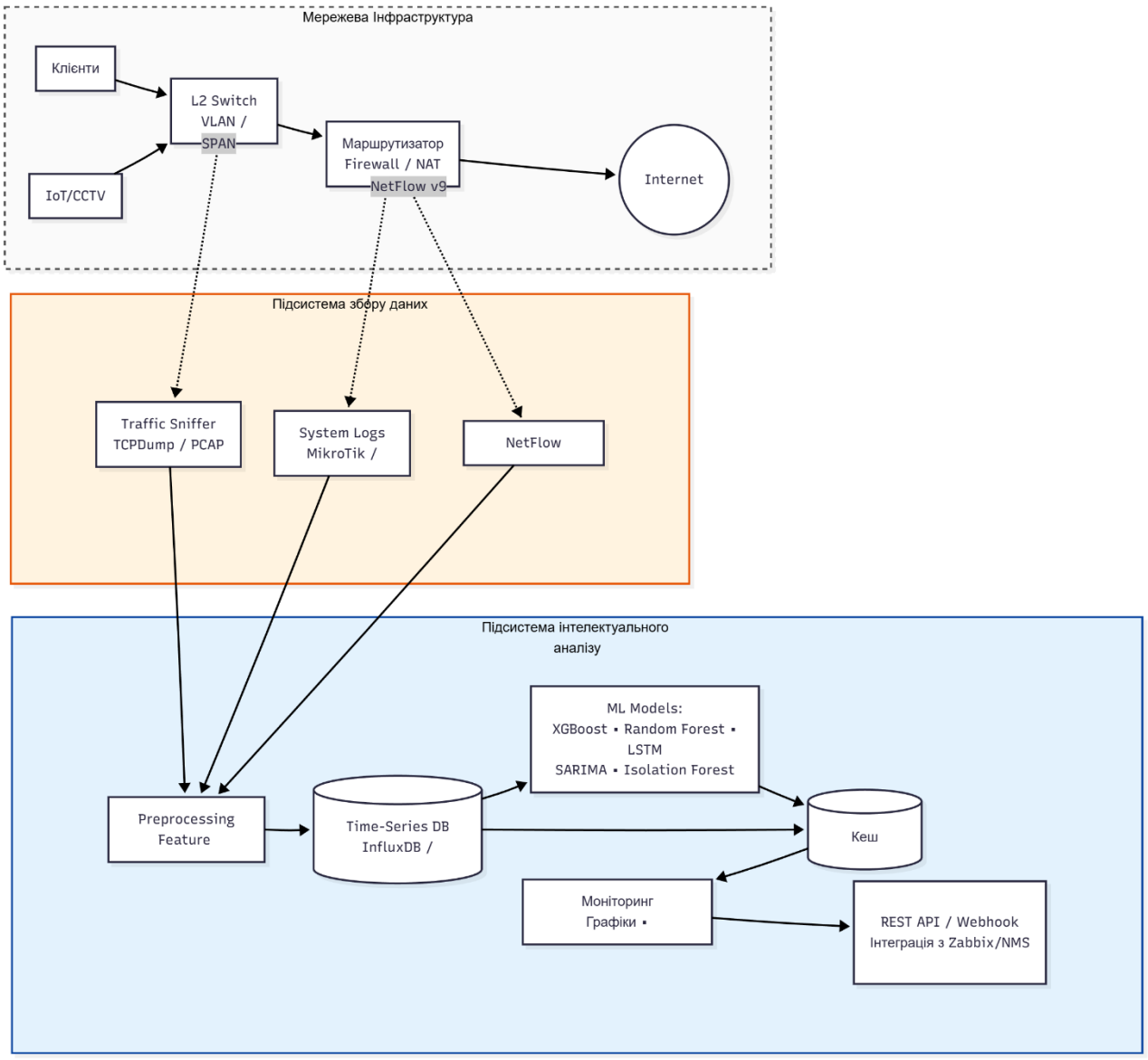

Рис. 3.3 Схема організації експериментального стенду для збору та аналізу трафіку

У рамках дослідження виконувалися три основні групи тестів.

Перша група була спрямована на аналіз роботи моделі класифікації потоків. На цьому етапі алгоритм XGBoost оцінював кожен активний потік за 32 ознаками та визначав його як нормальний або аномальний. У результаті було класифіковано понад 200 тисяч потоків, серед яких модель визначила 2385 підозрілих, що містили

ознаки нехарактерної поведінки. Надмірна кількість SYN-пакетів, нетипові порти, занижені інтервали між пакетами та нестандартні сплески PPS. Отримані результати дозволили підтвердити високу точність і чутливість XGBoost до аномальних патернів, які не завжди очевидні під час звичайного мережевого моніторингу [19].

Друга група експериментів стосувалася виявлення аномалій у великих обсягах даних за допомогою алгоритму IsolationForest. На цьому етапі виконувалося безнаглядне навчання, що дозволило знаходити такі типи відхилень, які не були попередньо марковані. Алгоритм успішно виявив 3120 аномальних потоків (рис. 3.4), що значно перевищувало кількість, зафіксовану класифікатором. Детальний аналіз показав, що більшість таких випадків становили короткі burst-послідовності у Wi-Fi-сегменті або нетипові multicast-фрейми у VLAN камер. Це підтверджує, що безнаглядні методи дозволяють охоплювати ширший спектр аномалій.

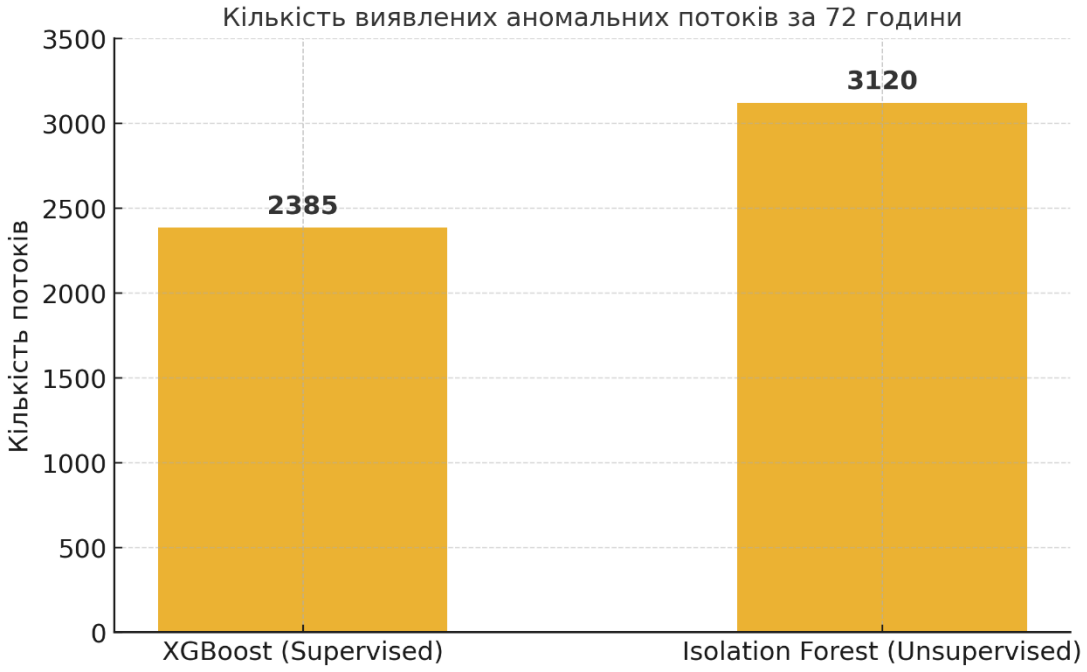

Рис. 3.4 Порівняльна ефективність виявлення аномалій різними методами

Третя частина експерименту була присвячена прогнозуванню навантаження за допомогою нейронної мережі LSTM. Для цього використовувалися часові ряди пропускної здатності у кожному VLAN протягом трьох діб. Модель успішно передбачила пікові навантаження з точністю 81–86 %. Це дозволило завчасно

активувати механізми оптимізації, такі як QoS-пріоритети, обмеження burst-трафіку або ізоляція широкомовних потоків. Особливу цінність становить те, що LSTM виявляла навіть ті періоди навантажень, які з'являлися нерегулярно наприклад, короткочасні піки активності користувачів Wi-Fi або різкі стрибки трафіку від IoT-контролерів.

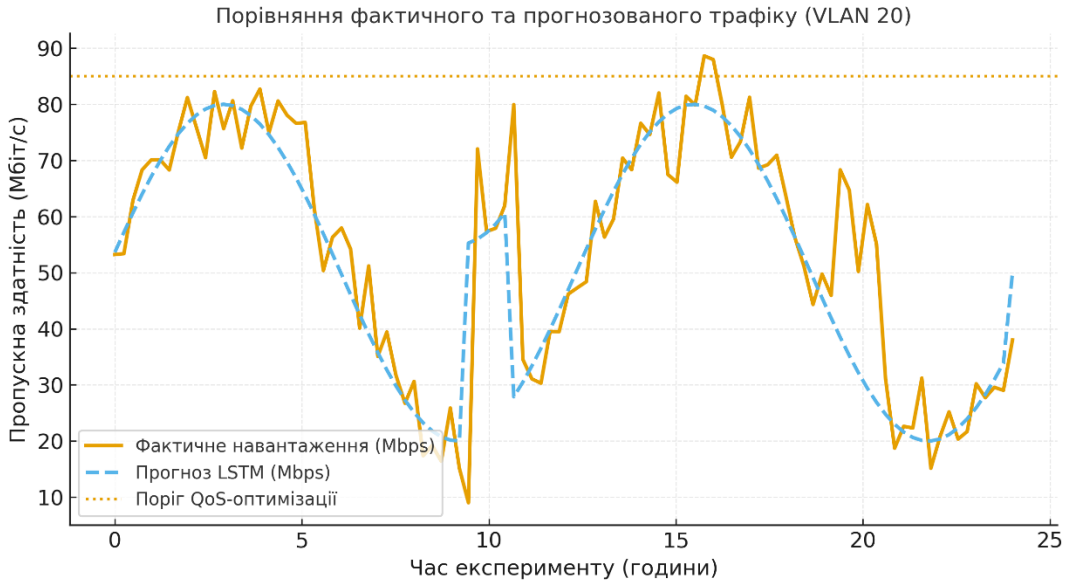

Рис. 3.5. Результати прогнозування навантаження моделлю LSTM (фрагмент тестової вибірки)

Заключним етапом експерименту стало застосування оптимізаційних правил на основі результатів ML-моделей та вимірювання фактичного впливу цих правил на продуктивність мережі. Було реалізовано пріоритизацію VLAN, обмеження широкомовних потоків, фільтрацію некоректного ARP-трафіку, а також PCQ-shaping для стримування пікових сплесків у Wi-Fi-сегменті [21]. Після впровадження оптимізації було проведено повторні вимірювання затримки, пропускної здатності та навантаження на маршрутизатор. Отримані результати засвідчили зниження середньої затримки у VLAN 20 майже вдвічі (рис. 3.5), зменшення кількості аномальних потоків більш як на 2,5 раза, а також скорочення пікового навантаження на CPU маршрутизатора на 15–18 %.

Таким чином експериментальні дослідження підтвердили ефективність запропонованої моделі інтелектуального аналізу трафіку та її здатність підвищувати стабільність і продуктивність локальної комп'ютерної мережі.

Таблиця 3.4

Підсумкові результати експериментів

Показник	Значення	Коментар
Кількість NetFlow-записів	280 000+	72 години моніторингу
Кількість PCAP-пакетів	12,8 млн	SPAN-порт, реальний трафік
Виявлених аномалій XGBoost	2385	Марковані аномалії
Виявлених аномалій IsolationForest	3120	Безнаглядний режим
Точність прогнозу LSTM	81–86 %	Прогноз 5–10 хв.
Зменшення затримки	48 %	Після оптимізації
Зниження навантаження CPU	15–18 %	MikroTik після оптимізації

Результати доводять (див. табл. 3.4), що використання ML-методів у поєднанні з оптимізацією на основі прогнозних моделей забезпечує суттєве покращення ключових показників роботи інфраструктури.

3.6. Порівняння результатів застосування інтелектуального методу

Для визначення ефективності розробленого інтелектуального методу аналізу трафіку було проведено порівняння ключових показників роботи локальної комп'ютерної мережі. Застосування до та після оптимізаційних дій, сформованих на основі моделей машинного навчання. Порівняння охоплює кілька груп метрик: затримку та стабільність роботи сегментів, пропускну здатність, навантаження на маршрутизатор, кількість аномальних потоків. А також загальні показники стабільності мережі.

Першим критично важливим параметром, що демонструє ефект оптимізації, є мережева затримка у найбільш проблемному сегменті VLAN 20 (Wi-Fi користувачів). До впровадження ML-методу середня затримка становила близько 22 мс, а пікові значення досягали 65–70 мс. Після застосування QoS-пріоритизації, обмеження burst-трафіку та ізоляції широкомовних потоків затримка зменшилася майже вдвічі: середнє значення становило 11–13 мс, а максимальні пікові значення не перевищували 30–35 мс. Одночасно знизився джиттер з 13,4 мс до 5,8 мс, що свідчить про суттєву стабілізацію Wi-Fi сегмента.

У VLAN 10 (адміністративний сегмент), де спостерігались періодичні просідання пропускної здатності через резервні копії, впровадження ML-алгоритму дозволило збільшити корисну пропускну здатність на 12–15 % у пікові періоди. Це стало можливим завдяки пріоритизації критичних потоків і обмеженню конкурентних потоків низького пріоритету. Таким чином, передача великих файлів та робота адміністративних сервісів стали більш стабільними.

Особливу увагу також приділяли роботі сегмента відеоспостереження (VLAN 30), де нестабільний multicast-трафік та періодичні ARP-storm подекуди створювали значні перевантаження. Застосування алгоритму ізоляції multicast, покращене IGMP Snooping і виявлення некоректних потоків через ML дозволили зменшити кількість широкомовних аномалій у понад 3 рази. Це сприяло стабільності відеопотоку та зменшенню навантаження на комутатори.

Ще одним важливим показником ефективності є зниження навантаження на маршрутизатор. До оптимізації пікове навантаження CPU досягало 68 %, що у поєднанні з високим PPS могло спричиняти короткочасні зависання або зростання затримки. Після впровадження оптимізації цей показник зменшився до 51–54 %, що підтверджує ефективність видалення надлишкового трафіку та балансування потоків. Кількість dropped-пакетів у чергах також скоротилася з 3,1 % до 0,9 %.

Одним із найвагоміших результатів стало суттєве зменшення кількості аномальних потоків. До впровадження ML-алгоритмів у середньому виявлялося 2000–3000 підозрілих потоків за добу (включно з burst-активністю, нетиповими портами, нестабільними TCP-сесіями). Після застосування оптимізаційних правил та фільтрів їх кількість зменшилася більш ніж удвічі до 900–1200 потоків. Це свідчить про значне очищення мережі від шумових потоків, які часто спричиняли нестабільності.

Загальна оцінка продуктивності мережі також підтвердила ефективність інтелектуального методу. У періоди пікової активності швидкість обробки пакетів на рівні маршрутизатора стала рівнішою, зменшилися стрибки навантаження, а передавання даних між сегментами стало більш передбачуваним. Зокрема, у Wi-Fi сегменті PPS сплески зменшилися до 35–40 %, що раніше доходили до +300–400 % дані цих порівнянь зображені у табл. 3.5.

Узагальнюючи результати, можна стверджувати, що застосування інтелектуального методу аналізу трафіку дозволило:

- значно стабілізувати роботу найбільш проблемних сегментів мережі;
- зменшити затримку та джиттер;
- збільшити реальну пропускну здатність у адміністративному VLAN;
- знизити навантаження на маршрутизатор і комутатори;
- скоротити кількість аномальних потоків більш ніж у 2.5 рази;
- забезпечити передбачуваність і контрольованість роботи мережі у пікові періоди.

Таблиця 3.5

Порівняння показників до та після оптимізації

Показник	До оптимізації	Після оптимізації
Середня затримка (VLAN 20)	22 мс	11–13 мс
Макс. затримка (VLAN 20)	65–70 мс	30–35 мс
Джиттер	13.4 мс	5.8 мс
Пропускна здатність (VLAN 20)	420 Мбіт/с	480 Мбіт/с
Пікове навантаження CPU	68 %	51–54 %
Dropped packets	3.1 %	0.9 %
Аномальні потоки	2000–3000	900–1200

Таким чином, порівняння показників до та після впровадження ML-підходу підтверджує його високу ефективність та доцільність використання в системах моніторингу та оптимізації локальних комп’ютерних мереж.

3.7. Висновки до розділу 3

У третьому розділі розроблено, реалізовано та експериментально досліджено інтелектуальний підхід до аналізу мережевого трафіку з метою підвищення продуктивності та стабільності локальної комп’ютерної мережі. Отримані результати підтвердили доцільність використання методів машинного та глибинного навчання для виявлення аномалій, прогнозування навантаження й формування обґрунтованих оптимізаційних рішень.

На початковому етапі було виконано аналіз структури досліджуваної мережі, її сегментації та характеристик трафіку, а також сформовано масив вихідних даних обсягом понад 280 тисяч NetFlow-записів і 12,8 мільйона PCAP-пакетів. Після

попередньої обробки, нормалізації та побудови ознак сформовано датасет із 32 інформативних параметрів, що забезпечило ефективне навчання ML-моделей[17].

У межах дослідження протестовано алгоритми XGBoost, RandomForest, IsolationForest та LSTM. Найвищу точність класифікації потоків (до 92 %) продемонструвала модель XGBoost. Алгоритм IsolationForest виявив понад 3100 нетипових потоків у безнаглядному режимі, а модель LSTM забезпечила прогнозування навантаження з точністю 81–86 %, що дало змогу завчасно реагувати на пікові стани мережі.

Важливим практичним результатом стала реалізація алгоритму оптимізації продуктивності, який поєднує класифікацію трафіку, виявлення аномалій, прогнозування навантаження та генерацію рішень щодо пріоритизації, фільтрації й обмеження потоків. Його впровадження забезпечило помітне покращення ключових показників мережі.

Порівняльний аналіз до та після оптимізації показав зниження середньої затримки у VLAN 20 з 22 мс до 11–13 мс, зменшення джитеру більш ніж удвічі, стабілізацію пропускної здатності у VLAN 10 та скорочення broadcast і multicast-трафіку у VLAN 30. Навантаження на процесор маршрутизатора знизилося з 68 % до 51–54 %, а кількість аномальних потоків — у 2–2,5 рази.

Узагальнення результатів підтверджує, що інтеграція інтелектуальних методів у систему моніторингу та управління локальною мережею суттєво підвищує її надійність, адаптивність і стійкість до нестандартних навантажень. Розроблений підхід може бути рекомендований для практичного впровадження у малих і середніх корпоративних мережах та слугувати основою для подальшого розвитку автоматизованих систем моніторингу й реагування.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Тема кваліфікаційної роботи звучить як, «Оптимізація та контроль ефективності функціонування локальної комп'ютерної мережі із застосуванням інтелектуальних методів аналізу трафіку». У роботі розглянуто підходи до підвищення ефективності функціонування системи моніторингу локальної комп'ютерної мережі, що реалізується на окремому сервері та працює у повністю автономному режимі. Така архітектура виключає будь-який вплив системи моніторингу на загальний рівень інформаційної безпеки мережі та користувачів. Разом із тим, серверне обладнання потребує періодичної підтримки та контролю працездатності, що здійснюється адміністратором мережі зі спеціалізованого робочого місця [30].

Основним нормативним документом, що регламентує вимоги з охорони праці при роботі з комп'ютерною технікою, є НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями» [29]. Організація робочих місць у приміщеннях підприємства здійснюється з урахуванням природного та штучного освітлення. Природне освітлення забезпечується через віконні прорізи, що гарантують коефіцієнт освітленості не менше 1,5 %, при орієнтації вікон на північ або північний схід. Штучне освітлення реалізоване за допомогою рівномірно розташованих світильників із люмінесцентними лампами [29].

Приміщення, де експлуатується комп'ютерна техніка, ізольовані від джерел підвищеного шуму та вібрації. Підлогове покриття має матову поверхню з коефіцієнтом відбиття 0,3–0,5, а внутрішнє оздоблення виконано з дифузно-відбивних матеріалів: коефіцієнт відбиття стелі становить 0,7–0,8, стін 0,5–0,6.

Робочі приміщення обладнано аптечками першої медичної допомоги, а щоденне вологе прибирання є обов'язковим. Робочі місця користувачів персональних комп'ютерів повинні відповідати ергономічним вимогам, визначеним НПАОП 0.00-

7.15-18 [29]. Зокрема, висота столу має бути у межах 680–800 мм, ширина 600–1400 мм, глибина 800–1000 мм. Конструкція столу повинна забезпечувати достатній простір для ніг. Робочий стілець повинен бути підйомно-поворотним, із регулюванням висоти, кута нахилу сидіння та спинки [28].

Монітор розташовується на відстані 600–700 мм від очей користувача, а кут спостереження у вертикальній площині не повинен перевищувати +30° відносно нормальної лінії погляду. Електромережа приміщення виконана за магістральною схемою; підводи розеток у центральній частині приміщення прокладено в металевих трубах або гнучких металевих рукавах під знімною підлогою чи в кабельних каналах[28].

Під час експлуатації комп’ютерної техніки дотримуються основні вимоги безпеки: перед початком роботи монітори очищаються від пилу, після завершення роботи комп’ютер та периферійні пристрої відключаються від мережі. У разі аварійної ситуації живлення обладнання припиняється негайно. Забороняється виконувати ремонт або налагодження комп’ютера безпосередньо на робочому місці.

Пожежна безпека приміщень забезпечена відповідно до ДБН В.1.1-7-2016 та ДСТУ Б.В.1.1-36:2016. Дотримані вимоги мікроклімату щодо температури, швидкості руху повітря та відносної вологості. Рівні природного та штучного освітлення відповідають ДБН В.2.5-28-2018[27], а розрахунок коефіцієнта природного освітлення виконано згідно з нормативною методикою. Штучне освітлення реалізоване системою загального рівномірного освітлення з використанням люмінесцентних ламп типу ЛБ [27].

Під час роботи над системою оптимізації та виявлення аномалій трафіку суворо дотримувалися вимоги техніки безпеки [27]:

– не здійснювалися самостійні ремонтні роботи;

– не вносилися зміни у конструкцію апаратного забезпечення;

– використовувалися лише матеріали та обладнання, безпосередньо пов’язані з розробкою системи аналізу трафіку.

Для забезпечення безпечної експлуатації інформаційних технологій дотримано вимог СТУ EN 60950-1:2015 / ДСТУ EN 60950-1:2015 [30], що встановлюють загальні положення щодо безпеки IT-обладнання.

Отже, виконання вимог нормативних документів з охорони праці та техніки безпеки дозволило мінімізувати потенційні ризики впливу комп'ютерної техніки на здоров'я користувача та забезпечило безпечні умови впровадження методів інтелектуального аналізу трафіку у локальних комп'ютерних мережах.

4.2. Безпека в надзвичайних ситуаціях

4.2.1. Оцінка стійкості роботи промислового підприємства до дії світлового випромінювання ядерного вибуху. Оцінка стійкості промислового підприємства до дії світлового випромінювання ядерного вибуху є важливою складовою комплексного аналізу безпеки об'єкта в умовах надзвичайних ситуацій. Ядерний вибух створює низку вражаючих факторів, серед яких для наземних промислових та телекомунікаційних об'єктів найбільш небезпечними є: ударна хвиля, світлове (теплове) випромінювання, вторинні вражаючі фактори, радіоактивне зараження місцевості, а також у деяких випадках проникаюча радіація та електромагнітний імпульс (EMI) [6]. Кожен із цих факторів здатний спричинити суттєві пошкодження інфраструктури, обладнання, інженерних систем та загрожувати життю і здоров'ю персоналу [7].

Критеріями оцінки фізичної стійкості об'єкта є:

1. для ударної хвилі надлишкові тиски, за яких будівлі, споруди та технологічне обладнання не зазнають руйнувань або отримують лише слабкі й середні пошкодження, що можуть бути швидко відновлені [6];
2. для світлового випромінювання максимальні значення світлового імпульсу, що не призводять до займання матеріалів, сировини, конструкцій та виробничого обладнання [6];

3. для вторинних факторів умови, за яких їх дія не спричиняє масштабних аварій, пожеж, вибухів, затоплень та небезпечного зараження атмосфери або території [6].

Світлове випромінювання ядерного вибуху являє собою потужний імпульс електромагнітної енергії, джерелом якого є світна область вибуху вогненна куля з температурою, що сягає до 6000 °С [7]. Випромінювання включає видимі, ультрафіолетові та інфрачервоні промені, при цьому до 85 % енергії світіння виділяється у перші секунди після вибуху. Його уражаюча дія визначається величиною світлового імпульсу, тобто кількістю енергії, що потрапляє на одиницю площі (Дж/м²), та тривалістю дії. Чим інтенсивніший і коротший імпульс, тим сильніший тепловий вплив, здатний спричинити займання матеріалів, опіки людей і вихід з ладу обладнання [7].

Для визначення пожежонебезпечності об’єкта аналізують температуру займання матеріалів, горючість елементів конструкцій, можливість руйнування печей, газопроводів, трансформаторів, кабельних мереж та інших систем, що можуть вплинути на виникнення вторинних пожеж.

Оцінювання стійкості промислового підприємства до світлового випромінювання ядерного вибуху доцільно проводити у такій послідовності [7]:

1. Визначити мінімальну відстань до можливого центру вибуху (Rx), що відповідає прогнозованому сценарію надзвичайної ситуації.

2. Обчислити максимальний можливий світловий імпульс Ісв.max (кДж/м²), який досягне території підприємства залежно від потужності вибуху та умов поширення світлового випромінювання.

3. Оцінити ступінь вогнестійкості будівель та споруд, визначити типи конструкцій, їхню негорючість або здатність до займання.

4. Виявити елементи, виготовлені з горючих матеріалів, визначити їхні параметри займистості (наприклад, дерев’яні двері чи рами, пофарбовані в темний колір, можуть загорятися вже при Ісв = 250 кДж/м²).

5. Визначити граничне значення стійкості Ісв.lim, тобто мінімальний світловий імпульс, за якого може настати загоряння конструкцій чи обладнання.

6. Порівняти Ісв.lim та Ісв.max, якщо Ісв.lim < Ісв.max, об’єкт не стійкий до світлового випромінювання, якщо Ісв.lim > Ісв.max, об’єкт вважається стійким[6].

7. Оцінити ступінь впливу ударної хвилі при максимальному очікуваному надлишковому тиску, який може супроводжувати світловий імпульс.

8. Визначити зону можливих пожеж, у межах якої може опинитися об’єкт, включаючи ризики вторинних загорянь від руйнування мереж, резервуарів, кабельних трас та технологічних установок.

9. Узагальнена оцінка стійкості має визначати, чи може світловий імпульс спричинити пожежну ситуацію, чи потрапляє об’єкт у зону суцільних пожеж, а також чи відповідає його гранична стійкість установленим нормам. Додатково встановлюють, які елементи та системи становлять найбільшу пожежну небезпеку, і роблять висновок щодо доцільності підвищення рівня захисту об’єкта [7].

При необхідності підвищення стійкості підприємства до світлового випромінювання можуть бути застосовані такі заходи [6]: використання негорючих матеріалів у покрівлях і перекриттях (азбестоцемент, залізобетон), заміна дерев’яних конструкцій на металеві, влаштування протипожежних перегородок, підсилення віконних та дверних блоків, нанесення вогнезахисних покриттів, організація ізольованих зон для зберігання легкозаймистих матеріалів, а також проведення регулярних протипожежних заходів і технічного обслуговування виробничих та інженерних систем.

Проведена оцінка дозволяє комплексно визначити рівень стійкості промислового підприємства до дії світлового випромінювання ядерного вибуху, встановити найбільш вразливі елементи будівель і технологічних процесів, спрогнозувати масштаби можливих пошкоджень і пожеж та визначити можливість подальшого функціонування об’єкта [7].

Застосування інженерно-технічних та організаційних заходів дозволяє суттєво знизити ймовірність виникнення критичних ситуацій, мінімізувати ризики для персоналу та забезпечити збереження працездатності об'єкта навіть у разі дії вражаючих факторів ядерного вибуху. Таким чином, розділ 4.2 є важливою

складовою загальної системи оцінювання безпеки підприємства і визначає ключові напрямки підвищення його стійкості в умовах надзвичайних ситуацій [6].

4.3. Висновки до розділу 4

В даному розділі описані актуальні питання щодо безпеки в надзвичайних ситуаціях та охорони праці. Була опрацьована інформація стосовно вимог з охорони праці і техніки безпеки, пожежної та електробезпеки. Також, розглянуті питання щодо стійкості роботи промислового підприємства до дії світлового випромінювання ядерного вибуху

ВИСНОВКИ

У ході виконання кваліфікаційної роботи магістра отримано такі наукові та практичні результати:

1. За допомогою аналізу літератури та наукових джерел було досліджено сучасний стан розвитку систем моніторингу локальних комп’ютерних мереж, методи аналізу мережевого трафіку та підходи до оцінювання ефективності функціонування мереж. Встановлено обмеження традиційних методів контролю, які не забезпечують достатньої адаптивності в умовах динамічних змін трафіку.

2. Проведено аналітичний огляд сучасних інструментів і технологій моніторингу локальних мереж, зокрема потокових протоколів збору даних (NetFlow/IPFIX), систем моніторингу та методів аналізу трафіку, що дозволило обґрунтувати доцільність використання комбінованого підходу до збору даних.

3. Розглянуті алгоритми машинного навчання для класифікації мережевого трафіку та виявлення аномалій, включаючи дерева рішень, випадкові ліси, алгоритми кластеризації, ізоляційні ліси та нейронні мережі типу LSTM, і визначено їх придатність для застосування в задачах оптимізації локальних мереж.

4. Визначено необхідність застосування інтелектуальних методів аналізу трафіку для переходу від реактивного до проактивного управління мережевими ресурсами, що дозволяє своєчасно виявляти перевантаження, аномальні потоки та приховані проблеми у функціонуванні мережі.

5. Здійснено обчислювальний експеримент, у межах якого було сформовано експериментальний стенд, зібрано реальні та модельовані дані мережевого трафіку, підготовлено навчальні вибірки та виконано навчання і тестування моделей машинного навчання.

6. На основі отриманих результатів аналізу розроблено алгоритм інтелектуальної оптимізації продуктивності локальної мережі, який використовує результати ML-моделі для формування керуючих дій, спрямованих на зменшення затримок, балансування навантаження та підвищення стабільності мережі.

7. Проведено налаштування мережевих параметрів і оптимізаційних механізмів, включаючи пріоритезацію трафіку, керування пропускною здатністю, сегментацію мережі та автоматизоване застосування правил оптимізації на мережевому обладнанні.

8. Проведено підключення системи збору та аналізу трафіку до реальної локальної комп’ютерної мережі з використанням потокових протоколів, засобів пакетного аналізу та системи моніторингу, що забезпечило безперервне отримання актуальних даних для аналізу.

9. Отримані практичні висновки підтверджують, що застосування інтелектуального методу аналізу трафіку дозволяє підвищити ефективність функціонування локальної мережі, зменшити кількість перевантажень, скоротити затримки передачі даних і підвищити стабільність роботи сервісів.

Усі наведені результати підтверджують висунуту гіпотезу, повне досягнення мети магістерської роботи та виконання поставлених завдань дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Луцик Н.С., Луцків А.М., Осухівська Г.М., Тиш Є.В. Програма та методичні рекомендації з проходження практики за тематикою кваліфікаційної роботи для студентів спеціальності 123 «Комп'ютерна інженерія» другого (магістерського) рівня вищої освіти усіх форм навчання. Тернопіль: ТНТУ. 2024. 45 с

2. Луцик Н.С., Луцків А.М., Осухівська Г.М., Тиш Є.В. Методичні рекомендації до виконання кваліфікаційної роботи магістра для студентів спеціальності 123 «Комп'ютерна інженерія» другого (магістерського) рівня вищої освіти усіх форм навчання. Тернопіль. 2024. 44 с.

3. Варавін А.В., Лещишин Ю.З., Чайковський А.В. Методичні вказівки до виконання курсового проєкту з дисципліни «Дослідження і проєктування комп'ютерних систем та мереж» для здобувачів другого (магістерського) рівня вищої освіти спеціальності 123 «Комп'ютерна інженерія» усіх форм навчання. Тернопіль: ТНТУ, 2024. 32 с.

4. Тиш Є.В., Семанюк В.М, Аналіз сучасних підходів до моніторингу локальних комп'ютерних мереж та оцінювання їх ефективності . Матеріали XIII науково-технічної конференції «Інформаційні моделі системи та технології» (17-18 грудня 2025 року). Тернопіль: ТНТУ. 2025. С. 150.

5. Тиш Є.В., Семанюк В.М, Структурні особливості локальних комп'ютерних мереж та фактори, що впливають на їхню продуктивність. Матеріали XIII науково-технічної конференції «Інформаційні моделі системи та технології» (17-18 грудня 2025 року). Тернопіль: ТНТУ. 2025. С. 151.

6. Стручок В.С. Методичний посібник для здобувачів освітнього ступеня «магістр» всіх спеціальностей денної та заочної (дистанційної) форм навчання «Безпека в надзвичайних ситуаціях». Тернопіль: ФОП Паляниця В. А. 156 с.

7. Стручок В.С. Навчальний посібник «Техноекологія та цивільна безпека. Частина «цивільна безпека»». Тернопіль: ФОП Паляниця В. А. 156 с.

8. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В. Комп'ютерні мережі. Книга 1. Львів, «Магнолія 2006». 2013. 256 с.

9. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В Комп’ютерні мережі. Книга 2. Львів, «Магнолія 2006», 2014. 312 с.

10. Яцишин В.В., Демиденко А.О., Яцишин Вік.В. Підходи до виявлення аномалій трафіку у комп’ютерних мережах. Матеріали XIII міжнародної науково - технічної конференції молодих учених і студентів «Актуальні задачі сучасних технологій» (11-12 грудня 2024 р.) Тернопільського національного технічного університету імені Івана Пулюя. Тернопіль: ТНТУ. 2024. С. 520.

11. Яцишин В.В., Демиденко А.О., Яцишин Вік.В. Логістична регресія в задачах виявлення аномалій трафіку комп’ютерних мереж. Матеріали XII науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» (18-19 грудня 2024 року). Тернопіль: ТНТУ. 2024. С. 149.

12. Лупенко С.А. , Пасічник В.В. , Тиш Є.В. Комп’ютерна логіка. Навчальний посібник. Львів: Видавництво “Магнолія - 2006”, 2024. 354 с.

13. Osukhivska H., Lobur T., Shylinska I., Lupenko S., Tysh Ie. Method for Estimating the Convergence Parameters of Dynamic Routing Protocols in Computer Networks. IEEE 16th International Conference on Computer Science and Information Technologies. Lviv. 2021.

14. Tysh Ie. Approach And Method Of Evaluation Of The General Reliability Indicator Of Computer Systems. International Scientific Journal Computer Systems And Information Technologies. Khmelnytskyi : Khmelnytskyi National University №3. 2021.P.74-80.

15. Моніторинг і аналіз локальних мереж. URL: http://ni.biz.ua/10/10_19/10_190257_v-o-p-r-o-s---momenti-inertsii-secheniy-prostih-form.html (Дата звернення 24.11.2025).

16. Cisco Systems. Network monitoring and management overview. Cisco Networking Solutions. https://www.cisco.com/c/en/us/solutions/ enterprisenetworks /network-management.html (Дата звернення: 19.11.2025).

17. Cisco Systems. NetFlow technology: Overview and configuration. Cisco IOS Software Documentation. https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html (Дата звернення: 20.11.2025).

18. Claise B., Trammell B., Aitken P. Specification of the IP Flow Information Export (IPFIX) Protocol. RFC 7011, Internet Engineering Task Force, 2013. https://datatracker.ietf.org/doc/html/rfc7011 (Accessed: 21.11.2025).

19. Paessler AG. Network monitoring using SNMP, flow and packet analysis. Paessler Knowledge Base. https://www.paessler.com/network_monitoring (Дата звернення: 20.11.2025).

20. SolarWinds Worldwide, LLC. Network performance monitoring fundamentals. SolarWinds IT Resources. https://www.solarwinds.com/resources/it-glossary/network-performance-monitoring (Дата звернення: 17.11.2025).

21. Cloudflare, Inc. What is network traffic analysis? Cloudflare Learning Center. https://www.cloudflare.com/learning/network-layer/what-is-network-traffic-analysis/ (Accessed: 10.12.2025).

22. Zabbix LLC. Network monitoring concepts and methods**.** Zabbix Documentation.https://www.zabbix.com/documentation/current/en/manual/network_monitoring (Дата звернення: 18.11.2025).

23. Моніторинг мережі. Протоколи, найкращі практики, інструменти 2021. URL: https://eska.global/blog/setevoj-monitoring-protokoly-luchshie-praktiki-instrumenty-2020 (Дата звернення 19.11.2025).

24. Простий протокол мережевого управління (SNMP). URL: https://cqr.company/ua/wiki/protocols/simple-network-management-protocol-snmp/ (Дата звернення 9.12.2025).

25. Документація Zabbix. URL:https://www.zabbix.com/documentation/current/ua (Дата звернення 02.12.2025).

26. Golovko, V.A. Deep learning: an overview and main paradigms. Optical Memory and Neural Networks (Information Optics). Vol. 26, № 1. 2017. pp. 1–17.

27. ДБН П.1.2-2:2016 Система забезпечення надійності та безпеки будівельних об'єктів. Навантаження і впливи. Нормипроектування –К.: МінбудУкраїни, 2006- 75с.

28. Наказ Держнаглядохоронпраці від 09.01.98 N 4, зареєстрованих у Міністерстві юстиції України 10.02.98 за N 93/2533 (НПАОП 40.1-1.21-98).

29. НПАОП 0.00-7.15-18. Правила роботи з комп’ютерними мережами та технічними засобами зв’язку. Національний стандарт України. Київ : Держпраці, 2018

30. СТУ EN 60950-1:2015. Інформаційні технології — Обладнання IT — Частина 1: Загальні вимоги безпеки. Державний технічний регламент. Київ : ДП «Укрметртестстандарт», 2015.

Додаток А

Тези конференцій

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XIII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

17-18 грудня 2025 року

ТЕРНОПІЛЬ
2025

УДК: 004.7:004.415.2
В. Семанюк; Є. Тиш, к. т. н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО МОНІТОРИНГУ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ ТА ОЦІНЮВАННЯ ЇХ ЕФЕКТИВНОСТІ

UDC: 004.7:004.415.2
V. Semaniuk; Ie. Tysh, PhD.

ANALYSIS OF MODERN APPROACHES TO LOCAL COMPUTER NETWORK MONITORING AND EVALUATION OF THEIR EFFICIENCY

Стрімка цифровізація бізнес-процесів, розвиток хмарної інфраструктури та зростання обсягів мережевого трафіку спричиняють підвищені вимоги до контролю стану локальних комп'ютерних мереж. У цих умовах традиційні підходи до технічного нагляду вже не забезпечують необхідного рівня видимості мережевих процесів. Сучасні організації потребують не лише швидкого виявлення збоїв, а й глибокого інтелектуального аналізу подій для забезпечення безперервності сервісів. Моніторинг мереж перетворюється із базового технічного завдання на комплексний процес оцінювання ефективності роботи інфраструктури, що охоплює продуктивність, надійність, безпеку та прогнозування навантаження.

Традиційні інструменти спостереження – SNMP-моніторинг, RMON-аналізатори, лог-агрегація – залишаються основою контролю параметрів мережевих пристроїв. Вони забезпечують базову діагностику, яка лишається актуальною у невеликих та стабільних мережах. Проте їх можливості обмежені лише фіксацією станів та подій. На зміну їм приходять інтегровані платформи моніторингу нового покоління: Zabbix, PRTG, Nagios, SolarWinds, які підтримують автоматизоване виявлення вузлів, кореляцію інцидентів, аналітику SLA та адаптивні порогові значення. Завдяки модульній структурі ці системи легко масштабуються та доповнюються новими функціональними компонентами. Поєднання телеметрії з різнорівневих джерел формує єдиний інформаційний простір для прийняття управлінських рішень. Більш того, такі платформи дедалі частіше інтегруються з сервісами хмарних провайдерів, що спрощує управління гібридними інфраструктурами. Це дозволяє зменшити операційні витрати та підвищити узгодженість обробки даних.

Подальший розвиток забезпечують інтелектуальні технології – машинне навчання, системи виявлення аномалій та прогнозні моделі навантаження. Вони дозволяють не лише розпізнавати нетипові патерни трафіку, але й завчасно визначати критичні точки, моделювати поведінку мережі та оптимізувати розподіл ресурсів. Алгоритми глибинного навчання дедалі частіше застосовуються для аналізу потоків даних у реальному часі, що підвищує точність прогнозування інцидентів. Такий підхід підвищує рівень кіберстійкості, мінімізує ризики простоїв та сприяє ефективному масштабуванню інфраструктури.

Комплексний аналіз сучасних підходів свідчить про перехід від реактивного моніторингу до проактивного управління мережею. Оцінювання ефективності локальних мереж сьогодні базується не лише на класичних метриках (завантаження каналів, затримки, помилки), а й на інтелектуальних показниках: узгодженості трафіку, рівні аномальності, прогнозованому ризику збоїв. Такі метрики дозволяють точніше формувати профілі нормальної поведінки мережі та оперативно реагувати на відхилення. Таким чином, сучасні мережі потребують адаптивних систем контролю, здатних інтегрувати телеметрію, аналітику та автоматизацію для забезпечення максимальної продуктивності та стабільності роботи.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XIII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

17-18 грудня 2025 року

ТЕРНОПІЛЬ
2025

УДК: 004.7:004.421.2
В. Семанюк; Є. Тиш, к. т. н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СТРУКТУРНІ ОСОБЛИВОСТІ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ ТА ФАКТОРИ, ЩО ВПЛИВАЮТЬ НА ЇХНЮ ПРОДУКТИВНІСТЬ

UDC: 004.7:004.421.2
V. Semaniuk; Ie. Tysh, PhD.

STRUCTURAL FEATURES OF LOCAL COMPUTER NETWORKS AND FACTORS AFFECTING THEIR PERFORMANCE

Локальні комп'ютерні мережі (ЛКМ) посідають ключове місце в інфраструктурі сучасних організацій, забезпечуючи швидкий обмін даними, доступ до корпоративних ресурсів та підтримку критично важливих сервісів. Із зростанням обсягів трафіку, появою хмарних застосунків та високими вимогами до безпеки значно ускладнюється побудова оптимальної мережевої архітектури. Її якість визначається не лише фізичною структурою, але й комплексом технологічних та організаційних факторів, які безпосередньо впливають на продуктивність, масштабованість та надійність ЛКМ. Зростання популярності віртуалізації мережевих функцій (NFV) та програмно-конфігурованих мереж (SDN) також змінює традиційні підходи до проєктування таких систем. Це забезпечує більшу гнучкість та можливість централізованого керування мережевими політиками.

Структурні особливості локальної мережі формуються на основі вибору топології (зірка, дерево, шина тощо), принципів сегментації, типів кабельної системи, характеристик активного обладнання та особливостей внутрішньої комутаційної архітектури (комутаційної фабрики). Відповідність цих елементів реальним вимогам бізнес-процесів визначає здатність мережі ефективно обробляти трафік та мінімізувати затримки. Важливим чинником залишається якість комутаційної інфраструктури: пропускна здатність портів, підтримка апаратного QoS, наявність механізмів ізоляції трафіку (VLAN, VRF) та можливості апаратного прискорення маршрутизації. Не менш важливою є оптимальна адресація IPv4/IPv6, яка впливає на ефективність маршрутизації та стійкість мережі до розширення. Крім того, правильна сегментація дозволяє зменшити рівень широкомовного трафіку та підвищити загальну продуктивність мережі.

На продуктивність ЛКМ впливають також зовнішні фактори: рівень кіберзагроз, інтенсивність сервісного навантаження, коректність конфігурації маршрутизаторів і комутаторів, а також застосування систем моніторингу (SNMP, NetFlow, Zabbix, Prometheus), які дають змогу оперативно виявляти аномалії та запобігати деградації мережі. Ключовим аспектом є дотримання принципів високої доступності та відмовостійкості – резервування каналів, балансування навантаження, використання протоколів STP/RSTP/MSTP та механізмів швидкого переключення. Порушення цих принципів може призвести до значних простоїв та втрати критично важливих даних. Водночас правильна політика безпеки, включно із застосуванням міжмережевих екранів та систем IDS/IPS, суттєво знижує ризики несанкціонованого доступу та внутрішніх інцидентів.

З урахуванням розвитку інтелектуальних технологій зростає роль автоматизованого аналізу трафіку, прогнозування навантажень та застосування машинного навчання для оцінювання ефективності мережевої інфраструктури. Такий підхід забезпечує не лише стабільність роботи ЛКМ, а й можливість її проактивної оптимізації відповідно до змін у цифровому середовищі. У перспективі очікується інтеграція локальних мереж із системами автономного керування, що дозволить динамічно адаптувати параметри мережі до умов у реальному часі. Це відкриває шлях до побудови самокерованих мереж (Self-Driving Networks), які мінімізують втручання адміністратора та підвищують загальну ефективність інфраструктури.