Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Моделі та методи прогнозування трафіку в корпоративній мережі

(тема)

Виконав:
здобувач 2 року навчання,
групи СПм-23-4
Олександр КОРОБЄЙНІКОВ
(власне ім'я, прізвище)

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

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

Освітня програма
Системне програмування
(повна назва освітньої програми)

Керівник: зав. каф. Андрій КОВАЛЕНКО
(посада, власне ім'я, прізвище)

Допускається до захисту

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

2025 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

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

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

Освітня програма Системне програмування
(повна назва)

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

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Коробєйнікову Олександру Борисовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Моделі та методи прогнозування трафіку в корпоративній мережі

затверджена наказом по університету від "21" квітня 2025 р. № 296 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 16 червня 2025 р.

3. Вхідні дані до роботи
корпоративна мережа
трафік
призначення завдання
Мережі Петрі

4. Перелік питань, що потрібно опрацювати у роботі
Аналіз сучасних методів прогнозування трафіку в корпоративних мережах
Теоретичні основи мереж Петрі для моделювання та прогнозування трафіку
Розробка моделей прогнозування трафіку на основі мереж Петрі
Практична реалізація та апробація моделей прогнозування

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій 16 слайдів

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

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

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
1	Отримання завдання та аналіз літератури	21.04.2025–29.04.2025	
2	Огляд існуючих моделей та методів	30.04.2025–11.05.2025	
3	Розробка методу	12.05.2025–22.05.2025	
4	Вибір програмних засобів	23.05.2025–30.05.2025	
5	Програмна реалізація	31.05.2025–02.06.2025	
6	Аналіз отриманих результатів	03.06.2025–05.06.2025	
7	Оформлення записки	06.06.2025–14.06.2025	

Дата видачі завдання " 21 " квітня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ зав. каф. Андрій КОВАЛЕНКО
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 68 с., 16 рис., 2 дод., 9 джерел.

МЕРЕЖА ПЕТРІ, ПРОГНОЗУВАННЯ ТРАФІКУ, КОЛЬОРОВА МЕРЕЖА ПЕТРІ, ШТУЧНА НЕЙРОННА МЕРЕЖА, СИМУЛЯЦІЙНЕ МОДЕЛЮВАННЯ, ІНТЕЛЕКТУАЛЬНІ АЛГОРИТМИ, УПРАВЛІННЯ НАВАНТАЖЕННЯМ, СТРУКТУРНЕ МОДЕЛЮВАННЯ, ПОВЕДІНКОВИЙ АНАЛІЗ, МАШИННЕ НАВЧАННЯ, АНАЛІТИКА ТРАФІКУ.

Метою кваліфікаційної роботи є розробка та апробація формальних моделей прогнозування трафіку, які дозволяють моделювати динамічні процеси в мережі з урахуванням їхньої паралельної, розподіленої та стохастичної природи. Для досягнення поставленої мети в роботі виконано аналіз існуючих підходів до прогнозування трафіку, виявлено їхні сильні та слабкі сторони, а також досліджено можливості використання мереж Петрі як інструменту структурного і поведінкового моделювання мережевих процесів.

У ході виконання кваліфікаційної роботи розроблено кілька варіантів мереж Петрі, у тому числі кольорові та розширені, які відображають маршрутизацію, балансування навантаження, фільтрацію запитів і взаємодію з підсистемами моніторингу та логування. Реалізовано симуляційне середовище з візуалізацією потоків, побудоване за допомогою Python та бібліотеки graphviz.

Для прогнозування використано як класичні методи (лінійна регресія, ковзне середнє), так і інтелектуальні моделі – зокрема штучні нейронні мережі типу MLP. Проведено порівняльний аналіз точності моделей на прикладах трьох типів трафіку: нормального, пікового та шумового.

ABSTRACT

Master’s thesis: 68 pages, 16 figures, 2 appendices, 9 sources.

PETRI NET, TRAFFIC FORECASTING, COLORED PETRI NET, ARTIFICIAL NEURAL NETWORK, SIMULATION MODELING, INTELLIGENT ALGORITHMS, LOAD MANAGEMENT, STRUCTURAL MODELING, BEHAVIORAL ANALYSIS, MACHINE LEARNING, TRAFFIC ANALYTICS.

The major goal of this thesis is the development and validation of formal traffic forecasting models that enable the simulation of dynamic network processes, considering their parallel, distributed, and stochastic nature. To achieve this objective, the study analyzes existing traffic prediction approaches, identifies their strengths and limitations, and investigates the applicability of Petri nets as a tool for structural and behavioral modeling of networked systems.

In order to several Petri net configurations were designed, including colored and extended variants that represent routing, load balancing, request filtering, and interaction with monitoring and logging subsystems. A simulation environment with traffic flow visualization was implemented using Python and the Graphviz library.

For forecasting purposes, both classical methods (linear regression, moving average) and intelligent models – specifically multilayer perceptron (MLP) neural networks – were applied. A comparative accuracy analysis of the models was conducted on three types of traffic: normal, peak, and noisy. The results demonstrate the effectiveness of combining formal modeling (Petri nets) with predictive algorithms to build an adaptive analytical system for supporting decision-making in telecommunications.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

AI – штучний інтелект

ANN – штучна нейронна мережа

API – інтерфейс прикладного програмування

CPN – кольорова мережа Петрі

EDA – розвідковий аналіз даних

FTP – протокол передавання файлів

HTTP – протокол передавання гіпертексту

IDS – система виявлення вторгнень

LSTM – довготривала короткочасна пам’ять (тип нейромережі)

MAE – середня абсолютна похибка

ML – машинне навчання

MLP – багатошаровий персептрон

MSE – середньоквадратична похибка

RMSE – корінь з середньоквадратичної похибки

SOC – центр операцій безпеки

ВСТУП

Сучасні корпоративні мережі є складними інформаційними системами, які характеризуються інтенсивним потоком даних та високими вимогами до якості й стабільності зв'язку. Ефективне управління трафіком у таких мережах відіграє ключову роль у забезпеченні їх безперебійної роботи, швидкості обробки інформації та задоволенні потреб користувачів. Зростання обсягів даних, зумовлене розвитком інформаційних технологій, створює додаткові виклики щодо прогнозування мережевого трафіку, вимагаючи вдосконалення методів і моделей прогнозування.

Актуальність дослідження зумовлена необхідністю розробки ефективних механізмів, здатних адаптивно реагувати на зміни трафіку та забезпечувати оптимальний режим функціонування корпоративних мереж. Особливо актуальним є використання формальних методів моделювання, таких як мережі Петрі, що дозволяють адекватно відображати складні системні взаємодії і забезпечують точні прогнози динаміки трафіку.

Метою роботи є розробка моделей і методів прогнозування трафіку у корпоративній мережі з використанням апарату мереж Петрі, а також їх практична апробація.

Для досягнення поставленої мети були визначені такі завдання:

- аналіз існуючих методів прогнозування трафіку;
- дослідження теоретичних основ мереж Петрі;
- розробка моделей на основі мереж Петрі для прогнозування трафіку;
- експериментальна перевірка запропонованих моделей і оцінка їх ефективності.

Об'єкт дослідження – процес управління трафіком у корпоративних мережах.

Предмет дослідження – моделі та методи прогнозування трафіку з використанням мереж Петрі.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

Корпоративні мережі є складними телекомунікаційними структурами, що створюються для підтримки інформаційної взаємодії між різними підрозділами однієї організації. Вони забезпечують внутрішній обмін даними, доступ до сервісів, централізоване зберігання інформації та координацію бізнес-процесів. Основними характеристиками корпоративних мереж є багаторівнева архітектура, різноманіття пристроїв і сервісів, значні обсяги трафіку та висока залежність від стабільності їх функціонування. Мережі такого типу, як правило, включають локальні та глобальні сегменти, з’єднані між собою через маршрутизатори, комутатори, шлюзи та інші вузлові пристрої. Це дозволяє інтегрувати в єдину інфраструктуру як центральні офіси, так і віддалені філії, забезпечуючи гнучкість та масштабованість системи.

Однією з головних особливостей корпоративного трафіку є його різнорідність та динамічність. У таких мережах одночасно циркулює великий обсяг інформації різного типу – від текстових повідомлень до потокового відео, від транзакцій баз даних до сеансів відеоконференцій. Частота, обсяг і природа цього трафіку можуть суттєво змінюватися залежно від часу доби, дня тижня або сезонних навантажень. Крім того, робота деяких бізнес-додатків генерує непередбачуване імпульсне навантаження, що значно ускладнює планування та управління пропускною здатністю мережі.

У таких умовах особливої актуальності набуває ефективне управління трафіком, що передбачає не лише моніторинг поточного стану мережі, але й здатність прогнозувати зміни навантаження, оптимізувати маршрутизацію, забезпечувати пріоритетність критичних сервісів та захищати систему від зовнішніх і внутрішніх загроз. Моніторинг передбачає безперервне відстеження параметрів трафіку, виявлення аномалій та вузьких місць у мережі. Прогнозування трафіку, у свою чергу, дозволяє заздалегідь виявити

потенційні перевантаження та вжити заходів для забезпечення стійкої роботи системи.

Одним з ключових напрямів управління трафіком є реалізація механізмів якості обслуговування (QoS), які дозволяють розмежовувати трафік за пріоритетами та гарантувати необхідний рівень сервісу для критично важливих додатків. Сюди ж належить і балансування навантаження, яке забезпечує рівномірний розподіл інформаційних потоків між різними елементами інфраструктури. Ще одним важливим аспектом є інтеграція засобів управління трафіком із системами інформаційної безпеки. У сучасних умовах, коли мережі є об'єктами постійних загроз, своєчасне виявлення та блокування шкідливих дій у мережевому трафіку є життєво необхідним для забезпечення цілісності та конфіденційності даних.

Таким чином, корпоративні мережі виступають як складні та динамічні системи, ефективне управління якими неможливе без точного моніторингу та прогнозування трафіку. Саме ці процеси дозволяють підтримувати високий рівень надійності, стабільності та безпеки інформаційної інфраструктури підприємства.

1.1 Особливості корпоративних мереж та вимоги до управління трафіком

Корпоративні мережі – це приватні телекомунікаційні системи, що об'єднують різні ресурси та користувачів в межах однієї організації або підприємства. Основною метою таких мереж є забезпечення надійного, безпечного та ефективного обміну даними між усіма структурними підрозділами організації.

Особливості корпоративних мереж:

- ієрархічна структура: включає декілька рівнів – від периферійних пристроїв до центральних вузлів обробки;

- інтенсивність трафіку: залежить від робочих процесів, взаємодії сервісів, резервного копіювання, хмарних рішень;

- висока вимогливість до надійності та безпеки: через критичність даних, які передаються мережею;

- різноманіття протоколів та служб: підтримка IP-телефонії, відеоконференцій, роботи з базами даних тощо.

Динамічне навантаження: трафік може змінюватися в залежності від часу доби, днів тижня, сезону або подій.

Управління трафіком у корпоративній мережі передбачає:

- моніторинг: постійне відстеження обсягів трафіку, виявлення аномалій;

- прогнозування: передбачення навантаження для своєчасного масштабування ресурсів;

- маршрутизація та балансування: забезпечення рівномірного розподілу навантаження;

- пріоритезація: виділення критично важливих потоків для безперебійної роботи.

Політики безпеки: контроль доступу, шифрування, захист від атак.

Ефективне управління трафіком дає змогу уникнути перевантаження мережі, зменшити затримки, підвищити якість обслуговування (QoS) та забезпечити високий рівень обслуговування кінцевих користувачів.

1.1.1 Складна багаторівнева архітектура

Однією з фундаментальних характеристик корпоративних мереж є їх складна багаторівнева архітектура, яка забезпечує логічну організацію та ефективне функціонування інформаційних потоків у межах великої та розгалуженої інфраструктури. Така архітектура формується з урахуванням масштабів організації, територіальної розгалуженості її структурних

підрозділів, типів застосовуваних сервісів, а також вимог до продуктивності, безпеки та відмовостійкості мережі.

Багаторівнева архітектура, як правило, передбачає розподіл мережевої інфраструктури на три основні рівні: рівень доступу, рівень агрегації (або рівень розподілу) та ядро мережі. Рівень доступу відповідає за підключення кінцевих пристроїв користувачів – робочих станцій, принтерів, точок бездротового доступу, IP-телефонів тощо. На цьому рівні реалізуються базові функції мережевого з’єднання та обмежене фільтрування трафіку. Особливістю цього рівня є велика кількість портів та необхідність забезпечення масштабованості в умовах зростання кількості пристроїв.

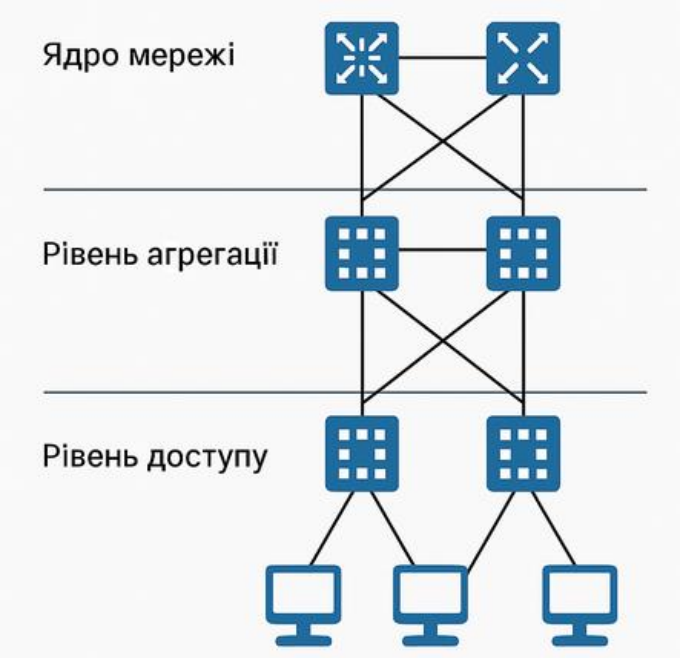


Рисунок 1.1 – Схема багаторівневої архітектури корпоративної мережі

Рівень агрегації виконує функцію об'єднання трафіку, що надходить з рівня доступу, та його маршрутизацію до ядра мережі. Тут зосереджено комутатори або маршрутизатори, що забезпечують міжмережеву маршрутизацію, політики безпеки, балансування навантаження та фільтрацію на рівні підмереж. Цей рівень також часто виступає точкою інтеграції з мережевими сервісами, зокрема із системами автентифікації, моніторингу, контролю доступу тощо.

Ядро мережі – це центральний рівень, через який проходять основні потоки інформації. Воно забезпечує високошвидкісне з'єднання між географічно рознесеними сегментами мережі, дата-центрами, інтернет-шлюзами та іншими критичними ресурсами. Від надійності та продуктивності цього рівня залежить загальна ефективність функціонування всієї мережевої інфраструктури. На цьому рівні зазвичай застосовуються потужні маршрутизатори, здатні обробляти великі обсяги трафіку з мінімальними затримками.

Таке багаторівневе структурування дозволяє розподіляти функції управління мережею, локалізувати можливі точки відмови, забезпечувати масштабованість та підвищену безпеку. Завдяки цьому, підприємство має змогу ефективно керувати як окремими сегментами мережі, так і всією інфраструктурою в цілому, адаптуючи її до змін організаційної структури або технологічних вимог.

Рисунок 1.1 ілюструє типову трирівневу архітектуру корпоративної мережі, поділену на три основні рівні:

- рівень доступу (Access Layer) – найнижчий рівень, до якого підключаються кінцеві пристрої користувачів (наприклад, комп’ютери, принтери, Wi-Fi точки). Тут забезпечується початковий мережевий зв’язок;
- рівень агрегації (або розподілу) – проміжний рівень, який збирає трафік з декількох вузлів рівня доступу та передає його до ядра. Тут здійснюється маршрутизація, фільтрація трафіку, політики безпеки та балансування навантаження;
- ядро мережі (Core Layer) – центральний рівень, який об'єднує всі сегменти мережі і відповідає за швидке та надійне пересилання трафіку між великими частинами інфраструктури, а також за зв’язок із зовнішнім світом (Інтернетом або іншими дата-центрами).

Зв'язки між рівнями показані лініями, що символізують канали передачі даних. Така архітектура дозволяє масштабувати мережу, забезпечує гнучкість, резервування та централізоване управління.

1.1.2 Гетерогенність пристроїв

Іншою визначальною особливістю корпоративних мереж є їх гетерогенність, що проявляється як у різноманітності апаратного забезпечення, так і в багатстві використаних комунікаційних протоколів. У межах однієї корпоративної мережі можуть взаємодіяти пристрої, що суттєво відрізняються за функціональним призначенням, архітектурою, обчислювальними ресурсами та програмним забезпеченням. Це включає як стандартні кінцеві пристрої (персональні комп'ютери, ноутбуки, мобільні телефони), так і сервери, маршрутизатори, комутатори, брандмауери, точки бездротового доступу, IP-телефони, камери відеоспостереження, а також спеціалізоване обладнання, наприклад, контролери мережевого доступу або пристрої для балансування навантаження.

Гетерогенність виникає не лише внаслідок різниці у виробниках чи моделях пристроїв, а й через інтеграцію різних підсистем, що виконують специфічні функції – наприклад, сервери додатків, системи керування базами даних, сховища даних, служби каталогів, платформи віртуалізації та хмарні сервіси. Водночас, мережа повинна забезпечувати їхню сумісну роботу, незалежно від використовуваних операційних систем або апаратних платформ. Це вимагає підтримки широкого спектра протоколів передачі даних, як-от TCP/IP, UDP, ICMP, SNMP, FTP, HTTP/HTTPS, SIP, VoIP, SMB, а також протоколів керування мережею та безпекою.

Крім того, до складу корпоративної мережі дедалі частіше включаються пристрої Інтернету речей (IoT), які мають обмежені ресурси, використовують власні, нестандартні протоколи комунікації та потребують специфічних механізмів автентифікації і захисту даних. Наявність таких пристроїв ще більше ускладнює процес забезпечення узгодженого функціонування всієї інфраструктури.

Управління гетерогенною мережею вимагає від IT-фахівців комплексного підходу, що охоплює стандартизацію мережевих конфігурацій,

централізоване управління пристроями, інтеграцію засобів моніторингу, уніфікацію політик безпеки та підтримку протоколів взаємодії між різними мережевими компонентами. Особливо важливим є використання протоколів автоматичного виявлення та конфігурації (наприклад, LLDP, CDP), а також платформ централізованого адміністрування, які дозволяють управляти великою кількістю різнорідних пристроїв із єдиного інтерфейсу.

1.1.3 Різнорідність трафіку

Різнорідність трафіку є однією з ключових характеристик корпоративного мережевого середовища, яка суттєво впливає на проектування, адміністрування та оптимізацію інформаційної інфраструктури. Під цим поняттям розуміється наявність у мережі інформаційних потоків, що відрізняються за структурою, призначенням, обсягом, характером передачі даних, чутливістю до затримок, а також вимогами до пропускної здатності та надійності.

У корпоративній мережі одночасно функціонують численні служби та сервіси, які генерують різні типи трафіку. Серед них – звичайні офісні додатки (електронна пошта, веб-доступ, документообіг), сервіси взаємодії з клієнтами (CRM-системи, кол-центри), системи корпоративного управління (ERP), платформи аналітики, бази даних, хмарні сервіси, служби резервного копіювання, VoIP, відеоконференцзв’язок, а також мультимедійний контент. Кожен із цих видів трафіку має специфічні технічні вимоги: наприклад, трафік відеоконференцій критично залежить від затримок і втрати пакетів, тоді як резервне копіювання може бути нечутливим до затримок, але споживає значну пропускну здатність.

Крім того, характер трафіку в корпоративній мережі може бути як постійним, так і імпульсним. Постійний трафік генерується системами моніторингу, синхронізації або безперервного збору даних, тоді як імпульсний виникає під час запуску звітів, оновлення програмного

забезпечення, проведення масових трансакцій або резервного копіювання. Раптові піки трафіку можуть спричинити перевантаження мережі, зниження якості сервісу або відмову у доступі до ресурсів.

Ще одним аспектом різнорідності є наявність внутрішнього та зовнішнього трафіку. Внутрішній трафік циркулює між підрозділами підприємства та внутрішніми сервісами, тоді як зовнішній – надходить від або надсилається до клієнтів, партнерів, віддалених працівників або хмарних платформ. Управління зовнішнім трафіком додатково ускладнюється вимогами до безпеки, контролю доступу та шифрування.

Забезпечення ефективної обробки різнорідного трафіку вимагає впровадження механізмів розмежування, класифікації та пріоритезації потоків. Зокрема, реалізація політик якості обслуговування (QoS) дозволяє гарантувати відповідні ресурси для критичних додатків, уникати конфліктів за пропускну здатність та зменшувати негативний вплив низькопріоритетних служб на загальну продуктивність мережі.

У підсумку, різнорідність трафіку відображає багатофункціональність корпоративної мережі та потребує комплексного підходу до її управління, що базується на аналізі типів трафіку, динаміки його зміни, взаємозв’язку з бізнес-процесами та сучасних технічних засобах його контролю і оптимізації.

1.1.4 Динамічні зміни навантаження

Динамічні зміни навантаження є невід’ємною властивістю корпоративного мережевого середовища, яка відображає змінність обсягів та інтенсивності передачі даних у межах інфраструктури в залежності від ряду зовнішніх і внутрішніх факторів. Ця змінність може мати як передбачуваний, так і непередбачуваний характер, що суттєво ускладнює процеси планування, управління ресурсами та забезпечення стабільної якості обслуговування користувачів.

Передбачувані коливання навантаження зазвичай пов’язані з добовими, тижневими або сезонними ритмами функціонування підприємства. Наприклад, у більшості офісів спостерігається інтенсивне використання мережі у ранкові та післяобідні години, коли працівники активно обмінюються документами, підключаються до корпоративних сервісів, проводять відеозустрічі або взаємодіють із базами даних. У позаробочий час, навпаки, мережеве навантаження суттєво знижується. Аналогічно, у деяких галузях можуть фіксуватись пікові навантаження у певні періоди року – наприклад, під час податкової звітності, маркетингових кампаній чи сезонних розпродажів.

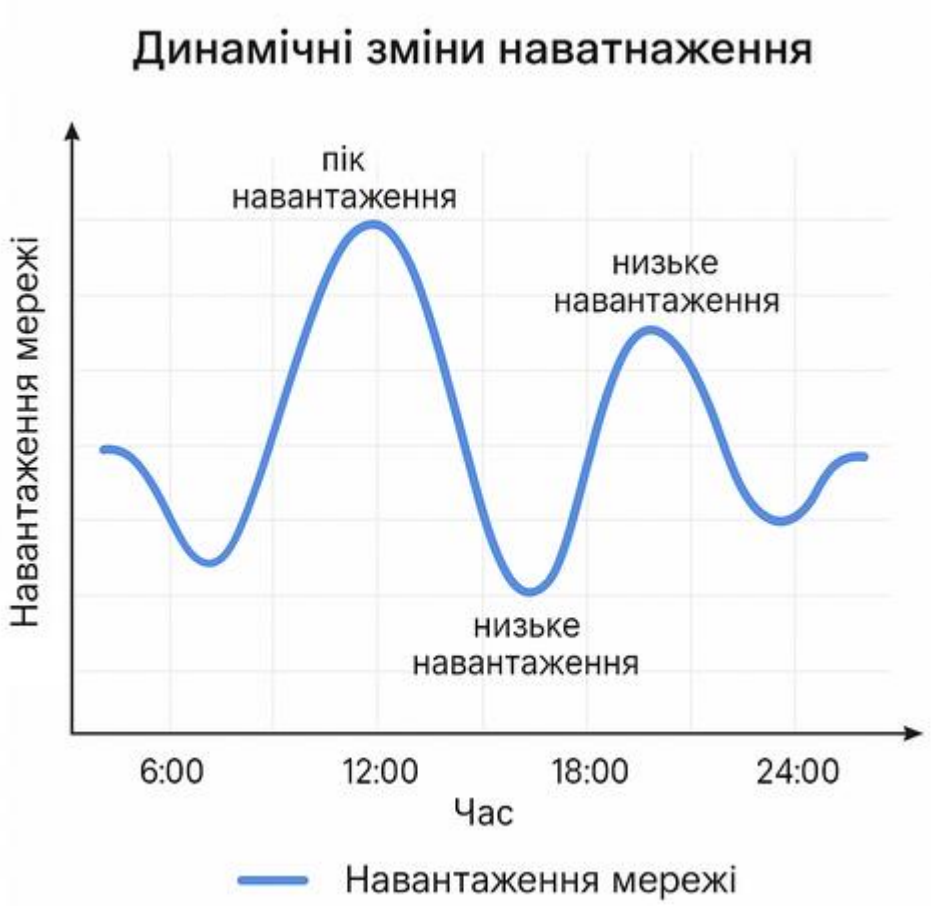


Рисунок 1.2 – Динамічні зміни навантаження

Непередбачувані зміни навантаження виникають у випадках аварій, атак, оновлень або змін у поведінці користувачів. Наприклад, масовий запуск ресурсоємного програмного забезпечення, збій в одному з вузлів мережі,

несанкціонований доступ або зовнішня DDoS-атака можуть призвести до різкого стрибка навантаження, що перевищує проектні можливості інфраструктури. У таких умовах можливе виникнення затримок, втрата пакетів, зниження якості обслуговування або навіть відмова в доступі до критичних сервісів.

З огляду на вищезазначене, динамічність навантаження вимагає від мережі здатності до адаптації – як в плані ресурсного резервування, так і з точки зору інтелектуального управління трафіком. Ефективними засобами реагування на зміни є використання механізмів динамічного маршрутизаційного протоколу, політик QoS, балансування навантаження, а також автоматизованих систем моніторингу, які в режимі реального часу аналізують стан трафіку та коригують параметри роботи мережі. Прогнозування динаміки навантаження з використанням математичних моделей або методів машинного навчання дозволяє додатково підвищити ефективність управління, оскільки забезпечує проактивний підхід до запобігання перевантаженням.

1.1.5 Забезпечення резервування та інформаційної безпеки

Одним з критичних аспектів надійного функціонування корпоративних мереж є забезпечення резервування, яке полягає у впровадженні технічних і логічних засобів, що гарантують безперервність роботи мережі навіть у випадку відмови окремих її компонентів. У сучасних інформаційних системах вимоги до доступності сервісів постійно зростають, особливо в умовах цілодобового доступу до ресурсів, розподілених бізнес-процесів та залежності від інтегрованих IT-сервісів. У цьому контексті резервування розглядається як ключовий елемент архітектури, який дозволяє підвищити відмовостійкість мережі та зменшити ризики виникнення простоїв.

Резервування може здійснюватися на різних рівнях. На фізичному рівні це передбачає дублювання комунікаційних каналів, мережевого обладнання

(наприклад, комутаторів, маршрутизаторів), джерел живлення та серверної інфраструктури. На логічному рівні використовуються протоколи високої доступності, зокрема HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol), протоколи агрегації каналів (LACP), а також маршрутизація з кількома шляхами (multipath routing). Для критично важливих ресурсів впроваджується кластеризація серверів, яка дозволяє автоматично перенаправляти запити у разі відмови одного з вузлів. Важливим елементом також є наявність резервних копій конфігурацій пристроїв, систем моніторингу стану мережі та автоматизованих механізмів перемикання на резервні траси. Таким чином, система резервування формує основу для забезпечення високої доступності (High Availability, HA) та підтримки безперервності бізнесу (Business Continuity).

Паралельно із забезпеченням відмовостійкості важливою складовою ефективного функціонування корпоративної мережі є інформаційна безпека. У контексті зростання кількості кіберзагроз, підвищеної вартості конфіденційних даних та активного використання віддаленого доступу, питання захисту інформації стає пріоритетним. Інформаційна безпека охоплює комплекс заходів, спрямованих на захист конфіденційності, цілісності та доступності даних, а також на запобігання несанкціонованому доступу до інформаційних ресурсів.

Забезпечення безпеки корпоративної мережі реалізується на декількох рівнях. На периметрі мережі встановлюються міжмережеві екрани, системи виявлення та запобігання вторгненням (IDS/IPS), шлюзи безпеки, а також засоби контролю доступу до Інтернету. Внутрішня безпека забезпечується за допомогою VLAN-сегментації, політик доступу до ресурсів (ACL), систем автентифікації та авторизації, а також шифрування трафіку за допомогою протоколів IPsec, TLS або SSL. Для моніторингу інцидентів застосовуються централізовані системи збору логів, SIEM-платформи, а також системи аудиту. Особливої уваги набуває захист кінцевих пристроїв і мобільного

доступу, що передбачає впровадження антивірусного ПЗ, клієнтських VPN та політик керування пристроями (MDM).

З огляду на комплексність загроз і розгалуженість мережевої інфраструктури, інформаційна безпека в корпоративних мережах потребує не лише технічних рішень, але й розробки внутрішніх політик, процедур реагування на інциденти, навчання персоналу та регулярного аудиту систем захисту. Такий підхід дозволяє сформувати стійку до зовнішніх та внутрішніх ризиків мережеву екосистему, що забезпечує надійний захист критичних активів організації.

1.2 Вимоги до управління трафіком в корпоративній мережі

Управління трафіком у корпоративному середовищі має вирішувати кілька критично важливих задач, від яких залежить стабільність та ефективність роботи мережі.

Моніторинг і аналіз трафіку:

- виявлення пікових навантажень, відстеження джерел трафіку, ідентифікація «важких» додатків;

- реалізується за допомогою SNMP, NetFlow, sFlow, DPI (глибокий аналіз пакетів).

Прогнозування навантаження:

- важливо для планування ресурсів, підвищення ефективності інфраструктури та запобігання перенавантаженню;

- прогнозування дає змогу адаптувати політики QoS, масштабувати ресурси, змінювати маршрути в залежності від передбачуваного попиту.

Пріоритезація трафіку:

- забезпечення переваги для критично важливих сервісів (відеоконференції, CRM, VoIP);

- використання механізмів маркування трафіку (DSCP, CoS), чергування, обмеження пропускної здатності.

Балансування навантаження:

- розподіл трафіку між кількома серверами чи каналами для зниження затримок і підвищення продуктивності;
- актуально для систем з великою кількістю запитів до веб-додатків, БД, API.

Автоматизоване управління політиками:

- динамічне регулювання правил доступу, фільтрації, перенаправлення трафіку в залежності від умов;
- використання SDN (software-defined networking) та мережевої оркестрації.

Інтеграція з інструментами безпеки:

- контроль SSL/HTTPS-трафіку, аналіз загроз, виявлення підозрілої активності;
- роль інтегрованих платформ: SIEM, NTA (Network Traffic Analysis), SOAR.

Управління трафіком у корпоративних мережах є комплексним завданням, що включає моніторинг, аналіз, прогнозування, оптимізацію та контроль за передачею даних між різними елементами мережевої інфраструктури. З огляду на складність сучасних корпоративних мереж, різноманіття трафіку, високі вимоги до якості обслуговування (QoS) та потребу у гарантуванні безпеки, до систем управління трафіком висувається низка важливих функціональних і технічних вимог.

Перш за все, управління трафіком повинно бути адаптивним. Це означає, що система має здатність реагувати на динамічні зміни навантаження, типів трафіку та структури мережі. В умовах постійних коливань обсягу переданих даних та змін у поведінці користувачів важливо забезпечити гнучке переналаштування маршрутів, автоматичну зміну пріоритетів або перенаправлення потоків у разі виявлення аномалій або перевантаження.

Другим критичним чинником є прогнозованість і проактивність системи. Сучасні засоби управління трафіком повинні мати можливість не лише фіксувати поточний стан мережі, але й прогнозувати майбутнє навантаження на основі історичних даних, шаблонів поведінки користувачів або подій у бізнес-процесах. Завдяки цьому забезпечується проактивне управління, що дозволяє уникнути критичних ситуацій, запобігти перевантаженням і забезпечити стабільність функціонування мережі.

Ще однією ключовою вимогою є пріоритезація трафіку відповідно до його важливості для організації. Критичні для бізнесу сервіси – такі як IP-телефонія, відеоконференції, доступ до баз даних або CRM-систем – повинні отримувати перевагу в обслуговуванні порівняно з менш важливими або фоновими потоками, як-от оновлення програмного забезпечення чи резервне копіювання. Для цього в системі повинні бути реалізовані політики QoS, механізми диференціації трафіку, керування чергами та управління затримками.

Також важливо забезпечити балансування навантаження, яке дозволяє рівномірно розподіляти трафік між декількома каналами, серверами або мережевими пристроями. Це знижує ризик перевантаження окремих сегментів мережі, підвищує ефективність використання ресурсів і забезпечує стійкість до збоїв. Особливо актуально це для хмарних рішень, систем віртуалізації та веб-сервісів, які обслуговують велику кількість одночасних запитів.

Крім того, управління трафіком має враховувати питання інформаційної безпеки. Контроль за джерелами трафіку, виявлення підозрілих потоків, обмеження доступу до певних ресурсів або сервісів, а також забезпечення шифрування трафіку є необхідними умовами для захисту мережі від внутрішніх і зовнішніх загроз.

Нарешті, ефективне управління трафіком передбачає централізованість та автоматизацію. Сучасні інструменти повинні забезпечувати єдиний інтерфейс для адміністрування політик, аналітики, звітності та реагування на

інциденти. Застосування технологій програмно-визначених мереж (SDN) та елементів штучного інтелекту дозволяє підвищити рівень автоматизації та зменшити залежність від ручного втручання, що значно покращує оперативність та точність управлінських рішень.

Таким чином, система управління трафіком у корпоративній мережі повинна поєднувати інтелектуальність, гнучкість, безпеку та високу адаптивність до змін, забезпечуючи при цьому стабільну роботу інформаційної інфраструктури відповідно до потреб бізнесу.

1.3 Огляд існуючих моделей прогнозування трафіку

Прогнозування мережевого трафіку є важливою складовою управління корпоративною мережею, оскільки дає змогу заздалегідь оцінити майбутні навантаження, виявити можливі загрози продуктивності та оптимізувати розподіл ресурсів. На сучасному етапі розвитку інформаційних технологій розроблено та апробовано низку підходів до прогнозування трафіку, які відрізняються як за методологією, так і за точністю, складністю реалізації та адаптивністю. У цьому підпункті розглянемо основні типи моделей: статистичні, нейромережеві та евристичні.

Статистичні моделі прогнозування ґрунтуються на аналізі історичних даних трафіку та пошуку закономірностей, що дозволяють робити припущення щодо майбутніх значень. До класичних статистичних методів належать моделі авторегресії (AR), авторегресії з рухомим середнім (ARMA), авторегресивна інтегрована модель ковзного середнього (ARIMA), а також сезонні варіанти цих моделей (SARIMA). Основною перевагою статистичних моделей є відносна простота реалізації, наявність усталених математичних основ та можливість інтерпретації результатів. Однак, ці моделі мають низку обмежень: вони погано справляються з нелінійними залежностями, чутливі до шумів та часто потребують попередньої обробки і стаціонарності даних.

Крім того, статистичні методи мають обмежену здатність до адаптації в умовах різкої зміни структури трафіку.

На противагу їм, нейромережеві методи, зокрема штучні нейронні мережі (ШНМ), довели високу ефективність у прогнозуванні складних, нелінійних і хаотичних процесів, характерних для трафіку в корпоративних мережах. Найбільш поширеними є багатошарові перцептрони (MLP), рекурентні нейронні мережі (RNN), довгострокова короткочасна пам'ять (LSTM), а також згорткові нейронні мережі (CNN) для просторово-часового аналізу. Головною перевагою цих підходів є здатність виявляти складні закономірності без явного формалізування, а також навчання на великих обсягах даних. Водночас, їх недоліками є висока обчислювальна складність, необхідність у значному обсязі навчальних даних, складність у поясненні результатів (чорний ящик), а також складність налаштування гіперпараметрів.

Евристичні методи прогнозування трафіку включають підходи, засновані на експертних правилах, адаптивних алгоритмах, генетичних алгоритмах, логіці нечітких множин (fuzzy logic), а також елементах машинного навчання без контролю (наприклад, кластеризація). Вони орієнтовані на врахування специфічних особливостей мережі, швидке реагування на зміни та використання знань предметної області. Переваги цих методів – це гнучкість, здатність до адаптації та можливість комбінування з іншими моделями в гібридних рішеннях. Водночас, евристики часто не гарантують точності результатів, можуть давати нестабільні прогнози в умовах високої варіативності даних і потребують ретельної валідації.

Таким чином, кожна з розглянутих груп моделей має свої переваги й недоліки, і вибір оптимального підходу залежить від конкретного завдання, доступних ресурсів, обсягу історичних даних та вимог до точності прогнозу. У практиці часто застосовуються гібридні моделі, які поєднують сильні сторони кількох підходів – наприклад, статистичних і нейромережевих – з

метою підвищення загальної ефективності прогнозування трафіку в корпоративних мережах.

На рисунку 1.3 представлено інтегрований підхід до прогнозування та маршрутизації мережевого трафіку, який базується на поєднанні двох методів – короткострокового прогнозування інтенсивності трафіку та методів динамічної маршрутизації.

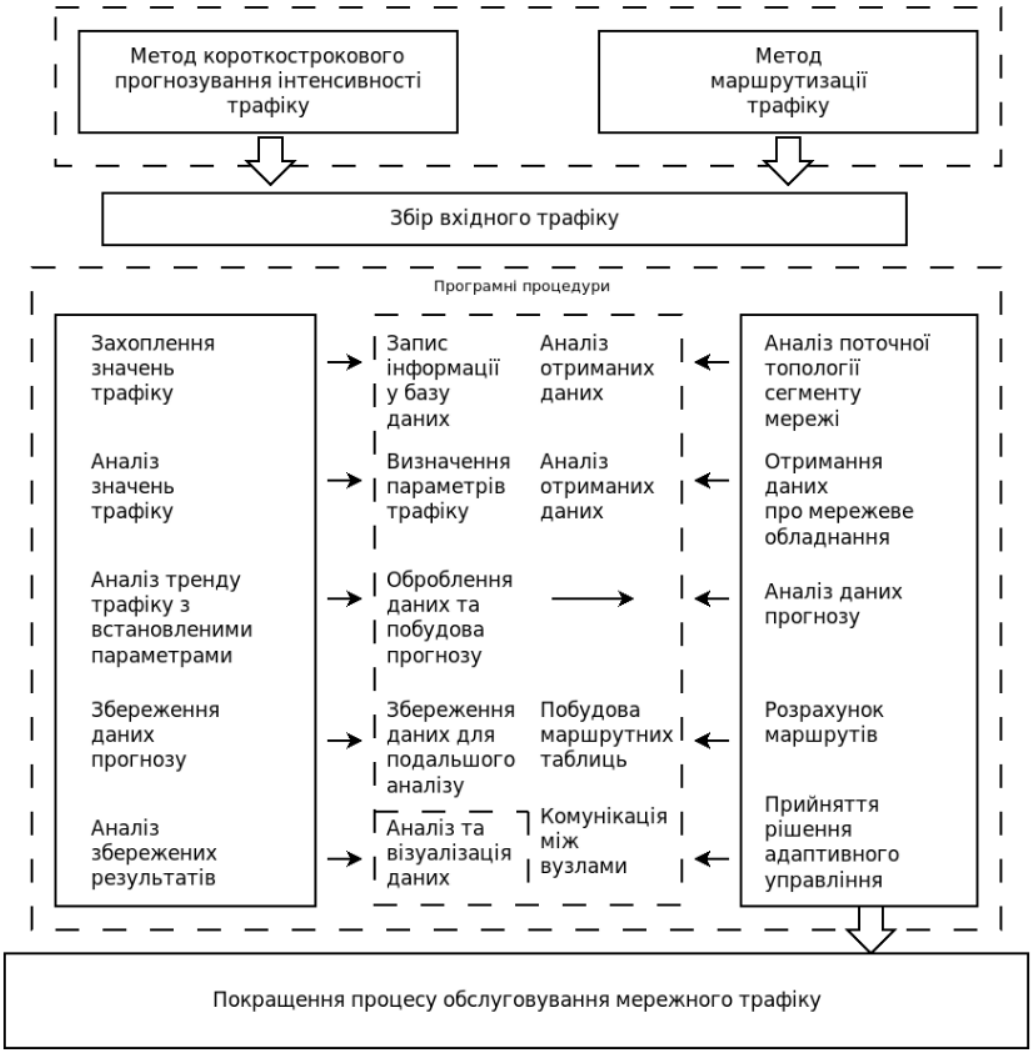


Рисунок 1.3 – Схема застосування інформаційної технології для завдання прогнозування трафіку

Метою такої інтеграції є покращення процесу обслуговування мережевого трафіку шляхом більш точного передбачення навантаження і відповідної адаптації маршрутів передавання даних. У центрі схеми

знаходиться етап збору вхідного трафіку, який виступає як основа для подальшої обробки та аналізу даних у межах обох підходів.

Ліва частина схеми репрезентує етапи, що пов’язані з прогнозуванням. Зокрема, вона охоплює захоплення значень трафіку, аналіз їхньої динаміки з урахуванням попередньо встановлених параметрів, збереження та обробку отриманих даних у базах даних, а також побудову короткострокових прогнозів. Результати прогнозування зберігаються для подальшого використання у процесі маршрутизації. Центральним компонентом є аналітична обробка отриманих даних, що дозволяє здійснити узгодження між елементами прогнозування та маршрутного прийняття рішень.

Права частина схеми присвячена маршрутизаційним процедурам, які включають аналіз поточної топології мережі, стану її окремих сегментів та обладнання. У межах цього підходу проводиться оцінка релевантних параметрів для формування оптимальних маршрутів, а також здійснюється прийняття рішень щодо адаптивної маршрутизації трафіку відповідно до змін у мережевому середовищі.

Схема демонструє логічну і функціональну інтеграцію між етапами прогнозування та маршрутизації. Прогнозні дані слугують вхідними параметрами для формування маршрутів, а зміни в маршрутизаційній політиці, своєю чергою, впливають на зворотний цикл прогнозування, формуючи замкнутий контур адаптивного керування трафіком. Такий підхід дозволяє забезпечити підвищену ефективність роботи мережі, адаптивність до коливань навантаження та зменшення часу реакції на потенційні загрози перевантаження.

Узагальнюючи, подана схема ілюструє сучасну концепцію інтелектуального управління трафіком, яка ґрунтується на синергії прогнозної аналітики та гнучких методів маршрутизації, що у сукупності сприяє підвищенню якості обслуговування користувачів та оптимальному використанню мережевих ресурсів.

1.4 Порівняльний аналіз методів прогнозування

Зважаючи на широкий спектр методів прогнозування трафіку, що використовуються в корпоративних мережах, актуальним є їх системне порівняння за низкою ключових критеріїв. Такий аналіз дозволяє визначити найбільш доцільні підходи для застосування в конкретних умовах, з урахуванням ресурсних обмежень, вимог до точності та швидкості реакції системи.

До основних параметрів, що використовуються для порівняльного аналізу моделей, належать точність прогнозування, складність реалізації, швидкість обчислень та адаптивність до змінних умов. Ці характеристики є критично важливими при виборі методології прогнозування в рамках проєктування або вдосконалення систем управління трафіком.

Статистичні моделі, як правило, забезпечують середній рівень точності, оскільки ефективно працюють за умов наявності стаціонарних даних та чітко виражених закономірностей. Водночас вони відзначаються низькою складністю реалізації та високою швидкістю обчислень, що робить їх привабливими для впровадження у мережах з обмеженими ресурсами. Однак їх здатність адаптуватися до різких змін у структурі трафіку є обмеженою.

Нейромережеві методи, зокрема ті, що базуються на глибокому навчанні (Deep Learning), демонструють високу точність навіть у випадках складних, нелінійних або нестабільних даних. Їхня адаптивність дозволяє швидко підлаштовуватися до змін у середовищі, що є критично важливим для сучасних корпоративних мереж. Проте ці методи вимагають значних обчислювальних ресурсів, глибоких технічних знань для налаштування та значного часу для навчання, що зумовлює високу складність їх реалізації і низьку швидкість виконання в режимі реального часу без спеціального апаратного забезпечення.

Метод	Точність	Складність реалізації	Швидкість обчислень	Адаптивність
Статистичні моделі	Середня	Низька	Висока	Низька
Нейромережеві методи	Висока	Висока	Низька	Висока
Евристичні підходи	Змінна	Середня	Середня	Висока

Рисунок 1.4 – Порівняльний аналіз методів прогнозування

Евристичні підходи, навпаки, відзначаються гнучкістю і здатністю враховувати специфічні особливості мережі або вимоги бізнесу. Вони часто використовуються в гібридних системах та в умовах неповноти даних. Точність їх прогнозів може змінюватися залежно від сценарію, однак вони забезпечують прийнятний компроміс між точністю, швидкістю і адаптивністю. Складність реалізації таких методів зазвичай середня, що дозволяє ефективно поєднувати їх з іншими технологіями.

Результати порівняльного аналізу представлено у таблиці, яка дає змогу швидко оцінити переваги й недоліки кожного з підходів у контексті вимог до корпоративних мереж. Таким чином, вибір моделі прогнозування має базуватися на збалансованому аналізі технічних можливостей, характеру трафіку та очікувань щодо якості обслуговування.

2 ТЕОРЕТИЧНІ ОСНОВИ МЕРЕЖ ПЕТРІ ДЛЯ МОДЕЛЮВАННЯ ТА ПРОГНОЗУВАННЯ ТРАФІКУ

2.1 Мережі Петрі

Теорія обчислювальних мереж тісно пов’язана з аналізом розподілених систем і процесів, які в них відбуваються. Для опису систем у статичному стані застосовуються елементарні немарковані мережі, що дозволяють зафіксувати їх структурні характеристики без урахування змін у часі. Натомість динаміку функціонування таких систем – зокрема, характер взаємодії елементів, розвиток процесів і зміну станів – досліджують за допомогою маркованих мереж. У цьому контексті маркована мережа розглядається як орієнтований граф, що містить два типи вершин: перший відповідає за локальні атомарні стани, а другий – за переходи між ними. Зв’язки між вершинами реалізуються спрямованими дугами, які визначають причинно-наслідкові відносини між станами й переходами. Структура мережі задає її топологію, а маркування – поточний стан системи, тобто розміщення спеціальних об’єктів, що називаються фішками, у певних вершинах графа.

Поведінка такої мережі регулюється правилами активації переходів, які визначають умови, за яких можлива зміна маркування. Зміна маркування вказує на динамічні зміни у стані системи, що і є предметом аналізу. Значна частина досліджень у межах цієї теорії зосереджується на мережах Петрі – окремому класі маркованих мереж, в яких фішки не мають внутрішньої структури. Мережі Петрі відзначаються простотою та виразною здатністю до моделювання розподілених процесів. Вони дозволяють точно фіксувати три базові типи взаємозв’язків між переходами у системі: послідовність (один перехід настає за іншим), вибір (відбувається один з можливих переходів) та паралелізм (переходи відбуваються одночасно, незалежно один від одного).

Попри свою зручність, класичні мережі Петрі мають обмеження, зокрема труднощі у визначенні реальної структури системи та її поточного стану, особливо у складних моделях. Для подолання цих обмежень застосовуються модифіковані марковані мережі, у яких фішки мають внутрішню структуру, що дозволяє враховувати додаткову інформацію про стан елементів. Якщо локальні стани розглядати як умови, а переходи як події, то кожен перехід можна інтерпретувати як перетворення умовного стану в інший у результаті настання події. Наприклад, якщо умова c переходить у c' через подію e, то це відображається у вигляді запису c[e>c'. Такий формалізм дозволяє більш гнучко описувати еволюцію системи, що ілюструється графічно на відповідних схемах.

Перехід в стан 'показаний на рисунку 2.1

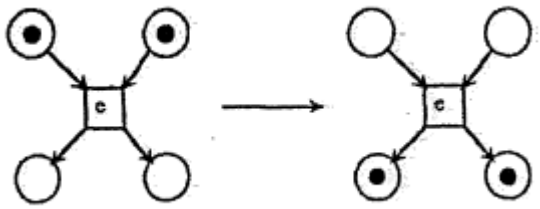


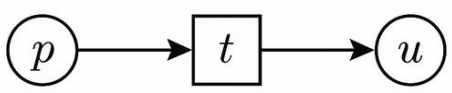
Рисунок 2.1 – Перехід в інший стан

У загальноприйнятому математичному формалізмі мережа визначається як структура, що складається з трьох основних компонентів і позначається у вигляді трійки N = (P, T, F), де P – це скінченна, непорожня множина місць, T – скінченна, непорожня множина переходів, а F – множина зв’язків або дуг, які відображають напрямки взаємодії між елементами. При цьому множини P і T є взаємно неперетинні, тобто $P \cap T = \emptyset$, що гарантує чітке розмежування між двома функціональними типами компонентів мережі. Об'єднання множин місць і переходів утворює множину елементів мережі, яка позначається як $X = P \cup T$. Саме ця множина визначає повний склад структурних одиниць мережі N та слугує базою для побудови формальних моделей поведінки системи.

$$F \subseteq (P \times T) \cup (T \times P), dom(F) \cup cod(F) = P \cup T, \tag{2.1}$$

Продовжуючи формалізацію мережі, варто уточнити, що компонент F у структурі N = (P, T, F) визначає множину дуг або зв’язків, які встановлюють напрямки взаємодії між місцями та переходами. Формально F є підмножиною декартового добутку (P × T) ∪ (T × P), що означає: дуги можуть бути спрямовані або від місця до переходу, або навпаки – від переходу до місця. Така структура забезпечує основу для моделювання причинно-наслідкових зв’язків у межах системи, зокрема тих процесів, що відбуваються внаслідок активації певних умов або подій.

Для повноцінного опису динамічного стану мережі вводиться поняття маркування. Маркування визначає розподіл певних об’єктів – фішок – по множині місць P. Кожне місце може містити від нуля до кількох фішок, залежно від поточного стану системи. Таким чином, маркування виконує роль змінної, що відображає внутрішній стан мережі у кожен момент часу. Позначається воно, як правило, функцією M: P → ℕ₀, де M(p) вказує на кількість фішок у місці p ∈ P.



$$P = \{p, u\}$$
$$T = \{t\}$$
$$F = \{(p, t), (t, u)\}$$

Рисунок 2.2 – Базова структура мережі Петрі

Рисунок 2.2 ілюструє базову структуру мережі Петрі, задану у вигляді трійки N=(P,T,F), де:

- P={p,u} – множина місць, позначених кружечками (у прикладі: p і u);
- T={t} – множина переходів, позначена прямокутником (у прикладі: один перехід t);

- $F=\{(p,t),(t,u)\}$ – множина дуг, що описують напрямок передачі між місцями і переходами.

У графічному представленні видно, що фішка (умовна одиниця маркування) спочатку перебуває в місці pp, далі передається через перехід tt до місця uu. Це найпростіший приклад, який демонструє послідовність подій: одне місце активує перехід, і після його спрацьовування фішка переміщується до іншого місця. Така структура слугує основою для моделювання більш складних динамічних процесів у системах з розподіленими ресурсами.

Зміна маркування відбувається в результаті спрацьовування переходів, яке можливе лише тоді, коли виконано певні умови: з усіх місць, що входять до переходу, наявна необхідна кількість фішок. У результаті спрацьовування відбувається вилучення фішок із вхідних місць та їх перенаправлення до вихідних місць згідно зі структурою дуг F. Такий механізм забезпечує моделювання динамічної поведінки системи, дозволяючи фіксувати послідовність подій, паралелізм дій, конфлікти доступу до ресурсів, а також інші аспекти функціонування розподілених процесів.

Цей формалізм лежить в основі класичних мереж Петрі, які набули широкого застосування для аналізу складних дискретних систем, зокрема в телекомунікаціях, управлінні ресурсами, інформаційній безпеці та бізнес-процесах.

2.2 Переходи в мережах Петрі

Одним із перспективних напрямів розвитку теорії мереж Петрі є дослідження паралельних та розподілених систем, у яких особлива увага приділяється аналізу тимчасових і причинно-наслідкових (каузальних) порядків виникнення подій. У межах традиційного підходу, заснованого на так званій неінтерлівінговій інтерпретації, паралельні події розглядаються як такі, що можуть виникати в довільному порядку. Це спрощує аналіз, однак

водночас призводить до втрати інформації про реальну конкуренцію між подіями. Для подолання цього обмеження в теоретичних моделях, орієнтованих на реалістичне відображення паралелізму, застосовуються часткові порядки, які дозволяють більш точно описувати як часові залежності, так і причинно-наслідкові взаємозв'язки між подіями.

Такий підхід зумовлює новий погляд на природу паралелізму в мережах Петрі, де традиційно вважається, що конкуренція між подіями не виникає внаслідок розгляду лише лінійних (послідовних) варіантів спрацьовування переходів. Проте поведінковий аналіз мереж свідчить, що навіть у межах послідовностей активацій переходів можлива поява обмежених форм конкуренції, яка не є очевидною на рівні формальної структури, але проявляється при конкретних сценаріях виконання.

Саме тому значна кількість досліджень була присвячена вивченню механізмів, що керують послідовностями спрацьовувань переходів, з метою виявлення потенційної конкуренції між подіями. Основна мета таких досліджень полягає у виявленні максимально повної інформації про характер взаємодії між елементами системи, що дозволяє глибше зрозуміти поведінку моделі. На основі запропонованих теоретичних концепцій розроблено метод, що дозволяє аналізувати конкуренцію в системах через вивчення структурних властивостей мережі Петрі та динамічних даних, отриманих із послідовностей спрацьовувань переходів. Такий підхід відкриває нові можливості для формалізованого аналізу розподілених процесів, де взаємодія подій відіграє ключову роль у формуванні загальної поведінки системи.

Мережі Петрі є потужним інструментом для формального опису складних обчислювальних конструкцій, а також для моделювання взаємодії між ресурсами системи та процесами, що відбуваються всередині неї. Завдяки своїй графовій природі та строгій математичній формалізації вони здатні відображати як структурну організацію системи, так і її поведінкові аспекти. Водночас ключова подія в мережах Петрі – спрацьовування переходу – не завжди однозначно інтерпретується в контексті виконання дій,

що може створювати певні труднощі при моделюванні конкретних архітектур або програмних конструкцій.

У випадках, коли мережа Петрі використовується для опису поведінки послідовної програми, виникає потреба у чіткій відповідності між переходами та процесами. У такому підході кожен перехід репрезентує певний процес або фрагмент виконання програми, тоді як події виступають як точки синхронізації чи взаємодії між окремими процесами, а не як самостійні операції. Подібне трактування дозволяє моделювати контрольні залежності, логіку переходів між станами та координацію дій у програмному середовищі.

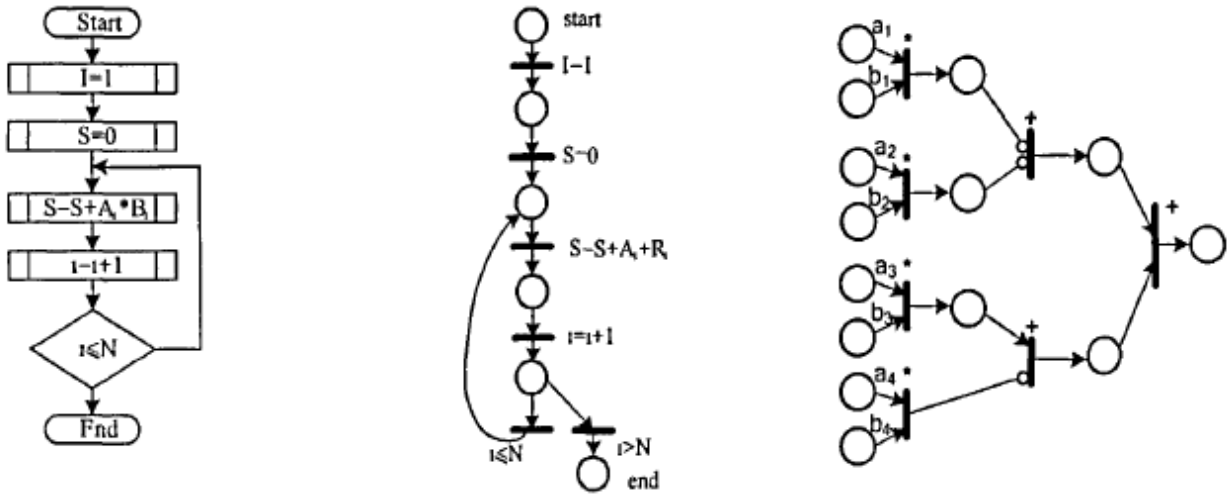


Рисунок 2.3 – Алгоритмічна схема і еквівалентні їй мережі Петрі

З іншого боку, в контексті потокової обробки даних, зокрема в так званих потокових мережах Петрі або при моделюванні машин потоку операндів, інтерпретація елементів мережі змінюється. У таких випадках переходи ототожнюються з окремими операціями або командами, що виконуються над операндами, тоді як місця виступають у ролі сховищ або каналів передачі операндів. Функціонування мережі в цьому разі відображає логіку обробки даних у системах з глибоким конвеєрним паралелізмом або потоковими архітектурами.

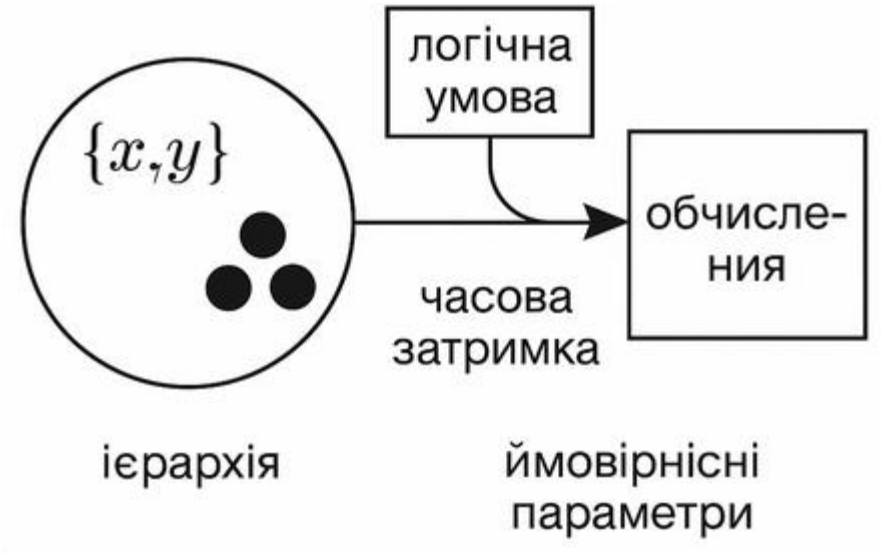


Рисунок 2.4 – Основні компоненти розширених мереж Петрі

Ці два підходи демонструють гнучкість мереж Петрі щодо інтерпретації їхніх базових елементів у залежності від предметної області та завдань моделювання. Саме ця адаптивність дозволяє ефективно використовувати мережі Петрі для аналізу як програмної логіки, так і апаратних архітектур, з урахуванням специфіки обчислювальних процесів.

2.3 Розширені мережі Петрі

Розширені мережі Петрі являють собою подальший розвиток класичної теорії мереж Петрі, метою якого є подолання обмежень традиційної моделі в контексті опису складних, динамічних і гетерогенних систем. У класичному формалізмі елементи мережі – місця, переходи та фішки – мають просту структуру, що забезпечує зручність у моделюванні базових механізмів взаємодії, але виявляється недостатнім для адекватного представлення систем із багатим внутрішнім станом, логічними залежностями чи часовими обмеженнями. Розширення моделі здійснюється за рахунок введення додаткових властивостей, структур та механізмів, які надають мережам Петрі значно ширші аналітичні й виражальні можливості.

Одним із напрямів розширення є надання фішкам внутрішньої структури або значення, що дозволяє відображати передачу даних або станів між елементами системи. У такому контексті місця слугують не лише умовами для активації переходів, але й носіями інформації, тоді як переходи виконують обчислення чи перетворення. Іншим важливим елементом є ієрархізація моделі, коли мережа організується у вигляді модулів або підмереж, що дозволяє ефективно моделювати великі системи шляхом декомпозиції їх на логічно завершені компоненти. Також розширення може включати часові аспекти, завдяки яким модель здатна описувати затримки, часові вікна, дедлайни або періодичність подій. Деякі варіації включають логічні умови, що регулюють спрацьовування переходів, або стохастичні параметри, які дозволяють відображати ймовірнісну природу подій.

Таким чином, розширені мережі Петрі виступають універсальним інструментом для опису складних сценаріїв поведінки системи, зокрема в галузях, де важливою є взаємодія між обчисленням, передачею даних та часовими обмеженнями. Вони знаходять застосування в автоматизованих системах управління, моделюванні бізнес-процесів, аналізі мережевих протоколів, розробці програмного забезпечення та кіберфізичних системах. Їхня формальна строгість у поєднанні з високим ступенем моделювальної потужності забезпечує аналітичну точність при збереженні наочності структурної репрезентації системи.

2.4 Опис розроблювальної моделі

Для прогнозування трафіку в корпоративній мережі доцільно використовувати розширену модель мережі Петрі з кольоровими фішками (Coloured Petri Nets – CPN). Вибір цього типу обумовлений необхідністю обробки різних типів трафіку, що мають специфічні характеристики, такі як джерело, призначення, інтенсивність і час передачі. Кожна фішка має внутрішню структуру, що зберігає інформацію про трафік (тип, обсяг, час).

Вузлами мережі є місця, які репрезентують різні сегменти корпоративної мережі (сервери, маршрутизатори, точки доступу) і переходи, які моделюють процес передачі трафіку між вузлами. Стан мережі визначається кількістю та типами фішок у місцях, що відображає інтенсивність трафіку на вузлах.

Дуги зв’язують місця та переходи, визначаючи правила передачі трафіку в системі. Переходи можуть активуватись залежно від умов, які моделюють доступність ресурсів, пропускну здатність каналів, або час передачі.

2.5 Опис методу прогнозування

Прогнозування будується на аналізі історичних даних про переміщення фішок у мережі. Перший крок – це збирання даних про історичний трафік (кількість і тип фішок, інтенсивність передачі). Далі використовуються статистичні або нейромережеві моделі, що аналізують ці дані і визначають закономірності, які дозволяють спрогнозувати майбутні переміщення фішок між місцями.

Зокрема, прогноз може ґрунтуватися на аналізі частоти спрацьовування переходів та динаміки змін у маркуваннях місць. Отримані результати використовуються для автоматичного налаштування параметрів мережі Петрі, зокрема зміни пропускної здатності каналів або вибору оптимального шляху трафіку.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ МЕТОДУ ТА АНАЛІЗ РЕЗУЛЬТАТІВ

3.1 Програмна реалізація методу та вибір програмних засобів

Для побудови моделі буде використовуватися бібліотека Python Snakes для створення мереж Петрі., використання Pandas для обробки історичних даних, а використання бібліотеки машинного навчання (наприклад, scikit-learn) для прогнозування.

Кроки реалізації:

- імпорт необхідних бібліотек:
- створення мережі Петрі;
- генерація тестових даних;
- навчання моделі прогнозування даних;
- візуалізація мережі Петрі.

Описані модель та метод дозволяють ефективно прогнозувати та аналізувати трафік у корпоративних мережах, використовуючи гнучкість і потужність розширених мереж Петрі в поєднанні з прогнозними алгоритмами.

Лістинг коду представлений в додатку Б.

3.2 Метод прогнозування трафіку на основі розширених мереж Петрі: покроковий опис

Крок 1. Формалізація мережі як моделі Петрі.

На цьому етапі створюється базова модель корпоративної мережі у вигляді розширеної мережі Петрі. Формалізація включає:

- визначення місць (P) – це логічні або фізичні вузли мережі, наприклад: сервери, маршрутизатори, точки доступу, сегменти;

- визначення переходів (T) – це процеси або події, що відбуваються в мережі: передача трафіку, зміна маршруту, фільтрація, балансування;
- визначення дуг (F) – зв’язків між місцями й переходами.
- призначення фішок зі структурою (тип трафіку, обсяг, час, джерело/призначення).

Мета етапу: створити абстрактну модель топології та функціонування мережі для подальшої аналітики.

Крок 2. Збір історичних даних трафіку

На цьому етапі виконується моніторинг і фіксація фактичних даних про трафік, що проходив через мережу:

- кількість пакетів у кожному місці;
- час між активацією переходів;
- типи переданого трафіку (http, ftp, VoIP);
- завантаженість вузлів мережі.

Дані збираються за певні періоди (наприклад, щогодини або щохвилини) і зберігаються у таблицях.

Мета етапу: забезпечити базу для аналізу закономірностей у поведінці трафіку.

Крок 3. Аналіз маркування та спрацьовувань.

Далі аналізується, як змінювалось маркування мережі (розподіл фішок) у часі:

- визначаються частоти спрацьовування переходів;
- вивчаються послідовності переходів;
- будуються множини станів і сценарії динаміки системи.

Це дозволяє виявити, як трафік поширюється по мережі у відповідь на події – наприклад, навантаження на конкретний сегмент призводить до перенаправлення потоків.

Мета етапу: формалізувати поведінку мережі як часову послідовність переходів і станів.

Крок 4. Вибір методу прогнозування.

На основі зібраних даних обирається алгоритм прогнозування. Є кілька варіантів:

- статистичні методи (ARIMA, ковзне середнє) – для регулярних трафіків;

- машинне навчання (регресія, дерева рішень) – для адаптивного прогнозу;

- нейронні мережі (LSTM) – для складних патернів трафіку.

Мета етапу: передбачити майбутнє навантаження на основі закономірностей із минулого.

Крок 5. Побудова прогнозної моделі

- формалізується сам процес прогнозування:

- вхідні дані: часові ряди трафіку, топологія мережі Петрі;

- вихідні дані: оцінка інтенсивності трафіку у певних місцях/на дугах;

- алгоритм: аналіз маркувань, спрацьовування переходів, обрахунок майбутніх сценаріїв на основі ймовірностей або функцій.

Прогнозна модель також може інтегрувати часові обмеження, логіку пріоритетів або зважування трафіку за типом.

Мета етапу: отримати функцію, яка описує очікуване навантаження на мережу.

Крок 6. Реалізація в середовищі моделювання

Модель реалізується в програмному середовищі (наприклад, Google Colab):

- реалізація мережі Петрі: бібліотека Snakes, petrinet, pm4py;

- побудова та візуалізація мережі;

- імпорт даних, навчання моделі;

- інтерфейс користувача (графіки, таблиці, вивід результатів).

Мета етапу: надати доступний інструмент для симуляції й перевірки прогнозів.

Крок 7. Валідація та коригування. Після реалізації моделі виконується:

- порівняння прогнозних значень з фактичними;

- обчислення похибок (MAE, RMSE);
- корекція моделі при відхиленнях;
- тестування на нових даних.

Мета етапу: забезпечити надійність прогнозу в реальному середовищі.

3.3 Аналіз результатів

Рисунок 3.1 – Генерація тестового трафіку

На рисунку 3.1 представлено комплексну візуалізацію результатів аналізу мережевого трафіку, що охоплює як розподільчі, так і часові характеристики даних. У верхньому рядку зображень візуалізовано гістограми та діаграми розсіювання. Зокрема, гістограма трафіку дозволяє оцінити його розподіл: вона демонструє значну скупченість значень у нижньому інтервалі, що може свідчити про асиметричний характер розподілу. Гістограма ковзного середнього навпаки показує більш рівномірний розподіл, що вказує на ефективне згладжування вихідних даних. Діаграма розсіювання між часом і трафіком виявляє тенденцію до зниження інтенсивності трафіку з плином часу, хоча й з певними відхиленнями, зумовленими випадковими флуктуаціями. Натомість кореляційна залежність між вихідним трафіком і його ковзним середнім чітко простежується: графік відображає лінійний зв’язок, що є індикатором коректності обраного підходу до згладжування.

У нижньому ряду зображень подано часові графіки. На першому з них відображено зміну трафіку в часі у вигляді кривої, що фіксує загальну тенденцію з коливаннями. Аналогічний графік побудовано і для ковзного середнього, який характеризується менш вираженими флуктуаціями. Одне з вікон демонструє сталу кількість спостережень у часі, що підтверджує рівномірність збирання даних. Інші графіки ілюструють загальні тенденції зміни окремих параметрів: один відображає приріст або лінійне зростання, інший фіксує коливання трафіку, можливо, у результаті зовнішніх впливів або внутрішньосистемних процесів. У сукупності ці візуалізації дозволяють не лише оцінити динаміку трафіку, але й перевірити адекватність вибраних методів згладжування та моделювання.

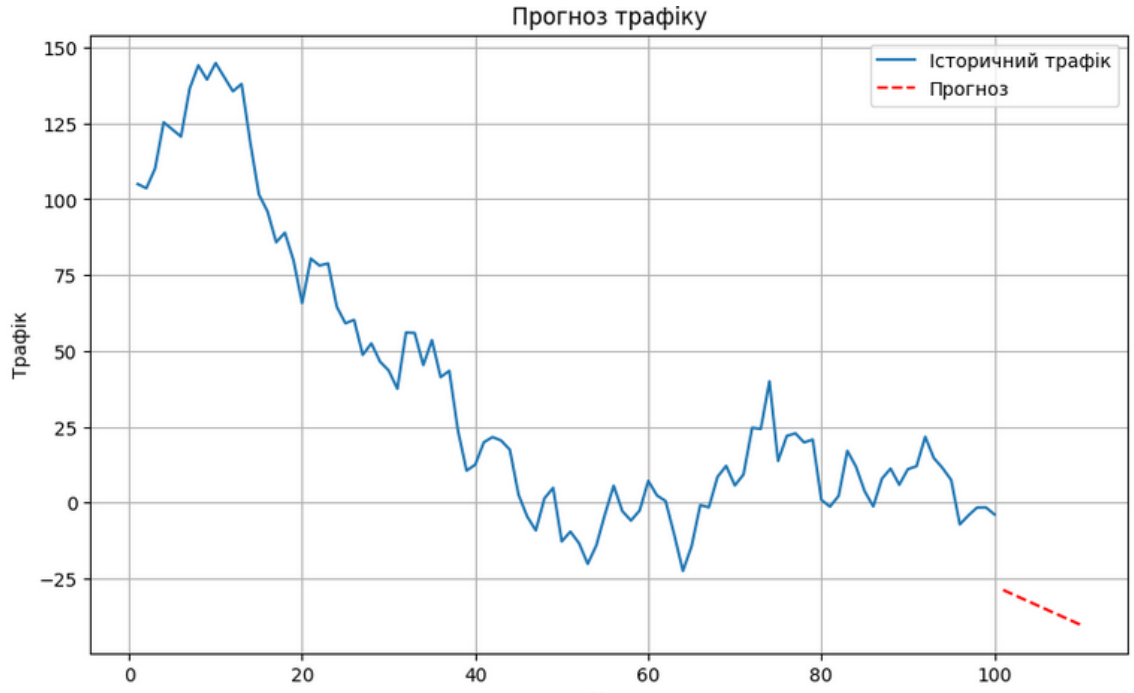


Рисунок 3.2 – Прогноз трафіку

На рисунку 3.2 зображено результат прогнозування мережевого трафіку, що складається з двох ключових елементів: історичних даних та прогнозної моделі. Суцільна синя лінія репрезентує історичний трафік – реальні значення, зафіксовані у попередні часові відрізки. Цей фрагмент графіка ілюструє характерну нелінійну динаміку: на початку спостерігається різке зростання трафіку до пікових значень, після чого простежується

поступове зниження з численними локальними коливаннями, що вказує на наявність флуктуацій та періодичних змін у навантаженні мережі.

Пунктирна червона лінія на правому краю графіка представляє прогноз – результат моделі, яка базується на попередньому тренді та статистичних або машинно-навчальних підходах. Видиме продовження низхідної тенденції в прогнозі свідчить про припущення моделі щодо подальшого зниження трафіку. Водночас, відхилення прогнозу нижче нуля може свідчити про обмеження моделі: або недостатню адаптацію до специфіки даних, або відсутність коригування для реалістичних меж (наприклад, трафік фізично не може бути від'ємним). Це підкреслює важливість застосування додаткових методів нормалізації, перевірки адекватності прогнозної моделі та її валідації на контрольних вибірках.

У цілому графік виконує важливу функцію візуального порівняння між реальною поведінкою системи і її математичною моделлю, що є критично важливим етапом у процесі аналізу ефективності прогнозування. За потреби можу доповнити аналіз автоматичним визначенням аномалій, побудовою довірчого інтервалу або використанням моделей, стійких до шуму.

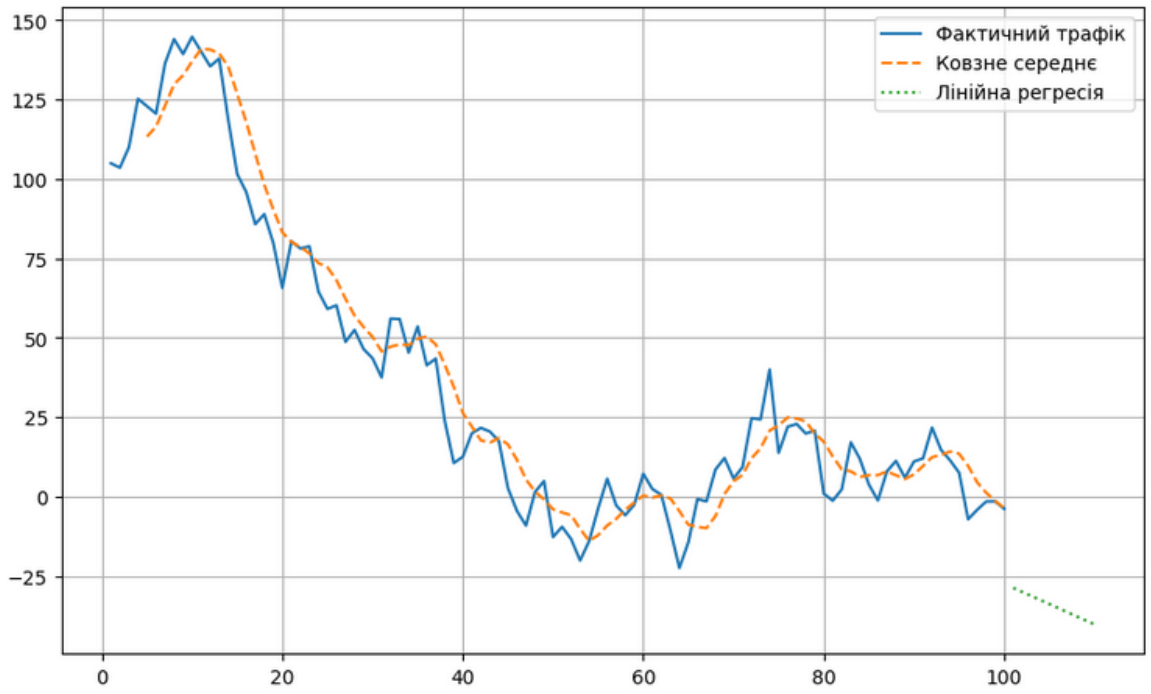


Рисунок 3.3 – Порівняння з ковзним середнім

Рисунок 3.3 демонструє порівняльний аналіз трьох підходів до представлення та прогнозування мережевого трафіку: фактичних значень, згладжування за допомогою ковзного середнього та прогнозу, побудованого за допомогою лінійної регресії. Суцільна синя лінія ілюструє реальний трафік, який характеризується вираженою волатильністю, наявністю різких піків та спадів, що вказує на нестабільну поведінку системи протягом спостережуваного періоду. Такий тип часових рядів є типовим для корпоративних мереж, де навантаження змінюється під впливом як внутрішніх, так і зовнішніх факторів.

Помаранчева пунктирна лінія відображає ковзне середнє, яке застосовується для згладжування флуктуацій і виявлення базової тенденції. Як видно з графіка, ця лінія слідує за основною формою фактичного трафіку, але приглушує різкі коливання, дозволяючи краще візуалізувати тренд. Ковзне середнє виступає ефективним методом попередньої обробки даних, особливо у випадках, коли необхідно зменшити вплив шуму перед побудовою моделі прогнозу.

Зелена штрихова лінія репрезентує результат застосування лінійної регресії. Вона надає найпростішу апроксимацію загального тренду, проектуючи зниження трафіку в майбутнє. Однак варто зазначити, що такий підхід не враховує нелінійних змін, сезонності або циклічності, які можуть бути властивими для реального трафіку. Це може призводити до суттєвих відхилень між прогнозом і фактичними значеннями, особливо при довгостроковому прогнозуванні.

Загалом, графік ілюструє важливість поєднання кількох аналітичних методів – ля виявлення трендів, згладжування даних та формування прогнозу. Такий підхід дозволяє побудувати більш обґрунтовану модель, що може бути адаптована до складних динамічних процесів у мережевому середовищі.

Рисунок 3.4 – Проста модель мережі Петрі

На рисунку 3.4 представлено просту модель мережі Петрі, що ілюструє процес передачі трафіку між двома серверами через маршрутизатор. Схема складається з трьох основних місць – Сервер 1», «Маршрутизатор» та «Сервер 2», які з’єднані між собою через два переходи (прямокутники), що символізують дії або події: передача трафіку від першого сервера до маршрутизатора, а потім від маршрутизатора до другого сервера.

Ця модель добре демонструє послідовну передачу даних: у класичному формалізмі мереж Петрі вона може інтерпретуватися як обробка інформації або транзакцій, де фішка (умовно – пакет або запит) переміщується через вузли мережі. Кожен перехід відбувається лише за умови, що у відповідному місці присутня фішка, тобто трафік фізично надходить до вузла, здатного його обробити чи передати далі.

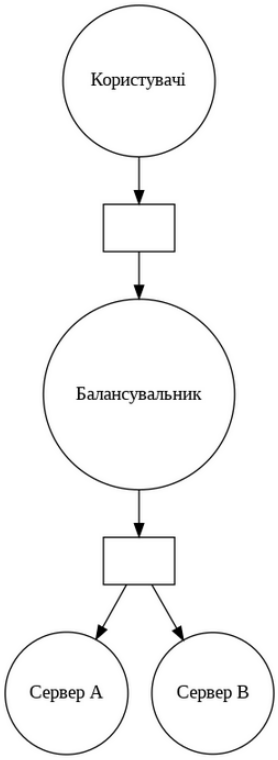


Рисунок 3.5 – Навантаження на сервери

На рисунку 3.5 подано розширену модель мережі Петрі, яка ілюструє процес балансування навантаження між двома серверами. Структура містить ключові елементи: місце "Користувачі", перехід до вузла "Балансувальник", після якого відбувається розгалуження на два окремі місця – "Сервер А" і "Сервер В".

У термінах мереж Петрі, фішка (яка в цьому випадку може означати запит користувача або пакет даних) надходить від місця "Користувачі" до переходу, що ініціює взаємодію з балансувальником. Балансувальник виступає як проміжний вузол, який приймає вхідні фішки та передає їх до іншого переходу. Саме на цьому етапі реалізується розподіл трафіку, тобто фішка може бути надіслана або до сервера А, або до сервера В.

Цей сценарій демонструє недетермінізм або паралелізм у мережах Петрі: після активації балансу фішка може піти будь-яким із доступних шляхів, що відображає реальну логіку роботи балансувальників у корпоративних мережах. Така модель дозволяє аналізувати ефективність

розподілу навантаження, виявляти потенційні вузькі місця або дисбаланс у використанні серверних ресурсів.

Модель може бути легко ускладнена за рахунок додавання умов переходу (наприклад, пріоритети, типи трафіку), часових обмежень або інтеграції з модулями моніторингу.

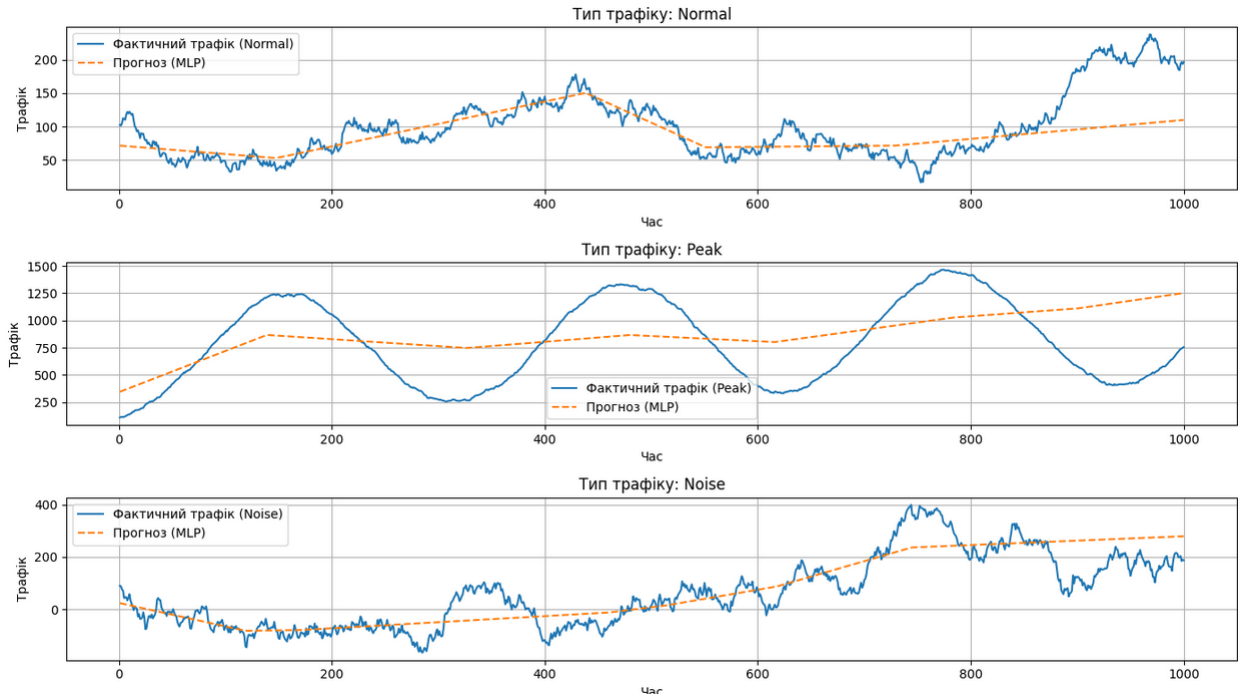


Рисунок 3.6 – Порівняння реальних і передбачених значень з різними типами трафіку

На рисунку 3.6 представлено результати прогнозування трьох різних типів мережевого трафіку за допомогою штучної нейронної мережі, зокрема моделі багатошарового персептрону (MLP). Графік поділений на три секції, кожна з яких демонструє співставлення між фактичним трафіком (суцільна синя лінія) та прогнозованим значенням (пунктирна помаранчева лінія) для відповідного типу навантаження: «Normal», «Peak» та «Noise».

У першій частині показано звичайний (Normal) трафік. Він характеризується загальною стабільністю з помірними флуктуаціями, що створює сприятливі умови для прогнозування. Прогноз моделі MLP в цілому відображає глобальну тенденцію зростання, однак через лінійний характер

прогнозної траєкторії не враховує локальних відхилень, характерних для фактичних даних. Це свідчить про обмеження моделі в деталізації короткострокових коливань.

Другий графік ілюструє піковий (Peak) трафік, який має яскраво виражену синусоїдальну природу, тобто періодичні коливання великої амплітуди. У цьому випадку модель MLP не встигає за змінами та апроксимує коливальний процес за допомогою згладженого зростання. Це свідчить про недостатню здатність базової нейромережевої моделі відтворити складну циклічну динаміку без попередньої обробки або застосування спеціалізованих архітектур, таких як рекурентні мережі.

На третьому графіку відображено шумовий (Noise) трафік, що характеризується високою мінливістю та стохастичною природою змін. Незважаючи на значні коливання, прогнозна лінія демонструє загальний тренд, який частково відображає зростання у структурі даних. Водночас сильна варіативність у реальних значеннях значною мірою перевищує можливості моделі забезпечити точне відтворення.

Загалом аналіз демонструє, що модель MLP здатна уловлювати загальні тенденції, однак її точність залежить від характеру трафіку: вона є більш ефективною для згладжених або трендових даних і менш надійною в умовах складної періодичності або високого рівня шуму. Це підкреслює необхідність адаптації моделі до типу вхідних даних або поєднання кількох методів для досягнення точнішого прогнозу.

На зображенні представлено розширену кольорову мережу Петрі, яка моделює процес обробки трафіку в залежності від його типу. Візуалізація охоплює кілька логічних етапів: ідентифікацію типу трафіку, фільтрацію, централізовану обробку, а також розподіл результатів на моніторинг або логування. Колірне кодування допомагає відрізняти типи вхідних даних та функціональні елементи мережі.

У верхній частині схеми знаходяться три місця, які відповідають за надходження різних типів трафіку: Normal (блакитний), Peak (помаранчевий)

і Noise (сірий). Кожен із цих потоків надходить до відповідного фільтра – окремого вузла, який виконує попередню обробку. Ці фільтри представлені зеленими колами і позначені як Фільтр 1, Фільтр 2 та Фільтр 3 відповідно. Далі трафік через переходи передається до центрального вузла – Процесора (жовтий елемент), який виконує основну обробку незалежно від типу вхідного трафіку.

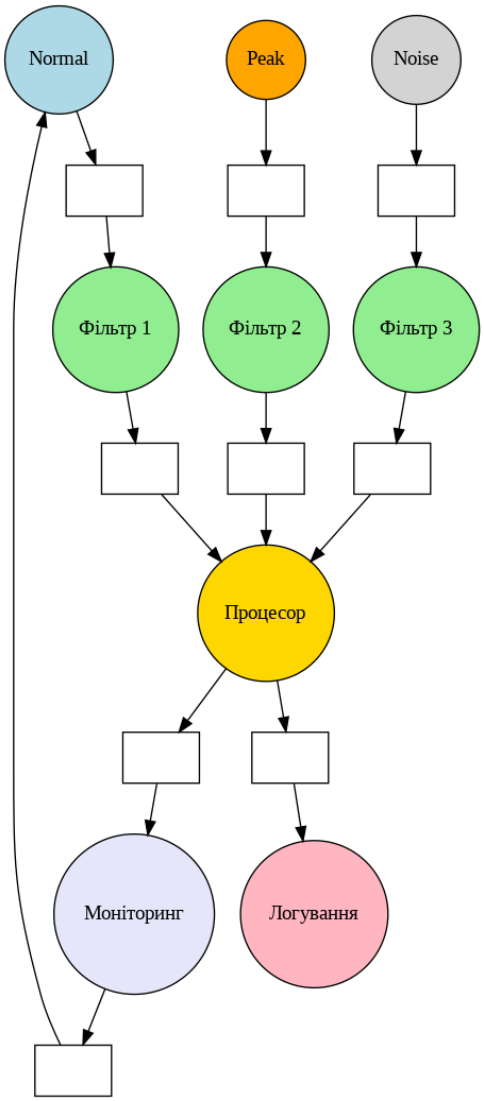


Рисунок 3.7 – Розширена кольорова мережа Петрі: Обробка різного трафіку та маршрутизація

Після обробки система має два виходи: один веде до Модулю моніторингу (світло-фіолетовий вузол), інший – до Модуля логування (рожевий вузол). Це дозволяє розділяти результати в залежності від потреб

аналізу або архівування. Важливою деталлю є те, що з блоку моніторингу є зворотний зв’язок до початкового місця Normal, що відображає циклічну поведінку системи або можливість повторного аналізу/обробки.

Ця кольорова модель Петрі добре ілюструє багатоканальну обробку неоднорідного трафіку, а також демонструє можливість повторного використання або адаптації даних. Вона є придатною для опису архітектури реальних мережевих або інформаційних систем, де важливе значення має як тип навантаження, так і його обробка в залежності від призначення. Якщо потрібно – можу додати часову логіку переходів або інтегрувати модель з Python-симулятором для динамічного моделювання.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було всебічно досліджено проблематику прогнозування мережевого трафіку в умовах корпоративних інформаційних систем. Проведений аналіз сучасних підходів дозволив встановити, що ефективне управління трафіком вимагає не лише математично коректних моделей, але й адаптивних механізмів, здатних відображати складну динаміку і неоднорідність даних, притаманну реальним мережам.

Важливим теоретичним досягненням стало обґрунтування доцільності використання мереж Петрі як базової формалізованої моделі для опису процесів у корпоративних мережах. Завдяки своїй здатності відображати паралелізм, конкуренцію, умовні переходи та причинно-наслідкові зв’язки, мережі Петрі продемонстрували високий рівень придатності для моделювання маршрутизації, балансування навантаження, фільтрації даних та взаємодії між функціональними блоками інфраструктури.

У роботі було реалізовано як базові, так і розширені варіанти мереж Петрі, зокрема – кольорові мережі, що дозволяють ураховувати тип трафіку або його джерело як атрибутивні характеристики фішок. Такі моделі виявилися особливо ефективними для моделювання потоків різної природи – нормального, пікового та шумового, що імітує поведінку корпоративної мережі у реальних умовах.

Для прогнозування трафіку було застосовано як класичні методи (ковзне середнє, лінійна регресія), так і підходи на основі машинного навчання, зокрема штучні нейронні мережі (MLPRegressor). Результати експериментального моделювання засвідчили, що нейромережеві моделі демонструють вищу здатність до узагальнення трендів у складних або зашумлених даних, хоча можуть поступатися простішим алгоритмам у випадках із чітко вираженою періодичністю. Було також підтверджено, що

ефективність прогнозу значною мірою залежить від типу вхідного трафіку, що ще раз підкреслює важливість правильної класифікації даних.

Інтеграція моделей прогнозування у структуру мереж Петрі дозволила реалізувати не лише аналітичне, а й симуляційне середовище, придатне для подальших досліджень, зокрема динамічного аналізу навантаження в реальному часі. В роботі представлено приклади візуалізації, реалізовані за допомогою Python та бібліотеки graphviz, що зробило описані процеси більш наочними і прикладними.

Отже, результати проведеного дослідження підтверджують доцільність використання мереж Петрі як універсального інструменту для моделювання і прогнозування мережевого трафіку в корпоративних системах. Запропоновані методики можуть бути адаптовані для побудови реальних аналітичних платформ, розширення засобів мережевого моніторингу, автоматичного балансування навантаження та прийняття управлінських рішень у сфері інформаційної інфраструктури.

За результатами роботи опубліковано статтю в фаховому виданні [9].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Michael J. Kavis. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). 1st ed, Wiley, 2014. 224 p.

2. Jean-Georges Perrin. Spark in Action. 2nd ed, Manning, 2020. 576 p.

3. Jack G Nestell, David L Olson Professor. Successful ERP Systems: A Guide for Businesses and Executives. Business Expert Press, 2017. 134 p.

4. Brij Kishore Pandey, Emily Ro Schoof. Building ETL Pipelines with Python: Create and deploy enterprise-ready ETL pipelines by employing modern methods. 1st ed, Packt Publishing, 2023. 246 p.

5. Edward Pollack. Analytics Optimization with Columnstore Indexes in Microsoft SQL Server: Optimizing OLAP Workloads. 1st ed, Apress, 2022. 300 p.

6. Flach P. A. Machine Learning: The Art and Science of Algoritms that Makes Sense of Data. Cambridge: Cambridge University Press, 2012. 291 p. https://doi.org/10.1017/CBO9780511973000

7. Rolf Oppliger. Ssl and Tls: Theory and Practice.3rd ed, Artech House, 2023. 388 p.

8. Dr. Logan Song. The Self-Taught Cloud Computing Engineer: A comprehensive professional study guide to AWS, Azure, and GCP. 1st ed., Packt Publishing, 2023. 472 p.

9. Diachenko D., Korobeinikov M., Korobeinikov O., Kovalenko A., Kravchenko P. Data processing methods in a corporate network. Системи управління, навігації та зв’язку, вип.3. Полтава, 2025. С. 81-86.