Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інфокомунікаційних систем і технологій

Бакалаврська кваліфікаційна робота на тему:

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОЗПОДІЛУ ТРАФІКУ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Виконав: студент 4-го курсу, групи ПЗТ-21б
спеціальності 172 – Телекомунікації та радіотехніка
Валігура Д.В.

Керівник: д.т.н., доц., проф. каф. ІКСТ
Михалевський Д.В.
«12» червня 2025 р.

Рецензент: д.т.н., доц., доцент каф. ІРТС
Осадчук Я.О.
«12» червня 2025 р.

Допущено до захисту
Завідувач кафедри ІКСТ
д.т.н., проф. Кичак В.М.
«12» 06 2025 р.

Вінниця ВНТУ – 2025 рік

Вінницький національний технічний університет

Факультет інформаційних електронних систем

Кафедра інфокомунікаційних систем і технологій

Рівень вищої освіти перший (бакалаврський)

Галузь знань 17 – Електроніка та телекомунікації

Спеціальність 172 –Телекомунікації та радіотехніка

Освітня програма – Програмне забезпечення телекомунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКСТ
д.т.н., професор В.М.Кичак
"5" 05 2025 р.

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ

Валігурі Данилу Вадимовичу .
(прізвище, ім'я, по батькові)

1. Тема роботи: Підвищення ефективності розподілу трафіку у телекомунікаційних мережах

керівник роботи Михалевський Дмитро Валерійович, д.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ВНТУ від "20" березня 2025 року № 97

2. Строк подання студентом роботи: 9 червня 2025 року

3. Вихідні дані до роботи: інтенсивність трафіку – середня; швидкість передачі даних – 1–300Мбіт/с; розмір мережі – 10–100 вузлів; топологія – динамічна; протокол – AODV, OLSR, B.A.T.M.A.N.; область застосування – мережа передачі даних

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): огляд теоретичних аспектів; аналіз існуючих методів розподілу трафіку; оптимізація розподілу трафіку; модель ефективного розподілу трафіку, охорона праці.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Архітектура існуючих телекомунікаційних мереж; Класифікація телекомунікаційних мереж; Маршрутизація; Класифікація протоколів маршрутизації; Порівняння протоколів маршрутизації; Алгоритм конструювання трафіку

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийня
Спеціальна частина	Михалевський Д.В. професор кафедри ІКСТ	05.05.2025	12.06.2025
Охорона праці	Дембіцька С. В. професор кафедри БЖДПБ	05.05.2025	12.06.2025

7. Дата видачі завдання «5» травня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської кваліфікаційної роботи	Строк виконання етапів роботи	При
1	Формування та затвердження теми та індивідуального завдання бакалаврської кваліфікаційної роботи (БКР)	06.05.2025р.	
2	Виконання спеціальної частини БКР. Перший рубіжний контроль виконання БКР	19.05.2025р.	
3	Виконання спеціальної частини БКР. Другий рубіжний контроль виконання БКР	31.05.2025р.	
4	Виконання розділу «Охорона праці»	04.06.2025р.	
5	Нормоконтроль БКР	09.06.2025р.	
6	Попередній захист БКР	10.06.2025р.	
7	Рецензування БКР	11.06.2025р.	
8	Захист БКР	13.06.2025р.	

Студент _____ (підпис) Валігура Д.В.

Керівник роботи _____ (підпис) Михалевський Д.В.

АНОТАЦІЯ

УДК 621.397

Валігура Данило Вадимович. Підвищення ефективності розподілу трафіку у телекомунікаційних мережах. – Вінниця: ВНТУ, 2025. – 86с.

На українській мові. Бібліогр.: 32 назв; Рис.: 40; Табл.: 9.

Бакалаврська кваліфікаційна робота присвячена дослідженню ефективних методів розподілу траіку у сучасних телекомуніаційних мережа. У роботі було проаналізовано традиційні та новітні методи маршрутизації та баналсування трафіку. Запропоновано метод констуювання трафіку. Розглянуто питання безпеки життєдіяльності та охорони праці.

Ключові слова: трафік, мережа, маршрутизація.

ANNOTATION

UDK 621.397

Valihura Danylo Vadymovych. Increasing the efficiency of traffic distribution in telecommunication networks. Bachelor thesis. – Vinnytsya: VNTU, 2025. – 86 pp.

In Ukrainian language. Refs.: 32 titles; Figs.: 40; Tables: 9.

The bachelor thesis is devoted to the study of effective methods of traffic distribution in modern telecommunication networks. The work analyzed traditional and modern methods of routing and traffic banalization. A method of traffic construction is proposed. Issues of industrial and occupational safety were considered.

Keywords: traffic, network, routing.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

МН – машинне навчання

ШІ – штучний інтелект

5G – fifth generation

AI – Artificial Intelligence

BGP – Border Gateway Protocol,

CDN – content delivery network

DDoS – denial-of-service attack

ECMP – Equal Cost Multi-Path

FTTx – fiber to the x

IGRP – Interior Gateway Routing Protocol

IoT – Internet of things

LTE– Long-term evolution

ML – Machine Learning

MPLS – Multiprotocol Label Switching

NFV – Network Function Virtualization

OSI – Open Systems Interconnection

OSPF – Open Shortest Path First

PBR – Policy-Based Routing

RED – Random Early Detection

RIP – Routing Information Protocol

RL – Reinforcement Learning

SDN – Software-Defined Networking

STP – Spanning Tree Protocol

VLAN – Virtual Local Area Network

VoIP – Voice over Internet Protocol

VPN – Virtual Private Network

QoS – Quality of service

ВСТУП

Актуальність теми. Інформаційні технології стали невід'ємною частиною сучасного світу. З кожним роком кількість користувачів телекомунікаційних послуг стрімко зростає, а разом із цим зростають і вимоги до якості та швидкості передавання даних. На фоні цифровізації всіх сфер життя – від побуту до промисловості та державного управління – телекомунікаційна інфраструктура набуває статусу критично важливої. Саме тому питання ефективного функціонування телекомунікаційних мереж, зокрема ефективного розподілу трафіку, є надзвичайно актуальним.

Під терміном «розподіл трафіку» розуміють процес маршрутизації інформаційних потоків у межах мережі з метою оптимального використання її ресурсів. Від якості організації цього процесу залежить затримка передачі даних, пропускна здатність каналів зв’язку, надійність і стійкість мережі до збоїв. Невдалий або застарілий підхід до розподілу трафіку може призвести до перевантаження окремих вузлів, втрати пакетів, збільшення часу відповіді сервісів або навіть до часткової відмови мережі.

У класичних мережах, побудованих на базі традиційних маршрутизаторів, розподіл трафіку зазвичай здійснюється на основі статичних або динамічних маршрутів. Проте у складних та масштабованих топологіях цього часто виявляється недостатньо. З появою інтелектуальних алгоритмів маршрутизації, технологій програмно-конфігурованих мереж (SDN), багатошляхової маршрутизації (ECMP), а також засобів балансування навантаження, відкрилися нові можливості для ефективного управління трафіком.

Водночас зростання популярності потокового відео, хмарних сервісів, інтернету речей (IoT), віртуальних приватних мереж (VPN) та мобільного інтернету (особливо у 5G-мережах) створює нові виклики. Структура трафіку стає дедалі більш динамічною, непередбачуваною і неоднорідною, що ускладнює завдання ефективного його розподілу.

Актуальність дослідження полягає у необхідності знаходження нових або

вдосконалення існуючих підходів до управління трафіком, які дозволять забезпечити високу якість обслуговування (QoS), гнучкість, масштабованість і стійкість телекомунікаційних мереж до збоїв і атак. Саме ефективне управління трафіком є тим інструментом, що дозволяє досягати оптимального балансу між навантаженням на інфраструктуру і якістю надання послуг.

Аналіз останніх досліджень. Вирішенню проблеми розподілу трафіка у телекомунікаційних мережах присвячено праці відомих вітчизняних та закордонних вчених, таких як Климаш М.М., Ложковський А.Г., Захарченко С.М.,. та інші [1–8].

Об'єкт дослідження – телекомунікаційні мережі, що функціонують у динамічному середовищі з високим навантаженням.

Предмет дослідження – методи та алгоритми розподілу трафіку, які спрямовані на підвищення ефективності функціонування телекомунікаційних мереж.

Мета та задачі дослідження. Метою даної бакалаврської кваліфікаційної роботи є аналіз сучасних підходів до розподілу трафіку в телекомунікаційних мережах та дослідження можливостей їх вдосконалення з метою підвищення ефективності роботи мережевої інфраструктури.

Для досягнення мети необхідно розв'язати такі задачі:

а) провести огляд сучасного стану телекомунікаційних мереж та методів розподілу трафіку;

б) проаналізувати наявні проблеми та обмеження існуючих рішень;

в) дослідити перспективні підходи до підвищення ефективності розподілу трафіку;

г) сформулювати рекомендації щодо покращення функціонування телекомунікаційних мереж.

Апробація результатів роботи. Основні ідеї роботи доповідались і обговорювались на LIV Всеукраїнській науково-технічній конференції підрозділів Вінницького національного технічного університету (2025).

1 ОГЛЯД ТЕОРЕТИЧНИХ АСПЕКТІВ

1.1 Основні поняття та характеристики телекомунікаційного трафіку

Телекомунікаційний трафік є ключовим поняттям у сфері побудови та функціонування комп'ютерних і телекомунікаційних мереж. Під трафіком у загальному розумінні мають на увазі обсяг даних, що передається мережею між її вузлами протягом певного проміжку часу. Саме обробка, передача та ефективний розподіл трафіку визначають продуктивність і якість роботи телекомунікаційної інфраструктури.

З огляду на постійне зростання кількості інтернет-користувачів, а також розвиток хмарних технологій, мультимедійних сервісів, мобільного зв'язку та Інтернету речей (IoT), трафік в телекомунікаційних мережах набуває нових масштабів та характеристик. Це створює додаткові виклики щодо управління та маршрутизації потоків даних.

Телекомунікаційний трафік можна класифікувати за низкою ознак:

За характером переданих даних розрізняють:

а) Голосовий трафік – потребує мінімальної затримки та джиттера.

б) Відеотрафік) – потребує стабільної пропускної здатності.

в) Дані – більш гнучкі до затримок.

г) Машинний трафік – часто має періодичний або сигнальний характер, але може бути критичним за пріоритетністю.

За напрямом руху розрізняють:

д) Вхідний трафік (downlink) – від зовнішніх джерел до користувача (наприлад, завантаження вебсторінки).

е) Вихідний трафік (uplink) – від користувача до сервера (наприклад, відправлення електронної пошти).

ж) Транзитний трафік – проходить через мережу без зміни джерела чи кінцевого одержувача.

За типом з'єднання розрізняють:

а) Унікаст (unicast) – передача даних від одного джерела до одного одержувача.

б)Мультикаст (multicast) – передача від одного джерела до групи адресатів.

в)Бродкаст (broadcast) – передача до всіх пристроїв у мережі.

За часом активності розрізняють:

а)Постійний (потоковий) – безперервний трафік (наприклад, відеоконференції).

б)Інтервальний (імпульсний) – дані передаються періодично або за потреби.

Для аналізу ефективності розподілу трафіку важливо враховувати його основні технічні характеристики.

Пропускна здатність – це максимальний обсяг даних, який може бути переданий через канал зв’язку за одиницю часу, вимірюється в біт/с (bps). Визначає загальну «ємність» мережі.

Затримка – це час, необхідний для доставки пакета від джерела до призначення. Суттєво впливає на якість голосових та відеосервісів.

Джиттер – це варіація затримки доставки пакетів. Особливо критичний для трафіку реального часу, оскільки нестабільна доставка призводить до втрати якості звуку чи зображення.

Втрати пакетів – це частина трафіку, що не доходить до призначення. Може бути спричинена перевантаженням, помилками або збоєм в обладнанні.

Щільність – це співвідношення між фактичним і максимальним обсягом трафіку на каналі. Визначає ступінь навантаження мережі.

Середній розмір пакета може впливати на ефективність маршрутизації і на вибір оптимального алгоритму обробки трафіку.

Особливістю сучасного трафіку є його висока варіативність у часі та просторі. В години пікового навантаження (наприклад, з 19:00 до 22:00 у міських мережах) спостерігається значне зростання обсягів трафіку, що може призводити до перевантаження вузлів. З іншого боку, у корпоративних мережах найінте-

нсивніше навантаження фіксується в робочий час.

Також трафік може бути «симетричним» (вхідний дорівнює вихідному) або «асиметричним» (один з напрямків домінує), що важливо враховувати при проєктуванні систем маршрутизації.

У провайдерських мережах аналіз характеристик трафіку дозволяє:

а) планувати модернізацію каналів зв’язку;

б) виявляти DDoS-атаки або аномальні сплески навантаження;

в) оптимізувати розміщення кеш-серверів;

г) прогнозувати трафік для майбутніх періодів з використанням моделей машинного навчання.

У приватних корпоративних мережах трафік аналізується для:

а) визначення продуктивності окремих підрозділів;

в) забезпечення пріоритету критичних сервісів (наприклад, VoIP);

г) контролю доступу та безпеки.

1.2 Сучасні телекомунікаційні мережі

Телекомунікаційні мережі є критичною інфраструктурою сучасного цифрового суспільства (рис.1.1). Вони забезпечують безперервний потік інформації між користувачами, сервісами, пристроями та системами у глобальному масштабі. Для ефективного функціонування таких мереж важливим є правильний вибір їхньої структури (топології) та технологій, які визначають механізми обміну даними, рівень масштабованості, надійність і ефективність розподілу трафіку.

Основною тенденцією проєктування телекомунікаційних мереж є так звана «Трирівнева модель організації мережі» (рис.1.2). Вона є логічною і має високу ступінь надійності за рахунок апаратної надмірності. Мережа розділена на три рівні: ядро мережі (Core layer); рівень розподілу (Distribution layer); рівень доступу (Access layer)

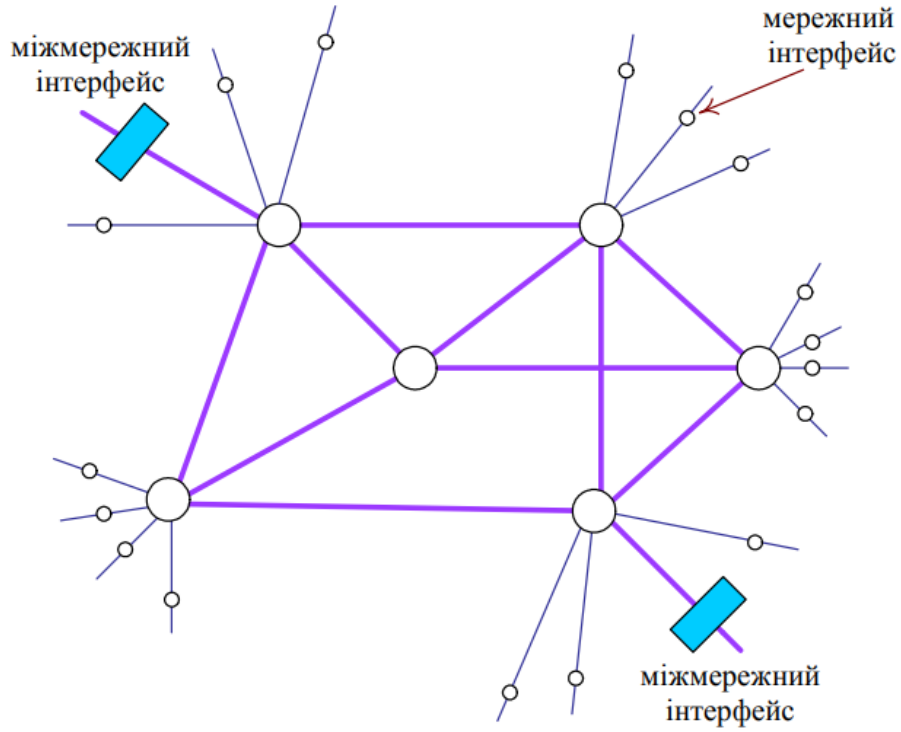


Рисунок 1.1 – Телекомунікаційна мережа

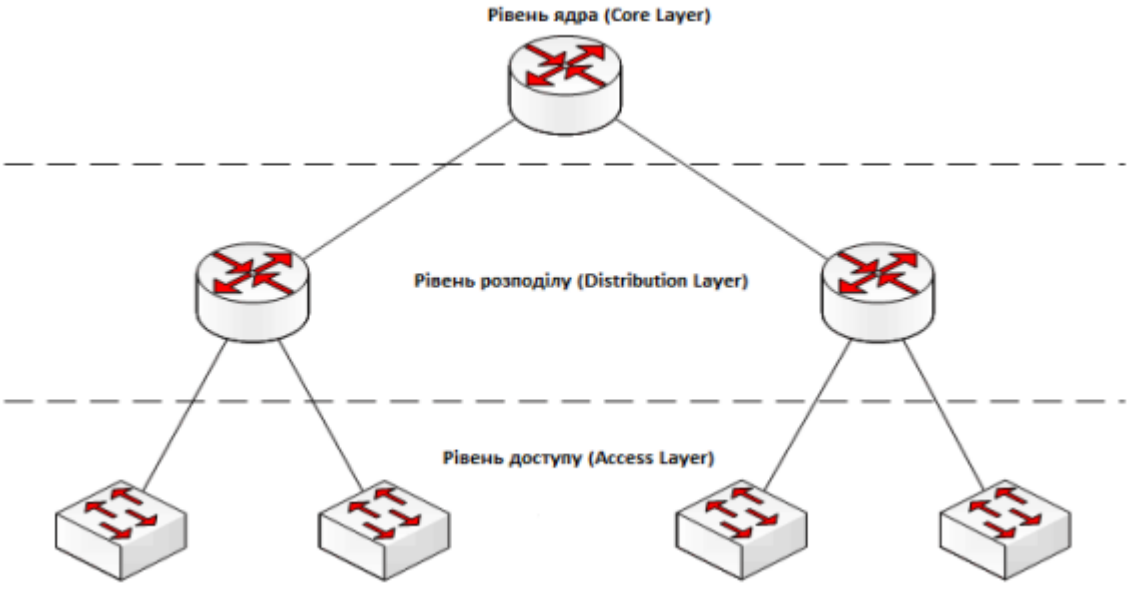


Рисунок 1.2 – Трирівнева ієрархічна модель організації мережі

Ядро мережі формується на рівні ядра (базовому). Цей рівень, найвищий у ієрархії, відповідає за швидку та надійне пересилання великих обсягів трафіку, а також за з’єднання мережі з мережами інших провайдерів. Якщо виникне-

помилка на базовому рівні, вона вплине на всіх користувачів. Отже, забезпечити високу надійність на базовому рівні має вирішальне значення. На цьому рівні обробляються значні кількості трафіку, тому важливо враховувати затримки та швидкість. На цьому рівні повнозв’язана топологія буде прийнятною.

Рівень робочих груп, також відомий як рівень розподілу, розташований між рівнем доступу та базовим рівнем. Рівень розподілу повинен розробити найшвидший метод обробки запитів від служб. Після визначення найкращого шляху доступу на рівні розподілу запит може бути переданий на базовий рівень. На цьому рівні запит можна швидко доставити до потрібної служби. Маршрутизація, фільтрація та доступ до регіональних мереж є основними завданнями рівня розподілу, а також, якщо необхідно, визначення правил доступу пакетів до базового рівня. У топології цього рівня використовується кільце або подвійне кільце.

Рівень доступу: дозволяє користувачам і робочим групам контролювати доступ до ресурсів об'єднаної мережі. Користувачі безпосередньо фізично підключаються до рівня доступу. Цей рівень має деревоподібну топологію.

Топологія мережі – це логічна або фізична структура, яка визначає, як вузли з'єднані між собою і як відбувається передача даних. Кожен тип топології має свої переваги та недоліки щодо складності реалізації, вартості, стійкості до збоїв і здатності до масштабування.

Шинна мережа (рис.1.3) – усі вузли підключені до одного загального каналу передачі даних. Переваги: простота реалізації, низька вартість. Недоліки: обмежена пропускна здатність, складність виявлення помилок.

Зірка (рис.1.4) – усі вузли підключені до центрального комутатора або маршрутизатора. Це одна з найпоширеніших топологій. Переваги: простота управління, ізоляція збоїв. Недоліки: вразливість до відмови центрального вузла.

Кільцева (рис.1.5)– вузли з’єднані послідовно і формують замкнуте коло. Пакети передаються від одного вузла до іншого за заданим напрямом. Переваги: чітке управління трафіком. Недоліки: вихід з ладу одного вузла може призвести до відмови мережі.

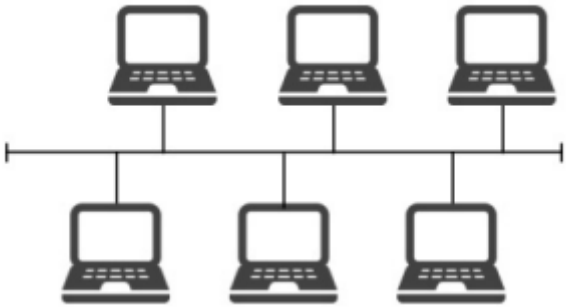


Рисунок 1.3 – Топологія «Шина»

Рисунок 1.4 – Топологія «Зірка»

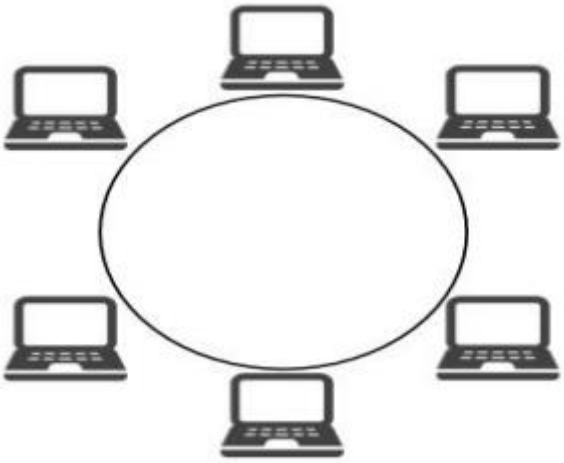


Рисунок 1.5 – Топологія «Кільце»

Комірчаста (рис.1.6)– кожен вузол підключений до кількох інших вузлів, забезпечуючи декілька шляхів передачі. Переваги: висока надійність і відмовостійкість. Недоліки: складність конфігурації, висока вартість.

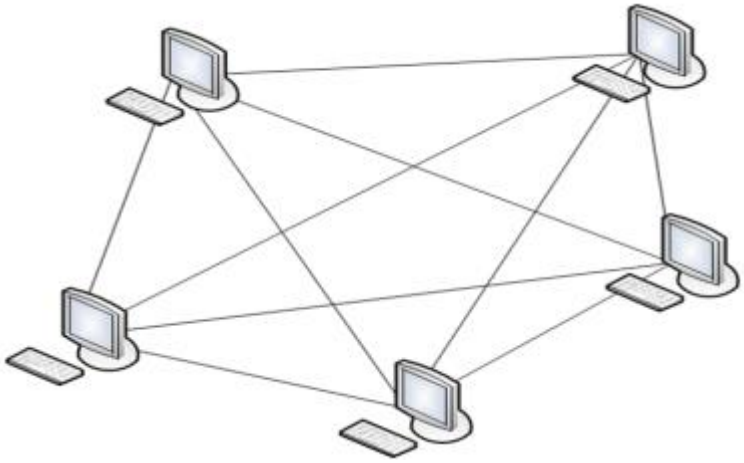


Рисунок 1.7 – Топологія «Комірчаста»

Ієрархічна (деревовидна) – комбінує принципи зірки та шини. Вузли організовані у вигляді дерева з коренем у центральному маршрутизаторі. Підходить для масштабованих корпоративних мереж.

У сучасних умовах дедалі частіше використовуються гібридні топології, які поєднують кілька варіантів одночасно, забезпечуючи баланс між продуктивністю та гнучкістю мережі.

Технології телекомунікаційних мереж постійно еволюціонують – від традиційних дротових з'єднань до бездротових і програмно-керованих рішень. Нижче подано огляд основних технологій, що використовуються у побудові сучасних мереж:

Ethernet і Fast Ethernet/Gigabit Ethernet – це найпоширеніша технологія локальних мереж (LAN). Вона забезпечує швидкість передачі від 100 Мбіт/с до 100 Гбіт/с та працює за принципом комутації кадрів і підтримує топології «зірка» та «сітка».

xDSL (Digital Subscriber Line) – це технологія широкосмугового доступу

через телефонні лінії, яка використовується в домашніх мережах та малому бізнесі. Застаріла у великих масштабах, але досі актуальна в регіонах без оптоволокна.

Оптоволоконні технології (FTTx) мають надзвичайно високуа пропускну здатність (до кількох терабіт/с), а також підвищені стабільність і надійність. Підходять для побудови магістральних мереж (backbone) та дата-центрів.

Бездротові технології (Wi-Fi, LTE, 5G). Wi-Fi є основними в домашніх і офісних мережах. LTE/4G/5G – мобільний широкосмуговий доступ, зростаюча роль у розподілених мережах і IoT. Переваги: мобільність, простота розгортання. Недоліки: змінна якість зв’язку.

MPLS (Multiprotocol Label Switching) – це протокол передачі даних, який дозволяє маршрутизувати трафік не за IP-адресами, а за мітками (labels). Підвищує швидкість передачі та забезпечує можливість створення віртуальних приватних мереж (VPN). Використовується у мережах операторського класу.

SDN (Software-Defined Networking) – це інноваційна архітектура, що відокремлює контрольний рівень від рівня пересилання даних. Дозволяє централізовано керувати всією мережею через програмний контролер. Значно спрощує розподіл трафіку, динамічну маршрутизацію, адаптацію до навантаження.

NFV (Network Function Virtualization) – віртуалізація мережевих функцій, таких як маршрутизатори, фаєрволи, балансувальники навантаження. Дозволяє запускати мережеві сервіси як програмні додатки на звичайних серверах.

Сучасні телекомунікаційні мережі повинні відповідати ряду критеріїв. Масштабованість – це здатність обробляти збільшення кількості користувачів і трафіку. Відмовостійкість – здатність зберігати працездатність у разі збоїв. Гнучкість – можливість швидкої адаптації до нових потреб та технологій. Безпека – захист від несанкціонованого доступу та кіберзагроз. Продуктивність – висока швидкість передачі даних і мінімальні затримки.

Вибір топології та технологій безпосередньо впливає на ефективність розподілу трафіку. У топології «сітка» легше реалізувати балансування навантаження, оскільки існує багато альтернативних маршрутів. Оптоволоконні мережі

дозволяють обслуговувати великі обсяги трафіку з мінімальними затримками. Технології SDN дозволяють централізовано перенаправляти трафік в реальному часі відповідно до змін у навантаженні.

Таким чином, сучасні мережі повинні будуватися з урахуванням не лише поточних, але й прогнозованих потреб користувачів, враховуючи гнучкість, надійність і здатність до інтелектуального управління потоками трафіку.

1.3 Методи розподілу трафіку

Ефективне управління телекомунікаційним трафіком є одним із ключових завдань при проєктуванні та експлуатації мереж. У зв'язку з постійним зростанням обсягів переданих даних, підвищенням кількості підключених пристроїв та широким розповсюдженням сервісів реального часу, розподіл трафіку набуває стратегічного значення. Сучасні мережі мають забезпечувати мінімальні затримки, високу пропускну здатність і гарантовану якість обслуговування, що вимагає застосування як класичних, так і інноваційних методів розподілу трафіку.

Маршрутизатори передають дані між мережами. Цей пристрій працює на мережевому рівні моделі Open Systems Interconnection (OSI). Вибір оптимального шляху до мережі призначення та комутація пакетів для передачі є основними завданнями маршрутизатора. Маршрутизатори потребують складної структури мережі, яка включає багато маршрутів і надлишкових зв'язків, а також різні технології передачі даних на фізичному і канальному рівнях.

Коли пристрій має кілька шляхів до пункту призначення, він завжди вибирає найкращий (рис.1.8). Маршрутизація виконується за допомогою маршрутизаторів або за допомогою програмних процесів. Маршрутизатори, засновані на програмному забезпеченні, мають обмежену область дії та обмежені функції. Мета маршрутизації – це вибір найкращого способу перенесення даних з однієї мережі в іншу. Таблиці маршрутизації створюються для забезпечення маршрутизації.

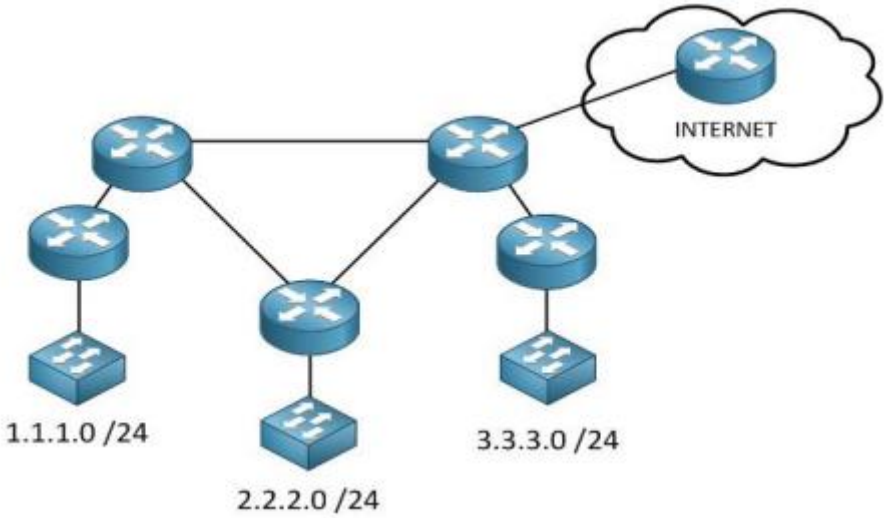


Рисунок 1.8 – Принцип дії маршрутизаторів

Існують декілька традиційних підходів, що використовувалися ще з початку розвитку комп'ютерних мереж.

Найбільш відомий – це статична маршрутизація. В її основі лежать заздалегідь визначені маршрути, які не змінюються автоматично при зміні стану мережі. Переваги – простота реалізації, мінімальні витрати на обчислення. Основний недолік – негнучкість: при виникненні збоїв або перевантажень – ефективність різко знижується.

Також існує динамічна маршрутизація. Використовує протоколи маршрутизації (RIP, OSPF, BGP), які самостійно оновлюють маршрути на основі поточного стану мережі. Переваги: адаптація до змін, можливість масштабування. Недоліки: потреба в періодичному обміні службовими даними, затримки при перерахунку маршрутів.

Відомі спеціальні механізми балансування навантаження (рис.1.9). Трафік розподіляється між кількома каналами або серверами, щоб уникнути перевантаження одного з елементів. Відомі методи – Round Robin, Least Connections, IP Hash. Часто використовується у дата-центрах, хмарних сервісах, мережах CDN.

Рисунок 1.9 – Класифікація алгоритмів балансування навантаження

QoS (Quality of Service) – це система пріоритетів і класифікації трафіку. Критичний трафік (відеоконференції, VoIP) має вищий пріоритет над некритичним (наприклад, завантаження файлів). Дозволяє зменшити затримки, джиттер та втрати пакетів для важливих застосунків.

Ще один підхід – Policy-Based Routing (PBR). Тут рішення про маршрут приймається не лише на основі IP-адрес, а й за іншими ознаками (тип трафіку, додаток, користувач). Застосовується для реалізації індивідуальних сценаріїв обробки трафіку.

З розвитком технологій і зростанням складності мереж виникла потреба в нових, інтелектуальних та адаптивних методах розподілу трафіку. Серед них можна виділити наступні.

SDN (Software-Defined Networking) розділяє контрольний і транспортний рівні, дозволяючи централізовано керувати розподілом трафіку через контролер. Основні переваги: швидке перенаправлення трафіку в разі зміни навантаження; автоматичне резервування та балансування маршрутів; гнучка адаптація до нових вимог сервісів.

Інтелектуальні алгоритми з використанням штучного інтелекту та ма-

шинного навчання (AI/ML). Вони використовуються для прогнозування піків навантаження, виявлення аномалій, оптимізація маршрутів. Алгоритми аналізують історичні дані та поведінку користувачів для визначення найкращих шляхів передачі. Наразі вони впроваджуються в телеком-операторів для автоматизованого управління мережею.

Трафік-інжиніринг – це оптимізація розміщення трафіку з урахуванням мережевих ресурсів, використовується в мережах MPLS та SDN та забезпечує мінімізацію затримок, балансування пропускної здатності та гарантує якість обслуговування.

Content Delivery Networks (CDN) передбачає розміщення контенту на серверах, розташованих ближче до кінцевих користувачів, значно зменшує трафік у магістральних каналах і підвищує швидкість доступу до контенту, активно застосовується для стрімінгових сервісів, онлайн-ігор, медіаплатформ.

Edge Computing передбачає, що обробка трафіку відбувається ближче до джерела даних (на периферії мережі). Це Зменшує обсяг даних, що передаються до центрів обробки, а отже – знижує затримки. Це критично важливо для IoT та автономних систем (розумне місто, транспорт).

Intent-Based Networking (IBN) – це система, що автоматично налаштовує мережу згідно з описаними політиками (наміром користувача). Контролер самостійно визначає, як реалізувати задану політику розподілу трафіку.

Порівняльна характеристика підходів до розподілу трафіку подана у таблиці 1.1.

Розподіл трафіку в телекомунікаційних мережах є багатовимірною задачею, яка вимагає комплексного підходу. У той час як класичні методи забезпечують базову функціональність, інноваційні технології надають інструменти для гнучкого, адаптивного і масштабованого управління мережею в умовах динамічних змін трафіку. У поєднанні з новітніми підходами – такими як SDN, AI/ML, edge computing – можна досягти значного підвищення ефективності роботи мережі, що є особливо актуальним у контексті цифрової трансформації суспільства.

Таблиця 1.1 – Порівняльна характеристика методів розподілу трафіка

Метод	Адаптивність	Масштабованість	Складність реалізації	Використання
Статична маршрутизація	Низька	Низька	Низька	Малі мережі
Динамічна маршрутизація	Середня	Висока	Середня	Провайдери, корпоративні мережі
QoS та PBR	Висока	Середня	Середня	VoIP, відео
SDN	Висока	Висока	Висока	Хмарні середовища, дата-центри
AI/ML	Дуже висока	Висока	Дуже висока	Розподілені мережі, автоматизація
CDN / Edge	Висока	Висока	Середня	Медіасервіси, IoT

2 АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ РОЗПОДІЛУ ТРАФІКУ

2.1 Загальні підходи до класифікації методів розподілу трафіку

Розподіл трафіку в телекомунікаційних мережах є складним завданням, що вимагає врахування багатьох факторів – від фізичних характеристик мережі до логіки роботи протоколів і вимог кінцевих користувачів. Залежно від цілей, архітектури та технічних можливостей мережі, існує велика кількість підходів до реалізації механізмів маршрутизації та балансування навантаження. Для їх систематизації застосовують класифікацію за низкою ключових критеріїв.

За типом керування виділяють централізоване і децентралізоване керування. У централізованих системах рішення щодо маршрутизації приймається одним або кількома центральними контролерами, які мають повну або часткову інформацію про топологію мережі та її стан. Прикладом таких підходів є SDN (Software Defined Networking), де контролер обирає маршрути для всіх пристроїв мережі. Переваги: глобальна оптимізація, гнучкість, можливість інтеграції AI/ML. Недоліки: потенційна точка відмови, складність реалізації, потреба в резервуванні.

При децентралізованому управлінні кожен вузол самостійно приймає рішення про маршрутизацію на основі локальної інформації та обміну даними з сусідніми вузлами (як у протоколах RIP, OSPF, BGP). Переваги: висока надійність, простота масштабування. Недоліки: повільна конвергенція, обмежена можливість глобальної оптимізації.

За характером маршрутизації розрізняють статичні і динамічні методи. У статичних методах маршрути налаштовуються вручну і залишаються незмінними незалежно від змін у мережі. Використовуються у малих або стабільних мережах. У динамічних методах маршрути визначаються автоматично на основі поточного стану мережі. Протоколи самостійно оновлюють таблиці маршрутизації у відповідь на зміни.

Також можна виокремити гібридні методи, які поєднують елементи ста-

тичної та динамічної маршрутизації для досягнення балансу між стабільністю та адаптивністю (рис.2.1).

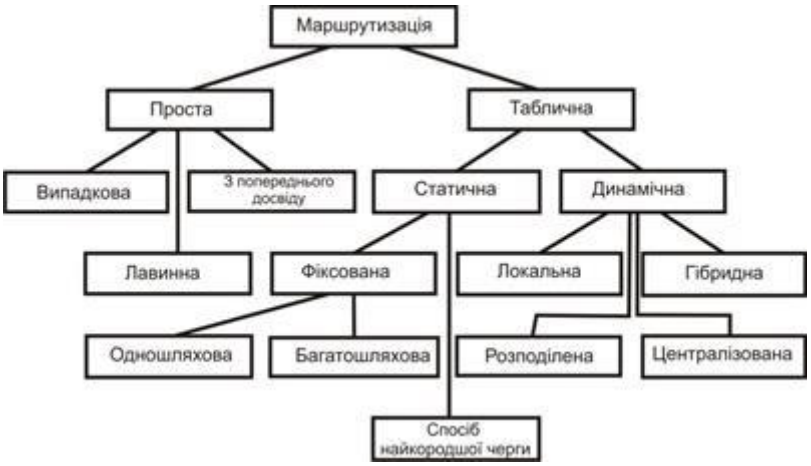


Рисунок 2.1– Способи маршрутизації в мережі

Методи можуть орієнтуватися на різні метрики, що визначають «якість» маршруту. Це може бути :

а) Найкоротший шлях – обирається маршрут із мінімальною кількістю хопів.

б) Найменша затримка – вибираються маршрути з мінімальною затримкою передачі пакетів.

в) Максимальна пропускна здатність – маршрути з найбільшим доступним обсягом передачі.

г) Навантаження – розподіл трафіку по кількох маршрутах для уникнення перевантаження.

д) Надійність – використання резервних маршрутів у випадку збою основного каналу.

Деякі методи комбінують декілька метрик у єдиний зважений критерій.
За принципом реалізації розрізняють табличні, графові, ймовірнісні та інтелектуальні методи.

Табличні методи передбачають використання заздалегідь розрахованих таблиць маршрутизації, що оновлюються за допомогою протоколів або вручну.

Графові методи передбачають застосування математичних моделей у вигляді графів (вузли – мережеві пристрої, ребра – канали зв’язку) для динамічного вибору маршруту з використанням алгоритмів, таких як Dijkstra або Bellman-Ford.

Імовірнісні методи застосовуються у системах з випадковим або стохастичним розподілом трафіку (наприклад, у peer-to-peer мережах).

Інтелектуальні методи побудовані на базі нейронних мереж, генетичних алгоритмів, машинного навчання та інших AI/ML-технологій.

Методи розподілу трафіку можуть реалізовуватись на різних рівнях моделі OSI (рис.2.2). Балансування реалізується за допомогою Ethernet-технологій (VLAN, STP) на канальному рівні. На мережевому рівні (рис.2.3) працює більшість класичних протоколів маршрутизації (OSPF, BGP). Контроль потоків, з’єднань і QoS виконується на транспортному рівні (рис.2.4). На прикладному рівні здійснюється контентно-орієнтоване балансування, як у веб-серверах та CDN (рис.2.5).

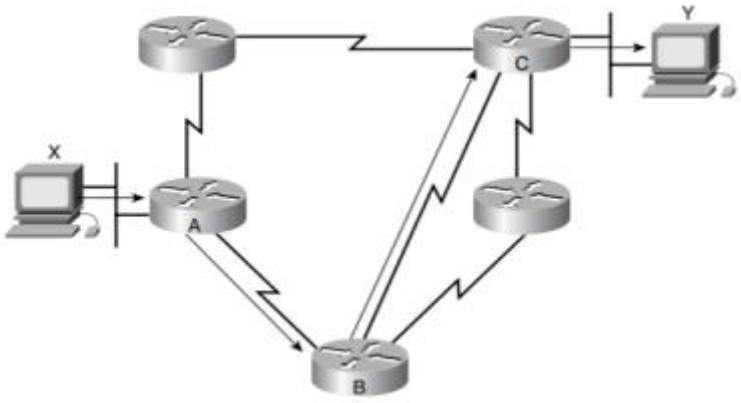


Рисунок 2.2 – Принцип дії протоколу мережевого рівня

Деякі алгоритми орієнтовані на специфіку трафіку, що обслуговується. Наприклад, потоковий трафік (Streaming), з низькою допустимою затримкою. Інтерактивний трафік (VoIP, відеозв’язок) вимагає стабільної пропускної здатності. Фоновий трафік (завантаження файлів, оновлення) може оброблятись у другу чергу. Цей підхід в основі систем QoS та Policy-Based Routing, де марш-

рутизація з урахуванням типу трафіку або вимог до сервісу.

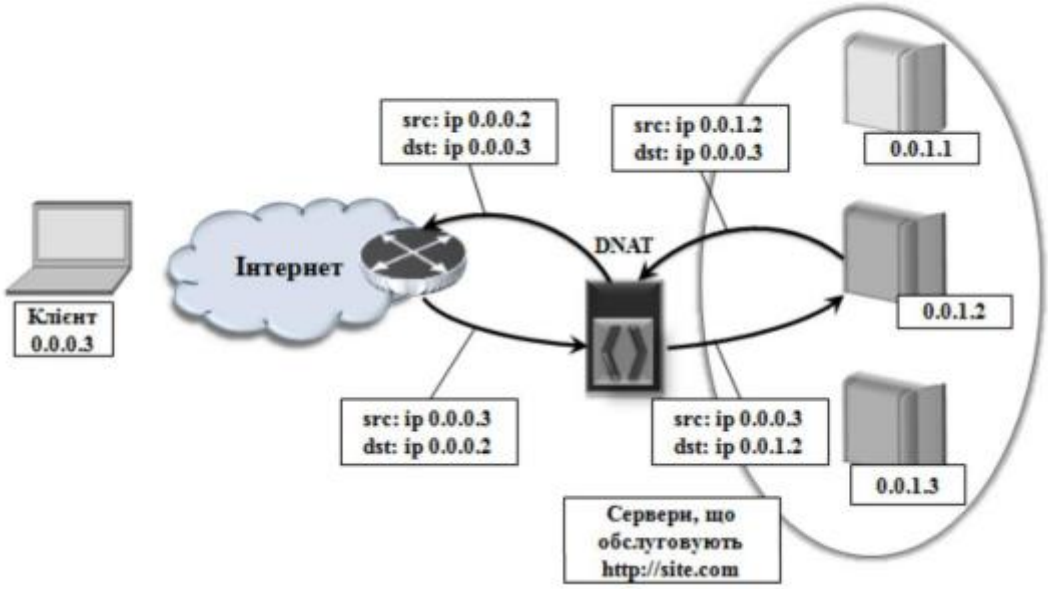


Рисунок 2.3 – Балансування на мережевому рівні моделі OSI

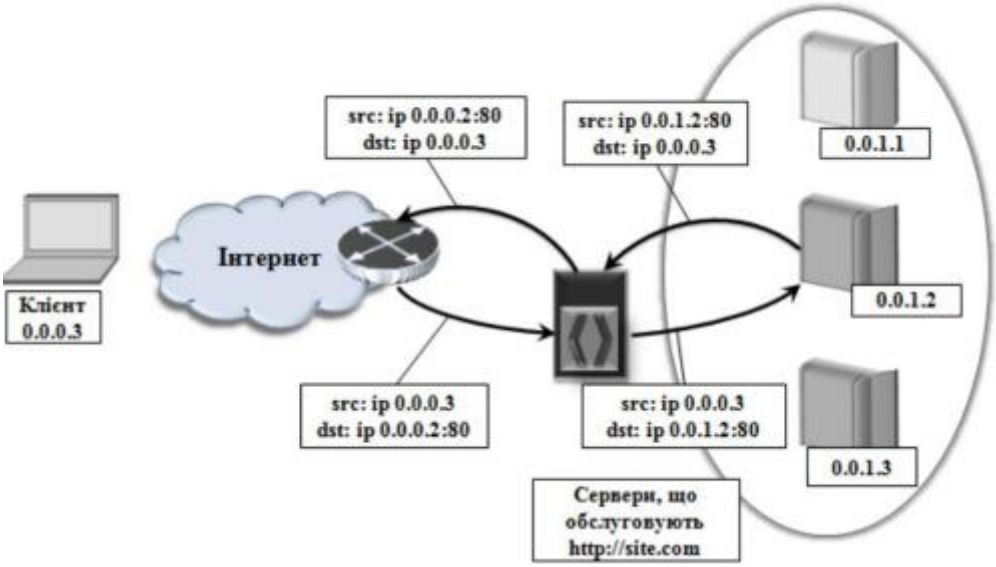


Рисунок 2.4 – Балансування на транспортному рівні моделі OSI

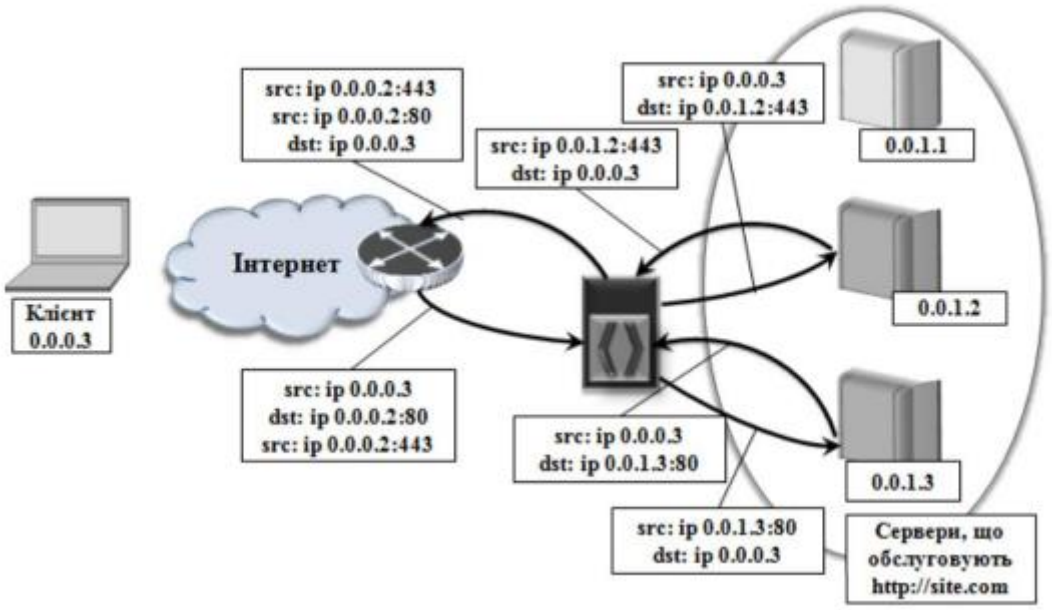


Рисунок 2.5 – Балансування на прикладному рівні моделі OSI

За ступенем інтелектуальності розрізняють:

а) Традиційні методи – статичні або детерміновані, не враховують зміни в контексті.

б) Адаптивні методи – враховують зміни навантаження, оновлюють маршрути в реальному часі.

в) Самонавчальні системи – використовують AI/ML для виявлення шаблонів і прийняття рішень без жорсткого програмування.

Розгляд загальних підходів до класифікації методів розподілу трафіку демонструє надзвичайну різноманітність як архітектурних, так і алгоритмічних рішень. Різні методи мають свої переваги й обмеження в контексті конкретних задач та умов функціонування мережі.

2.2 Традиційні методи маршрутизації

Традиційні методи маршрутизації є основою для більшості телекомунікаційних мереж і лежать в основі принципів роботи протоколів маршрутизації, які використовуються в мережах Ethernet, IP, MPLS та інших. Вони включають

кілька основних підходів, які активно застосовуються в сучасних мережах для управління трафіком і визначення найкращих маршрутів передачі даних.

Статична маршрутизація – це метод, при якому маршрути визначаються вручну адміністратором мережі та фіксовані в таблицях маршрутизації на всіх мережевих пристроях. Такий підхід не вимагає обміну інформацією між маршрутизаторами та не змінюється в реальному часі залежно від стану мережі.

До його основних характеристик можна віднести простоту налаштування оскільки маршрути визначаються вручну, їх конфігурація є відносно простою. Окрім того не потрібно використовувати додаткові ресурси для обміну інформацією між пристроями. Також при цьому шляхи залишаються фіксованими, навіть якщо мережа змінюється, наприклад, при відмові каналу. До переваг цього способу маршрутизації належать мінімальна навантаженість мережі та маршрутизаторів, оскільки немає потреби у взаємодії з іншими пристроями для визначення маршруту. Цей спосіб підходить для малих або стабільних мереж, де топологія не змінюється. В той же час, його недоліками недостатня гнучкість – якщо одна з ліній виходить з ладу або змінюється топологія мережі, маршрути треба оновлювати вручну, а також відсутність адаптивності до зміни навантаження або затримок у мережі.

Статична маршрутизація широко використовується в малих офісних мережах або в мережах, де маршрути не змінюються з часом, наприклад, для з'єднання двох віддалених локацій через стабільні лінії зв'язку.

Динамічна маршрутизація використовує спеціалізовані протоколи для автоматичного визначення найкращих маршрутів у мережі. При цьому маршрутизатори обмінюються між собою інформацією про стан мережі та оновлюють таблиці маршрутизації в реальному часі, щоб адаптуватися до змін у топології або навантаженні.

Динамічні маршрутизаційні протоколи діляться на кілька категорій в залежності від методу обміну інформацією та алгоритмів вибору маршруту.

Цей тип протоколів використовує відстань для визначення найкращого маршруту. Відстань може бути виміряна в хопах (кількість маршрутизаторів на

шляху), затримці, пропускній здатності або іншій метриці.

RIP (Routing Information Protocol) – це один із найстаріших протоколів, який використовує кількість хопів як метрику відстані. RIP має обмеження – максимальна кількість хопів для маршруту – 15, що обмежує його використання в великих мережах (рис.2.6).

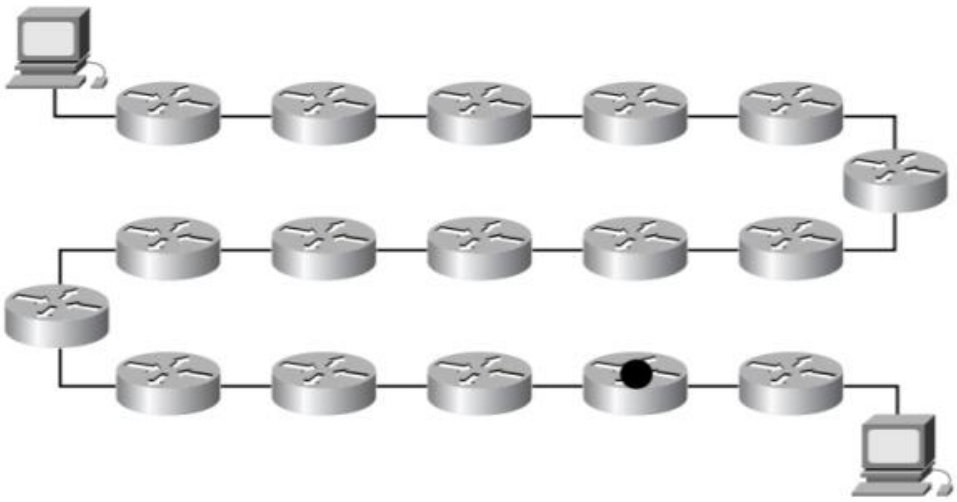


Рисунок 2.6 – Протокол RIP використовує в якості метрики лічильник транзитних вузлів

IGRP (Interior Gateway Routing Protocol) – це протокол, який використовує кілька метрик, включаючи пропускну здатність, затримку, надійність каналу.

Перевагами протоколів цього типу є простота реалізації та налаштування, а також швидке виявлення змін у топології. Недоліками є обмежена гнучкість через використання лише кількості хопів як основної метрики та повільне реагування на зміни в мережі (повільна конвергенція), особливо в RIP.

У цьому випадку маршрутизатори обмінюються інформацією про стан ліній зв'язку, включаючи їх пропускну здатність, навантаження та інші характеристики. Зазвичай такі протоколи використовують більш складні алгоритми для визначення оптимального маршруту.

OSPF (Open Shortest Path First) – це протокол з відкритим вихідним кодом, який використовує алгоритм Дейкстри для пошуку найкоротшого шляху.

OSPF є більш масштабованим та ефективним у великих мережах, порівняно з RIP.

Протокол IS-IS (Intermediate System to Intermediate System) схожий на OSPF, але використовує іншу архітектуру та підходи для визначення маршрутів. Часто використовується в провайдерських мережах.

Перевагами протоколів цього типу є висока масштабованість та гнучкість, а також Оперативне оновлення маршрутів у разі змін у мережі.

Недоліками вища складність налаштування та адміністрування, а також великий обсяг трафіку для обміну інформацією між маршрутизаторами.

BGP (Border Gateway Protocol) – це протокол маршрутизації між автономними системами, що використовується для забезпечення маршрутизації на рівні Інтернету. BGP дозволяє організаціям обмінюватися маршрутами через різні провайдери або різні частини мережі, створюючи можливості для глобального розподілу трафіку.

Він використовує політики для вибору маршрутів, а не лише метрики, такі як пропускна здатність чи кількість хопів. Підтримує концепцію неконвергентних мереж, що дозволяє вибір оптимального маршруту в складних і великомасштабних мережах.

Його перевагами є широка підтримка та масштабованість, а також гнучкість в управлінні трафіком між різними автономними системами.

До недоліків можна віднести повільне оновлення маршрутів через велику кількість маршрутизаторів у глобальній мережі, а також складність налаштування та підтримки.

Приклад застосування: BGP активно використовується для управління трафіком між великими мережами та Інтернет-провайдерами.

Традиційні методи маршрутизації, зокрема статичні та динамічні протоколи, залишаються основою багатьох телекомунікаційних мереж. Кожен з цих підходів має свої сильні та слабкі сторони, залежно від масштабів та динаміки мережі. Статична маршрутизація добре підходить для простих і стабільних мереж, тоді як динамічні протоколи маршрутизації забезпечують більш високий

рівень гнучкості та адаптивності для великих, змінних мереж.

Протоколи на основі відстані, стану каналу та BGP дають можливість ефективно управляти маршрутизацією в різних умовах і на різних рівнях мережі, але потребують значних обчислювальних ресурсів і правильного налаштування.

2.3 Методи на основі штучного інтелекту та машинного навчання

В умовах стрімкого зростання обсягів даних і ускладнення мережевої інфраструктури, класичні алгоритми розподілу трафіку вже не завжди можуть забезпечити потрібну гнучкість, адаптивність та оперативність. Це зумовлює зростаючий інтерес до використання технологій штучного інтелекту (ШІ, англ. AI – Artificial Intelligence) та машинного навчання (МН, англ. Machine Learning) у сфері мережевого управління, зокрема – для вирішення задач розподілу трафіку в телекомунікаційних мережах.

Загалом методи на основі штучного інтелекту дозволяють вирішувати такі задачі. Прогнозування трафіку – визначення майбутнього навантаження на мережу на основі історичних даних. Адаптивна маршрутизація – вибір оптимальних маршрутів залежно від поточної ситуації в мережі. Виявлення аномалій – виявлення нехарактерної поведінки трафіку (наприклад, DDoS-атаки або збої). Автоматичне масштабування ресурсів – динамічне виділення каналів або серверів залежно від навантаження.

Залежно від поставлених задач, застосовуються різні алгоритми машинного навчання.

Інтелектуальна система розподілу трафіку зазвичай має таку структуру:

а) Збір даних, збираються дані про навантаження на мережу, затримки, втрачені пакети, типи трафіку тощо. Джерела: SNMP, NetFlow, sFlow, телеметрія, лог-файли.

б) Попередня обробка даних: нормалізація очищення, агрегація даних.

в) Аналіз та моделювання, побудова моделей на основі нейронних мереж,

дерев рішень, кластерного аналізу, методів підкріплення, навчання моделей на історичних даних.

г) Прийняття рішень, вибір маршруту, зміна пріоритетів, балансування трафіку.

д) Застосування змін, взаємодія з мережевим обладнанням через API, SDN-контролери, системи управління політиками.

Основними перевагами використання систем на основі ШІ для розподілу трафіку у телекомунікаційних мережах є висока адаптивність, так як системи самостійно пристосовуються до змін трафіку в реальному часі. Окрім того, має місце оптимізація задач прогнозування та планування – системи ШІ дозволяють уникати перевантажень до того, як вони стануть критичними. Також можливе зниження втрат пакетів і затримок за рахунок проактивної маршрутизації. Ще онією перевагою є масштабованість, тобто можливість керувати складними топологіями та мільйонами підключень. Також забезпечується автоматизація управління, що ведедо зменшення потреби у втручанні адміністратора.

Попри значні переваги, використання ШІ у мережевих системах має низку недоліків. Це висока вартість впровадження – потреба у обчислювальних ресурсах та спеціалізованого ПЗ. Також існує необхідність великих обсягів навчальних даних, адже точність моделей залежить від якості вхідних даних. Ще оним недоліком є сас на навчання моделей: деякі алгоритми потребують значного часу на побудову та тестування. Окрім того слабким місцем є безпека та контроль – інтелектуальні системи повинні бути прозорими для аудиту, щоб уникнути небажаних змін у критичних сегментах мережі.

Методи, що базуються на штучному інтелекті та машинному навчанні, відкривають нові горизонти для управління телекомунікаційними мережами. Вони дозволяють не лише адаптивно реагувати на поточні зміни трафіку, а й передбачати майбутні навантаження, запобігати збоям. Попри певні технічні складнощі та вартість впровадження, ШІ-рішення вже демонструють свою ефективність у великих корпоративних мережах і продовжують активно розвиватися, стаючи ключовим фактором цифрової трансформації галузі.

2.4 Порівняння традиційних методів з новітніми підходами

Інновації в управлінні трафіком у телекомунікаційних мережах, зокрема використання технологій штучного інтелекту та машинного навчання, дозволяють значно покращити ефективність маршрутизації, оптимізацію використання мережевих ресурсів та забезпечення високої якості обслуговування. Традиційні методи, такі як статична та динамічна маршрутизація, мають певні обмеження в умовах швидко змінюваних або масштабованих мереж. З іншого боку, нові підходи з використанням AI/ML дозволяють розв'язати ряд складних задач, таких як адаптивна маршрутизація, прогнозування навантаження, а також виявлення та уникнення аномалій.

Нижче наведена таблиця 2.1 , що порівнює традиційні методи маршрутизації з новими підходами, орієнтуючись на важливі критерії.

Традиційна маршрутизація ґрунтується на заздалегідь налаштованих маршрутах або стандартних алгоритмах, таких як RIP чи OSPF, що працюють на основі статичних або обмежено адаптивних правил. В той час як ШІ-орієнтовані підходи постійно моніторять стан мережі та змінюють маршрути в реальному часі, спираючись на глибокі аналітичні моделі та адаптивні алгоритми.

Порівняння традиційних методів з новими підходами до маршрутизації в телекомунікаційних мережах показує, що, хоча традиційні методи продовжують відігравати важливу роль у стабільних і малих мережах, інновації на основі AI/ML значно підвищують ефективність, гнучкість і стійкість мереж до змін. Застосування AI/ML дає змогу не тільки підвищити адаптивність, але й здійснювати прогнозування, оптимізацію та виявлення аномалій, що є важливими для забезпечення високої якості обслуговування та надійності мереж.

Таблиця 2.1 – Порівняння методів маршрутизації

Критерії	Традиційні методи маршрутизації	Новітні методи
Адаптивність	Обмежена, статичні маршрути не змінюються без ручного втручання.	Висока адаптивність, автоматична зміна маршруту в реальному часі.
Складність налаштування	Низька для статичних, висока для динамічних.	Вища через необхідність навчання моделей AI/ML.
Час конвергенції	Повільна, особливо в старих протоколах, таких як RIP.	Швидка, завдяки прогнозуванню та адаптивності моделей.
Можливості прогнозування	Обмежені, маршрут вибирається на основі поточного стану.	Прогнозування трафіку та навантаження на основі історичних даних.
Резистентність до аномалій	Низька, відсутня здатність виявляти аномалії без спеціальних налаштувань.	Висока, AI/ML моделі можуть передбачити і виявити аномалії в мережі.

Адаптивна маршрутизація з використанням машинного навчання. В умовах змінного трафіку та умов мережі, алгоритми машинного навчання можуть адаптувати маршрути в реальному часі на основі передбачень про навантаження і потенційні збої. Наприклад, алгоритм Reinforcement Learning (RL) може використовуватися для того, щоб оптимізувати маршрути, навчатися з історичних даних і виявляти найефективніші шляхи для передавання даних, з мінімальною затримкою та перевантаженнями.

Прогнозування навантаження за допомогою глибинного навчання. Використання нейронних мереж для прогнозування трафіку дозволяє точно передбачати пікові навантаження, що дає змогу більш ефективно розподіляти ресурси та уникати перевантажень у мережах. Наприклад, технологія LSTM (Long Short-Term Memory) може аналізувати історичні дані для визначення патернів навантаження і здійснювати прогнозування на кілька кроків уперед, що дозволяє керувати трафіком ще до того, як виникнуть проблеми.

Виявлення аномалій з використанням ШІ. ШІ-методи, зокрема нейронні мережі, можуть використовуватися для виявлення аномальних ситуацій у мережі, таких як атаки типу DoS або DDoS, збої в обладнанні або неочікувані змі-

ни в навантаженні. Машинне навчання дозволяє виявляти нетипові патерни і попереджати адміністраторів або автоматично змінювати маршрути для запобігання проблемам.

Одним із успішних прикладів використання ШІ для маршрутизації є застосування Software Defined Networking (SDN) разом з ШІ для інтелектуальної маршрутизації. В SDN мережах є центральний контролер, який управляє маршрутизацією, і цей контролер може бути інтегрований з алгоритмами ШІ для адаптації маршрутів залежно від змін в мережі.

Приміром, компанії, що використовують SDN з підтримкою ШІ, можуть застосовувати моделі машинного навчання для автоматичного регулювання потужностей каналу, визначення найкращих маршрутів у разі збоїв або перенаправлення трафіку у відповідь на зміни в реальному часі.

3 ОПТИМІЗАЦІЯ РОЗПОДІЛУ ТРАФІКУ

3.1 Поняття трафік-інжинірингу

Інженерія трафіку (traffic engineering, TE) відноситься до процесу оптимізації ефективності трафіку, зазвичай у контексті інфокомунікаційної мережі. Ця дисципліна включає проектування, впровадження та управління мережевими ресурсами для забезпечення плавного і надійного зв'язку і передачі даних.

Інженерія трафіку є найважливішим аспектом управління мережею, оскільки вона допомагає адміністраторам мережі ефективно розподіляти та використовувати мережні ресурси. Її мета – покращити продуктивність мережі, знизити завантаженість та забезпечити якість обслуговування QoS для різних типів мережного трафіку. Застосовуючи різні техніки та стратегії, інженерія трафіку відіграє значну роль у підтримці стабільності та ефективності роботи мережі.

Враховуються фактори, такі як топологія мережі, доступність смуги пропускання та географічне розподілення при проектуванні мережі. Цей процес забезпечує здатність мережі справлятися з очікуваним навантаженням та надає ефективні маршрути передачі даних.

Моніторинг мережного трафіку допомагає виявляти тенденції та шаблони, виявляти області завантаженості та вживати запобіжних заходів для запобігання можливим проблемам.

Використовуються техніки балансування навантаження для розподілу трафіку за кількома мережевими посиланнями. Розподіляючи навантаження рівномірно, вони запобігають перевантаженню на якомусь одному посиланні, забезпечуючи кращу продуктивність і надійність. Балансування навантаження оптимізує використання мережевих ресурсів та мінімізує ризик завантаженості чи погіршення продуктивності.

Основна проблема з організацією конструювання трафіку в мережі полягає в тому, що стратегія ТЕ на вузлі відправнику не визначена відповідно до параметрів QoS. У процесі маршрутизації можуть виникнути проблеми, такі як перевантаження шляхів, аварії або переміщення вузла в мобільні мережі, які не завжди можуть бути вирішені традиційними методами.

Основною метою мережі зв'язку є передача даних, тобто різних типів інформації, від одного вузла мережі до іншого по встановленим маршрутам, щоб забезпечити необхідний рівень обслуговування користувачів. Для досягнення цієї цілі виконуються дві операції:

а) маршрутизація – визначення та створення маршрутів, по яким будуть передаватись дані;

б) конструювання трафіку – передача даних по існуючим маршрутам, щоб забезпечити необхідний рівень обслуговування користувачів, одночасно уникаючи перевантаження маршрутів і утворення заторів в мережі.

Мета методів конструювання трафіку полягає в тому, щоб передача даних по мережі була якомога ефективною, надійною та швидкою. У програмно-конфігурованих мережах ці методи виконує контролер, окремий пристрій у мережі, який відповідає за рівень управління, налаштування всіх пристроїв у мережі та керування трафіком. Як наслідок, конструювання трафіку можна визначити як: визначення способу розподілу трафіку між кількома маршрутами, щоб забезпечити ефективну, швидку і надійну передачу даних; визначення методів поведінки передачі даних у випадках перешкоджань, таких як заторів або конфліктів, вихід з ладу вузла в маршруті, тощо.

3.2 Програмно-конфігуровані мережі

SDN (Software Defined Networking) – це нова ідея архітектури мережі, яка дозволяє відокремити частину мережі, відповідальну за передачу даних, від іншої. Завдяки цьому розділенню SDN дозволяє керувати мережевими пристроями централізовано. Це також спрощує налаштування та керування, а також за-

безпечує високу гнучкість у створенні та зміні мережевих топологій. Кожен із трьох основних елементів архітектури SDN має вирішальне значення для забезпечення ефективності та гнучкості мережі.

Архітектура SDN дозволяє створювати нові можливості для динамічного і централізованого управління мережею завдяки відокремленню планів передачі даних і управління. Це дозволяє розробляти ефективні методи балансування навантаження. Балансування навантаження в SDN-мережах є важливою частиною забезпечення ефективної маршрутизації та оптимального використання ресурсів. Традиційні методи, такі як хешування або статичне балансування, прості та ефективні для малих мереж і стабільних навантажень. Але для великих мереж, які постійно змінюються, потрібні адаптивні методи, які можуть змінювати маршрути та перенаправляти трафік відповідно до поточного стану мережі. Такі методи, як динамічне перенаправлення трафіку та алгоритми машинного навчання, зменшують затримки та збільшують пропускну здатність, особливо в умовах змінного навантаження.

Основною метою SDN є відділення рівня передачі даних від рівня управління та рівня додатків від рівня управління. Оскільки виконання логічних функцій переноситься на вищий рівень, складність фізичних пристроїв значно знижується. Це не тільки здешевлює фізичні пристрої, але й покращує їх надійність і робить управління мережею більш простим. Тепер звичайні комутатори можна використовувати замість маршрутизаторів. Буде значно легше для адміністратора мережі в цілому керувати мережею в цілому. Крім того, оскільки рівень управління зв’язується з рівнем даних через стандартний інтерфейс, це дозволяє уникати використання окремих пристроїв. Крім того, це значно спрощує взаємодію між пристроями різних виробників, а також скорочує час, необхідний для налаштування та підготовки або ремонту всієї мережі [11].

Крім того, побудова мережі таким чином значно прискорює створення нових мережевих додатків. Програмістам більше не потрібно думати про те, як передавати команди та запити до мережі, оскільки стандартний інтерфейс використовується для взаємодії рівнів додатків і управління. Основним завданням

є виконання основних функцій програми, а інтерфейси, які були визначені раніше, будуть використані для взаємодії з рівнем контролю [10]. В таблиці 3.1 наведено порівняльний аналітик, щоб допомогти вам краще зрозуміти основні відмінності між SDN і традиційною мережею.

Таблиця 3.1 – Порівняння підходу SDN з традиційними мережами

Характеристика	Традиційні мережі	SDN
Контроль за конфігурацією	Постачальник апаратного забезпечення	Користувач
Відкритість мережі	Закрита структура	Відкрита структура
Сумісність	Незалежні протоколи	Стандартизовані протоколи
Управління мережею	Управління на низькому рівні	Управління на логічному рівні
Адаптація нових технологій	Відповідно до потреб постачальника	Відповідно до потреб користувача

3.3 Проблема розподілу трафіку

Управління на рівні потоків є однією з основних переваг SDN, оскільки воно полегшує як управління мережею, так і управління трафіком у корпоративних мережах і мережах центрів обробки даних. На основі багатошляхової маршрутизації в SDN необхідно організувати централізоване формування множини шляхів, щоб скоротити час ТЕ та підвищити якість послуг. Наявність кількох маршрутів практично виключена затримка або втрата пакетів під час процесу ремаршрутизації трафіку. З іншого боку, більше шляхів буде створено в SDN контролері, менше ймовірності затримки або втрати пакетів. Додатково варто враховувати завантаженість шляхів і тип трафіку, що передається в мережі, для більш точної маршрутизації трафіку.

В програмно конфігурованій мережі, як і в традиційних мережах, основною проблемою організації конструювання трафіку є невідповідність стратегії ТЕ на вузлі відправнику відповідно до параметрів QoS. У процесі маршрутизації можуть виникнути проблеми, такі як перевантаження шляхів, вихід з ладу або переміщення вузла в мобільні мережі, які не завжди можуть бути вирішені традиційними методами.

Мета методів конструювання трафіку полягає в тому, щоб передача даних по мережі була якомога ефективною, надійною та швидкою. У програмно-конфігурованих мережах ці методи виконує контролер, окремий пристрій у мережі, який відповідає за рівень управління, налаштування всіх пристроїв у мережі та керування трафіком. Як наслідок, конструювання трафіку можна визначити як: визначення способу розподілу трафіку між кількома маршрутами, щоб забезпечити ефективну, швидку та надійну передачу даних; визначення методів поведінки передачі даних у випадках перешкоджань, таких як заторів або конфліктів, несправності вузла на маршруті тощо.

3.4 Алгоритм розподілу трафіку

Для того, щоб дані передавались відповідно до хорошої якості технічного обслуговування, в процесі проектування трафіку необхідно розглянути стан маршрутів, тип потоку та параметри маршрутів (наприклад, довжина та надійність), тому алгоритм конструювання повинен бути включений у всі ці компоненти для забезпечення максимальної надійності.

Такий алгоритм повинен направляти трафік на вузлі «відправника» за типом трафіку та параметрами маршруту. Щоб уникнути втрати даних, потрібно надіислати важливі дані по безпечним маршрутам. Короткі маршрути мають найвищий пріоритет, оскільки дані чутливі до часу. Нарешті, відповідно до ресурсів, що залишилися, маршрути мають бути навантажені даними нечутливими до часу.

Оскільки попередні методи не враховували стан мережі та тип трафіку, запропоноване рішення буде досягати кращого балансування навантажень ніж традиційні методи.

Трафік мережі поділяється на дві основні категорії: еластичний і нееластичний. Еластичний тип трафіку може адаптуватися до змін затримки та пропускної здатності в широкому діапазоні значень, одночасно задовольняючи потреби різних застосувань, таких як обмін файлами та електронна пошта. Надійність доставки, тобто те, що вся інформація повинна бути доставлена, є важливою метрикою для такого трафіку. Нееластичний трафік – це такий, який погано адаптується або не може адаптуватися до змін затримки та пропускної здатності мережі. Наприклад, трафік реального часу, аудіо або відео конференції є таким типом трафіку. Отже, час затримки є ключовою характеристикою для такого трафіку.

Маршрути можуть бути охарактеризовані з використанням таких параметрів як: пропускна здатність, швидкість передачі даних; час затримки; завантаженість; надійність.

При плануванні трафіку метрики кожного відповідного шляху повинні бути враховані [12]. Це робиться для того, щоб розподіл даних між маршрутами та на вузлівідправнику відбувався з урахуванням QoS для кожного типу трафіку.

Метрика враховує всі необхідні показники маршруту, а вагові коефіцієнти дозволяють розподілити важливість цих параметрів відповідно до кожної категорії трафіку. У результаті надійність має більше значення для еластичного трафіку, тому ваговий коефіцієнт при надійності буде вищим у формулі, а час затримки має більше значення для нееластичного трафіку [7]. Якщо існує кілька шляхів між двома вершинами, то потрібно вибрати найкращий, враховуючи метрику.

Пропонований алгоритм конструювання трафіку працює за допомогою такої послідовності дій (рис.3.1.):

Рисунок 3.1 – Алгоритм конструювання трафіку

1. Визначається категорія трафіку
2. Обчислюється значень узагальненої метрики для кожного маршруту від відправника до отримувача.
3. Якщо є більше одного маршруту та якщо завантаженість невелика, то маршрут з низькою надійністю ігнорується
4. Обирається найкращий маршрут на основі метрики з урахуванням розподілу трафіку
5. Відправляється пакет за обраним маршрутом

Суть методу полягає в тому, що при наявності достатньої кількості альтернативних незавантажених маршрутів маршрут з показником надійності менше 50% буде ігноруватися. Це дозволяє найкращим маршрутам розподілити інформацію рівномірно. ТЕ з урахуванням завантаженості шляхів дозволяє економніше використовувати ресурси мережі та мінімізувати затори.

3.5 Розрахунок якості маршруту

Прпонована інтегральна метрика якості маршруту розраховується так:

$$IQM = w_1 \cdot \frac{1}{D} + w_s \cdot \frac{1}{L} + w_3 \cdot \frac{1}{J} + w_4 \cdot A, \tag{3.1}$$

де D – пропускна здатність каналу маршруту, Мбіт/с;

L – затримка, мс;

J – джитер, мс;

A – доступність, значення в межах [0,1];

w_1, w_2, w_3, w_4 – вагові коефіцієнти, що відображають пріоритетність параметрів.

Чим вище значення IQM – тим кращий маршрут. Вагові коефіцієнти можна налаштовувати під специфіку мережі (наприклад, для голосових

викликів більше значення має затримка, а для відео – пропускна здатність і джитер).

Тепер проведемо розрахунок. Початкові умови подано в табл. 3.2.

Таблиця 3.2 – Початкові умови

Параметр	Маршрут A	Маршрут B	Маршрут C
Пропускна здатність, Мбіт/с	100	50	80
Затримка, мс	20	10	30
Джитер, мс	5	3	10
Доступність	0,95	0,90	0,98

Припустимо, що ми обираємо такі ваги:

w_1=0,3 – вага пропускної здатності;

w_2 =0,3 – вага затримки;

w_3=0,2 – вага джитера;

w_4=0,2 – вага доступності;

Після проведення розрахунків маємо наступне.

Для маршрута A інтегральна метрика якості становить: IQM_A= 0,248.

Для маршрута B інтегральна метрика якості складає: IQM_B= 0,2826.

Для маршрута C інтегральна метрика якості дорівнює: IQM_C= 0,2297.

Таким чином, IQM_B=0,2826 – найвищий показник, отже маршрут B є найкращим згідно заданої метрики.

4 МОДЕЛЬ ЕФЕКТИВНОГО РОЗПОДІЛУ ТРАФІКУ

4.1 Основні вимоги до моделі

Для ефективного розподілу трафіку у телекомунікаційних мережах необхідно створити модель, яка задовольняє кілька ключових вимог. Від правильного визначення цих вимог залежить успішна реалізація системи управління трафіком та її здатність адаптуватися до змінюваних умов мережі. Модель має бути здатною виконувати ці завдання з високою ефективністю, при цьому мінімізуючи ризики перевантаження та забезпечуючи найкращу якість обслуговування для кінцевих користувачів.

Адаптивність є однією з основних характеристик моделі ефективного розподілу трафіку. Мережі часто стикаються з динамічними змінами, такими як зміна трафіків, збої у вузлах, зміна пропускної здатності або навіть зловмисні атаки. Відповідно, модель повинна мати здатність до автоматичного оновлення стратегій маршрутизації й перерозподілу трафіку на основі змін у реальному часі.

Адаптивна модель має ряд особливостей. Так, є можливість перерозподілу трафіку після виявлення перевантаження або неефективного використання мережевих ресурсів. Вона здатна виявляти і прогнозувати змін в трафіку за допомогою алгоритмів машинного навчання. Підтримується перехід до альтернативних маршрутів у разі збоїв або непередбачених подій.

Ефективне управління розподілом трафіку вимагає централізованої системи, яка буде мати повний доступ до інформації про стан усіх компонентів мережі. Це дасть змогу здійснювати централізоване керування процесами балансування навантаження, резервування каналів та прийняття рішень на основі глобального огляду стану мережі.

Централізоване управління має ряд основних характеристик.

Для забезпечення повного контролю збирання телеметрії відбувається з усіх вузлів мережі. Має місце оперативне реагування на зміни навантаження та оновлення політик у мережі. Наявне спрощення адміністрування та моніторингу за рахунок єдиного інтерфейсу для управління мережею.

Інтелектуальність моделі передбачає використання передових технологій аналізу даних і машинного навчання для автоматичного прийняття рішень і прогнозування змін в мережі. Застосування таких технологій дозволить створити мережу, яка здатна вчитися на основі попередніх ситуацій, прогнозувати навантаження і динамічно оптимізувати маршрути трафіку.

Інтелектуальні системи мають ряд особливостей. Вони використовують моделі машинного навчання для виявлення аномалій у трафіку. Здійснюється прогнозування майбутніх змін трафіку, що дозволяє завчасно підготувати мережу до можливих піків навантаження. Також має місце автоматичне регулювання політик розподілу трафіку на основі історичних даних і поточного стану мережі.

Для забезпечення високої якості обслуговування модель повинна мати механізми пріоритетизації трафіку, що дозволяє керувати різними типами даних в залежності від їх важливості та чутливості до затримок. Наприклад, для голосового та відеотрафіку необхідно забезпечити мінімальні затримки та високу стабільність з’єднання, в той час як для фонових процесів (наприклад, оновлення) можна використовувати менш критичні параметри.

Пріоритетизація трафіку повинна включати визначення пріоритетів для різних типів трафіку (наприклад, відеоконференції, VoIP, вебтрафік, масові оновлення), забезпечення механізмів QoS для гарантування мінімальної пропускної здатності для критичних сервісів та адаптацію до зміни умов навантаження, щоб забезпечити стабільну якість обслуговування для користувачів.

Масштабованість моделі розподілу трафіку є критично важливим фактором для телекомунікаційних мереж, оскільки ці мережі часто зазнають значних змін у розмірі та складності. Модель повинна бути здатною масштабуватися як

горизонтально, так і вертикально, щоб ефективно обробляти зростаючі обсяги даних і нові користувацькі вимоги.

Масштабованість має ряд особливостей, до яких відноситься можливість інтеграції нових мережевих пристроїв, серверів, каналів без значних змін в архітектурі; автоматичне розширення ресурсів і коригування політик маршрутизації в разі збільшення навантаження; підтримка хмарних інфраструктур, що дозволяє швидко адаптувати модель до нових вимог і зміни ландшафту трафіку.

Безпека є невід'ємною складовою ефективного розподілу трафіку. Модель повинна забезпечувати як захист від зовнішніх атак (наприклад, DDoS), так і безпеку внутрішніх мережевих комунікацій. Це включає використання шифрування, виявлення та блокування аномальних пакетів, а також забезпечення політик доступу для контролю користувачів та пристроїв.

Механізми безпеки включають: виявлення та запобігання атакам типу DDoS через аналіз трафіку, використання шифрування для захисту чутливих даних, інтеграція засобів моніторингу та аудиту для виявлення потенційних загроз.

Надійність є критично важливим аспектом для системи, що відповідає за розподіл трафіку, особливо в умовах постійного збільшення навантаження та зростаючих вимог до безперервності сервісів. Модель повинна бути побудована таким чином, щоб навіть у разі відмови одного з елементів мережі інші елементи могли продовжити виконувати свої функції без помітних перебоїв.

Надійність і відмовостійкість мають забезпечувати такі аспекти, як вбудовані механізми резервування і автоматичного відновлення, використання розподілених архітектур для запобігання єдиній точці відмови, аварійне переключення на резервні канали та вузли у разі збою.

Модель повинна прагнути до максимальної ефективності використання наявних мережевих ресурсів, зменшуючи надлишкові витрати на пропускну здатність, енергоспоживання та інші ресурси. Зокрема, це включає зниження витрат на обслуговування зберігання та передачі даних без втрати якості.

Ефективність використання ресурсів повинна включати оптимізацію маршрутів з урахуванням поточного навантаження та пропускної здатності, використання ресурсів у межах фізичних і віртуальних інфраструктур, таке керування трафіком, щоб уникнути непотрібних затримок або збоїв.

Модель ефективного розподілу трафіку повинна бути багатофункціональною, гнучкою, здатною адаптуватися до змін в мережі та забезпечувати високий рівень якості обслуговування для кінцевих користувачів. Застосування сучасних підходів, таких як адаптивність, інтелектуальні алгоритми, а також пріоритетизація трафіку і масштабованість, допоможе оптимізувати використання ресурсів і забезпечити безперервну роботу мережі.

4.2 Архітектура моделі

Архітектура концептуальної моделі ефективного розподілу трафіку є основою для побудови системи, яка може динамічно адаптуватися до змінних умов мережі, забезпечувати рівномірне навантаження на вузли та підтримувати високу якість обслуговування. Правильна архітектура дозволяє зберігати стабільність роботи мережі, зменшувати затримки та підвищувати її загальну ефективність. У підрозділі розглянемо основні компоненти архітектури концептуальної моделі, їх функції та взаємодії.

Архітектура концептуальної моделі складається з кількох ключових елементів, які забезпечують балансування трафіку, моніторинг, оптимізацію і забезпечення надійності (рис.4.1). Розглянем основні компоненти архітектури.

Мережеві пристрої, такі як маршрутизатори і комутатори, займають основне місце в архітектурі моделі. Вони відповідають за передачу і маршрутизацію даних по мережі, а також можуть виконувати функції балансування навантаження на рівні мережевих протоколів. Ці пристрої повинні мати здатність динамічно адаптуватися до змінних умов навантаження, оптимізувати маршрути і знижувати затримки. Їх основні функції, це реалізація алгоритмів маршрутиза-

ції і балансування навантаження, обробка трафіку на основі критеріїв QoS та політик, виявлення перевантаження та автоматичне перенаправлення трафіку.

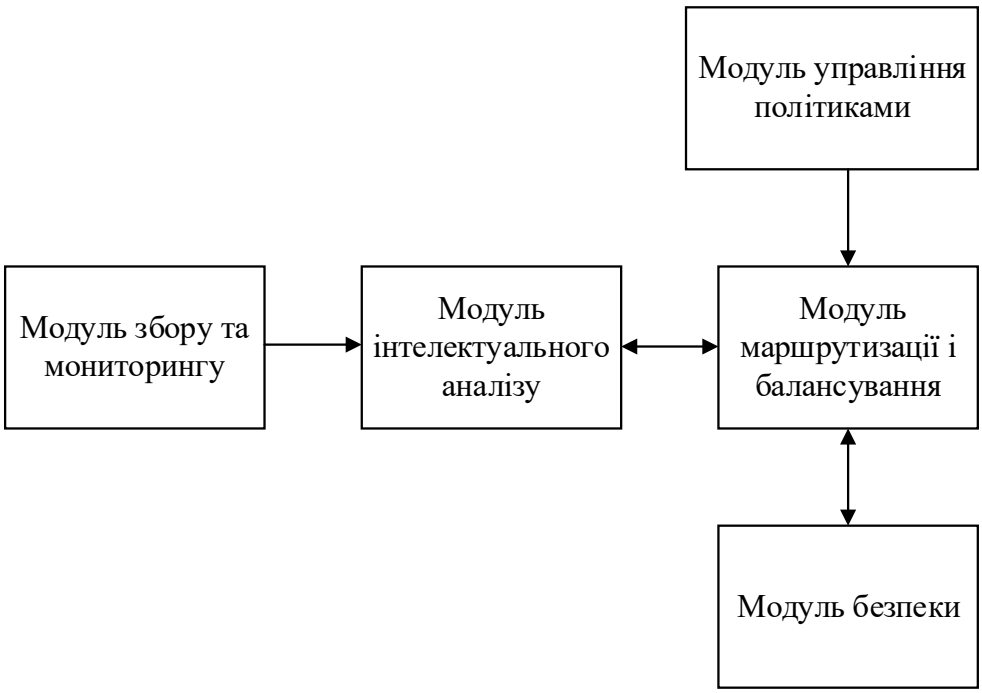


Рисунок 4.1 – Модель ефективного розподілу трафіку

Баласувальники навантаження є основним компонентом для рівномірного розподілу трафіку між декількома серверами або каналами зв’язку. Вони можуть бути як апаратними, так і програмними. Балансувальники використовують різні алгоритми для визначення найкращого шляху для передачі даних, зокрема Round Robin, Least Connections, Weighted Round Robin, і інші. Їх основні функції – це розподіл трафіку між серверами або вузлами, перевірка стану серверів і коригування маршруту в разі відмови, пріоритетизація трафіку на основі заданих політик.

Моніторинг є невід’ємною частиною концептуальної моделі, оскільки він дозволяє стежити за станом мережі в режимі реального часу. За допомогою систем моніторингу можна збирати дані про завантаження каналів, наявність збоїв, затримки та інші важливі параметри мережі. Це дає змогу швидко виявляти проблеми та автоматично адаптувати маршрутизацію трафіку. Їх основні функції – це збір і аналіз даних про стан мережі, виявлення аномалій і перевanта-

жень у мережі, оповіщення адміністратора або автоматичне коригування політик маршрутизації.

Система управління політиками маршрутизації дозволяє визначати правила для розподілу трафіку на основі критеріїв, таких як тип трафіку, пріоритет, джерело або призначення. Це дає змогу керувати трафіком з урахуванням важливості кожного з'єднання і забезпечувати гарантовану якість обслуговування для критичних додатків, таких як VoIP або відеоконференції. Її основні функції – це визначення та застосування політик маршрутизації, пріоритетизація трафіку та забезпечення QoS, гнучке налаштування маршрутизаторів і балансувальників на основі змін в умовах мережі.

Для досягнення високої ефективності моделі важливо використовувати інтелектуальні алгоритми для аналізу трафіку, які базуються на машинному навчанні та великих даних. Алгоритми можуть прогнозувати навантаження на основі історичних даних, виявляти аномалії, оптимізувати розподіл трафіку та автоматично регулювати мережеві ресурси. Їх основні функції: аналіз і прогнозування навантаження на мережу, виявлення аномальних патернів трафіку, оптимізація налаштувань мережі для підвищення ефективності.

Компоненти архітектури концептуальної моделі взаємодіють між собою, забезпечуючи безперервну передачу даних і ефективний розподіл трафіку:

1. Збір і обробка даних: Моніторинг збирає інформацію про стан мережі, яку потім аналізує система управління політиками маршрутизації та інтелектуальні алгоритми для виявлення необхідних змін.

2. Аналіз і прогнозування: На основі аналізу даних, що надходять від моніторингової системи, інтелектуальні алгоритми прогнозують майбутні навантаження і підбирають оптимальні шляхи для розподілу трафіку.

3. Реалізація політик: Після прийняття рішень про зміну маршрутів чи налаштування політик, ці зміни впроваджуються через систему управління політиками маршрутизації та балансувальники навантаження, які забезпечують фактичний розподіл трафіку між мережевими вузлами.

4. Коригування на основі результатів: Якщо виявляються помилки або перевантаження на конкретному маршруті чи вузлі, система автоматично коригує маршрутизацію для оптимізації використання ресурсів мережі.

Архітектура концептуальної моделі базується на модульному підході, що дозволяє спростити розширення системи, додавання нових компонентів і адаптацію до змінних умов. Кожен з компонентів може бути масштабований або оновлений незалежно, що підвищує гнучкість і надійність системи. Модуль моніторингу відповідає за збір і передачу даних в реальному часі. Модуль аналізу використовує отримані дані для виявлення патернів, прогнозування навантаження та оптимізації трафіку. Модуль балансування здійснює розподіл трафіку за допомогою різних алгоритмів, адаптуючи маршрути під поточне навантаження. Модуль управління політиками забезпечує реалізацію QoS, пріоритетизацію трафіку та управління маршрутизацією.

Такий модульний підхід дозволяє швидко реагувати на зміни в мережі, адаптуючи функціонування системи без значних витрат на модернізацію.

Безпека в архітектурі концептуальної моделі є важливим аспектом, який забезпечує захист мережі від зовнішніх загроз і внутрішніх порушень. Моделі, орієнтовані на ефективне розподілення трафіку, мають бути здатними до використання шифрування для захисту даних, ідентифікації і аутентифікації користувачів і пристроїв, виявлення і блокування аномальних або шкідливих спроб доступу.

Архітектура концептуальної моделі ефективного розподілу трафіку має бути багатофункціональною, гнучкою та здатною адаптуватися до швидко змінюваних умов мережі. Вона повинна включати основні компоненти, такі як балансувальники навантаження, моніторингові системи, аналітичні модулі і механізми управління політиками, що забезпечують оптимальний розподіл трафіку. Модульна структура дозволяє ефективно масштабувати систему та додавати нові функції без порушення роботи вже існуючих компонентів.

4.3 Компоненти моделі

Компоненти моделі ефективного розподілу трафіку є основними елементами, що забезпечують її функціонування та досягнення поставлених цілей, таких як оптимізація використання мережевих ресурсів, покращення якості обслуговування користувачів (QoS), балансування навантаження і забезпечення надійності мережі. Кожен компонент моделі виконує специфічну функцію, і всі вони взаємодіють між собою, створюючи ефективну та динамічну систему управління трафіком. У цьому підрозділі будуть детально розглянуті основні компоненти концептуальної моделі.

Модуль збору та моніторингу даних є основою для управління трафіком, оскільки він надає актуальну інформацію про стан мережі. Завдяки моніторингу можна оперативно виявляти перевантаження, виявляти збої в роботі вузлів і прогнозувати зміни в навантаженні. Це дозволяє системі приймати обґрунтовані рішення для оптимізації маршрутизації трафіку в реальному часі.

Система моніторингу збирає дані з мережевих пристроїв, таких як маршрутизатори, комутатори та балансувальники навантаження. Це включає інформацію про пропускну здатність, затримки, втрати пакетів і навантаження на канали. За допомогою інструментів аналізу визначається структура трафіку в мережі (типи даних, джерела та призначення) та аномальні патерни (наприклад, перенавантаження або збої). Виконується перевірка параметрів якості обслуговування (QoS), таких як затримки, пакетні втрати і пропускна здатність для забезпечення відповідності умовам SLA (Service Level Agreement).

Модуль моніторингу є джерелом інформації для інших компонентів моделі, що дозволяє реагувати на зміни в мережі та вчасно адаптувати стратегії розподілу трафіку.

Збір даних про стан мережі дозволяє проактивно усувати потенційні проблеми, до того як вони перетворяться на серйозні збої в роботі мережі.

Цей компонент є основою для забезпечення рівномірного розподілу трафіку між різними вузлами мережі, що сприяє оптимальному використанню ресурсів і запобігає перевантаженню окремих маршрутів або каналів.

Модуль відповідає за рівномірний розподіл трафіку між кількома доступними маршрутамі або серверами. Алгоритми балансування можуть варіюватися від простих (наприклад, Round Robin) до складних (наприклад, адаптивне балансування на основі поточного навантаження).

Маршрутизація трафіку змінюється в реальному часі на основі даних моніторингу, виявлених аномалій і змін у навантаженні мережі. У разі перевантаження одного з каналів система автоматично вибирає інші менш навантажені маршрути. Модуль може перенаправляти трафік в разі збоїв або відмов в мережевих вузлах, забезпечуючи безперервність зв’язку та максимальну доступність сервісів.

Модуль маршрутизації і балансування трафіку забезпечує мінімізацію часу затримки та переривань у роботі мережі, що безпосередньо впливає на якість обслуговування.

Система здатна адаптуватися до змін в умовах трафіку, балансуючи навантаження відповідно до поточних вимог.

Інтелектуальний аналіз і прогнозування є важливим компонентом моделі, що використовує методи машинного навчання та аналізу великих даних для обробки величезних обсягів інформації про мережу і трафік. Це дозволяє прогнозувати навантаження на мережу та оптимізувати стратегії розподілу трафіку на основі минулого досвіду та трендів.

Модуль прогнозує піки навантаження, що дозволяє заздалегідь підготувати мережу до високих навантажень, змінюючи маршрутизацію або активуючи додаткові ресурси. У модулі алгоритми машинного навчання використовуються для виявлення аномальних патернів у трафіку, таких як сплески навантаження, підозрілі підключення або потенційні зловмисні атаки. На основі аналізу та прогнозування модуль може автоматично налаштовувати параметри балансу-

вання навантаження або приймати рішення щодо маршрутизації трафіку, зменшуючи затримки та підвищуючи ефективність.

Модуль інтелектуального аналізу дозволяє моделі «вчитися» на історичних даних, що підвищує її ефективність з часом. Це дозволяє передбачати потенційні проблеми, до того як вони виникнуть, і забезпечувати більш стабільну та ефективну роботу мережі.

Модуль управління політиками відповідає за визначення і реалізацію політик маршрутизації та управління якістю обслуговування (QoS). Це важливий елемент для досягнення високої якості обслуговування кінцевих користувачів, оскільки різні типи трафіку (голос, відео, дані) мають різні вимоги до пропускної здатності, затримок і надійності.

Модуль дозволяє визначати пріоритети для різних типів трафіку, гарантуючи, що критичні додатки, як-от VoIP або відеоконференції, отримають необхідні ресурси для безперебійної роботи. Виконується моделювання політик QoS: встановлення специфічних параметрів QoS для різних груп користувачів або типів трафіку, таких як максимальні затримки, мінімальна пропускна здатність або рівень надійності. Також має місце гнучка настройка політик: можливість коригувати політики QoS залежно від змін в умовах мережі або вимог користувачів.

Модуль управління політиками гарантує, що мережа надає необхідні ресурси для високопріоритетних додатків і сервісів, покращуючи досвід користувачів. Це дозволяє досягти потрібного рівня надійності та якості для різних типів сервісів, зокрема для чутливих до затримок додатків.

Модуль безпеки забезпечує з ахист мережі від несанкціонованого доступу, атак типу DDoS, витоків даних та інших загроз. Безпека є критично важливою для підтримки стабільної роботи мережі, особливо коли мова йде про великий обсяг трафіку і потенційно вразливі сервіси.

Його основні функції – це ідентифікація і аутентифікація, тобто перевірка користувачів і пристроїв, що підключаються до мережі, для запобігання несанкціонованому доступу; захист від DDoS атак шляхом виявлення та блокування

шкідливого трафіку, що може спричинити перевантаження мережі; шифрування даних, тобто забезпечення конфіденційності і цілісності переданих даних за допомогою шифрування.

Модуль безпеки дозволяє захищати мережу від зовнішніх і внутрішніх загроз, забезпечуючи безперервну і безпечну роботу системи. Забезпечення безпеки допомагає запобігти значним фінансовим і репутаційним збиткам у разі атак або витоків даних.

Компоненти моделі ефективного розподілу трафіку повинні працювати в тісній взаємодії, щоб забезпечити оптимальний баланс між ефективністю використання мережевих ресурсів і якістю обслуговування. Кожен з компонентів моделі виконує важливу роль, від збору і моніторингу даних до управління політиками та забезпечення безпеки. Забезпечення їхньої інтеграції і взаємодії є ключовим фактором для досягнення цілей ефективного управління трафіком у телекомунікаційних мережах.

4.4 Алгоритмічна складова

Алгоритмічна складова є серцем концептуальної моделі ефективного розподілу трафіку. Вона визначає, як саме будуть здійснюватися операції маршрутизації, балансування навантаження, адаптація до змінних умов мережі та забезпечення гарантованої якості обслуговування (QoS). Алгоритми повинні враховувати багато факторів, таких як стан мережі, пріоритетність трафіку, пропускну здатність каналів, затримки, навантаження на сервери і багато інших параметрів. У цьому підрозділі розглянемо основні алгоритми, що використовуються для оптимізації розподілу трафіку, їх принципи роботи та застосування в різних сценаріях.

Алгоритми маршрутизації є ключовим елементом в управлінні трафіком мережі, оскільки вони визначають, як пакети даних будуть пересуватися від джерела до призначення. Існує кілька основних типів алгоритмів маршрутизації, кожен з яких має свої особливості та сфери застосування.

Розглянемо основні типи алгоритмів маршрутизації:

Алгоритм Дейкстри (алгоритм найкоротшого шляху) є одним з найпоширеніших методів для пошуку найкоротшого шляху між вузлами в мережі (рис.4.2). Він будує таблицю маршрутизації на основі ваги кожного шляху, де вага може включати затримки, пропускну здатність або інші параметри. Алгоритм є ефективним для статичних або напівстатичних мереж, де топологія не змінюється часто. Його основні функції – це пошук найкоротшого маршруту між вузлами, підтримка мінімальних затримок і оптимізації використання ресурсів. Переваги алгоритму – простота реалізації та гарантована оптимальність маршруту за умов стабільної топології. Недолік – погано справляється з динамічними змінами в мережі.

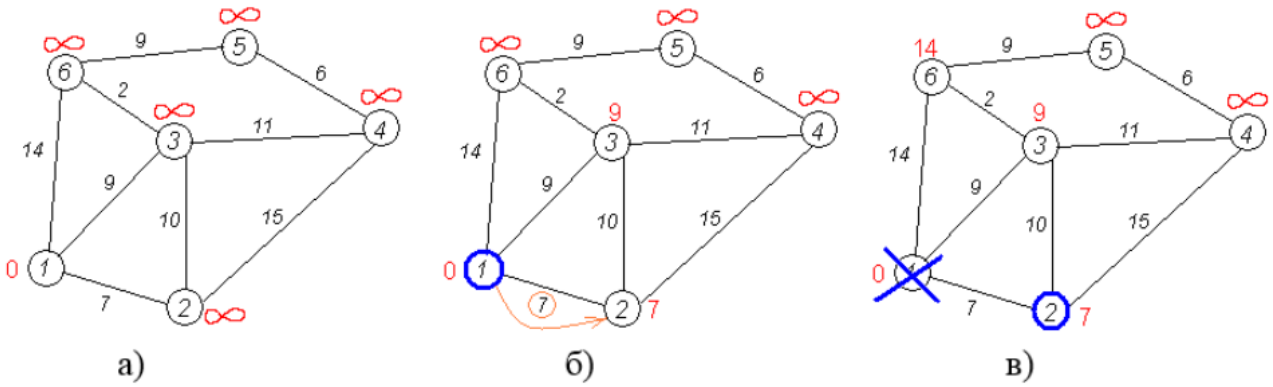


Рисунок 4.2 – Схематичне зображення алгоритму Дейкстри

Алгоритм Беллмана-Форда є ще одним класичним методом маршрутизації, який дозволяє знаходити найкоротші шляхи, навіть якщо є негативні ваги (наприклад, при розрахунку маршруту, де деякі шляхи можуть бути переважними через велику пропускну здатність). Однак він менш ефективний за алгоритм Дейкстри, оскільки потребує більше обчислювальних ресурсів. Основні функції – знайдення оптимальних маршрутів навіть при змінних параметрах, гнучкість у виборі шляху з урахуванням зміни топології. Переваги – можливість роботи з негативними вагами та стійкість до змін у мережі. Недолік –

більш висока обчислювальна складність в порівнянні з алгоритмом Дейкстри.

Алгоритм OSPF (Open Shortest Path First) є протоколом внутрішньої маршрутизації (IGP), який використовує алгоритм Дейкстри для пошуку найкоротших шляхів. Він динамічно оновлює таблиці маршрутизації та реагує на зміни в топології мережі, що дозволяє ефективно працювати в умовах часто змінюваних мереж. Основні функції – автоматичне оновлення таблиць маршрутизації та швидка адаптація до змін у мережі. Переваги – динамічна адаптація до змін у топології, підтримка великих мереж. Недоліки – високі вимоги до ресурсів і пам'яті.

Алгоритм BGP (Border Gateway Protocol) є протоколом зовнішньої маршрутизації, який використовується для зв’язку між автономними системами (AS). Він здатний оптимізувати маршрутизацію для глобальних мереж, таких як Інтернет. BGP використовує атрибути, такі як префікс мережі і політики маршрутизації для вибору оптимальних шляхів. Основні функції – оновлення маршрутизації в глобальних мережах, використання політик для визначення оптимальних маршрутів. Переваги – підтримка великомасштабних мереж і політик маршрутизації, можливість адаптації до змін в мережевій топології. Недоліки – складність налаштування і управління, може бути повільнішим у порівнянні з іншими протоколами для внутрішньої маршрутизації.

Балансування навантаження є важливим аспектом для досягнення оптимальної продуктивності в телекомунікаційних мережах. Алгоритми балансування навантаження визначають, як рівномірно розподілити трафік між декількома серверами або мережевими каналами, щоб уникнути перевантажень і зменшити час відгуку.

Розглянемо основні алгоритми.

Round Robin (Круговий розподіл) – це один із найпростіших і найбільш використовуваних алгоритмів балансування навантаження. Алгоритм розподіляє вхідний трафік рівномірно між усіма доступними серверами, передаючи кожному новому запиту на черзі. Переваги – простота реалізації та рівномірне розподілення навантаження між серверами. Недолік – не враховує поточне на-

вантаження на сервери, тому може бути неефективним, коли деякі сервери вже переповнені.

Алгоритм "мінімум з'єднань" направляє нові запити на сервер з найменшою кількістю поточних з'єднань. Цей підхід забезпечує балансування навантаження на основі реального стану серверів, що дозволяє ефективніше використовувати ресурси. Переваги – враховує поточне навантаження серверів, може забезпечити кращу ефективність в умовах динамічного трафіку. Недолік – не враховує характеристики серверів, такі як пропускна здатність чи швидкість обробки запитів.

Алгоритм вагового кругового розподілу є модифікацією стандартного Round Robin, де кожному серверу надається певна вага, що відображає його потужність або можливість обробляти запити. Серверам з більшою вагою передається більше запитів. Переваги – більш ефективний, коли сервери мають різні можливості, забезпечує кращий контроль над розподілом трафіку. Недолік – може бути складніше налаштувати для великих мереж з різними типами серверів.

Алгоритм IP Hash використовує хешування IP-адреси клієнта для визначення сервера, до якого буде направлений запит. Це дозволяє забезпечити стійкість сеансів і дозволяє клієнтам підключатися до одного й того ж сервера протягом всього сеансу. Переваги – забезпечує стійкість сеансів, розподіляє запити на основі унікальних характеристик клієнта. Недолік – може бути менш рівномірним в розподілі навантаження.

Для забезпечення якості обслуговування (QoS) в телекомунікаційних мережах використовуються алгоритми, які дозволяють гарантувати відповідний рівень затримок, пропускної здатності та надійності для різних типів трафіку.

Алгоритм Weighted Fair Queuing (WFQ) – це один із алгоритмів чергування, що забезпечує справедливий доступ до каналів зв'язку для різних типів трафіку, з урахуванням їх ваги. Всі потоки отримують частину пропускної здатності, пропорційну їх вазі, що дозволяє досягти високої ефективності та справедливості в розподілі ресурсів.

Алгоритм Random Early Detection (RED) є алгоритмом управління чергами, який використовує статистичні методи для визначення, коли почати скидати пакети, щоб уникнути перевантажень. Він виявляє, коли черга наближається до межі заповнення, і приймає рішення про скидання певних пакетів для уникнення переповнення.

Алгоритмічна складова концептуальної моделі ефективного розподілу трафіку є основою для досягнення оптимального функціонування телекомунікаційних мереж. Використання різноманітних алгоритмів маршрутизації, балансування навантаження та забезпечення якості обслуговування дозволяє динамічно реагувати на зміни умов роботи мережі і забезпечувати максимальну ефективність і надійність. Використання цих алгоритмів у комплексі дає змогу покращити пропускну здатність мережі, знизити затримки і підвищити задоволеність кінцевих користувачів.

4.5 Приклад сценарію роботи

Для кращого розуміння застосування концептуальної моделі ефективного розподілу трафіку, наведемо приклад сценарію роботи, який ілюструє, як алгоритми маршрутизації, балансування навантаження та управління якістю обслуговування (QoS) взаємодіють між собою в реальній телекомунікаційній мережі. Цей сценарій демонструє, як різні компоненти системи можуть забезпечити ефективний розподіл трафіку в умовах змінного навантаження та змінної мережевої топології, а також як машинне навчання (МН) та штучний інтелект (ШІ) можуть покращити цей процес.

Уявімо собі компанію, яка використовує корпоративну мережу для обміну даними між віддаленими офісами, розташованими в різних регіонах. Мережа має кілька серверів, що обробляють запити користувачів з різних офісів, а також з'єднання з Інтернетом для доступу до зовнішніх ресурсів. У певний момент часу навантаження на мережу зростає через збільшення кількості користувачів і даних, що передаються.

Компанія впроваджує концептуальну модель ефективного розподілу трафіку для забезпечення стабільної роботи системи навіть у разі високих навантажень. Модель включає алгоритми маршрутизації, балансування навантаження та підтримки QoS, а також використовує машинне навчання (МН) та штучний інтелект (ШІ) для вдосконалення управлінських рішень.

Кроки виконання алгоритмів з використанням МН та ШІ.

Крок 1: Оцінка навантаження на мережу з використанням МН

Першим етапом роботи моделі є оцінка поточного стану мережі. За допомогою машинного навчання система аналізує поточні дані (пропускна здатність каналів, час затримки, обсяг трафіку, використання серверів) і визначає ймовірність перевантаження в кожному сегменті мережі. Алгоритм, наприклад рекурентні нейронні мережі (RNN) або LSTM (Long Short-Term Memory), аналізує історичні дані, щоб прогнозувати майбутнє навантаження, зважаючи на різні фактори, як час доби, події або зміни в інфраструктурі. Приклад застосування – прогнозування піків трафіку. Система може прогнозувати високий рівень трафіку на основі сезонних змін (наприклад, святкові періоди, спеціальні події або збільшення попиту на певні послуги). Це дозволяє завчасно оптимізувати маршрути та обробку запитів.

Крок 2: Балансування навантаження за допомогою ШІ

Якщо прогнозовані дані вказують на перевантаження в певній частині мережі, модель використовує штучний інтелект для автоматичного балансування навантаження між різними серверами чи каналами зв'язку. Алгоритми машинного навчання можуть визначити, які сервери чи канали будуть найбільш ефективними для обробки додаткового трафіку, базуючись на їх поточній пропускній здатності та завантаженості. Приклад застосування: алгоритм reinforcement learning може вивчити оптимальні стратегії балансування навантаження, враховуючи минулі результати та зворотний зв'язок. Наприклад, в разі перевантаження сервера, система автоматично перенаправляє трафік на інші сервери або канали, що дозволяє мінімізувати затримки та покращити якість обслуговування.

Крок 3: Оптимізація маршрутизації з ШІ

На цьому етапі, система використовує штучний інтелект для оптимізації процесу маршрутизації, вибираючи найбільш ефективні шляхи для передавання трафіку між різними сегментами мережі. Алгоритм глибокого навчання може враховувати зміни в топології мережі, такі як зміни у пропускній здатності, час затримки чи доступність певних каналів. Приклад застосування: глибокі нейронні мережі можуть допомогти виявити найкращі маршрути на основі великої кількості параметрів, таких як поточні та прогнозовані умови мережі. AI може адаптувати маршрути для підтримки мінімальної затримки та максимального використання пропускної здатності.

Крок 4: Забезпечення якості обслуговування (QoS) з МН.

Алгоритми МНможуть бути використані для автоматичного налаштування пріоритетів обробки різних типів трафіку, щоб забезпечити стабільну роботу критичних додатків. Наприклад, WFQ (Weighted Fair Queuing) може бути адаптований з використанням алгоритмів машинного навчання для точнішого визначення пріоритетів залежно від зміни умов мережі та потреб користувачів. Приклад застосування – ШІ для динамічної зміни політик QoS. Штучний інтелект може визначати, які додатки потребують більшої пропускної здатності (наприклад, відеоконференції або онлайн-ігри), і автоматично коригувати політики QoS для надання їм переваги.

Крок 5: Самонавчання та адаптація мережі за допомогою МН та ШІ

Мережа постійно адаптується до змінюваних умов за допомогою самонавчання. Алгоритми машинного навчання на основі reinforcement learning або непрямого навчання можуть аналізувати ефективність своїх рішень у реальному часі та покращувати стратегії розподілу трафіку, маршрутизації та балансування навантаження. Приклад застосування – адаптивне регулювання налаштувань мережі. Система може самостійно адаптувати параметри маршрутизації та QoS, враховуючи зміни в мережевому трафіку, нові дані про канали зв'язку або користувацькі запити. Наприклад, якщо мережа відчуває затримки на певному маршруті, AI може автоматично вибрати новий, більш ефективний шлях.

Після виконання всіх етапів сценарію з використанням МН та ШІ можна провести оцінку результатів. Завдяки прогнозуванню навантаження та адаптації в реальному часі, пропускна здатність мережі значно зростає. ШІ і МН дозволяють мінімізувати затримки за рахунок оптимізації маршрутизації та приоритезації трафіку. Використання ШІ для самонавчання мережі дозволяє досягти високого рівня стабільності та стійкості до змін у навантаженні та топології.

Застосування машинного навчання та штучного інтелекту в сценарії ефективного розподілу трафіку дозволяє значно покращити управління ресурсами мережі. Ці технології дозволяють оптимізувати процеси маршрутизації, балансування навантаження, забезпечення QoS і адаптації мережі до змінних умов. Це забезпечує більшу ефективність, надійність і стабільність телекомунікаційної мережі, а також покращує якість обслуговування користувачів.

Запропонована концептуальна модель ефективного розподілу трафіку дозволяє вирішити ключові проблеми, виявлені на попередніх етапах дослідження. Вона поєднує новітні підходи – SDN, DPI, AI – і надає можливість створити динамічну, адаптивну та інтелектуальну систему управління трафіком, здатну відповідати викликам сучасного цифрового середовища.

5 ОХОРОНА ПРАЦІ

Система охорони праці в Україні постійно модернізується з метою підвищення рівня безпеки та збереження здоров’я працівників на їхніх робочих місцях. Протягом останніх років у цій сфері було впроваджено низку важливих законодавчих ініціатив, стратегій і регламентів, спрямованих на створення безпечного виробничого середовища та мінімізацію виробничих ризиків.

Ключовим нормативним документом залишається Закон України «Про охорону праці», який визначає основні права, обов’язки та відповідальність як роботодавців, так і працівників. Доповненням до нього слугують Державні будівельні норми (ДБН), а також санітарні регламенти, які регулюють вимоги до робочих приміщень, обладнання, організації праці тощо.

Держава також приділяє увагу підготовці кадрів, активно підтримуючи навчальні програми та курси підвищення кваліфікації в галузі безпеки праці. Це сприяє формуванню усвідомленого підходу до управління ризиками на підприємствах.

Крім того, сучасні українські компанії поступово інтегрують інноваційні технології в систему охорони праці: автоматизовані системи контролю, роботизоване обладнання та інші технічні рішення, які зменшують небезпеку для працівників під час виконання виробничих завдань.

Дослідження підвищення ефективності розподілу трафіку у телекомунікаційних мережах відбувалося в приміщені, яке обладнане робочими місцями з ПК.

На дослідника могли мати вплив такі небезпечні та шкідливі виробничі фактори:

1. Фізичні:

– підвищена запиленість та загазованість повітря робочої зони;
– підвищена чи понижена температура повітря робочої зони;
– підвищений рівень шуму на робочому місці;
– підвищена чи понижена вологість повітря;

– підвищений рівень електромагнітного випромінювання;
– підвищена чи понижена іонізація повітря;
– недостатня освітленість робочої зони;
– відсутність чи нестача природного освітлення.

2. Психофізіологічні:

– статичне перевантаження;
– розумове перевантаження;
– емоційні перевантаження.

Відповідно до наведених факторів здійснюємо планування щодо безпечного виконання роботи.

5.1 Технічні рішення щодо безпечного виконання роботи

Дослідження підвищення ефективності розподілу трафіку у телекомунікаційних мережах проводилося у приміщенні, де розміщені робочі місця з комп'ютерами. При проектуванні робочих місць були враховані ергономічні аспекти, зокрема: висота робочої поверхні, розміри простору для ніг, розташування документів (включаючи наявність та розміри підставки для них, можливість різного розташування), характеристики робочого крісла, вимоги до робочого столу та його регульованість.

Основними елементами робочого місця проектувальника є стіл і крісло. З вимог до робочого столу можна виділити наступне:

Висота столу повинна бути обрана так, щоб працівнику було зручно сидіти, вільно, в зручній позі, при необхідності відпочивати руки на підлокітниках.

Нижня частина столу повинна бути сконструйована так, щоб працівник міг зручно сидіти, не відчувавши дискомфорту у ногах.

Поверхня столу має уникати відблисків у полі зору працівника.

Конструкція столу повинна передбачати наявність висувних ящиків (принаймні трьох для зберігання документів, канцелярських товарів, особистих речей).

Рекомендована висота робочої поверхні столу становить від 680 до 760 мм, а висота поверхні, на якій розміщується клавіатура, має бути 650 мм.

Важливе значення надається характеристикам робочого крісла. Так, рекомендована висота сидіння має бути у межах 420-550 мм. Поверхню сидіння рекомендується робити м’якою з заокругленими краями, а кут нахилу спинки робочого крісла – регульованим [25].

Необхідно передбачити під час проектування можливість різного розміщення документів: збоку від терміналу, між монітором і клавіатурою тощо.

Також велике значення приділяється правильній робочій позі, оскільки при незручному розташуванні може виникнути біль у м’язах, суглобах і сухожиллях. Вимоги до робочої пози включають нахил шиї понад 20° від вісі "голова-шия" до вісі тулуба, розслаблені плечі та горизонтальне розташування передпліччя. Причини некомфортної пози можуть включати відсутність підставки для документів, надто високе розміщення клавіатури, надто низьке розташування документів, недостатній простір для ніг та відсутність місця для рук і кистей.

Створення сприятливих умов праці та естетичне оформлення робочих місць має важливе значення як для полегшення праці, так і для підвищення її привабливості, що позитивно впливає на продуктивність праці. Колірні рішення для приміщень та меблів повинні сприяти створенню позитивного візуального сприйняття та піднімати настрій. У робочих приміщеннях, де виконується монотонна розумова робота, що вимагає значного нервового напруження та концентрації, рекомендується використовувати спокійні тони, такі як малонасичені відтінки холодного зеленого чи блакитного.

Лінія електромережі для живлення персональних комп'ютерів, периферійних пристроїв (принтер, сканер та інші) в приміщенні реалізована як окрема групова трипровідна мережа за допомогою прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Нульовий захисний провід прокладено від стійки групового розподільчого щита, розподіль-

чого пункту до розеток живлення. Не допускається підключення на щиті до одного контактного затискача нульового робочого та нульового захисного провідників [26].

Усі провідники відповідають номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму тощо.

Не припустимим є підключення комп'ютерів та периферійних пристроїв до звичайної двопровідної електромережі, включаючи використання перехідних пристроїв.

5.2 Технічні рішення з гігієни праці та виробничої санітарії

Мікроклімат

Мікроклімат у виробничих приміщеннях, відомий як метеорологічні умови, має значний вплив на фізичний стан та продуктивність працівників. Це означає умови внутрішнього середовища, що впливають на тепловий режим організму людини взаємодії з оточенням. Мікроклімат складається з різних фізичних параметрів повітря, таких як температура, швидкість потоку повітря, вологість, барометричний тиск, а також температура навколишніх поверхонь і інтенсивність інфрачервоного випромінювання.

Нормується мікроклімат на робочому місці розробника згідно ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень» [27]. Проведення досліджень відноситься до категорії I а (енерговитрати до 139Дж/с) [28]. Допустимі параметри мікроклімату для цієї категорії наведені в табл.5.1.

Для досягнення встановлених нормативами параметрів мікроклімату в приміщенні передбачено природну вентиляцію. При цьому притікання повітря здійснюється через прорізі в дверях, а влітку - також через віконні прорізи. Крім того, у приміщенні є загальна система опалення, а також регулярно проводиться вологе прибирання.

Таблиця 5.1 – Параметри мікроклімату

Період року	Допустимі		
	t,°C	W, %	V, м/с
Теплий	22-28	55	0,1-0,2
Холодний	21-25	75	0,1

Склад повітря робочої зони

В приміщенні, де здійснюється дослідження, можливими шкідливими речовинами у повітрі є пил та озон. Джерелами цих речовин є офісна техніка. Пил потрапляє у приміщення ззовні. ГДК шкідливих речовин, які знаходяться в досліджуваному приміщені, наведені в таблиці 5.2.

Таблиця 5.2 – ГДК шкідливих речовин у повітрі

Назва речовини	ГДК, мг/м^3		Клас небезпечності
	Максимально разова	Середньо добова	
Пил нетоксичний	0,5	0,15	4
Озон	0,16	0,03	1

Параметри іонного складу повітря на робочому місці, що обладнане ПК, повинні відповідати допустимим нормам (табл.5.3).

Таблиця 5.3 – Рівні іонізації повітря приміщень при роботі на ПК

Рівні	Кількість іонів в 1 см^3	
	n+	n-
Мінімально необхідні	400	600
Оптимальні	1500-3000	3000-5000
Максимально необхідні	50000	50000

Для забезпечення припустимих значень мікроклімату та концентрації позитивних та негативних іонів необхідно встановлювати системи або пристрої для зволоження та/або штучної іонізації повітря, а також системи кондиціювання повітря.

Виробниче освітлення

Правильне освітлення робочого місця є одним з ключових факторів, який впливає на ефективність праці людини та сприяє зменшенню травматизму та професійних захворювань. Добре організоване освітлення створює комфортні умови для праці, що підвищує працездатність та продуктивність працівників. Освітлення робочого місця проектувальника повинно бути спроектоване таким чином, щоб працівник міг без надмірного напруження очей виконувати свої обов'язки. Втомленість очей може бути спричинена рядом факторів, таких як недостатня освітленість, зайве освітлення або неправильна орієнтація джерела світла.

У приміщенні, де виконується робота використовується штучне та природне освітлення. Норми освітленості при штучному освітленні та КПО (для III пояса світлового клімату) при природному та сумісному освітленні зазначені у таблиці 5.4.

Для забезпечення належного освітлення робочого місця передбачено такі заходи:

- Розташування робочого місця відносно вікон так, щоб природне світло надходило з лівого боку.
- Розміщення робочого місця з ПК так, щоб уникається пряме попадання світла в очі працівника.
- Розташування джерел штучного освітлення з обох боків від екрану, паралельно напрямку зору.
- Застосування антиблікових сіток, спеціальних фільтрів для екрану, захисних козирків або жалюзі на вікнах, щоб уникнути світових блисків від ек-

рану, клавіатури та освітлювальних пристроїв, а також від сонячного світла, що напрямується у напрямку очей.

- Наявність регульованих пристроїв для відкривання вікон у приміщенні.

Таблиця 5.4 - Норми освітленості в приміщенні

Характеристика зорової роботи	Найменший розмір об'єкта розрізнювання	Розряд зорової роботи	Підрозряд зорової роботи	Контраст об'єкта розрізнення з фоном	Характеристика фона	Освітленість, лк		КПО, $e_н$,%			
						Штучне освітлення		Природнє освітлення		Сумісне освітлення	
						Комбіноване	Загальне	Верхнє або верхнє і бокове	Бокове	Верхнє або верхнє і бокове	Бокове
Дуже високої точності	Від 0,15 до 0,3	II	г	великий	світлий	1000	300	7	2,5	4,2	1,5

Виробничий шум

Шум - це небажаний звук, який складається з різних інтенсивностей, частот і тиску, і має негативний вплив на організм людини, заважаючи відпочивати та працювати. Фізіологічно, шум може бути визначений як будь-який звук, що сприймається органами слуху людини і викликає дискомфорт.

Рівні шуму на робочих місцях осіб, що працюють з ПК, визначаються відповідно до ДСН 3.3.6.037-99 [29]. Допустимі рівні звукового тиску під час побудови інтелектуальної мережі зв’язку наведені в таблиці 5.5.

Для забезпечення виробничих приміщень та робочих місць нормованими рівнями шуму використовуються засоби зменшення шуму, вибір яких базується на спеціальних інженерно-акустичних розрахунках.

Таблиця 5.5 – Допустимі рівні звукового тиску і рівні звуку для постійного широкополосного шуму

Характер робіт	Допустимі рівні звукового тиску (дБ) в стандартизованих октавних смугах зі середньогеометричними частинами (Гц)									Допустимий рівень звуку, дБА
	32	63	125	250	500	1000	2000	4000	8000	
Виробничі приміщення	86	71	61	54	49	45	42	40	38	50

Виробничі випромінювання

Вимоги щодо рівня неіонізуючих електромагнітних випромінювань, електростатичних та магнітних полів встановлюються відповідно до ДсанПіН 3.3.2.007-98 [30]. Допустимі параметри електромагнітних неіонізуючих випромінювань і електростатичного поля для виконання дослідження наведені в таблиці 5.6.

Для забезпечення вказаних параметрів під час виконання завдань, рекомендується використовувати обладнання, що відповідає міжнародним стандартам, а також дотримуватися оптимального режиму роботи за персональним комп'ютером.

5.3 Пожежна безпека

В Україні прийнята система класифікації виробничих приміщень та будівель за рівнем вибухопожежної та пожежної небезпеки. Ця система визначає комплекс пожежно-технічних заходів, спрямованих на забезпечення безпеки людей і збереження матеріальних цінностей. Встановлення категорії визначає протипожежні вимоги до планування та забудови промислових підприємств, вогнестійкості будівельних конструкцій, розмірів пожежних відсіків, а також розташування і довжини шляхів евакуації. Ці вимоги також включають засто-

сування конструкцій, що можуть легко зніматися, тощо. Зазначений перелік заходів підкреслює важливість правильного визначення категорії, оскільки помилки в цьому можуть вплинути на ефективність заходів щодо попередження пожеж та захисту від них на протязі багатьох років.

Таблиця 5.6. - Допустимі параметри електромагнітних неіонізуючих випромінювань і електростатичного поля

Види поля	Допустимі параметри поля		Допустима поверхнева щільність потоку енергії (інтенсивність потоку енергії), Вт/кв.м
Напруженість електромагнітного поля	за електричною складовою (Е), В/м	за магнітною складовою (Н), А/м	
60 кГц до 3 мГц	50	5	
3 кГц до 30 мГц	20	-	
30 кГц до 50 мГц	10	0,3	
30 кГц до 300 мГц 5	5	-	
300 кГц до 300 гГц	-	-	
Електромагнітне поле оптичного діапазону в ультрафіолетовій частині спектру			
УФ-С (220 – 280 мм)			0,001
УФ-В (280 – 320 мм)	-	-	0,01
УФ-А (320 – 400 мм)			10,0
в видимій частині спектру 400 – 760 мм			10,0
0,76 – 10,0 мкм			35,0 – 70,0
Напруженість електричного поля ВДТ			20кВ/м

В приміщенні, де здійснювалася робота використовуються тільки негорючі речовини та матеріали у холодному стані, тому за ступенем вибухопожежної та пожежної небезпеки приміщення відноситься до категорії «Д». Пожежну небезпеку несуть у собі лише кабельні електропроводки до обладнання, що є припустимим для даної категорії приміщень [31].

За вогнестійкістю приміщення відноситься до другої категорії [31]. Мінімальні межі вогнестійкості будівельних конструкцій і максимальні межі розпо-

всюдження полум'я по них для II категорії наведені в таблиці 5.7.

Таблиця 5.7 – Мінімальні межі вогнестійкості будівельних конструкцій (у год.) і максимальні межі розповсюдження полум'я по них (у см) для II ступеня вогнестійкості будівель

Ступінь вогнестійкості будівлі	Стіни				Колони	Сходові площадки, балки, косоури, марші сходових клітків	Плити, настили, (з утеплювачем), інші несучі конструкції перекрить	Елементи перекрить	
	Несучі	Самонесучі	Зовнішні ненесучі	Внутрішні ненесучі (перегородки)				Плити, настили, прогони	Балки, ферми, арки, рами
II	2 0	1 0	0.25 0	0.25 0	2 0	1 0	0.75 0	0.25 0	0.25 0

Забезпечення пожежної безпеки на підприємстві базується на кількох основних компонентах виробництва:

1. Технічна система, яка охоплює надійність обладнання, використання безпечних технологій, визначення обсягу вибухопожежонебезпечних матеріалів, проектування рішень з пожежної безпеки, впровадження систем виявлення та тушіння пожеж тощо.

2. Персонал, його підготовка, ознайомлення з регламентами і правилами безпечної роботи.

3. Система управління, що включає в себе регулювання та контроль за всіма аспектами пожежної безпеки на підприємстві.

Технічні рішення системи запобігання пожежі

Серед основних причин пожеж у приміщення можуть виникнути наступні ситуації:

- Небезпека виникнення загоряння через значну кількість паперу та

паперового пилу внаслідок непильного поводження з вогнем, особливо це актуально при відключенні електроенергії.

- Несправність електропроводки.

Для запобігання пожежонебезпечним ситуаціям проводяться профілактичні заходи, зокрема, перевірка справності електропроводки та мережі щоквартально. Робітники також мають зобов'язання сповіщати відповідальну особу про будь-які порушення приладів чи розеток.

Крім того, для профілактики пожеж регулярно проводяться чотири рази на рік протипожежні інструктажі, після яких працівники обов'язково ставлять свої підписи в журналі обліку проведених інструктажів. Додатково використовується візуальна агітація у вигляді попереджувальних знаків «Курити заборонено» для збільшення уваги до пожежної безпеки.

Технічні рішення системи протипожежного захисту

Протипожежний захист на підприємстві включає наступні основні складові:

- Підготовка та видання письмового наказу щодо організації пожежної безпеки на наступний рік.
- Організація та проведення протипожежних інструктажів та спеціального навчання з пожежної безпеки для посадових осіб та працівників відповідно до встановлених норм.
- Встановлення правил щодо можливості паління, відкритого вогню та порядку проведення вогневих робіт.
- Створення та організація роботи пожежно-технічної комісії відповідно до Типового положення про ПТК.
- Забезпечення території та об’єктів підприємства засобами пожежогасіння згідно з встановленими нормами.
- Встановлення автоматичних установок пожежогасіння та пожежної сигналізації на об’єктах підприємства відповідно до вимог.

- Встановлення системи оповіщення людей про пожежу та ознайомлення всіх працівників з нею.
- Реагування керівника підприємства на факти порушень чи невиконання посадовими особами та іншими працівниками встановленого протипожежного режиму.

Додатково, для обмеження розповсюдження пожежі в приміщенні передбачено наявність переносного вуглекислотного вогнегасника типу ОУ-5. Також забезпечено вільний доступ до засобів первинного пожежогасіння та можливість відключення електросхем устаткування.

У будинку передбачено 6 шляхів евакуації для людей, з коридорами шириною 2,4 метри, що відповідає нормам. Ширина дверей евакуаційних виходів також відповідає встановленим нормам.

ВИСНОВКИ

У бакалаврській кваліфікаційній роботі було проведено дослідження проблеми ефективного розподілу трафіку у сучасних телекомунікаційних мережах, що набуває все більшої актуальності в умовах стрімкого зростання обсягів переданих даних, ускладнення мережевих топологій та підвищення вимог до якості обслуговування.

Здійснено огляд теоретичних засад телекомунікаційного трафіку, класифікацій методів його розподілу, а також проаналізовано архітектуру сучасних телекомунікаційних мереж. Було охарактеризовано традиційні топології, технології маршрутизації та визначено основні проблеми, пов’язані з динамічним управлінням навантаженням.

Детально розглянуто існуючі методи маршрутизації: від класичних протоколів (OSPF, BGP, RIP) до сучасних підходів з використанням штучного інтелекту. Особливу увагу приділено аналізу переваг і недоліків кожного методу, а також здійснено порівняння традиційних і інтелектуальних рішень.

Було розроблено концептуальну модель, що базується на ефективному розподілі трафіку з урахуванням адаптивних алгоритмів балансування навантаження, оптимізації маршрутизації та управління якістю обслуговування. Така модель дозволяє знижувати затримки, підвищувати пропускну здатність і забезпечувати рівень QoS, відповідно до вимог користувачів.

Розроблено алгоритм конструювання трафіку в програмно-конфігурованих мережах, який базується на основі узагальненої метрики маршрутів та станом мережі. Запропонований спосіб відрізняється від існуючих меншою швидкістю на ремаршрутизацію трафіку та дозволяє зменшити відсоток втрати пакетів в програмно-конфігурованій мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Захарченко С. М. Метод вдосконалення одношляхових протоколів динамічної маршрутизації / С. М. Захарченко, К. І. Шевчук // Інформаційні технології та комп'ютерна інженерія. - 2018. - № 2. - С. 16-25. - Режим доступу: http://nbuv.gov.ua/UJRN/Itki_2018_2_5
2. Климаш М.М. Підвищення ефективності розподілу ресурсів телекомунікаційної мережі шляхом зміни маршрутів передавання даних [Електронний ресурс] / М.М. Климаш, Б.А. Бугиль, О.А. Лаврів, І.В. Демидов // Проблеми телекомунікацій. – 2012. – № 4 (9). – С. 32 – 44.
3. Лемешко О. В., Єременко О. С. Розробка та дослідження лінійної оптимізаційної моделі швидкої перемаршрутизації з балансуванням навантаження в телекомунікаційних мережах. Радиоэлектроника и информатика. 2017. № 4 (79). С. 18–25.
4. Лемешко О. В., Єременко О. С. Динамічна модель маршрутизації при забезпеченні якості обслуговування за показником ймовірності своєчасної доставки пакетів. XI Міжнародна науково-технічна конференція «Проблеми телекомунікацій» ПТ-2017: збірник матеріалів конференції (м. Київ, 18–21 квітня 2017). Київ: КПІ ім. Ігоря Сікорського, 2017. С. 285–287.
5. Лемешко, О. В., Шаповалова, А. С., Єременко, О. С., Євдокименко, М. О., Хайлан, А. М. (2019), “Математична модель швидкої перемаршрутизації з балансуванням навантаження та диференційованого обмеження трафіка в мережах SD-WAN“, Системи управління, навігації та зв’язку, No. 4(56), С. 63-71.
6. Климаш Ю.В. Комплексний метод маршрутизації інформаційних потоків у самоорганізованих мережах / Ю.В. Климаш, О.М. Шпур, М.В. Кайдан // Вісник Національного університету «Львівська політехніка». Радіоелектроніка та телекомунікації №885 – Львів. – 2017. – С.76-87
7. Куліш Є. Б. Оптимальна маршрутизація ефективного використання пропускної здатності мультисервісної мережі зв’язку / Є. Б. Куліш, А. Г. Лож-

ковський, В. Ю. Гордієнко // Наукові праці ОНАЗ ім. О. С. Попова. - 2013. - № 1. - С. 106-109.

8. Стрихалюк Б.М. Підвищення ефективності динамічної маршрутизації у гетерогенних сервісно-орієнтованих системах з використанням гіперболічних потоків Річчі / Б.М. Стрихалюк, 1Ю.В. Климаш, І.Б. Стрихалюк, Б. В. Коваль // Вісник Національного університету «Львівська політехніка» №818
9. Євдокименко, М. О., Шаповалова, А. С., Шаповал, М. М. (2020), "Потокова модель маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей", Проблеми телекомунікацій, No. 1(26), С. 48-62.
10.. Радіоелектроніка та телекомунікації. – Львів. – 2015.– С. 189-194.
11. Гоголева М.А. Потоковая модель маршрутизации в MESH-сети / М.А. Гоголева, Н.В. Качан // 3-й Международный радиоэлектронный Форум «Прикладная радиоэлектроника. Состояние и перспективы развития» (МРФ-2008): Сб. материалов форума. – Харьков: ХНУРЭ, 2008. – С. 41-43.
12. Іванісенко Игор. Методи балансування з урахуванням мульти - фрактальних властивостей навантаження/ Людмила Кирченко, Тамара Радивілова – International Journal "Information Content and Processing", Volume 2, Number 4, 2015 – 345 с.
13. Пермяков, Олександр, Наталія Королюк, Дмитро Голубничий, and Петро Скоропанюк. "Алгоритм мультифрактального балансування навантаження інформаційно-телекомунікаційних мереж спеціального призначення." *Сучасні інформаційні технології у сфері безпеки та оборони* 42, no. 3 (December 17, 2021): 63–70.
14. Тимченко О.В. Методи справедливого розподілу ресурсів інфокомунікаційних мереж / Тимченко О.В., Кирик М.І., Самі Аскар // XXVI Науково-технічна конференція "Моделювання". ІПМЕ НАН України. Тези конференції. 11-12 січня 2007 року. – К.: 2007. – 86 с. –С.67-69.
15. Кирик М.І. Забезпечення якості передачі мультимедійного трафіку при багатоадресній передачі / Кирик М.І., Самі Аскар // Науково-практична конфе-

ренція „Сучасні проблеми телекомунікацій – 2008”. Матеріали конференції. 29-30 жовтня 2008 р. – Львів: 2008. – С.15-17.

16. Куліш Є.Б. Використання адаптивної динамічної маршрутизації на мультисервісних мережах зв’язку / Є.Б. Куліш, А.Г. Ложковський, В.В. Кичак // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2013. - №1. – С. 198-201.
17. Пономаренко Н.Є., Коляда К.В. Модифікований метод балансування навантаження для розподіленого хмарного сховища // Прикладна математика та комп'ютинг 2023. – Київ, 2023. – С. 434 – 438
18. Щур В. Аналіз сучасних методів балансування навантаження в SDN мережах / В. Щур, Ю. Кулаков // Вісник Хмельницького національного університету. – 2023. - №4. – С. 352-357.
19. Погорілий С.Д. Генетичний алгоритм розв'язання задачі маршрутизації в мережах / С.Д. Погорілий, Р.В. Білоус// Пробл. програмув. – 2010. – № 2-3. – С. 171-177.
20. Семко О.В. Управління маршрутизацією в бездротових сенсорних мережах. Інформаційні технології управління екологічною безпекою, природокористуванням, заходами в надзвичайних ситуаціях: Колективна монографія за матеріалами XVII Міжнародної науково-практичної конференції (м.Київ, 25-26 вересня 2018 р.). м.Київ. 2018.С.103-106.
21. Семко О. Логіко-семантична модель управління маршрутизацією потоків даних в сенсорних мережах. Системи управління, навігації та зв’язку. 2018. №52. С.135-139.
22. Семко О., Семко В., Бурячок В., Складанний П. Методологія інтелектуального управління маршрутизацією в конфліктуючих сенсорних мережах варіативної топології. Сучасна спеціальна техніка. 2018. №55. С.64-76.
23. Семко О.В., В.В.Семко. Розробка формальної моделі інтелектуального управління маршрутизацією в конфліктуючих сенсорних мережах варіативної топології. Математичне моделювання в економіці. 2019. № 1. С.5-19.

24. ДСТУ ISO 45001:2019 Системи управління охороною здоров’я та безпекою праці. Вимоги та настанови щодо застосування (ISO 45001:2018, IDT). URL: http://online.budstandart.com/ua/catalog/ doc-page.html?id_doc=88004.
25. ДСТУ 8604:2015 Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги. URL: http://online.budstandart. com/ua/catalog/doc-page?id_doc=71028
26. НПАОП 0.00-7.15-18 Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями. URL: http://sop.zp.ua/norm_npaop _0 _ 00-7_ 15-18_01_ua.php. 14. Про мінімальні вимоги безпеки при роботі з дисплейним обладнгям
27. ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень. - [Електронний ресурс] - Режим доступу: http://mozdocs.kiev.ua/view.php?id=1972
28. Гігієнічна класифікація праці (за показниками шкідливості і небезпеки факторів виробничого середовища від 12.08.1986 № 4137-86. - [Електронний ресурс] - Режим доступу: http://zakon4.rada.gov.ua/laws/show/v4137400-86
29. ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку. - [Електронний ресурс] - Режим доступу: http://document.ua/sanitarni-normi-virobnichogo-shumu-ultrazvuku-ta-infrazvuku-nor4878.html
30. Про мінімальні вимоги безпеки при роботі з дисплейним обладнанням: 90/270/ЕЭС. Брюссель : Рада Європейських співтовариств, 1990. URL: http://docs.pravo.ru/document/view/32704903/
31. ДБН В.1.1-7:2016 Пожежна безпека об`єктів будівництва. Загальні ви моги. URL: http://www.poliplast.ua/doc/dbn _v.1.1-7-2002.pdf.
32. ДСТУ Б В.1.1-36:2016 Визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпек. URL: https://dbn.co.ua/load/normativy/dstu/dstu_b_v_1_1_36/5-1-0-1759

Додаток А
(обов’язковий)

ІЛЮСТРАТИВНА ЧАСТИНА
ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОЗПОДІЛУ ТРАФІКУ
У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ
назва бакалаврської кваліфікаційної роботи

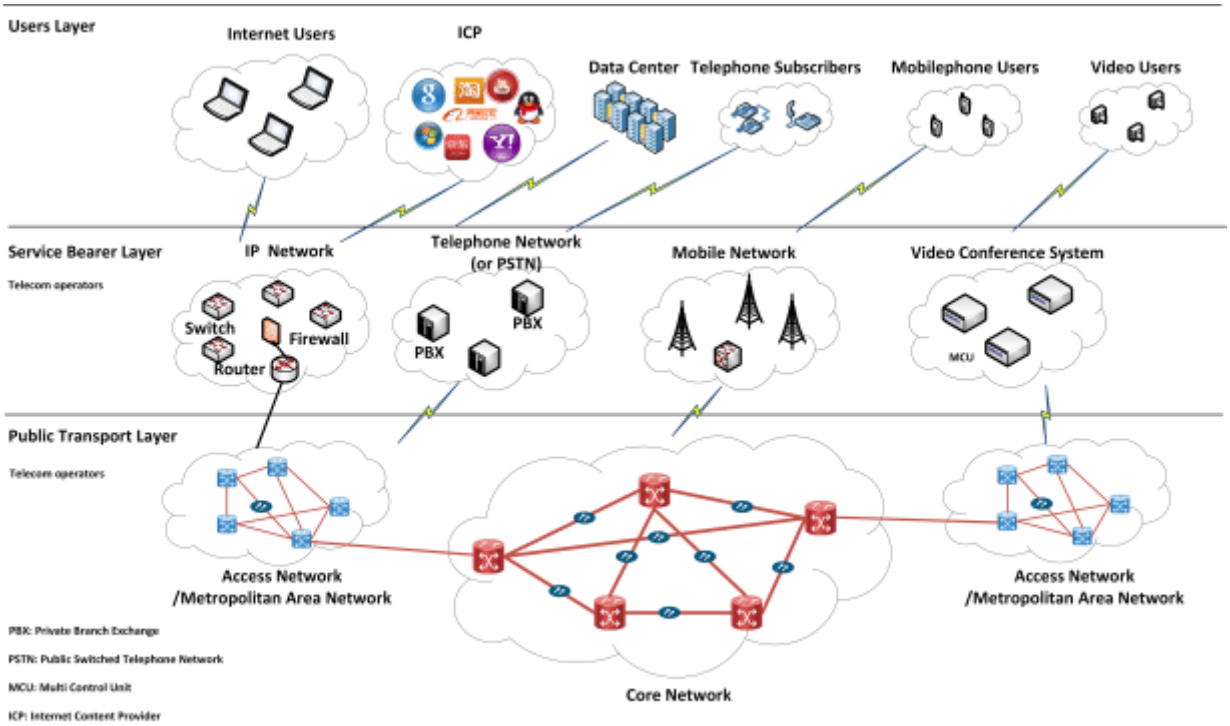


Рисунок 1 – Архітектура існуючих телекомунікаційних мереж

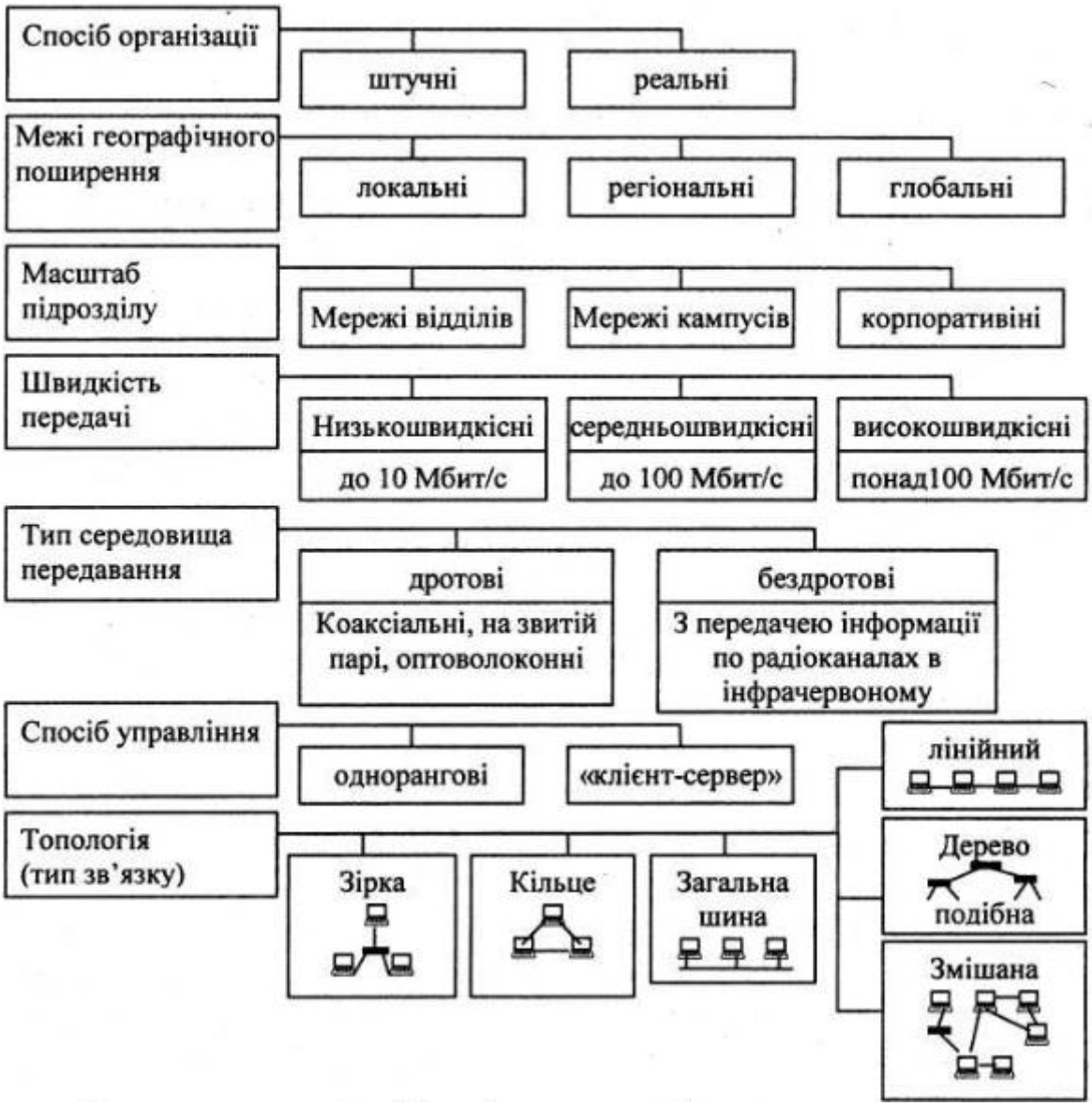
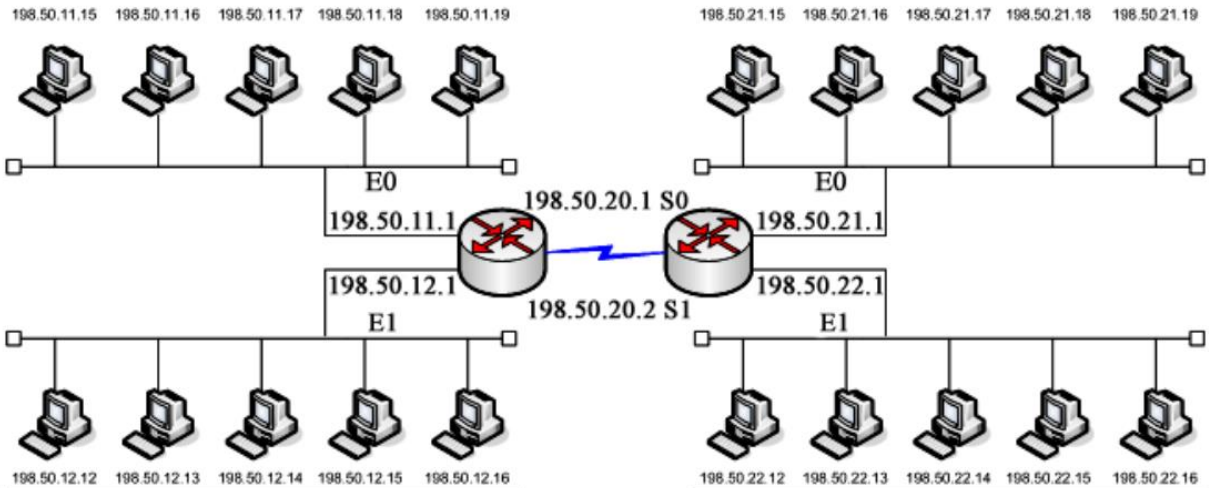


Рисунок 2 – Класифікація телекомунікаційних мереж



Таблиця маршрутизації

Звідки отримано	Мережна адреса	Лічильник вузлів	Інтерфейс
C	192.50.11.0	0	E0
C	192.50.12.0	0	E1
C	192.50.13.0	0	S0
R	192.50.14.0	1	S0
R	192.50.15.0	1	S0

Таблиця маршрутизації

Звідки отримано	Мережна адреса	Лічильник вузлів	Інтерфейс
C	192.50.21.0	0	E0
C	192.50.22.0	0	E1
C	192.50.23.0	0	S1
R	192.50.24.0	1	S1
R	192.50.25.0	1	S1

Рисунок 3 – Маршрутизація

Рисунок 4 – Класифікація протоколів маршрутизації

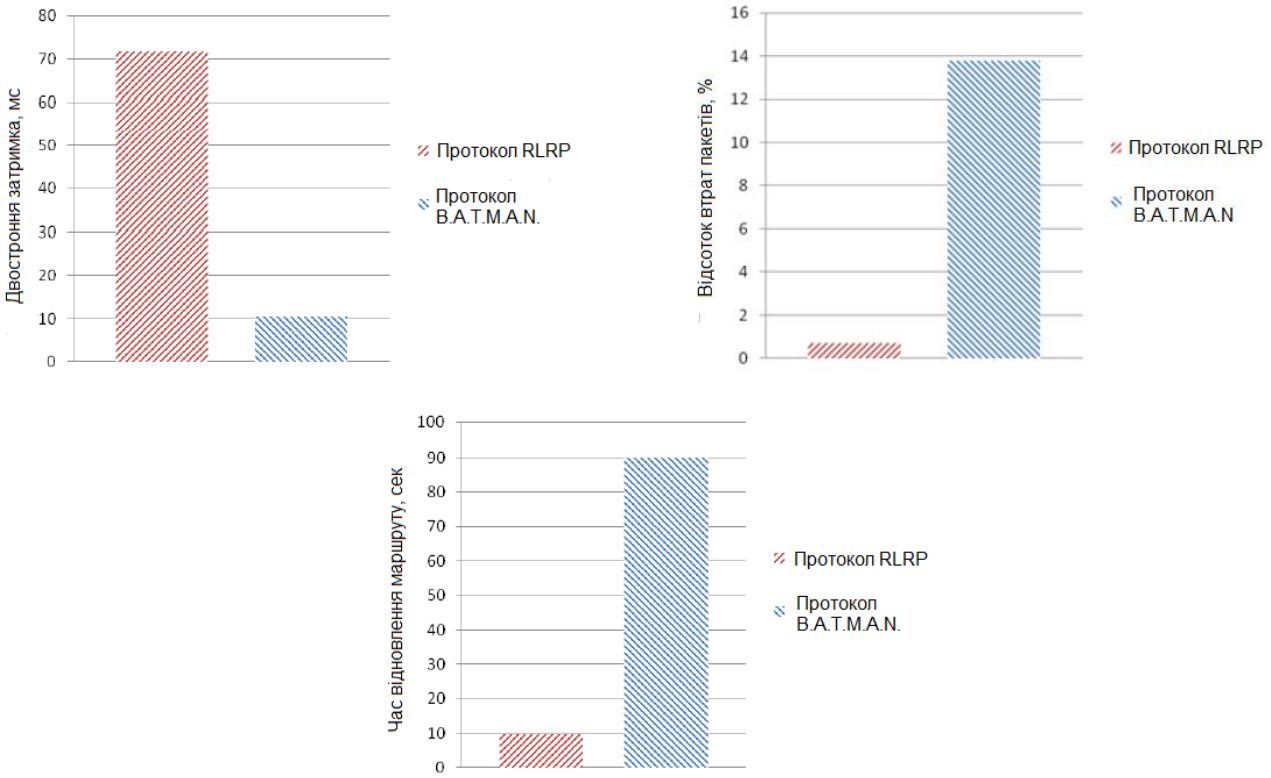


Рисунок 5 – Порівняння протоколів маршрутизації

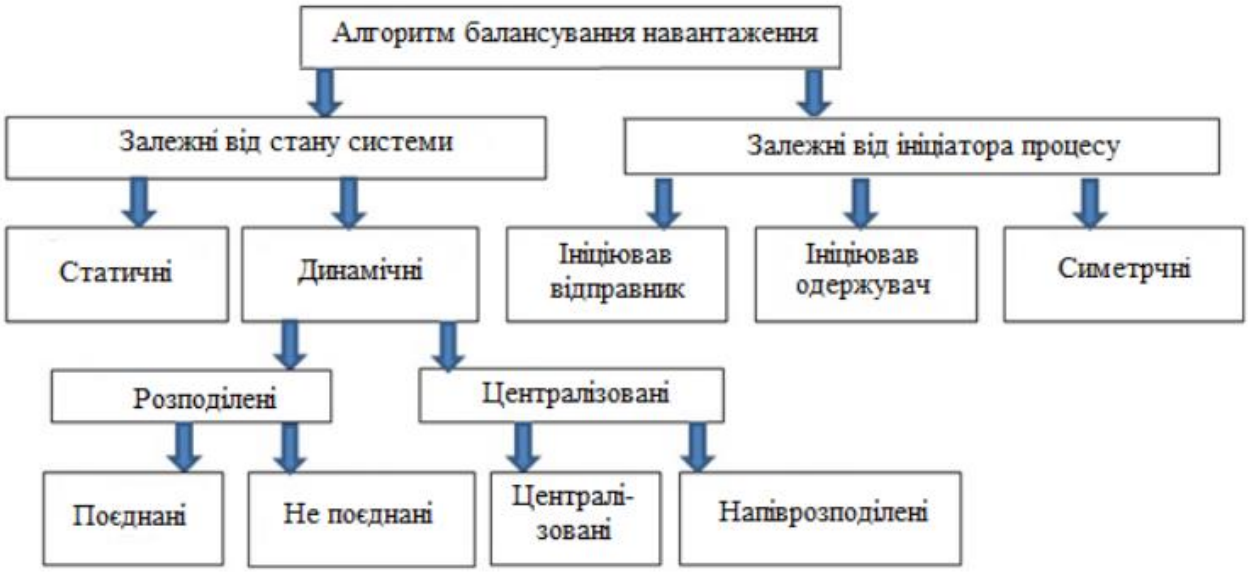


Рисунок 6 – Класифікація алгоритмів балансування навантаження

Таблиця 1 – Порівняльна характеристика методів розподілу трафіка

Метод	Адаптивність	Масштабованість	Складність реалізації	Використання
Статична маршрутизація	Низька	Низька	Низька	Малі мережі
Динамічна маршрутизація	Середня	Висока	Середня	Провайдери, корпоративні мережі
QoS та PBR	Висока	Середня	Середня	VoIP, відео
SDN	Висока	Висока	Висока	Хмарні середовища, датацентри
AI/ML	Дуже висока	Висока	Дуже висока	Розподілені мережі, автоматизація
CDN / Edge	Висока	Висока	Середня	Медіасервіси, IoT

Таблиця 2 – Порівняння методів маршрутизації

Критерії	Традиційні методи маршрутизації	Новітні методи
Адаптивність	Обмежена, статичні маршрути не змінюються без ручного втручання.	Висока адаптивність, автоматична зміна маршруту в реальному часі.
Складність налаштування	Низька для статичних, висока для динамічних.	Вища через необхідність навчання моделей AI/ML.
Час конвергенції	Повільна, особливо в старих протоколах, таких як RIP.	Швидка, завдяки прогнозуванню та адаптивності моделей.
Можливості прогнозування	Обмежені, маршрут вибирається на основі поточного стану.	Прогнозування трафіку та навантаження на основі історичних даних.
Резистентність до аномалій	Низька, відсутня здатність виявляти аномалії без спеціальних налаштувань.	Висока, AI/ML моделі можуть передбачити і виявити аномалії в мережі.

Рисунок 7 – Алгоритм конструювання трафіку

Додаток Б

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: Підвищення ефективності розподілу трафіку у телекомунікаційних мережах

Тип роботи: бакалаврська кваліфікаційна робота
(бакалаврська кваліфікаційна робота / магістерська кваліфікаційна робота)

Підрозділ кафедра ІКСТ, факультет ІЕС, група ПЗТ-21б
(кафедра, факультет, навчальна група)

Коефіцієнт подібності текстових запозичень, виявлених у роботі системою StrikePlagiarism 7,08 %

Висновок щодо перевірки кваліфікаційної роботи (відмітити потрібне)

☐ Запозичення, виявлені у роботі, є законними і не містять ознак плагіату, фабрикації, фальсифікації. Роботу прийняти до захисту

☐ У роботі не виявлено ознак плагіату, фабрикації, фальсифікації, але надмірна кількість текстових запозичень та/або наявність типових розрахунків не дозволяють прийняти рішення про оригінальність та самостійність її виконання. Роботу направити на доопрацювання.

☐ У роботі виявлено ознаки плагіату та/або текстових маніпуляцій як спроб укриття плагіату, фабрикації, фальсифікації, що суперечить вимогам законодавства та нормам академічної доброчесності. Робота до захисту не приймається.

Експертна комісія:

Кичак В.М., завідувач кафедри ІКСТ _____
(прізвище, ініціали, посада) (підпис)

Васильківський М.В., гарант ОПП _____
(прізвище, ініціали, посада) (підпис)

Особа, відповідальна за перевірку _____ Васильківський М.В.
(підпис) (прізвище, ініціали)

З висновком експертної комісії ознайомлений(-на)

Керівник _____ Михалевський Д.В., д.т.н., професор
(підпис) (прізвище, ініціали, посада)

Здобувач _____ Валігура Д.В.
(підпис) (прізвище, ініціали)