ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «**МЕТОДИ УПРАВЛІННЯ УСУНЕННЯ ВІДМОВ У МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ ДЛЯ ПІДВИЩЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ КОРИСТУВАЧІВ**»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Жанна ШУЛЬГА
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Виконала: здобувачка вищої освіти гр. ТСДМ-61
Жанна ШУЛЬГА
Ім'я, ПРІЗВИЩЕ

Керівник: Ганна ГРИНКЕВИЧ
д.т.н., професор *Ім'я, ПРІЗВИЩЕ*

Рецензент: _____
Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Телекомунікацій

Кафедра ___Телекомунікаційних систем та мереж_____
Ступінь вищої освіти __магістр_____
Спеціальність ___172 Електронні комунікації та радіотехніка _____
Освітньо-професійна програма _____Телекомунікаційні системи та мережі_____

ЗАТВЕРДЖУЮ
Завідувач кафедри __ТСМ_____
_____ Віктор ЗАЇКА
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Шульзі Жанні Олександрівні
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Методи управління усуненням відмов у мультисервісних мережах для підвищення якості обслуговування користувачів
керівник кваліфікаційної роботи Ганна ГРИНКЕВИЧ, д.т.н., доцент
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від « » 2025 р. №

2. Строк подання кваліфікаційної роботи «___» _____ 2025 р.

3. Вихідні дані до кваліфікаційної роботи:
1. Оптимізація архітектури мультисервісної мережі.
2. Вимоги користувачів.
3. Використання гібридної архітектури.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Архітектура для користувачів.
2. Оптимізація навантаження мережі.
3. Управління передчасною оптимізацією архітектури.
4. Впровадження гібридної архітектури.

5. Перелік ілюстративного матеріалу: ___презентація на слайдах_____

6. Дата видачі завдання «___» _____ 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір та аналіз науково-технічної літератури	03.10.2025	Викон.
2	Розробка першого розділу	10.10.2025	Викон.
3	Розробка другого розділу	17.10.2025	Викон.
4	Розробка третього розділу	24.10.2025	Викон.
5	Висновки, вступ, реферат	10.11.2025	Викон.
6	Розробка презентації	30.11.2025	Викон.

Здобувач вищої освіти _____ Жанна ШУЛЬГА
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ганна ГРИНКЕВИЧ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувачка Шульга Ж.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)
на тему: «Методи управління усуненням відмов у мультисервісних мережах для підвищення якості обслуговування користувачів»

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувачка Шульга Жанна Олександрівна показала гарну теоретичну та інженерну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявила ініціативність, сумлінність та хист до наукової роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувачки Шульги Жанни Олександрівни на оцінку «відмінно» та присвоїти йому кваліфікацію магістр з електронних комунікацій та радіотехніки.

Керівник кваліфікаційної роботи _____ Ганна ГРИНКЕВИЧ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Шульга Ж.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри телекомунікаційних систем та мереж _____ Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня магістра

здобувачки вищої освіти Шульги Жанни Олександрівни
(прізвище, ім'я, по батькові)
на тему «Методи управління усуненням відмов у мультисервісних мережах для підвищення якості обслуговування користувачів»

Актуальність. Розвиток сучасних мультисервісних телекомунікаційних мереж супроводжується постійним зростанням вимог до надійності, відмовостійкості та стабільності обслуговування користувачів. У мережах NGN із високою інтенсивністю трафіку навіть короткочасні відмови призводять до втрати даних, деградації QoS та порушення роботи критично важливих сервісів. Забезпечення швидкого виявлення, локалізації та усунення збоїв є ключовою умовою працездатності мережі та мінімізації операційних витрат операторів зв'язку. У цьому контексті дослідження методів управління усуненням відмов у мультисервісних мережах, удосконалення алгоритмів моніторингу, прогнозування, активного й пасивного контролю, а також підвищення якості відновлення мережевих ресурсів є актуальним завданням і повністю відповідає сучасним тенденціям розвитку телекомунікаційних систем.

Позитивні сторони:
1. Робота комплексно розглядає ключові методи підвищення відмовостійкості та якості обслуговування у мультисервісних мережах.
2. Запропоновані підходи мають практичну цінність і можуть бути застосовані для зменшення часу відновлення мережевих ресурсів.

Недоліки :
1. У роботі недостатньо представлено експериментальне підтвердження ефективності запропонованих методів.
2. Не повністю розкрито питання масштабованості та застосування рішень у великомасштабних телекомунікаційних системах.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської кваліфікаційної роботи

Висновок: *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "відмінно", а здобувачка Шульга Жанна Олександрівна заслуговує присвоєння кваліфікації: магістр з електронних комунікацій та радіотехніки.*

Рецензент _____ _____
науковий ступінь, (підпис) *(Ім'я ПРІЗВИЩЕ)*
вчене звання

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 61 стор., 22 рис., 3 табл., 34 джерела.

Метою роботи є розробка методу управління усуненням відмов у мультисервісних мережах, який забезпечить підвищення якості обслуговування користувачів шляхом зменшення часу відновлення працездатності мережі та зниження витрат трафіку.

Об'єктом дослідження є процеси управління усуненням відмов у мультисервісних телекомунікаційних мережах.

Предметом дослідження є методи, алгоритми та моделі управління усуненням відмов у мультисервісних мережах, спрямовані на підвищення якості обслуговування користувачів.

Короткий зміст роботи: У роботі досліджено методи управління усуненням відмов у мультисервісних телекомунікаційних мережах та проаналізовано підходи до підвищення їх надійності й якості обслуговування користувачів. Розглянуто принципи роботи систем моніторингу, локалізації та класифікації збоїв, а також алгоритми активного й пасивного контролю. Показано, що поєднання адаптивних методів керування, прогнозування відмов і використання гібридної архітектури дозволяє мінімізувати час відновлення, зменшити ризик критичних несправностей та забезпечити стабільний рівень QoS у умовах змінного мережевого навантаження.

КЛЮЧОВІ СЛОВА: МУЛЬТИСЕРВІСНА МЕРЕЖА, NGN, SOFTWITCH, ВІДМОВОСТІЙКІСТЬ, НАДІЙНІСТЬ, БЕЗВІДМОВНІСТЬ, НАПРАЦЮВАННЯ, ВІДМОВА, ЗБІЙ, ВІДНОВЛЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ, ПРОГРАМНІ ВІДМОВИ, АПАРАТНІ ВІДМОВИ, МЕРЕЖЕВА ВІДМОВА, ЛОГІЧНА ВІДМОВА, NMS, OSS/BSS, ПРОДУКТИВНІСТЬ МЕРЕЖІ, QOE, QOS, SDN, NFV, ЗАТРИМКА, VOIP, ATA.

ABSTRACT

Text part of the qualification work for obtaining a master's degree: 61 pages, 22 figures, 3 tables, 34 sources.

The purpose of the work - is to develop a method for managing failure elimination in multiservice networks, which will improve the quality of user service by reducing network recovery time and traffic costs.

Object of research - is the processes of managing failure elimination in multiservice telecommunications networks.

Subject of research - is methods, algorithms, and models for managing failure elimination in multiservice networks, aimed at improving the quality of user service.

Summary of the work: The paper investigates methods for managing failure elimination in multiservice telecommunications networks and analyzes approaches to improving their reliability and quality of service. The principles of monitoring, localization, and classification of failures, as well as algorithms for active and passive control, are considered. It is shown that the combination of adaptive control methods, failure prediction, and the use of hybrid architecture minimizes recovery time, reduces the risk of critical failures, and ensures a stable level of QoS under variable network load conditions.

KEYWORDS: MULTISERVICE NETWORK, NGN, SOFTWITCH, FAULT TOLERANCE, RELIABILITY, FAILURE-FREE OPERATION, OPERATING TIME, FAILURE, CRASH, COMPUTER SYSTEM RECOVERY, SOFTWARE FAILURES, HARDWARE FAILURES, NETWORK FAILURE, LOGICAL FAILURE, NMS, OSS/BSS, NETWORK PERFORMANCE, QOE, QOS, SDN, NFV, DELAY, VOIP, ATA.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 10

ВСТУП 12

1 АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО УПРАВЛІННЯ ВІДМОВАМИ В МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ 14

1.1. Структура та особливості функціонування мультисервісних мереж 14

1.2. Надійність і відмовостійкість телекомунікаційних систем 23

1.3. Методи забезпечення якості обслуговування користувачів та управління відмовами 29

Висновок до розділу 1 34

АНАЛІЗ ТА ВИБІР ПОКАЗНИКІВ ДЛЯ ОЦІНЮВАННЯ СТАНУ ТА НАДІЙНОСТІ МЕРЕЖІ 36

2.1. Показники продуктивності та якості функціонування мультисервісних мереж 36

2.2. Вимоги різних типів трафіку до параметрів мережі та показників якості обслуговування 40

2.3 Обгрунтування вибору показників для моніторингу та управління станом мережі 45

Висновок до другого розділу 51

3 ВИЯВЛЕННЯ ТА УПРАВЛІННЯ ВІДМОВАМИ У МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ 53

3.1. Класифікація відмов та їх характеристик у мультисервісному середовищі 53

3.2. Аналіз методів моніторингу та діагностики стану елементів управління мультисервісними мережами 56

3.3. Оцінювання результативності процедур відновлення працездатності мережі 61

3.4. Побудова моделі керування процесами відновлення працездатності в мультисервісній мережі 66

Висновок до розділу 3 69

ВИСНОВКИ 70

ПЕРЕЛІК ПОСИЛАНЬ 73

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 77

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ATM-Asynchronous Transfer Mode

QoS-Quality of Service

CBR-Constant Bit Rate

VBR-Variable Bit Rate

ABR-Available Bit Rate

UBR-Unspecified Bit Rate

NGN -Next Generation Network

ITU-T - International Telecommunication Union – Telecommunication Standardization Sector

RTP (Real-Time Transport Protocol) -Протокол транспортування даних у реальному часі

RTCP (Real-Time Control Protocol) -Протокол керування передачею у реальному часі

RTSP (Real-Time Streaming Protocol) -Протокол потокової передачі у реальному часі

SIP (Session Initiation Protocol) -Протокол ініціації сесій

H.264 (Advanced Video Coding, AVC) -Стандарт кодування відео

Opus - аудіокодек для передачі мови та музики в реальному часі

AAC (Advanced Audio Coding) -розширене кодування аудіо

QoE -Quality of Experience

NMS – Системи управління мережею

OSS- Operation Support System (система підтримки операцій)

BSS -Business Support System (система підтримки бізнесу)

KPI - key performance indicator (ключові параметри якості)

SDN - Software-Defined Networking (Програмно конфігуровані мережі)

NFV- Network Functions Virtualization

IETF -Internet Engineering Task Force

ISO - International Organization for Standardization (Міжнародна організація зі стандартизації)

IEC - International Electrotechnical Commission (Міжнародна електротехнічна комісія)

ETSI - European Telecommunications Standards Institute (Європейський інститут стандартів у телекомунікаціях)

VoIP - voice over IP (голос через IP)

RFC - request for comments

TLS -Transport Layer Security

CM- системи моніторингу

SNMP -Simple Network Management Protocol (простий протокол керування мережею)

IP SLA -Internet Protocol Service Level Agreement

ВСТУП

Телекомунікації-це передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду дротовими, радіо, оптичними або іншими електромагнітними системами.

Телекомунікаційні технології можуть, перш за все, бути розділені на дротові та бездротові. Однак, в цілому, основна телекомунікаційна система складається з трьох частин, які завжди присутні в тій чи іншій формі:

- Передавач, який приймає інформацію та перетворює її в сигнал.
- Середовище передачі, яке також називається фізичним каналом, що несе сигнал. Прикладом може бути «вільний оптичний канал».
- Приймач, який приймає сигнал з каналу та перетворює його назад у доступну інформацію для одержувача.

Телекомунікаційна мережа – це сукупність передавачів, приймачів та каналів зв’язку, які передають повідомлення один одному. Аналогова система зв’язку складається з одного або декількох комутаторів, які встановлюють зв'язок між двома або більше користувачами. Для обох типів мереж можуть знадобитися репітери для посилення або відтворення сигналу, коли він передається на великі відстані. Репітери застосовують для боротьби з загасаннями сигналу, коли сигнал неможливо відрізнити від шуму [1].

Актуальність дослідження полягає в ефективному управлінні процесами виявлення, локалізації та усуненні відмов.

Сучасний етап розвитку інформаційного суспільства характеризується стрімким зростанням обсягів передавання даних та підвищенням вимог користувачів до якості надання телекомунікаційних послуг.

Мультисервісні мережі стали основою сучасних систем зв’язку, так як вони забезпечують об’єднання різних типів трафіку, а саме: голосового, відео, потокового мультимедіа, даних та сигналізації- у єдиній інфраструктурі.

Інфраструктура телекомунікацій належить до мережі обладнання, устаткування та технологій, що забезпечують зв'язок на великі відстані. Вона охоплює широкий спектр компонентів, включаючи кабелі, супутники, вежі,

маршрутизатори і комутатори. Інфраструктура телекомунікацій забезпечує життєво важливий зв'язок та вразлива до різних викликів і загроз. Усунення цих викликів є важливим для забезпечення надійності, безпеки і доступності комунікаційних послуг [2].

Зростання масштабів і складності мультисервісних мереж супроводжується збільшенням ймовірності виникнення відмов у їхніх елементах- каналах зв’язку, вузлах маршрутизації, серверах та програмному забезпеченні. Навіть короткочасна відмова одного з компонентів може призвести до деградації якості обслуговування або повного припинення надання окремих послуг. Вимоги користувачів до безперервного зв’язку, швидкості передачі даних та стабільності сервісів питання ефективного управління процесами виявлення, локалізації та усунення відмов набуває особливої актуальності.

Саме тому, **метою роботи** є розробка методу управління усуненням відмов у мультисервісних мережах, який забезпечить підвищення якості обслуговування користувачів шляхом зменшення часу відновлення працездатності мережі та зниження витрат трафіку.

Об’єктом дослідження є процеси управління усуненням відмов у мультисервісних телекомунікаційних мережах.

Предметом дослідження є методи, алгоритми та моделі управління усуненням відмов у мультисервісних мережах, спрямовані на підвищення якості обслуговування користувачів.

Практичне значення отриманих результатів полягає у можливості впровадження розробленого методу в системи моніторингу та управління мультисервісними мережами операторів зв’язку.

1 АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО УПРАВЛІННЯ ВІДМОВАМИ В МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ

1.1. Структура та особливості функціонування мультисервісних мереж

Мультисервісна мережа – це мережа нового покоління, що забезпечує інтегровану передачу різноманітних послуг, таких як голос, дані та мультимедіа, на базі єдиної IP-інфраструктури. Головними характеристиками є універсальність (підтримка багатьох типів послуг), масштабність, гнучкість, а також використання стандартизованих технологій та протоколів, наприклад, IP.

Принципом мультисервісних мереж є відокремлення один від одного функцій переносу та комутації, функцій управління викликом і функцій управління послугами.

Основною транспортною технологією мультисервісних мереж є технологія ATM(Asynchronous Transfer Mode). Для кожного типу служб ATM забезпечує задану якість обслуговування навантаження, яке оцінюється такими параметрами як затримка пакетів, дисперсія затримки та вірогідність втрати пакетів. Ця опція називається QoS(Quality of Service). Забезпечення QoS є корінною відмінністю технології ATM від існуючих мережних технологій і дозволяє повноцінно передавати інтегральний трафік (голос, відео, дані).

Залежно від вимог джерел до швидкості передавання і QoS розрізняють такі основні категорії класів трафіка:

- з постійною бітовою швидкістю CBR(Constant Bit Rate);
- зі змінною бітовою швидкістю VBR(Variable Bit Rate);
- з доступною бітовою швидкістю ABR(Available Bit Rate);
- з негарантованою бітовою швидкістю UBR(Unspecified Bit Rate).

Обмежені можливості традиційних мереж є негативним чинником, який стримує на шляху до впровадження нових інфокомунікаційних послуг. Нарощування об'ємів інфокомунікаційних послуг може погано позначитися на

показниках якості обслуговування викликів базових послуг існуючих мереж зв'язку. Все це змушує враховувати наявність інфокомунікаційних послуг при плануванні способів розвитку традиційних мереж зв'язку в напрямі створення мультисервісних мереж.

NGN (Next Generation Network – мережа наступного покоління) – це мультисервісна мережа зв'язку, яка підтримує інтеграцію послуг передавання мови, даних та мультимедіа та базується на IP-мережі. Основна відмінність мереж наступного покоління від традиційних мереж в тому, що вся інформація, яка циркулює в мережі, розбита на дві складові. Це сигнальна інформація, що забезпечує комутацію абонентів та надання послуг, і безпосередньо дані користувача, що містять корисну інформацію, призначену абоненту (голос, відео, дані). Шляхи проходження сигнальних повідомлень і даних користувача можуть не збігатися [3].

Базовим принципом концепції NGN є відділення один від одного функцій перенесення і комутації, функцій керування викликом і функцій керування послугами. Функціональна модель мереж NGN має три рівня:

- транспортний рівень;
- рівень керування комутацією і передачею інформації;
- рівень керування послугами.

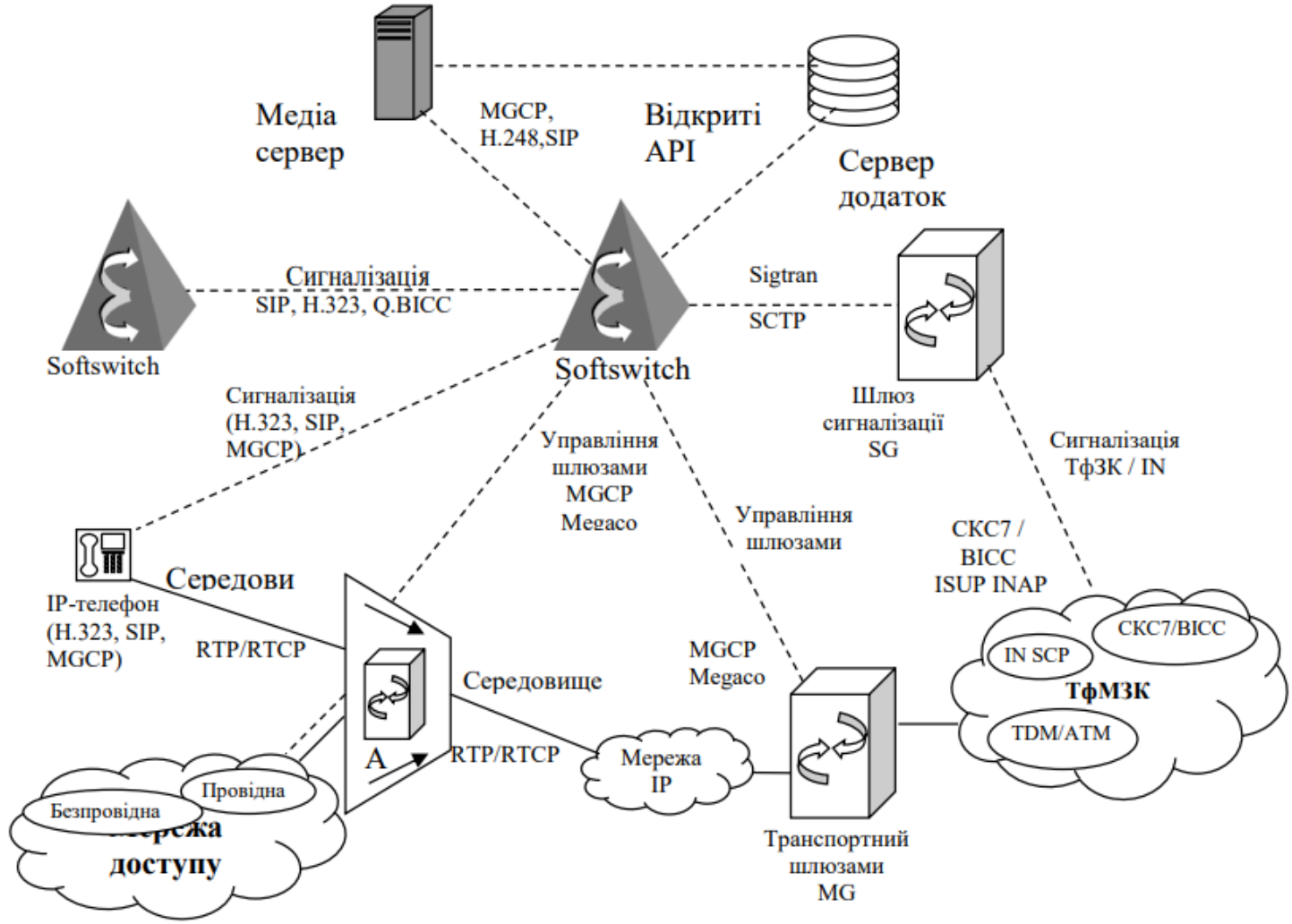


Рис.1.1. Архітектура мережі зв'язку NGN

Принципи побудови мережі нового покоління наступні:

- підключення до мережі має бути максимально простим і зручним, без використання проміжних систем, при цьому використання традиційно застосовуваних протоколів і сервісів повинно бути доступне в колишньому обсязі;
- перш за все будується базова пакетна транспортна мережа на базі комп'ютерних технологій, які забезпечують відповідну якість, надійність, гнучкість і масштабованість, а потім поверх цієї мережі будується потужний комплекс сервісів.

Softswitch (програмний комутатор) – гнучкий програмний комутатор, один з основних елементів мережі зв'язку наступного покоління NGN.

Softswitch – це пристрій керування мережею NGN, покликане відокремити функції управління з'єднаннями від функцій комутації, здатне обслуговувати велику кількість користувачів і взаємодіяти з серверами додатків, підтримуючи відкриті стандарти.

SoftSwitch є носієм інтелектуальних можливостей IP-мережі, він координує управління обслуговуванням викликів, сигналізацію і функції, що забезпечують встановлення з'єднання через одну або кілька мереж [4].

В свою чергу задачею транспортного рівня є комутація і прозора передача інформації користувача. Роллю рівня керування комутацією і передачею є обробка інформації сигналізації, маршрутизація викликів і керування потоками. Рівень керування послугами має функції керування логікою послуг і додатків і є розподіленим обчислювальним середовищем.

Транспортний рівень забезпечує виконання функції доставки інформації будь-якого типу між будь-якими двома географічно рознесеними терміналами. У загальному випадку на транспортному рівні може використовуватися довільна технологія комутації пакетів.

Але ITU-T вважає, що технологія IP є кращою для організації транспорту в NGN, оскільки має найбільшу повноту для виконання завдань мереж наступного покоління.

Проте на практиці найбільшого поширення набула чотирьохрівнева архітектура NGN.

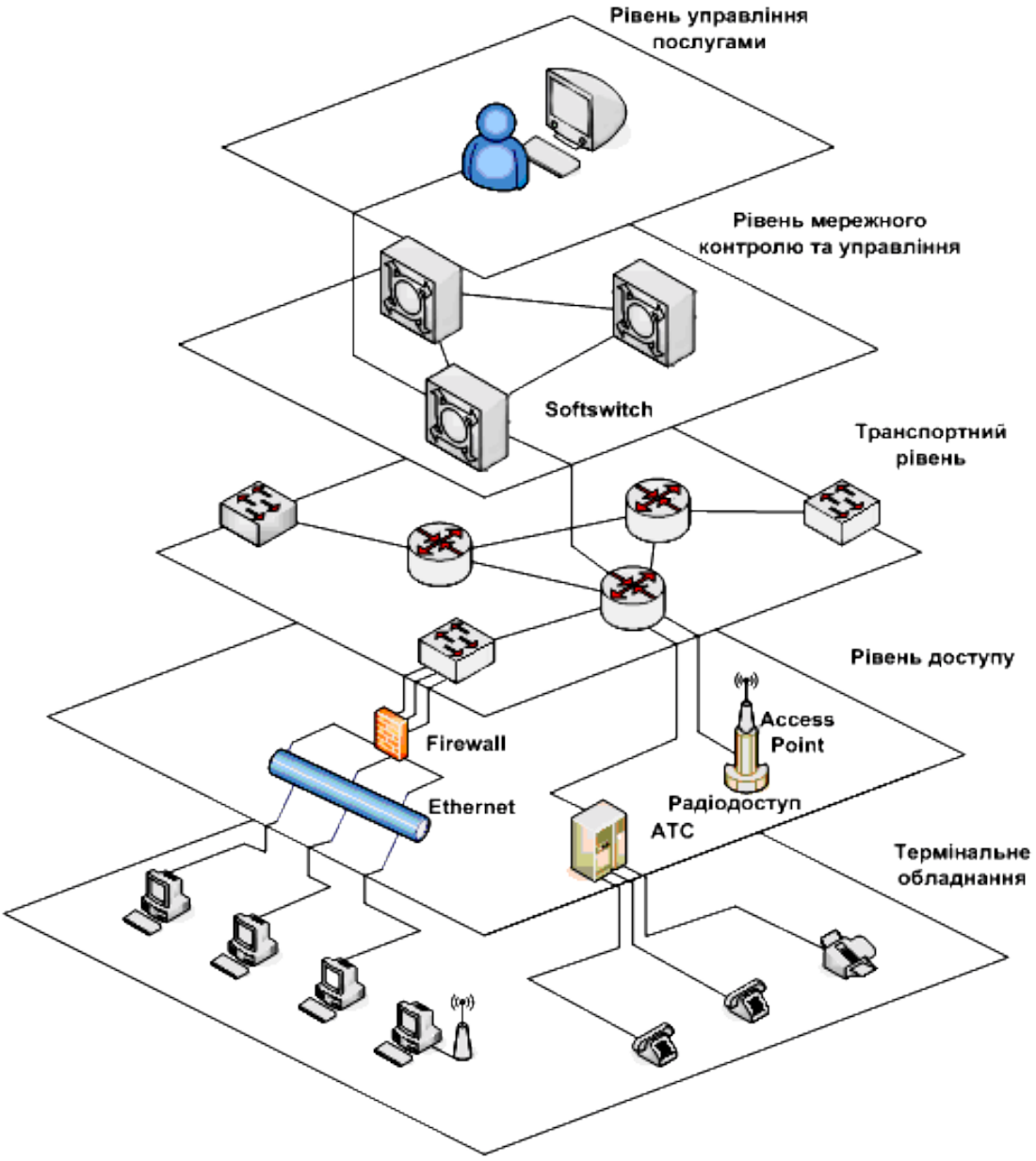


Рис.1.2. Чотирьохрівнева архітектура мережі наступного покоління

Рівень послуг і транспортний рівень в свою надалі розділились на такі рівні:

- рівень управління послугами (четвертий рівень);
- рівень мережного контролю й управління (третій рівень);
- транспортний рівень (другий рівень);
- рівень доступу (перший рівень);
- термінальне обладнання (нульовий рівень).

Рівень управління послугами має завдання управління логікою послуг і аплікацій і являє собою розподілене обчислювальне середовище, яке забезпечує:

- надання (підтримку) інфокомунікаційних послуг;
- управління послугами;
- створення та впровадження нових послуг;
- взаємодію різних послуг [5].

Сучасний стан розвитку телекомунікаційних мереж, вимагає передавання всіх типів даних від мережі, а не тільки традиційних.

QoS стає дуже важливим, коли мережа передає різноманітні види трафіка, як приклад голосовий і відео трафік. Причиною є те, що різні типи трафіку, потребують різні вимоги до QoS.

Розглядаючи поняття трафіку, можемо зазначити, що це обсяг інформації, що проходить через мережу за певний проміжок часу. Основна одиниця виміру - біт, але найчастіше для підрахунків використовується байт і похідні: мегабайт (МБ), гігабайт (ГБ) та терабайт (ТБ) [6].

Трафік забезпечує відвідуваність ресурсу і визначається кількістю користувачів на сайті за проміжок часу. Чим більше відвідуваність, тим краще, тому варто звертати увагу на всі типи трафіку і розвивати всі можливі канали.

Можемо зазначити таку класифікацію трафіку:

- *пошуковий трафік, він же органічний або природний*. Найбажаніший і найкращий спосіб отримання нових користувачів. Обумовлено це високою кількістю цільових відвідувачів, які перейшли на сайт невипадково. Такий трафік відмінно позначається на поведінкових факторах і приносить стабільний прибуток від реклами.

- *реферальний або контрольний трафік*. Приходить при переході по посиланнях, розміщеним на зовнішніх сайтах-донорах. Якість трафіку безпосередньо залежить від джерела, його контенту і семантики. Якщо власник ресурсу відповідально і грамотно підійшов до вибору донора, а також проконтролював розміщення посилання її анкор і контекст, то нові відвідувачі не тільки піднімуть показники, але і будуть корисні.
- *прямий трафік*. Це користувачі, які «прийшли» через введення адреси в рядку браузера. Такий рафік виходить за допомогою «сарафанного радіо». Також до цього типу трафіку відносяться користувачі, які переходять на сайт з закладок, розсилок або історії. Збільшення такого трафіку означає підвищення впізнаваності бренду.
- *соціальний трафік*. Відвідувачі з соціальних мереж. Це короткочасний потік відвідувачів, який спостерігається в період знаходження публікації в зоні видимості користувачів. Відноситься до різновиду реферального трафіку. Якість отриманого трафіку безпосередньо залежить від характеру контенту.
- *платний трафік*. Надходить на сайт в період дії рекламної компанії, закінчується разом з нею. Велика кількіть платного трафіку не завжди гарантує користь власнику. Окрім кількості, є ще такі характеристики, як окупність та рентабельність. Проте привертає на сайт тільки цільових користувачів (При правильному налаштуванні) [7].

Зазначимо, що організації мають здатність оцінювати якість обслуговування трафіку, використовуючи різні критерії, що вимірюються кількісно та відносяться до різних типів:

- *пропускна здатність*. Здатність мережі передавати максимальний обсяг даних з однієї точки до іншої за заданий проміжок часу;



Рис.1.3. Пропускна здатність

- *джитер*. Джитер - це будь-які відхилення в переданих сигналах, які можуть з'явитися в результаті зміни умов передачі, наприклад, параметрів лінії або швидкості поширення. Якщо значення джитеру занадто велике, це негативно впливає на якість відеозв'язку або голосових повідомлень;

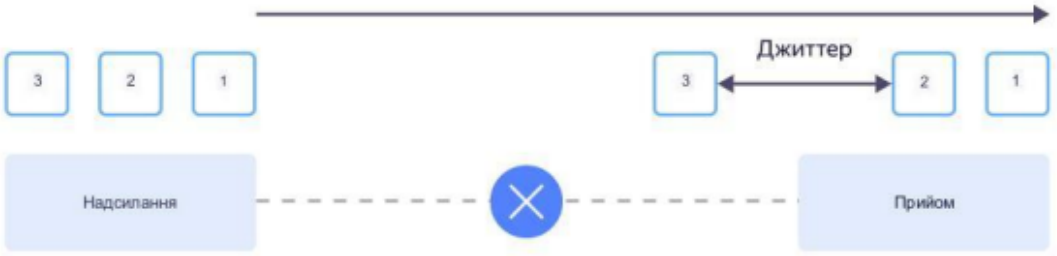


Рис.1.4. Джитер

- *затримка*. Час, потрібний для передачі пакету даних від джерела до призначення, є важливою характеристикою;

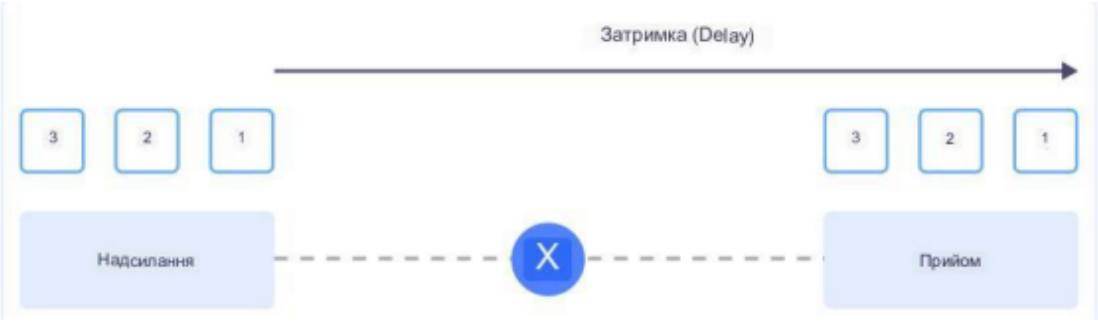


Рис.1.5. Затримка

- *втрата пакетів даних*. Це відбувається, коли мережеві канали перевантажені, а маршрутизатори та комутатори починають скидати пакети даних. Пакети також можуть зникати при переповненні черги, що очікують відправки даних [8].

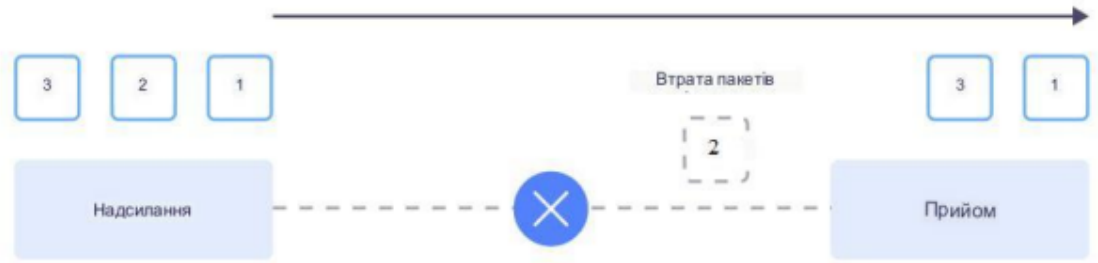


Рис.1.6. Втрата пакетів даних

Загалом, мультисервісне середовище- це це мережа, що одночасно підтримує передавання різних типів інформації: мультимедійних, інтерактивних та традиційних даних. Основна мета такої мережі – забезпечити сталу якість обслуговування (QoS) для кожного виду трафіку з урахуванням його специфічних вимог.

Мультимедійні потоки мають такі характеристики:

- **передача в реальному часі.** Дані повинні надходити без значних затримок (до 150–300 мс) і з мінімальними коливаннями часу доставки (джитером);

- **синхронізація потоків.** Для комфортного сприйняття та відео потрібна узгодженість у часі;
- **пріоритетність трафіку.** Мультимедійні дані отримують вищий пріоритет у мережі, щоб уникнути затримок;
- **спеціальні протоколи передачі.** Використовуються RTP, RTCP, RTSP, SIP – вони забезпечують керування сесіями та контроль якості;
- **компресія даних.** Застосовуються кодеки (H.264, Opus, AAC), які зменшують навантаження на мережу.

Особливостями передачі інтерактивних даних є:

- *двосторонній характер обміну.* Дані постійно надходять в обох напрямках (користувач-сервер або peer-to-peer);
- *високі вимоги до затримок.* Навіть невелика затримка (понад 100 мс) може негативно вплинути на взаємодію;
- *адаптивна передача.* Алгоритми автоматично змінюють якість потоку залежно від стану мережі (adaptive bitrate);
- *підтримка QoE (Quality of Experience).* Оцінюється не лише технічна якість, а й зручність сприйняття користувачем.

1.2. Надійність і відмовостійкість телекомунікаційних систем

Відмовостійкість- це властивість системи (часто комп'ютерної), що дозволяє їй продовжувати правильно діяти у випадку помилки або декількох помилок в деяких її частинах. Якщо при цьому падає якість експлуатації, то це відбувається пропорціонально до серйозності помилки, на відміну від наївно спроектованих систем, в яких навіть маленька помилка спричиняє загальну відмову. Відмовостійкість особливо популярна у високо доступних та життєво критичних системах [9].

Вимоги до відмовостійкості включають такі пункти:

- мати більш ніж одну точку відновлення (наприклад, перехоплення керування при відмові може бути виконано одним з двох серверів);
- локалізація пошкоджень у пошкодженому компоненті;
- обмеження розповсюдження несправності;
- доступність режимів реверсії.

Забезпечення надійності комп'ютерних систем здійснюється в двох напрямах. В першому випадку забезпечення надійності комп'ютерних систем визначається відсутністю відмов, збоїв, помилок та несправностей. В другому – можливістю швидкого відновлення апаратури та обчислювального процесу.

Надійність можна визначити як властивість об'єкта зберігати в часі у визначених межах значення всіх параметрів, які характеризують спроможність виконувати потрібні функції в заданих режимах і умовах застосування, технічного обслуговування, ремонтів, зберігання та транспортування. Надійність сама по собі - складна властивість, яка в залежності від призначення об'єкта та умов його експлуатації складається із сполучень властивостей: безвідмовності, довговічності, ремонтопридатності та збережності.

Безвідмовність – це властивість об'єкта безперервно зберігати працездатний стан в проміжку деякого часу часу або деякого напрацювання.

Напрацювання - це об'єм (час) роботи об'єкта. Може визначатися в іншій формі, наприклад, кількості вирішених задач або циклів роботи.

Відмова - подія, що являє собою порушення працездатності об'єкта. Вона в основному викликається фізичним руйнуванням елементів або поступовим погіршенням їх характеристик.

Збій - короткочасне порушення правильної роботи обчислювального пристрою або його елемента, після якого його працездатність самовідновлюється або відновлюється оператором без проведення ремонту. Збої можуть бути викликані внутрішніми або зовнішніми перешкодами.

Відновлення комп'ютерних систем – це приведення апаратури в

працездатний стан шляхом заміни окремих елементів, що відмовили. Основні якості обчислювальної техніки, пов’язані з її надійністю, описуються з розподіленням відмов у часі, процесами відновлення та організацією обслуговування [10].

Відмови можна класифікувати:

1. Апаратні;
2. Програмні;
3. Мережеві;
4. Логічні;

Апаратні відмови -це порушення працездатності або несправність технічного пристрою, що є частиною апаратної складової інформаційної системи.

Програмна відмова (або креш) – це серйозна помилка у програмному забезпеченні, що призводить до аварійного завершення роботи програми або операційної системи .

Часто помилка такого роду призводить до виходу з ураженої програми. Програма може не відповідати,доки служба звітності аварії не повідомить подробиці відмови. У разі, якщо програма є критичною частиною операційної системи, вся система може аварійно завершити роботу або зависнути, що часто призводить до поломки ядра або фатальної системної помилки [11].

Мережева відмова – це порушення або повне припинення працездатності елементів телекомунікаційної мережі, яке призводить до зниження якості обслуговування або втрати доступів до мережевих ресурсів. У мультисервісних середовищах, де одночасно передаються мультимедійні, інтерактивні та інформаційні потоки, навіть короткочасна відмова може викликати значні збої у роботі сервісів реального часу.

Основними причинами мережевих відмов у сьогоденні можемо виділяти такі фактори, як: апаратні збої, програмні помилки, перевантаження мережі, збої електроживлення, людський фактор та кібератаки.

Наслідком мережевих відмов може стати порушення цілісності переданих даних (втрата або пошкодження пакетів), зниження доступності мережевих

сервісів, погіршення якості мультимедійних потоків, втрата інтерактивності.

Логічна відмова - це порушення працездатності системи, яка виникає не через фізичне пошкодження обладнання, а внаслідок помилок у програмному забезпеченні, конфігурації або обробці даних. Такі відмови пов’язані з неправильними алгоритмами функціонування мережевих елементів чи сервісів, що призводить до збою в логіці їх взаємодії.

Сутність логічних відмов полягає в тому, що система технічно справна, але виконує неправильні або некоректні дії, наприклад: може передавати пакети у невірному порядку, створювати дублікати потоків, втрачати синхронізацію між аудіо та відео, неправильно визначати пріоритети трафіку.

Відмови за причинами виникнення можна поділити на:

а) *конструкційні* – зумовлені помилками при проектуванні, порушенням вимог державних стандартів, заниженням запасу міцності та ін.;

б) *виробничі* – спричинені порушенням технології виготовлення, невиконанням вимог технічної документації, застосуванням неякісних матеріалів і т. п.;

в) *експлуатаційні* – є наслідком порушень умов роботи машини, різних ушкоджень, невиконанням правил експлуатації, низької кваліфікації обслуговуючого персоналу, старінням машини та ін.



Рис.1.7. Класифікація відмов

Залежно від складності наслідків відмовам можна запобігати при технічному обслуговуванні, при середньому або капітальному ремонті.

Стійкість до відмов дозволяє забезпечувати працездатність системи і доступність її ресурсів у разі виходу з ладу окремих компонентів. Вимоги ранжирують залежно від кількості несправностей, за наявності яких зберігається працездатність системи, і від множини ресурсів, доступних в умовах виходу з ладу компонентів системи [12].

Системи моніторингу та управління мережею відіграють важливу роль у забезпеченні відмовостійкості.

Системи управління мережею (NMS) – це інструменти, за допомогою яких, організації можуть моніторити, управляти, аналізувати та оптимізувати мережеву інфраструктуру.

Системи NMS забезпечують можливість відстеження стану кожного пристрою у мережі в реальному часі. Це включає збір даних про:

- продуктивність;
- затримки;

- пропускну здатність;
- помилки та втрати пакетів.

Однією з ключових функцій NMS є можливість швидкого визначення проблем у мережі. Завдяки цим системам:

1. Адміністратори можуть отримувати повідомлення про несправності через SMS, email фбо інші канали;
2. Ведуть логування інцидентів, що дозволяє аналізувати причини та повторність проблем;
3. Деякі сучасні NMS використовують алгоритми машинного навчання для передбачення можливих несправностей. В результаті, це допомагає вирішувати проблеми ще до того, як вони вплинуть на роботі кінцевих користувачів.

OSS/BSS (Operation Support System/Business Support System – система підтримки операцій/система підтримки бізнесу, іноді BOSS, BSS/OSS, B/OSS) в електрозв'язку - загальна назва для категорії прикладного програмного забезпечення внутрішніх бізнес-процесів операторів зв'язку.

Підкатегорія OSS відноситься до програмного забезпечення, що взаємодіє з телекомунікаційним середовищем: мережами електрозв'язку, комутаційним обладнанням, АТС, апаратними комплексами забезпечення зв'язку і призначеним для підтримки експлуатації телекомунікаційних систем підприємства зв'язку (тому даний клас програмного забезпечення фігурує також як системи експлуатаційної підтримки). Основні функціональні можливості OSS охоплюють проблематику обліку та планування телекомунікаційних ресурсів (наприклад, номерних ємностей, трафіку), управління наданням послуг, управління показниками та рівнем якості послуг. До функціональних завдань OSS також відносяться контроль шахрайства на рівні телекомунікаційних даних, прогнозування та забезпечення попиту на послуги . Програмні рішення, що відповідають за безпосереднє сполучення програмної інфраструктури оператора з телекомунікаційною, називаються системами медіації і також включаються в категорію OSS.

До підкатегорії BSS входить прикладне програмне забезпечення для

підтримки бізнес-процесів підприємства електрозв'язку, насамперед – так чи інакше пов'язане з взаємодією з абонентами – білінг (підтримка взаєморозрахунків з абонентами, виставлення рахунків, обробка платежів, тарифікація), CRM (управління інформацією про абонентів, підтримка взаємодії з ними, продажі, маркетинговий аналіз) [13].

1.3. Методи забезпечення якості обслуговування користувачів та управління відмовами

Продуктивність мережі – це показники якості обслуговування мережі з точки зору клієнта.

Існує багато різних способів вимірювання продуктивності мережі, оскільки кожна мережа має свою специфіку та структуру. Продуктивність також можна моделювати та імітувати замість вимірювання; одним із прикладів є використання діаграм переходів між станами для моделювання продуктивності черг або використання мережевого симулятора [14].

Безпровідні мережі оцінюються критеріями KPI (key performance indicator – ключові параметри якості), які визначають ступінь задоволеності клієнтів та продуктивність оператора.

Одним із важливих параметрів є якість сприйняття послуг (QoE), який використовують для опису сприйняття наданих послуг кінцевим користувачам. QoS (якість обслуговування) описує здатність мережі надавати послуги з гарантованою якістю обслуговування.

При тому, що стандартна черга заповнюється повністю, будь-які нові пакети відкидаються без розбору, незалежно від класифікації або маркування пакета. QoS надає комутаторам і маршрутизаторам механізм постановки в чергу та обслуговування трафіку з вищим пріоритетом перед трафік із нижчим пріоритетом.

Якість досвіду (QoE або QoX) – це міра загального рівня задоволеності клієнта та його досвід роботи з продуктом або послугою та постачальником, який надає це продукт або послугу. QoE пов’язано з якістю обслуговування (QoS), хоча

ці дві концепції не збігаються.

Система підтримує три типи QoS: QoS програми, IP QoS і role QoS.

- QoS програми: контролює пропускну здатність, яку використовують програми.
- IP QoS: контролює пропускну здатність призначених IP-адрес.
- Рольовий QoS: також називається Role-based QoS. Він контролює пропускну здатність призначених ролей.

Якість обслуговування (QoS) і якість досвіду (QoE) є такими дві пов'язані, але різні концепції, які вимірюють продуктивність і задоволення від мережевої служби. Вони часто використовуються для оцінки та покращення доставки мультимедійних програм, таких як голос, відео та ігри, через Інтернет [15].

На рис. 1.8 наведено модель відображення параметрів QoS та QoE.



Рис.1.8. Модель відображення параметрів QoS та QoE

Відмови у мережі значно впливають на якість обслуговування (QoS) та якість користувацького досвіду (QoE), але їхній вплив проявляється на різних рівнях.

Коли трапляється відмова, наприклад, через збій обладнання, пошкодження каналу зв'язку або перевантаження мережі, зростає затримка передавання пакетів, з'являються коливання затримок (джитер), збільшується кількість втрачених пакетів, зменшується пропускна здатність і знижується доступність сервісу. Через це мережа стає менш стабільною і не може надати гарантію потрібного рівня технічних параметрів. Таким чином, відмови безпосередньо погіршують якість обслуговування.

В цей час **QoE** відображає сприйняття користувачем цієї якості. Це вже не ттехнічна, а емоційна й поведінкова оцінка. Коли через відмову відео починає буферизуватися, дзвінок у месенджері переривається або вебсайт довго не завантажується, користувач відчуває роздратування, втрату комфорту або довіру до сервісу. Навіть якщо проблема технічно короткочасна, вона може істотно зменшити рівень задоволення користувача, так як сприйняття якості часто формується на очікуваннях і попередньому досвіді.

Підсумовуючи, можемо говорити про те, що відмови негативно впливають на показники QoS та QoE.

Однією з головних задач забезпечення надійності та відмовостійкості є мінімізація простоїв та гарантування безперервності бізнес-процесів. Це особливо актуально для критично важливих систем, як-от банківські сервіси, системи управління виробництвом, медичні установи або служби швидкої допомоги. Зазначимо, що надійність мережі сприяє підтримці високому рівня безпеки, так як незаплановані відключення можуть створити вразливості для атак або втрати даних. Сьогодення показує, що більша залежність від цифрових технологій, забезпечення безперебійної роботи інфраструктури набуває стратегічного значення для успішного функціонування підприємств та організацій.

Прикладами реалізації забезпечення надійності та відмовостійкості в мережах можуть виступати як апаратні, так і програмні підходи. Серед апаратних рішень можемо виділити систему дублювання компонентів, що будуть

автоматично переключатися у випадку відмови основного елементу. Такі рішення дозволяють зменшити залежність від одного вузла та зберегти цілісність роботи мережі навіть при виникненні апаратних збоїв. Також широко застосовуються програмні технології, такі як кластеризація серверів, реплікація баз даних, віртуалізація ресурсів та балансування навантаження, що дозволяють адаптуватися до змін у навантаженні та швидко відновлювати роботу після збоїв [16].

Також можемо виділити такий підхід, як маршрутизація з відновленням. Основною суттю даного методу є те, що коли основний маршрут між двома вузлами мережі стає недоступним (через відмову лінії або вузла), маршрутизатори автоматично перенаправляють трафік через альтернативні маршрути. Саме такий план дій надає змогу відновити підключення без людського втручання. Перевагою є те, що відбувається швидке автоматичне відновлення маршруту без потреби ручного втручання. Але є і недолік- часом альтернативні маршрути можуть бути довшими або менш оптимальними, що може призвести до збільшення затримок чи перевантаження інших сегментів мережі.

Розглянемо також і баланс навантаження, суттю якого є розподіл мережевого трафіку чи запитів між кількома ресурсами (лінії зв’язку, сервера, маршрутизатори), так щоб уникнути перевантаження одного компонента та забезпечити резервність в роботі. Перевагою даного методу визначається підвищення продуктивності мережі та її стійкості, наприклад, якщо один ресурс виходить з ладу або перевантажений, то інші беруть на себе трафік. Але є і обмеження, а саме: складність алгоритмів управління, необхідність моніторингу, ризик неефективного розподілу при неправильному налаштуванні.

Програмно конфігуровані мережі (SDN - Software-Defined Networking) представляють собою революційний підхід до проектування, управління та експлуатації мереж. SDN дозволяє централізовано управляти мережею за допомогою програмного забезпечення, що розділяє контрольний рівень і рівень даних, які значно підвищують гнучкість, ефективність та продуктивність мережі.

Мета SDN полягає у створенні більш гнучкої та адаптивної мережевої архітектури, яка дозволяє швидко реагувати на змінні потреби користувачів та

бізнесу. За допомогою централізованого контролера, що керує всіма мережевими пристроями, адміністратори можуть динамічно налаштовувати маршрутизацію, балансувати навантаження та застосовувати політику безпеки в реальному часі [17].

Network Functions Virtualization (NFV) – це інноваційна технологія, що революціонізує традиційний підхід до мережевих послуг. Вона передбачає віртуалізацію мережевих функцій, таких як брандмауери, балансувальники навантаження та системи виявлення вторгнень, шляхом відокремлення їх від спеціалізованого обладнання. Це дозволяє розгортати мережеві функції у вигляді програмного забезпечення на стандартних серверах або хмарній інфраструктурі, що забезпечує більшу гнучкість, масштабованість та економічну ефективність [18].

Вивчаючи матеріали з відкритих джерел, можемо зазначати, що NFV працює шляхом відокремлення мережевих функцій від обладнання, на яке вони традиційно покладаються. Замість використання спеціалізованих фізичних пристроїв, NFV віртуалізує ці функції та запускає їх у вигляді програмних екземплярів на стандартних серверах або хмарній інфраструктурі [18]. Саме процес віртуалізації дозволяє динамічно розгортати, налаштовувати, масштабувати та керувати мережевими функціями без необхідності фізичних змін в інфраструктурі. Перевагами NFV можемо виділити те, що забезпечує такі показники як: економічна ефективність (зменшує потребу в спеціалізованому обладнанні, що призводить до економії коштів та ефективного використання ресурсів), масштабованість (передбачає легке масштабування мережеві функції), гнучкість (дозволить організаціям розгорнути і управляти мережевими функціями більш гнучким способом).

Тож, проведемо короткий аналіз стандартів та технологій, що регламентують управління якістю QoS та надійсністю телекомунікаційних мерж :

Таблиця 1.1

Ключові організації та їхні стандарти для забезпечення QoS і надійності

Організація / Стандарти	Основна роль	Значення
ITU-T (Міжнародний союз електрозв'язку, сектор телекомунікацій)	Формує рекомендації щодо якості обслуговування у мережах зв'язку	Визначає єдині показники та методики для вимірювання якості, дозволяє провайдерам гарантувати певний рівень сервісу
IETF (Internet Engineering Task Force)	Технологічна реалізація QoS	Створює практичні протоколи для управління трафіком та забезпечення QoS
ISO / IEC та ETSI	Стандарти надійності систем зв'язку	Задають управлінські та безпекові рамки, доповнюють технічні протоколи ITU та IETF

Висновок до розділу 1

Підводячи підсумок, можемо говорити про те, що мультисервісні мережі нового покоління (NGN) забезпечують інтегровану передачу голосових, даних та мультимедійних послуг на базі єдиної IP-інфраструктури, що гарантує універсальність, масштабність, гнучкість та використання стандартизованих протоколів. Основною особливістю виступає відокремлення функцій транспорту, керування викликами та послугами, що дозволяє підвищити ефективність роботи мережі та реалізувати якість обслуговування (QoS) для різних типів трафіку, включаючи мультимедійні та інтерактивні дані.

Надійність і відмовостійкість телекомунікаційних систем являються критично важливими для забезпечення безперервності роботи мережевих сервісів, особливо в час технічних прогресів. Вони досягаються шляхом дублювання компонентів, маршрутизації з відновленням, балансування навантаження, а також застосуванням сучасних програмних рішень – SDN та NFV.

Стандарти та організації, такі як ITU-T, IETF, ISO/IEC та ETSI, формують єдині методики вимірювання якості обслуговування та надійності мереж, задаючи рамки для технічних рішень та управлінських процесів. Усі ці елементи разом забезпечують ефективну, надійну та адаптивну роботу мультисервісних мереж, здатних підтримувати сучасні вимоги до передачі даних, мультимедіа та інтерактивних послуг.

Таким чином, впровадження мультисервісних технологій та сучасних підходів до управління мережею забезпечує високий рівень QoS і QoE, стійкість до відмов, масштабованість та гнучкість телекомунікаційної інфраструктури.

АНАЛІЗ ТА ВИБІР ПОКАЗНИКІВ ДЛЯ ОЦІНЮВАННЯ СТАНУ ТА НАДІЙНОСТІ МЕРЕЖІ

2.1. Показники продуктивності та якості функціонування мультисервісних мереж

Бурхливий розвиток телекомунікаційних систем та зростаюча потреба операторів зв'язку в підвищені продуктивності систем обробки інформації на базі сучасних інформаційних технологій вимагає створення розподілених інфраструктур мультисервісних мереж зв'язку з підвищеною ефективністю, що передбачають передачу мережевих додатків.

Ефективність функціонування мультисервісних мереж визначається сукупністю технічних показників, що характеризують якість передавання інформації, стабільність роботи мережевих елементів та здатність забезпечувати необхідний рівень обслуговування користувачів. Ці показники дають змогу здійснювати об'єктивну оцінку стану мережі, своєчасно виявляти аномалії в роботі та прогнозувати можливі відмови.

Вивчаючи інформацію відкритих джерел, можемо говорити про те, що у системі зв'язку мережеві додатки мультисервісних мереж телекомунікації можна поділити на три основні групи: передача даних, пакетна телефонія та потокове відео.

Зазначимо, основними параметрами, які можуть вплинути на якість обслуговування в мультисервісному середовищі, є затримка передачі даних, варіація затримки, втрати пакетів, пропускна здатність та рівень навантаження мережі. Кожен із цих параметрів має власну природу виникнення та по-різному впливає на якість різних типів трафіку.

Затримка -це час, необхідний для передачі даних від вашого пристрою до місця призначення і назад. Це може призвести до того, що ваш Інтернет буде повільним, особливо під час дій, які потребують швидкої відповіді, як-от ігри та відеодзвінки. Коли затримка висока, ви можете помітили лаги або «гальмування»

між тим, що ви робите, і тим, що відбувається на екрані [19].

Високі затримки особливо критичні для трафіку реального часу, такого як голосовий зв'язок (VoIP) або відеоконференції, де навіть затримка понад 150-200 мс може спричинити погіршення якості сприйняття користувачем.

VoIP (voice over IP – голос через IP) -технологія передачі медіа-даних у реальному часі [20].

Використовуючи послугу VoIP, ви можете дзвонити на стаціонарні, мобільні телефони або з комп'ютера на комп'ютер. Це означає, що вам не потрібен традиційний телефон, оскільки дзвінки можна здійснювати через інтернет.

Способи використання VoIP:

1. ATA = Analog Telephone Adapter = Аналоговий Телефонний Адаптер

ATA – це пристрій, який дозволяє підключити телефон до комп'ютера або до інтернету. Він приймає аналоговий сигнал з вашого телефону, перетворює його в цифрові дані і відправляє через інтернет. Також ці пристрої називають VoIP шлюз.

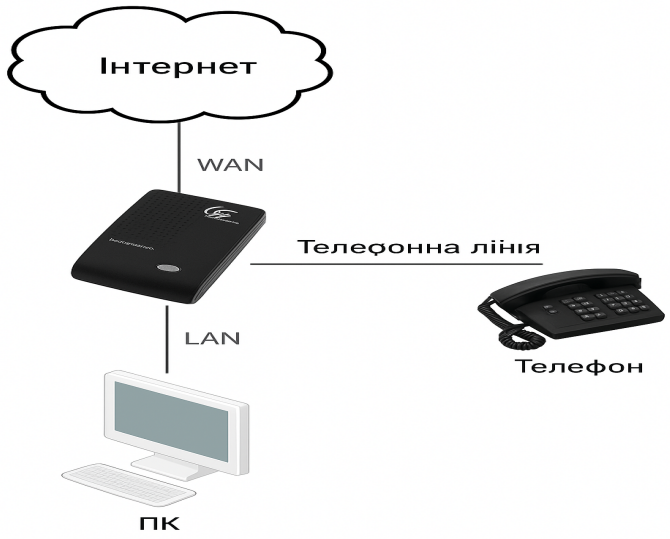


Рис.2.1. схема ATA

2. IP-телефони

Це спеціалізовані телефони, які виглядають так само, як звичайні телефони, але створені спеціально для VoIP.

3. Комп'ютер-комп'ютер

Це найпростіший спосіб використання VoIP, оскільки будь-який комп'ютер або інтелектуальний мобільний пристрій підтримує IP-виклики. Все, що потрібно зробити, - це переконатися, що всі сторони, що беруть участь, мають підключення до інтернету, відповідне програмне забезпечення VoIP, а також набір вбудованих або автономних мікрофонів і динаміків [21].

Джиттер може бути дуже руйнівним. Перервані дзвінки, перервані голоси та збої у відеоконференціях засмучують і можуть виставити вас у непрофесійному світлі.

Джиттер – це відхилення або затримка в доставці пакетів даних по мережі, тобто затримка між моментом передачі і прийому сигналу. Затримка/відхилення/зміна в часі являє собою порушення звичайної послідовності відправки пакетів даних і вимірюється в мілісекундах.

Джиттер впливає на онлайн-дії, які покладаються на двосторонній зв'язок, наприклад, на камери IP-безпеки та конференц-зв'язок. Коли ви відчуваєте тремтіння, у вашому з'єднанні виникають нестабільні затримки між пакетами даних. Кінцевими ефектами високого джиттера є:

- затримка дзвінка;
- статичний шум;
- ехо дзвінка;
- Аудіо- та відеоспотворення.

Більш негативний вплив відчувається, коли пакетам даних потрібно більше часу, щоб досягти місця призначення. Відповідні коливання викликають втрату пакетів голосу/даних [22].

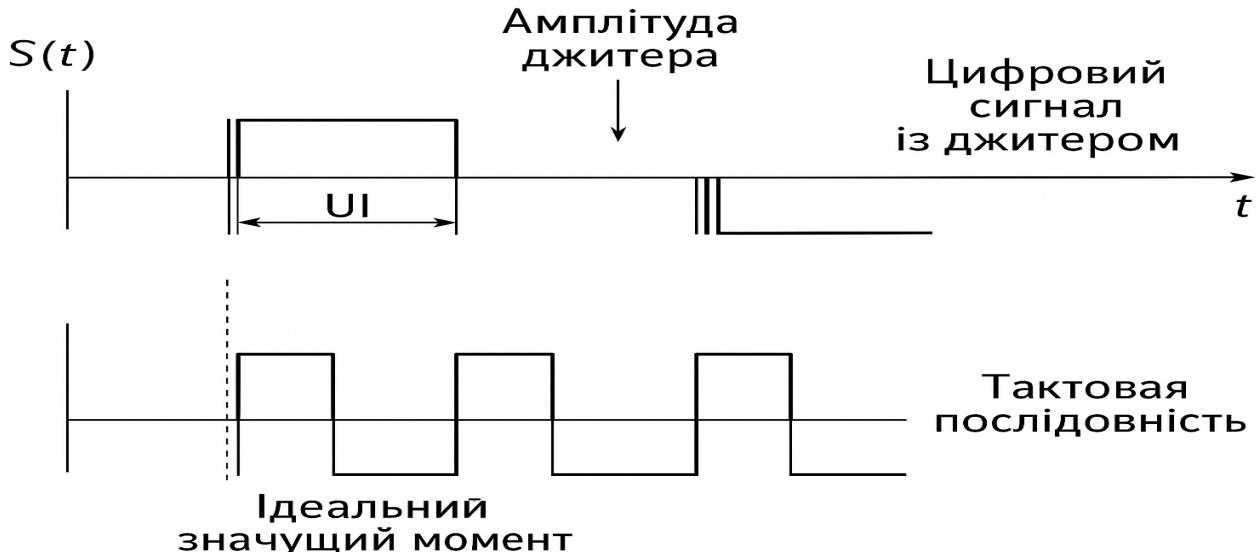


Рис.2.2. Тимчасові діаграми цифрового сигналу

Пропускна здатність – це показник кількості одиниць інформації, яку система може обробляти за певний проміжок часу. Цей термін широко застосовується до різного роду систем, починаючи від різних аспектів комп'ютерних та мережевих систем до організацій [23].

Пропускна здатність визначає потенційну продуктивність мережі та є одним із ключовх параметрів при оцінюванні її ефективності. Мала пропускна здатність може призвести до затримок, втрат пакетів і деградації сервісу.

Забезпечення стабільної пропускної здатності можна досягти шляхом оптимізації маршрутизації, балансування навантаження та використання адаптивних алгоритмів керування трафіком.

Ерланг (позначення Ерл) – безрозмірна одиниця інтенсивності навантаження (часто телефонного) або одиниця навантаження, використовувана для вираження величини навантаження, необхідної для підтримки зайнятості одного пристрою протягом певного періоду часу.

1 ерланг (1 Ерл) – відповідає безперервному користуванню одного голосового каналу протягом 1 години. Припустимо, якщо абонент проговорив з іншим абонентом протягом однієї години, то на телекомунікаційному обладнанні було створене навантаження в один Ерланг.

Ерланг використовується операторами зв'язку для обліку пропускної здатності при транзиті трафіку, так як телефонне навантаження - випадкова величина, яка визначається кількістю вхідних дзвінків за одиницю часу і часом обслуговування абонента. Інтенсивність навантаження є твором математичного очікування числа викликів за одиницю часу на середній час обслуговування виклику; така інтенсивність і вимірюється в Ерлангах [24].

2.2. Вимоги різних типів трафіку до параметрів мережі та показників якості обслуговування

У мультисервісних мережах одночасно передаються різні типи трафіку- від голосових та відеопотоків у реальному часі до звичайних транзакційних даних, наприклад, електронна пошта та файли тощо.

Основне завдання QoS – забезпечити гарантовану передачу певних пакетів даних непомітно для користувача. QoS можуть застосовувати скрізь: вдома, в офісі, бібліотеці, аеропорту тощо. За допомогою технології QoS можна гарантувати, що у користувачів не виникне проблем під час завантаження файлів, відеодзвінків, розмов по IP-телефонії, перегляду будь-яких онлайн-документів у локальній або глобальній мережі [25].

Особливого значення, а саме стратегічного, набуває питання забезпечення надійного, стійкого та захищеного звязку під час військового стану. Надійність таких мереж напряму впливає на координацію дій військових підрозділів, оперативність реагування органів влади, інформування населення та роботу критичної інфраструктури (енергетика, транспорт, медицина та комунікації).

Стабільність передачі інформації залежить від технічних характеристик каналів. Їх точне вимірювання дозволяє оптимізувати роботу систем керування трафіком [26].



Рис.2.3. Технічні характеристики QoS

В сучасних системах існує набір правил для виділення критичних потоків, основні методи, яких включають:

- FIFO (First In, Fist Out)-проста черга без пріоритетів
- Weighted Fair Queuing-динамічне розподілення ресурсів
- Class-Based Queuing-групування трафіку за категоріями

Для ефективного розподілу мережевих ресурсів існує низка чітких правил упорядкування даних. Для цього використовується механізм сортування трафіку та створення пріоритетних категорій. Такі механізми особливо важливі для корпоративних середовищ із високим навантаженням.

До прикладу, у банківських мережах часто застосовують такі правила розподілу пропускної здатності:

1. Резервування 30% каналу для транзакцій;
2. Обмеження швидкості для соціальних мереж;
3. Автоматичне перепризначення ресурсів у пікові години.

Дані налаштування в банківській системі можуть покращити швидкість

передачі критичних даних. Наприклад, відеоконферепнції в Cisco Webex отримують перевагу перед оновленням Windows.

Отож, правильна конфігурація політик зменшує затримки в 25-40%. Це особливо відчутно при роботі з хмарними сховищами або потоковими сервісами.

Вивчаючи матеріали відкритих джерел, робимо висновок, що біти передаються у вигляді електромагнітних сигналів. Швидкість поширення електромагнітних сигналів визначається середовищем, через яке вони проходять. Формула для розрахунку затримки поширення:

$$t = D/S,$$

де

D – відстань між відправником і одержувачем по каналу,

S – швидкість передачі [27].

По швидкості передачі даних трафік можна поділити на два типи:

1. потоковий- постійно продовжують роботу в своєму ритмі та постійною швидкістю;
2. пульсуючий- такий трафік є непередбачуваним, де періоди простою можуть змінюватися пульсацією трафіка, коли пакети слідують один за одним.

Зазначимо, що специфікаціях на послугу, які є частиною угоди про рівень обслуговування, зазначається взаємозв’язка між споживчими властивостями послуги та її показниками якості.

З відкритих джерел зазначимо більше інформації про VoIP. До прикладу, частина протоколів із сімейства VoIP затверджується Інтернет-співтовариством як RFC (request for comments), частина – міжнародними організаціями (IETF тощо) [20].

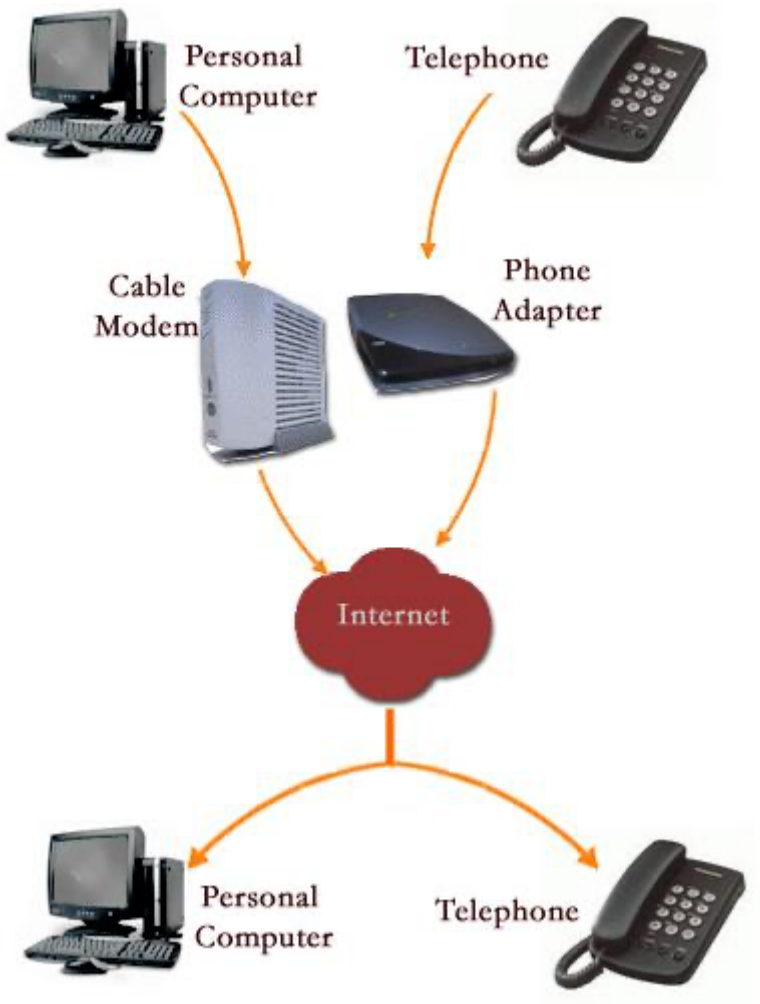


Рис.2.4. Загальна схема роботи інтернет-телефонії

Протоколи забезпечують реєстрацію IP-пристрою (шлюз, термінал або IP-телефон) на сервері або гейткіпері провайдера, виклик та/або переадресацію виклику, встановлення голосового з'єднання, передачу імені та/або номера абонента [20].

В історії зазначається, що можливість передачі голосових повідомлень через мережу з пакетною комутацією вперше була реалізована в 1993 році. Саме ця технологія отримала назву VoIP.



Рис.2.5. 1140E VoIP Phone

Основними перевагами даної технології можемо визначати- скорочення необхідної смуги пропускання каналу передачі, що забезпечуєтья обліком статистичних характеристик мовного трафіку:

- ❖ блокування передачі пауз, можуть складати до 40-50% часу зайнятості каналу;
- ❖ високою надмірністю мовного сигналу і його стисненням до 20-40% початковго сигналу.

Але, даний трафік критичний до затримок пакетів мережі, але стійкий щодо витрат окремих пакетів. Втрата до 5% пакетів не впливає на погіршення розбірливості мови.

TLS (Transport Layer Security) – це протокол шифрування, розроблений для захисту / шифрування SIP-повідомлень, що відправляються програмним телефоном або УАТС. Захищає зв'язок, що відбувається між додатком (частіше вашим браузером) та сервером [20].

IP-телефонія – це технологія, що дозволяє використовувати будь-яку IP-мережу як засіб організації та ведення телефонних розмов, передачі відеозображень та факсів у режимі реального часу [28].

2.3 Обгрунтування вибору показників для моніторингу та управління станом мережі

Один із важливих напрямків у науці й техніці - це розробка, виробництво й експлуатація складних об'єктів інформаційних систем з метою забезпечення необхідного рівня ефективності їх експлуатації [29].

Для початку, дамо визначення інформаційній системі. Це сукупність організаційних та технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів. Якщо говорити більш коротко та зрозуміло: комунікаційна система, яка забезпечує пошук, оброблення та пересилання інформації [30].

Вивчаючи інформацію, можемо говорити про те, що до числа основних причин, які стали наслідком недостатнього рівня експлуатаційної надійності інформаційних систем, виділені такі.

1. Мала увага зі сторони розробників техніки до складання і реалізації науково-обґрунтованих програм забезпечення надійності на всіх стадіях життєвого циклу інформаційних систем, наслідком цього являється недостатня ефективність даних програм; слабке методичне забезпечення планованих заходів і робіт, яке включає в себе сукупність нормативно-технічних і методичних документів щодо проведення аналізу й підвищення надійності систем.
2. Зменшення темпів росту надійності комплектуючих елементів від ступеня складності інформаційних систем і вимог до них за надійністю.
3. Недостатня увага, що приділяється питанням забезпечення високої ремонтопридатності інформаційних систем, а також розробці науковообґрунтованої системи ремонту, виходячи із її структури, складу, призначення, особливостей експлуатації та застосування.
4. Незавершеність наукової теорії експлуатації, обумовленої труднощами дослідно-теоретичного дослідження питань експлуатації, що являє собою 9 складну багатопараметричну, просторово-рознесену організаційно-технічну систему [29].

В теорії надійності можна визначити такі стани об’єктів: справний, несправний, працездатний, непрацездатний.

Справність визначається станом об’єкта, за яким він здатний виконувати всі задані функції.

Несправність - стан обєкта, коли він не здатний виконувати хоч одну із заданих функцій.

Працездатність визначається стан об’єкта, що характеризує його повну здатність виконувати потрібні функції.

Непрацездатність , стан, коли об’єкт не може виконувати бодай одну з потрібних функцій.

Таблиця 2.1

Класифікація відмов

Види відмов	**Класифікація**
Раптова/ Поступова відмова	Характер зміни параметра до моменту виникнення відмови
Незалежна/Залежна відмова	Зв'язок з відмовами інших елементів
Збій/Перемежована відмова	Характер вияву відмови
Конструкційна/Виробнича/Експлуатаційна відмова	Причина виникнення відмови
Повна/Часткова відмова	Ступінь впливу на працездатність об’єкта

Поняття *моніторинг* означає систему постійного спостереження за явищами і процесами, що проходять в навколишньому середовищі і суспільстві, результати якого служать для обгрунтування управлінських рішень по забезпеченню безпеки людей та об'єктів економіки.

Класифікація системи моніторингу являє собою спосіб упорядкування, встановлення зв'язків і відношень між властивостями і функціями СМ.

Розподіл СМ по класах здійснюється на основі найбільщ характерних ознак, які властиві СМ. Такими ознаками є:

– предметні області призначення СМ;

– масштабність;

– характер відношення об'єктів моніторингу до зовнішнього середовища;

– функціональна приналежність об'єктів, що спостерігаються;

– дисципліна дискретності спостереження.

В критеріях оцінки СМ *дискретність* займає важливе місце. Пояснити можна, що від неї залежить точність і складність побудови і забезпечення функціонування СМ. Даний критерій є основним показником для узгодження СМ з об'єктом спостереження, споживачами інформації СМ, пристроями перетворення інформації, що можуть входити до складу СМ або знаходиться за її межами.

Поняття *дискретності* можна тлумачити як, властивість, яка є протилежною до неперервності та означає роздільність, перервність.

SNMP (Simple Network Management Protocol – простий протокол керування мережею) – це протокол керування мережами зв’язку на основі архітектури TCP/IP [31].

SNMP – це технологія, яка покликана для забезпечення керування й контролю за пристроями й застосунками в мережі зв'язку шляхом обміну керівною інформацією між агентами, що розташовуються на мережних пристроях, і менеджерами, розташованими на станціях керування.

По суті SNMP агенти передають управлінську інформацію на керівні системи як змінні («вільна пам'ять», «ім'я системи», «кількість процесів, що працюють» тощо).

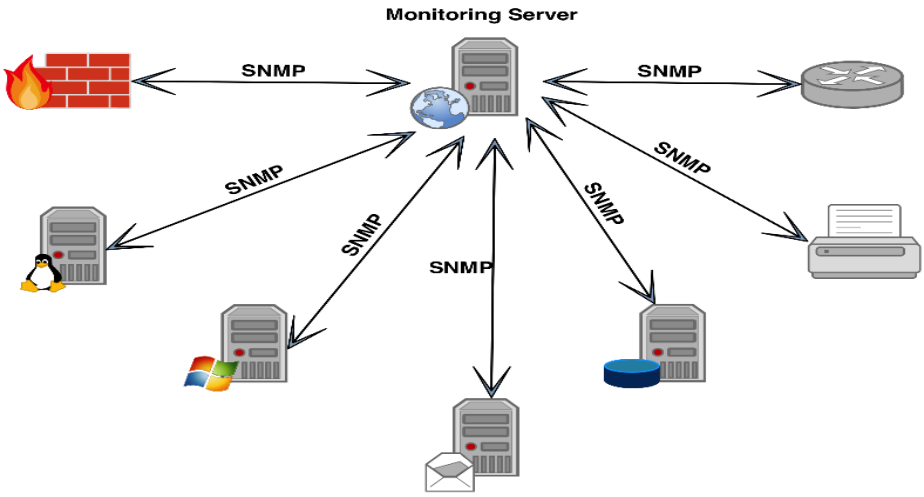


Рис. 2.6. Простий протокол керування мережею

Наступним протоколом будемо розглядати NetFlow.

Netflow – мережевий протокол, задачею якого є облік мережевого трафіку, розроблений компанією Cisco Systems. Є фактично промисловим стандартом і підтримується не тільки обладнаннями Cisco, а й багатьма іншими пристроями [32].

Для збору інформації про трафік за даним протоколом потрібні наступні компоненти:

- *Сенсор*. Збирає статистику щодо трафіку, що через нього проходить.
- *Колектор*. Збирає одержувані від сенсора дані та поміщає їх у сховище.
- *Аналізатор*. Аналізує зібрані колектором дані та формує придатні для читання людиною звітів (наприклад, у вигляді графіків).
- IP SLA (Internet Protocol Service Level Agreement) – це функція пристроїв Cisco, яка дозволяє адміністраторам мереж аналізувати, вимірювати та відстежувати продуктивність мереж або мережевих шляхів. Вона допомагає в моніторингу якості обслуговування (QoS) і гарантує, що продуктивність мережі відповідає угодам про рівень обслуговування [33].

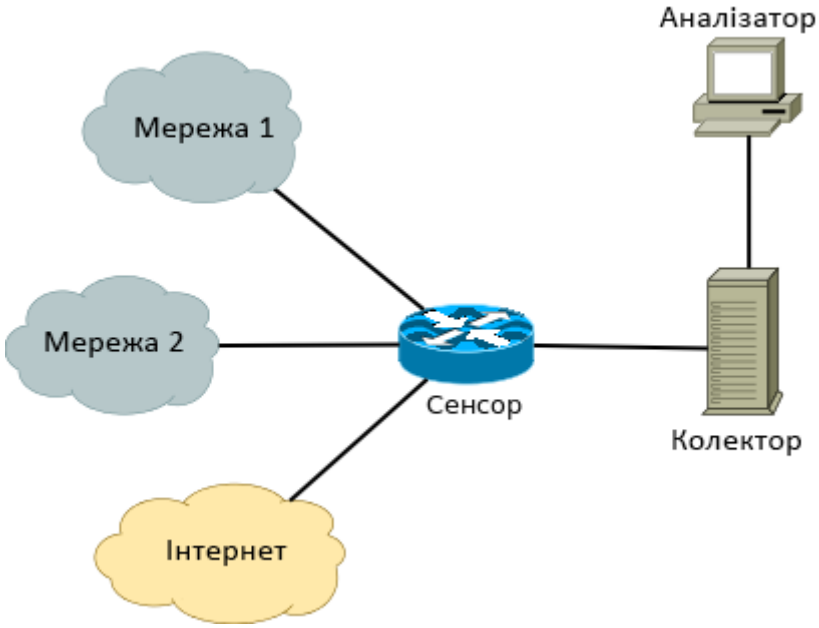


Рис.2.7. Архітектура NetFlow

IP SLA генерує та надсилає штучний графік через мережу, для симуляції даних реальних застосунків. Імітуючи шаблони трафіку та тестуючи певні мережеві шляхи/сервіси, IP SLA дає змогу адміністраторам визначати важливі вузькі місця, проблеми з затримкою або втратою пакетів, допомагаючи оптимізувати продуктивність мережі та виявляти проблеми.

Вивчаючи дані можемо виділяти такі переваги IP SLA:

1. Моніторинг та аналіз продуктивності. Дає можливість адміністраторам мереж контролювати продуктивність мережі в режимі реального часу, вимірюючи різні параметри;
2. Проактивне виявлення проблем. Адміністратори можуть встановлювати проактивні сповіщення, щоб отримувати повідомлення, коли продуктивність мережі падає нижче визначень порогових значень;
3. Аналіз історичних даних. Збирає та зберігає історичні дані стосовно продуктивності мереж, які адміністратори можуть аналізувати для виявлення шаблонів і тенденцій;
4. Дотримання угоди про рівень обслуговування. Допомагає контролювати та забезпечувати дотримання угод про рівень обслуговування.

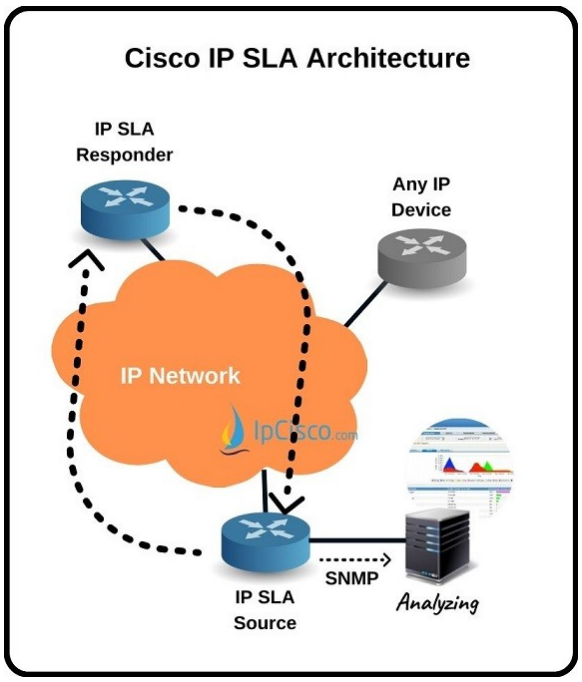


Рис.2.8. Архітектура Cisco IP SLA

Ефективність системи управління відмовами у мультисервісній мережі значною мірою залежить від правильного вибору показників, які використовуються для моніторингу, діагностики та оцінювання стану мережевої інфраструктури.

Для початку розглянемо характеристики відмов.

За типом відмови поділяються на: відмови функціонування та параметричні відмови.

Вивчаючи інформацію, можемо говорити про те, що за природою відмови поділяють на: *випадкові*(наприклад, непередбачені перевантаження) та *систематичні*(закономірні та неминучі явища).

Якщо розглядати, як приклад, розробку системи управління відмовами важливо визначати чіткі критерії, за якими здійснюється відбір самих інформативних та дієвих показників.

Першим таким критерієм може виступати *інформативність показника*. Даний показник має показувати фактичний стан мережі або зміни, які відбуваються при виникненні відмов. Наприклад, затримка, джиттер, втрата пакетів, пропускна здатність, рівень використання каналу, частота відмов, інтенсивність повторних

передач.

Чутливість трафіку до затримок пакетів. Можемо визначати основні види додатків стосовно чутливості по затримці пакетів даних, в порядку зменшення:

- трафік реального часу. Даний трафік включає в себе аудіо та відео інформацію, критичну до затримок при передачі. Допустимі значення затримок зазвичай не перевищують 0,1с.Також затримка повинна мати малі флуктуації (джиттер);
- трафік транзакцій. В момент, коли такий вид трафіку передається, його затримки не мають бути більшими за 1с, інакше робота користувачів буде перервана, через те що тільки після отримання відповід, вони можуть посилати дані. Час від часу, такі затримки, можуть призводити до збою роботи системи;
- трафік даних. В даному випадку, затримки можуть бути дуже великими, чисельне значення може рівнятись до кількох секунд. Для трафіку даних смуга пропускання більш важлива, ніж час затримок [34].

Далі можемо визначати *точність вимірювання*. Має бути можливість надійно виміряти показник в реальному часі.

Для виявлення потенційних відмов на ранніх етапах, показник має бути високочутливим до змін стану мережі.

Показник також має бути адаптивним до різних типів трафіку. Так як в мультисервісних мережах передається різнотипний трафік (реального часу, інтерактивний та трафік з передачею даних) під час воєнного стану даний критерій відіграє важливу роль в забезпеченні стабільності критичних комунікаційних каналів, навіть при деградації допоміжних сервісів.

А також, показники мають бути сумісними з наявними системами моніторингшу та легко інтегруватися у процеси автоматизованого керування.

Висновок до другого розділу

У ході дослідження було розглянуто основні параметри, що визначають

якість функціонування мультисервісних телекомунікаційних мереж, зокрема затримку передачі даних, джиттер, втрати пакетів, пропускну здатність та рівень навантаження.

Аналіз висвітлив, що ефективність роботи мережі безпосередньо залежить від своєчасного моніторингу її стану та використання систем управління відмовами. Для цього влучно використовувати так інструменти, як SNMP, NetFlow та IP SLA, які забезпечують збір, аналіз і контроль мережевих даних у реальному часі.

Для забезпечення надійності та стійкості мультисервісних мереж у сучасних умовах (зокрема під час воєнного стану) необхідно створювати адаптивні системи управління, здатні виявляти і локалізувати відмови на ранніх етапах, оптимізувати використання мережевих ресурсів і підтримувати безперервність критичних сервісів зв’язку.

3 ВИЯВЛЕННЯ ТА УПРАВЛІННЯ ВІДМОВАМИ У МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ

3.1. Класифікація відмов та їх характеристик у мультисервісному середовищі

Протягом останніх років не лише значно зросла залежність користувачів і сервісів від безперебійної роботи мережі, а й істотно ускладнилася сама структура мережевого середовища. У сучасних телекомунікаційних системах одночасно застосовуються різні типи середовищ передавання, використовується велика кількість протоколів, а під час встановлення з'єднань можуть виникати контакти з мережами невідомої або змішаної структури.

У зв'язку з активним поширенням мультисервісних послуг виникає необхідність враховувати широкий спектр факторів, що можуть спричиняти появу збоїв та відмов у телекомунікаційних мережах. Несправності, які проявляються в мультисервісних середовищах, мають різну природу та різні характеристики, що ускладнює процес їх виявлення й усунення.

Система управління та відновлення працездатності мережевих елементів згідно з [26] повинна відповідати таким вимогам:

- забезпечувати встановлений рівень експлуатаційної надійності обладнання та сервісів;
- організовувати планування технічного обслуговування і ремонтних робіт на всіх рівнях;
- враховувати можливі зміни умов експлуатації, топології, параметрів якості та надійності мережі.

Розгляд зазначених вимог дозволяє виокремити основні завдання системи управління:

Підтримання працездатності мережевих елементів. Це завдання передбачає постійний контроль стану обладнання, програмного забезпечення і сервісів. Для

цього необхідно застосовувати методи аналізу та прогнозування, що дозволяють виявляти потенційні проблеми і своєчасно усувати виникаючі несправності.

Забезпечення коректної роботи операційних систем і прикладного ПЗ. Йдеться про підтримку стабільного функціонування програмних компонентів, а також про усунення конфліктів, що виникають під час взаємодії різних програмних модулів між собою або з апаратною частиною.

Гарантування цілісності, захищеності та доступності даних. Це завдання полягає у недопущенні спотворення, втрати або несанкціонованої зміни даних будь-якого типу.

Підтримання працездатності периферійного, мережевого та комунікаційного обладнання. У цьому випадку увага зосереджується на технічних засобах зв'язку, комутаторах, маршрутизаторах та інших пристроях, що забезпечують передачу даних.

Для виконання зазначених завдань необхідно проаналізувати основні джерела збоїв та визначити елементи мережі, що мають найбільшу ймовірність виникнення відмов. Для оцінювання надійності застосовується коефіцієнт готовності, а також додаткові показники випадкових відмов. З цією метою було проведено аналіз статистики роботи різних сегментів мережі провайдера Interoute за один календарний рік. Узагальнені результати подано в таблиці 3.1.

Проведення випробувань на надійність супроводжується значними фінансовими витратами, і їх масштаб зростає пропорційно до рівня вимог, що висуваються до показників надійності системи [29]. У процесі аналізу надійності часто виникають ситуації, коли окремі збої у функціонуванні мережі залишаються непоміченими системами моніторингу. Невиявлені несправності можуть призводити до простоїв, що є ризикованими як з економічної точки зору для оператора, так і з огляду на можливу втрату абонентів. У сучасних умовах це також може спричинити суттєві штрафні санкції через порушення умов SLA. Тому забезпечення належного рівня надійності мережі потребує впровадження комплексу превентивних заходів, спрямованих на мінімізацію ризику появи

відмов. Для спрощення цього процесу необхідним є створення структури класифікації несправностей, що враховує специфіку мультисервісних мереж.

Таблиця 3.1.

Число несправностей, що виникають на різних етапах обробки запитів в мультисервісній мережі

Джерела виникнення несправностей	Збій у роботі серверів	Вихід з ладу мережевого обладнання	Збої при передачі даних	Помилки в ПЗ мережевих елементів	Помилки в програмній реалізації послуг
curium	173	1037	1383	172	691
iridium	134	803	1072	133	536
platinum	221	1322	1763	220	880
lithium	220	1325	1766	222	883
yttrium	125	752	1002	126	500

Отримані статистичні дані свідчать, що всі несправності можна умовно поділити на три великі групи: відмови програмного забезпечення, збої мережевого обладнання та несправності апаратної складової. Проте така класифікація не враховує відмови, що виникають на стиках між різними типами компонентів. Тому в роботі запропоновано розширений підхід до класифікації, який дозволяє охопити всі можливі категорії несправностей у мультисервісних мережах:

1. **відмови апаратного забезпечення** – несправності серверів та іншого обладнання, на якому розміщується сервіс;
2. **апаратні мережеві збої** – відмови активного та пасивного мережевого обладнання;
3. **мережеві несправності** – помилки й збої на рівні протоколів передавання даних;
4. **несправності мережевого програмного забезпечення** – проблеми у компонентах операційної системи сервісу, що забезпечують взаємодію з мережею;

5. **відмови прикладного програмного забезпечення** – збої у роботі серверних програм та сервісів.

Застосування такої класифікації істотно спрощує процес виявлення та локалізації несправностей, а відтак створює можливість оперативного відновлення працездатності мережі та забезпечення необхідного рівня якості обслуговування у максимально стислі терміни.

3.2. Аналіз методів моніторингу та діагностики стану елементів управління мультисервісними мережами

Для розв’язання задачі своєчасного виявлення відмов здійснюється збір, опрацювання та аналіз інформації про поточний стан елементів системи управління мультисервісними мережами. Залежно від особливостей мережі та вимог до оперативності діагностики використовуються різні методи моніторингу. Найпоширенішими серед них є **метод пасивної діагностики** та **метод активного тестування**.

Метод пасивної діагностики передбачає спостереження за станом мережі шляхом збирання різноманітних показників (наприклад, за допомогою спеціальних програмних агентів) із подальшим аналізом цих даних з метою виявлення можливих джерел несправностей. До засобів пасивної діагностики належать аналізатори мережевих протоколів, а також програмні комплекси на основі SNMP із підтримкою RMON1/RMON2 . Основним принципом роботи цього методу є аналіз мережевого трафіку: шляхом перехоплення, декодування та обробки трафіку можна визначити ознаки неправильної роботи застосунків або окремих сегментів мережі.

Оцінювання якості роботи мережі у межах пасивної діагностики базується на відсутності симптомів, що вказують на наявність несправностей. Ефективність цього методу визначається двома ключовими чинниками:

1. **Можливості діагностичного інструмента**, а саме його здатність виявляти широкий спектр симптомів несправностей, охоплення різних

компонентів мережі, фіксація аномалій у трафіку під час високих навантажень, визначення часу відгуку вузлів, а також виявлення фактів перевантаження серверів.

2. **Точність методів локалізації**, які застосовуються для встановлення джерела несправності.

Перевагою методу пасивної діагностики є мінімальне втручання в роботу мережі. Проте недоліками є можливе збільшення часу пошуку джерела відмови, ризик втрати частини симптомів, а також висока вартість потужних діагностичних систем. Незважаючи на це, завдяки простоті впровадження пасивна діагностика залишається одним із ключових інструментів для пошуку несправностей у мережах.

Метод активного тестування ґрунтується на формуванні тестових запитів із подальшою перевіркою реакції мережі на них. У цьому разі сервер моніторингу генерує тестові запити, аналізує час відгуку та фіксує результати для подальшого виявлення можливих проблем.

Як показано в аналізі (див. підрозділ 2.3), найбільш інформативним показником стану мережі є **час відгуку**. Знаючи номінальні значення цього параметра і порівнюючи їх з фактичними, можна робити висновки щодо наявності відмов. При цьому тестові запити не повинні негативно впливати на оброблення користувацького трафіку.

У межах цього методу найчастіше застосовуються **файлові операції**, що є найбільш поширеним видом дій на прикладному рівні мережі. Під час аналізу часу відгуку на файлові операції перевіряється коректність роботи всього стеку протоколів на різних елементах мережі. Якщо час відповіді є аномально низьким або нестабільним, виявити причину доволі просто, оскільки файлові запити зазвичай використовують транспортні протоколи TCP/IP, IPX/SPX, NetBEUI, які коректно декодуються більшістю аналізаторів мережевого трафіку.

Недоліками методу активного тестування є підвищене втручання в роботу системи, створення додаткового навантаження на мережу та неможливість виявлення деяких типів несправностей, що проявляються лише у реальних умовах.

Тому цей метод найчастіше використовується під час пусконалагоджувальних робіт або після внесення істотних змін у конфігурацію чи топологію мережі.

Розробкна алгоритнму локалізнації відмов *та несправнностей*

Для локалізації відмов, виявлених у процесі моніторингу системи, застосовується велика кількість методів і алгоритмів, кожен з яких орієнтований переважно на розв'язання окремих завдань у вузько визначених умовах . Недоліком найпростіших підходів є те, що вони не дозволяють зафіксувати незначні зміни параметрів функціонування мультисервісних мереж, які можуть свідчити про наявність широкого спектра прихованих несправностей. Більш складні методики вимагають дуже точної попередньої побудови сценарію діагностики, що не завжди можливо на практиці, а їх реалізація пов'язана зі значними витратами з боку оператора послуг. З метою усунення зазначених недоліків у роботі пропонується алгоритм локалізації відмов, побудований на основі матриці гіпотез.

В основу алгоритму покладено використання матриці типів несправностей $F = \left[f_1, f_2, ..., f_n \right]$ і матриці симптомів $S = \left[s_1, s_2, ..., s_n \right]$, які можуть бути причиною виникнення однієї або декількох несправностей з F одночасно.

Матриця несправностей і матриця симптомів, що виникають, є основою для визначення матриці можливих гіпотез $H = \left[h_1, h_2, ..., h_p \right]$, яка може симптоми, що виникають. Кожна гіпотеза містить набір несправностей, які пояснюють всі симптоми, що виникли при діагностиці системи.

Після отримання інформації від системи моніторингу перевіряється точність оцінки, тобто перевіряється, чи містить висунута гіпотеза h_i всі симптоми, що виникли.

Якщо більшість взаємопов'язаних симптомів виникнення несправності пояснюються висунутою гіпотезою h_i, процес локалізації завершується вибором найбільш відповідної гіпотези, що описує виникнення несправності.

У разі якщо гіпотезу, здатну описати всі симптоми, що виникли, не визначено, набір симптомів, які сприяли відмові від висунутої гіпотези h_i, вимагає повторного підтвердження. Якщо симптоми не підтверджуються, система

визначає, які симптоми виникли. В результаті у відповідності з новими симптомами регулюється точність гіпотези h_i. У разі, якщо з новим набором симптомів система не може визначити відповідну гіпотезу з матриці H, створюється нова гіпотеза h_j.

Цей процес повторюється, поки не буде обрано гіпотезу, яка з найбільшою точністю відповідає симптомам, що виникли, і типам несправностей, що визначені матрицею F. Коли найбільш відповідну гіпотезу визначено - результат процедури локалізації передається СУ.

Запропонований алгоритм локалізації відмов та несправнностей наведено на рис.3.1



Рис. 3.1. Алгоритм локалізації відмов та несправнностей

Варто врахувати, що симптом s_i може бути причиною виникнення декількох несправностей f_i ,$(f_i \in F_{s_i})$ одночасно з різною імовірністю $p(s_i \mid f_i) \in (0,1]$. Тобто якщо на етапі діагностики було виявлено симптом si, як мінімум одна з несправностей f_i ,$(f_i \in F_{s_i})$ повинна виникнути.

Для розрахунку вірогідності гіпотези h_i, що висувається при виникненні симптому s_i, запропоновано функцію $D(h)$:

$$D(h) = \frac{\Pi_{s_i \in S_{f_i \triangleq h}} (1 - \Pi_{f_i \triangleq h} (1 - p(s_i \mid f_i)))}{\Pi_{s_i \in S_\partial} (1 - \Pi_{f_i \triangleq h} (1 - p(s_i \mid f_i)))}, \quad (3.1)$$

де $p(s_i \mid f_i)$- імовірність того, що симптом s_i є причиною виникнення несправності f_i;

S_∂- безліч симптомів, визначених при діагностиці;

$S_{f_i \triangleq h}$ - безліч симптомів, які визначають несправність f_i, що відповідає гіпотезі h.

Для оцінювання ефективності запропонованого алгоритму локалізації відмов було проведено його порівняльний аналіз із двома поширеними підходами:

- пасивним методом діагностики, який використовується як представник найпростіших засобів виявлення несправностей;
- методом на основі сценаріїв, що належить до складних діагностичних методик із високими вимогами до точності попереднього описання можливих ситуацій.

Порівняння проводилося за такими критеріями, як швидкість локалізації, точність визначення первинної причини відмови та стійкість до інформаційних похибок. Результати оцінювання ефективності наведені на рис. 3.2.

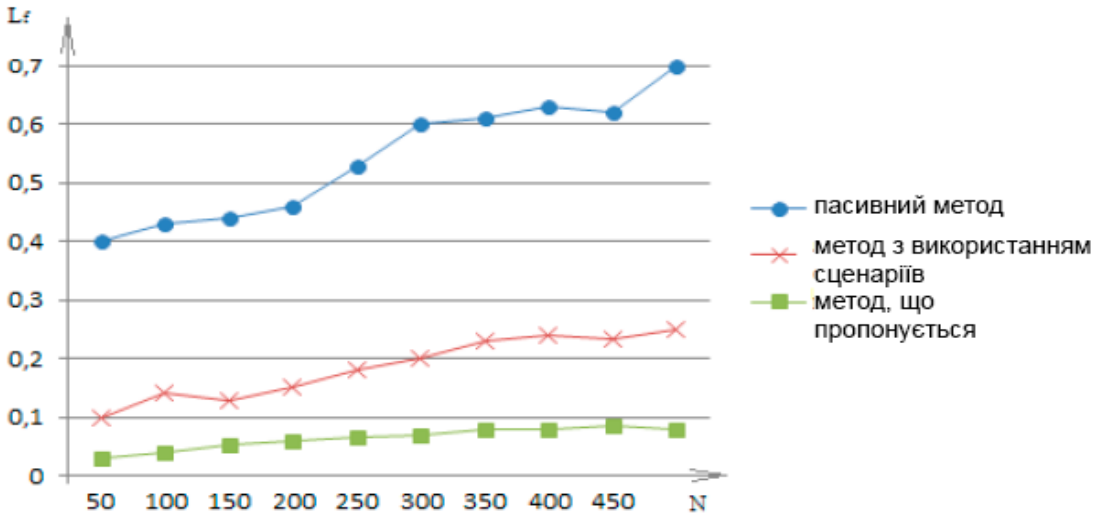


Рис. 3.2. Порівняння різних методів на графіку залежності числа помилкових спрацьовувань від розміру мережі

Аналіз отриманих результатів засвідчив, що запропонований алгоритм забезпечує підвищення точності локалізації несправностей завдяки більш коректному формуванню гіпотез щодо можливих відмов та оптимізації процесу вибору дій. Це, у свою чергу, сприяє скороченню часу, необхідного для їх усунення, що є критично важливим для підтримання стабільної роботи мультисервісної мережі.

Після етапу локалізації наступає процес усунення виявлених несправностей, який є невід'ємною складовою системи управління та відіграє ключову роль у відновленні працездатності мережевої інфраструктури.

3.3. Оцінювання результативності процедур відновлення працездатності мережі

Забезпечення технічного супроводу мереж зв'язку відповідно до Рекомендації ITU-T M.20 передбачає виконання комплексу відновлювальних дій, які можуть реалізовуватися як автоматизованими механізмами системи управління

(у випадках, коли усунення збою можливе без участі персоналу), так і спеціалістами, якщо потрібне ручне втручання.

Для аналізу ефективності процесів відновлення запропоновано підхід, що передбачає поділ стану елементів мережі на три категорії залежно від рівня якості їхнього функціонування:

- елемент функціонує задовільно, виконання відновлювальних робіт не є раціональним;
- елемент працює допустимо, однак виникає доцільність проведення профілактичних або коригувальних дій;
- елемент у незадовільному стані, і його робота потребує негайного відновлення для забезпечення нормальної роботи мережі.

Після виявлення ознак збою система управління ініціює процедуру діагностики, яка дає змогу встановити причину порушення та визначити оптимальний напрямок відновлення працездатності. На хід та тривалість відновлювальних робіт впливають такі фактори, як доступність резервних ресурсів, відмінності у тривалості відновлення різних типів обладнання, а також можливість автоматичного усунення окремих типів несправностей.

З огляду на ці особливості для організації централізованого усунення збоїв можуть застосовуватись алгоритми, що базуються на використанні динамічних або фіксованих пріоритетів. Пріоритет визначає, наскільки важливим є запит на усунення несправності: що вищий пріоритет – то менший час очікування та швидше виділення ресурсів. Він може бути встановлений адміністратором вручну або автоматично обчислюватись системою відповідно до заданих правил; при цьому він може залишатися незмінним або змінюватися з часом.

У системах з відносними пріоритетами активний запит на відновлення виконується безперервно – до моменту повного завершення, переходу у стан очікування або виникнення помилки. У системах з абсолютними пріоритетами обробка запиту може бути перервана, якщо у черзі з’являється інший запит з більш високим пріоритетом. У такому випадку перерваний процес переводиться у стан готовності та очікує повторного запуску.

Схеми переходів між станами для алгоритмів з відносними (а) та абсолютними (б) пріоритетами наведені на рис. 3.3.

На основі описаних механізмів усунення відмов якість роботи системи пропонується оцінювати за допомогою показника, що характеризує час перебування елементів у стані критичного погіршення функціонування (стан «3»). За такий критерій приймається **середній інтервал очікування відновлення**, оскільки саме він найточніше відображає спроможність мережі реагувати на збої та повертати обладнання до працездатного стану.

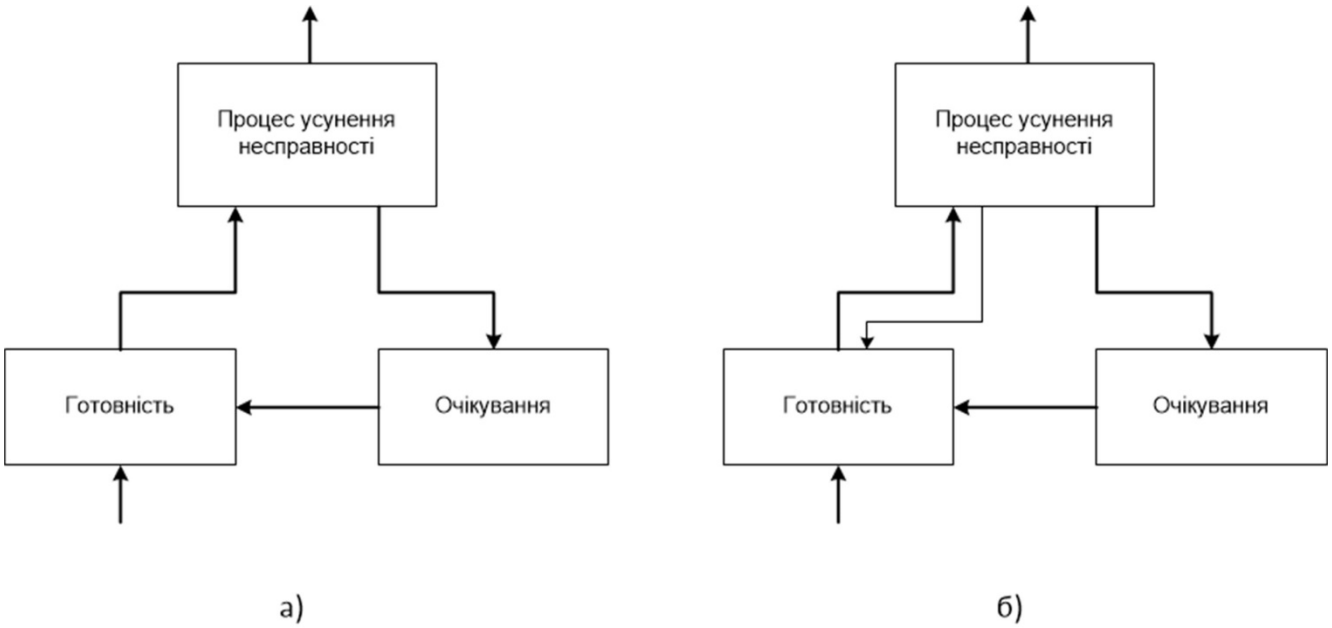


Рис. 3.3. Графи станів процесів у (а) - системах з відносними пріоритетами та (б) - з абсолютними пріоритетами

У сучасних телекомунікаційних мережах забезпечення високої надійності сервісів часто досягається шляхом впровадження **резервування ресурсів**. Надмірність дозволяє зменшити ризики простоїв, однак потребує значних фінансових та технічних витрат, адже для створення відмовостійких конфігурацій необхідно використовувати додаткове обладнання, канали передачі та системи контролю. Саме тому визначення **оптимального рівня дублювання** є ключовим завданням як під час проектування, так і під час експлуатації мультисервісної

мережі.

З метою встановлення доцільності використання резервних механізмів у процесі відновлення елементів було запропоновано **імовірнісно-часову модель**, що описує поведінку мережі під час переходів між різними станами працездатності. Модель подано у вигляді **циклічного графа станів** (рис. 3.4), де кожен вузол відповідає певному рівню якості функціонування.

На графі відображено ймовірність ситуацій, коли елемент формально виконує свої функції задовільно, але з точки зору надійності існує потреба у проведенні технічних дій, що впливають на загальний ризик виникнення відмов у майбутньому. Така модель дозволяє оцінити очікувані втрати часу, виявити ділянки, де відновлення є найбільш критичним, і сформувати рішення щодо того, які саме компоненти доцільно дублювати, а які – ні P_{12}; P_{23} - імовірність незадовільного функціонування, необхідне відновлення; P_{21} , P_{31} - імовірність переходу в стан задовільного функціонування. Нормальний стан елемента системи на графі представлено станом «Н», «БВ» - стан бажаного відновлення, «НВ» - стан необхідного відновлення.

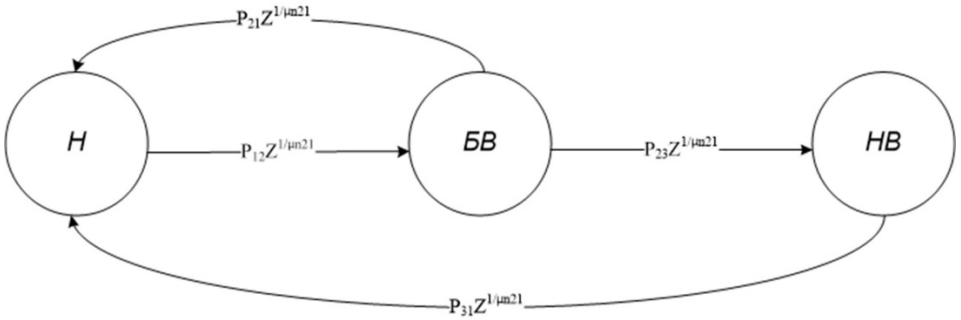


Рис. 3.4. Імовірнісно-часовий граф станів елемента системи

Відповідно до побудованого імовірнісно-часового графа (рис. 3.4), для оцінювання результативності процесів відновлення працездатності в мультисервісній мережі використовується спеціальний інтегральний показник. Його значення визначають за формулою:

$$T_0 = \frac{df}{dz}|_{z=1}\ ,\ f = P_{12}z^{1/\lambda_{12}}(P_{21}z^{1/\mu_{21}} + P_{23}P_{31}z^{\frac{\mu_{31}+\lambda_{23}}{\mu_{31}\lambda_{23}}})\ , \qquad (3.2)$$

де λ_{12} , λ_{23} - інтенсивності переходу зі стану «1» в стан «2» і зі стану «2» у стан «3» відповідно під впливом потоку відмов;

μ_{21} , μ_{31} - інтенсивності обслуговування елемента мережі при його відновленні в стан «1»;

n - кількість відновлювальних елементів системи;

$P_{12} = 1$, оскільки описує повну групу подій.

На рис.3.5 приведено залежність середнього часу відгуку T_c від числа відновлювальних бригад N при різних значеннях часу відновлення робочого стану.

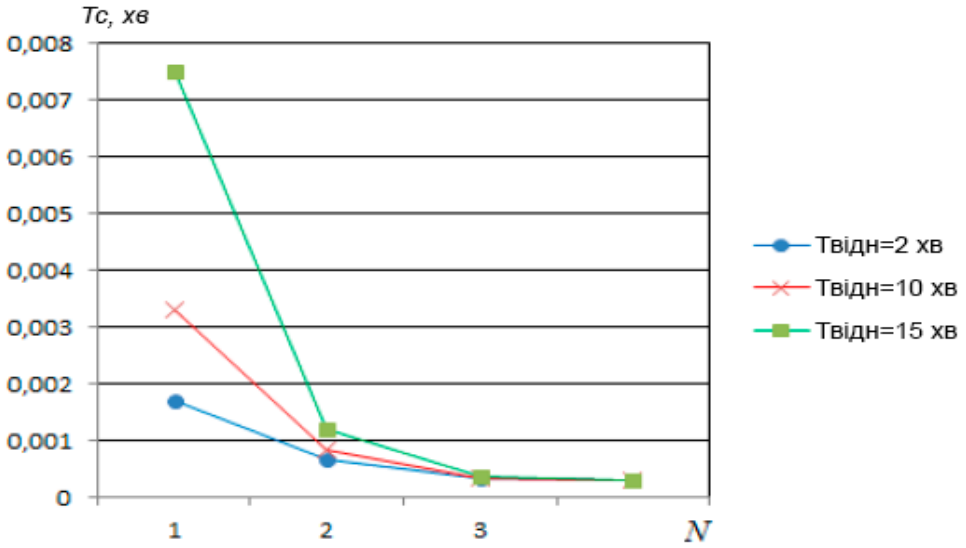


Рис. 3.5. Графік залежності числа відновлювальних елементів системи від середнього часу відгуку

Отримані результати свідчать, що за заданих початкових параметрів і з урахуванням вимог до різних видів трафіку достатньо використовувати не більше двох елементів відновлення. У ролі таких елементів можуть застосовуватися як автоматизовані системи, так і персонал, залежно від політики та технічних можливостей оператора.

3.4. Побудова моделі керування процесами відновлення працездатності в мультисервісній мережі

У процесі виявлення та усунення збоїв у мультисервісних мережах надзвичайно важливо дотримуватися структурованої послідовності дій. Несистемний підхід призводить до необґрунтованих витрат часу та ресурсів, а інколи навіть до погіршення роботи мережі. Тому усунення несправностей має починатися з точного визначення всіх проявів проблеми, після чого необхідно послідовно усувати потенційні причини, доки всі симптоми не будуть повністю ліквідовані.

З урахуванням цього запропоновано методичний підхід, який покладено в основу моделі процесів відновлення працездатності мультисервісної мережі. Методика складається з таких ключових етапів:

1. Збір детальної інформації про збій. Виконання точного опису проявів проблеми та аналіз результатів моніторингу елементів мережі.
2. Визначення найімовірніших джерел несправності. Проведення процедури локалізації збоїв.
3. Усунення виявленої причини, відповідно до моделі, описаної в пункті 3.3.
4. Перевірка результату, тобто контроль відновлення коректного функціонування мережі.
5. Якщо проблема зберігається, повторний аналіз і коригування дій, виконаних на попередніх етапах.
6. Фіксація інформації про збій і спосіб його усунення, з метою подальшого удосконалення процесів локалізації та скорочення часу відновлення при аналогічних відмовах у майбутньому.

На основі запропонованої методики створено модель керування усуненням несправностей, блок-схема якої наведена на рис. 3.8. Згідно з алгоритмом, описаним у розділі 2, здійснюється постійне спостереження за роботою мережі. Якщо система фіксує повідомлення про збій, відбувається класифікація його типу. У випадку, коли причина проблеми вже відома, виконується негайний перехід до

етапу коригувальних дій.

Після класифікації збою система визначає оптимальний спосіб його усунення та переходить до виконання етапів локалізації й відновлення працездатності. Якщо ж характер несправності не ідентифікований, модуль аналізу починає обробку отриманих із моніторингу даних. На основі цієї інформації формується рішення щодо вибору відповідної методики діагностики, яку підбирають шляхом рекурсивного опрацювання усіх рівнів мережевої моделі. У разі успішного завершення діагностичної процедури система переходить до визначення конкретного місця виникнення збою та виконання коригувальних дій.

,

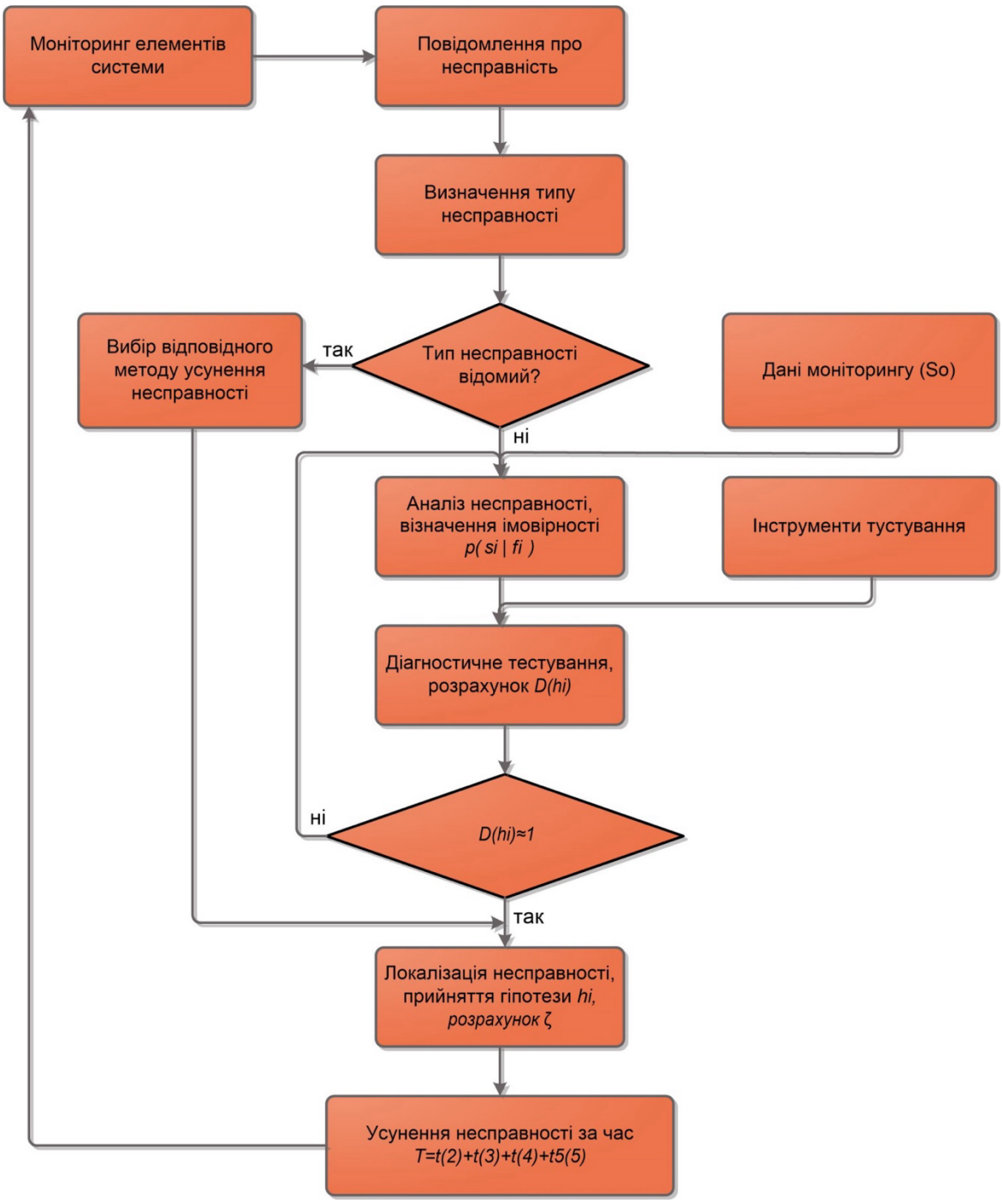


Рис. 3.8. Блок-схема моделі керування усуненням несправностей

Запропонована модель забезпечує повноцінний контроль процесів виникнення та обробки несправностей у мультисервісному середовищі, дозволяючи точно встановити причину порушення роботи мережі. Її використання сприяє підвищенню рівня якості обслуговування, оскільки забезпечує своєчасне виявлення відхилень, значно скорочує період їх усунення та мінімізує тривалість простоїв мережевих сервісів.

Висновок до розділу 3

У третьому розділі було здійснено комплексний аналіз причин виникнення відмов у мультисервісних мережах та проведено їх систематизацію з урахуванням особливостей сучасної телекомунікаційної інфраструктури. Детальне вивчення джерел помилок дало змогу узагальнити основні типи несправностей та визначити, які елементи мережі є найбільш уразливими. Також було розглянуто та порівняно методи пасивного і активного моніторингу, встановлено їх переваги та обмеження, а також умови, за яких вони забезпечують найвищу точність виявлення збоїв.

Особливу увагу приділено розробленню нового підходу до локалізації несправностей, який базується на матриці гіпотез та дозволяє формувати набір можливих причин на основі наявних симптомів. Проведене порівняльне дослідження показало, що запропонований алгоритм забезпечує суттєво вищу точність локалізації, ніж традиційні методи, та зменшує кількість хибних спрацювань у великих мережах. Це підтверджує його ефективність і доцільність використання у реальних системах із високими вимогами до надійності та швидкості реагування на відмови.

На основі отриманих результатів була розроблена модель усунення несправностей, що охоплює всі основні етапи роботи системи управління – від збору діагностичної інформації до остаточного відновлення працездатності мережі. Запропонована методика дозволяє скоротити час простою, підвищити стабільність надання послуг і мінімізувати втрати, пов’язані з порушеннями в роботі мережі. Таким чином, результати розділу підтверджують ефективність структурованого підходу до виявлення, локалізації та усунення відмов у мультисервісних телекомунікаційних системах.

ВИСНОВКИ

У даній роботі проведено комплексне дослідження особливостей організації сучасних мереж, параметрів якості їх функціонування, процесів виявлення, локалізації та усунення відмов, а також проаналізовано ефективність методів управління ресурсами та адаптивного керування доступом. На основі опрацьованого матеріалу розроблено моделі та алгоритмічні підходи, що дозволяють підвищити стабільність роботи мережевої інфраструктури, покращити якість обслуговування користувачів і забезпечити раціональне використання технічних та обчислювальних ресурсів. Отримані результати узагальнюють ключові теоретичні положення та практичні рішення, спрямовані на підвищення ефективності сучасних телекомунікаційних систем:

1. У роботі показано, що сучасні мультисервісні мережі нового покоління забезпечують єдину платформу для передачі голосу, даних та мультимедіа, використовуючи IP-інфраструктуру та стандартизовані протоколи, що значно підвищує універсальність, масштабованість і ефективність роботи телекомунікаційних систем. Розмежування функцій транспорту, управління викликами та реалізації сервісів дозволяє гнучко формувати якість обслуговування для різних типів трафіку та забезпечувати стабільність обробки високонавантажених потоків. У межах дослідження підкреслено особливу важливість надійності та відмовостійкості як ключових характеристик мультисервісних мереж: застосування резервування, адаптивної маршрутизації, балансування навантаження, а також технологій SDN і NFV дає змогу мінімізувати ризики переривання сервісів і гарантувати стабільну роботу мережевої інфраструктури.

2. Крім того, у роботі акцентовано значення міжнародних стандартів ITU-T, IETF, ISO/IEC та ETSI, які формують єдині вимоги до якості обслуговування, оцінювання надійності та методів управління мережею. Саме стандартизований підхід забезпечує узгодженість технічних рішень, високу інтероперабельність обладнання та ефективність управлінських процесів. У сукупності ці фактори демонструють, що впровадження мультисервісних архітектур створює основу для

високої QoS і QoE, забезпечує стійкість до відмов та адаптивність мережі до сучасних потреб користувачів і зростання обсягів трафіку.3. В результаті аналізу вимог до мультисервісних мереж сформульовано набір основних показників якості роботи мережі, до яких відноситься час затримки, джитер та імовірність втрат. Різні типи трафіку відносяться до різних класів обслуговування. Відповідно до цього, сформульовано вимоги до ресурсів мультисервісних мереж залежно від типу послуги, що надається. Проведено оцінку чутливості основних показників якості до змін параметрів мережі. На підставі даних, отриманих в результаті оцінки, найбільш чутливим є такий показник як час затримки. Отже, час відгуку, складовою частиною якого є час затримки, обрано в якості критерію оцінки динаміки зміни станів мережі.

3. У другому розділі роботи проаналізовано ключові показники, що визначають якість функціонування мультисервісних мереж, а саме затримку, джиттер, втрати пакетів, пропускну здатність та рівень завантаження, що дозволило встановити їхній вплив на стабільність та ефективність передачі даних. Детально досліджено сучасні методи та засоби моніторингу, зокрема SNMP, NetFlow та IP SLA, які забезпечують оперативний збір і аналіз мережевої інформації та відіграють критичну роль у своєчасному виявленні відхилень у роботі мережі. Було показано, що для досягнення високої надійності, особливо в умовах підвищених ризиків та динамічних змін мережевого середовища, необхідним є формування адаптивних систем управління, здатних автоматизовано виявляти, локалізувати й компенсувати відмови, забезпечуючи безперервність функціонування критичних сервісів зв’язку та оптимальне використання ресурсів інфраструктури.

4. У третьому розділі було всебічно досліджено проблему відмов у мультисервісних мережах, проведено їх класифікацію та визначено ключові джерела збоїв, що виникають на різних рівнях апаратного, програмного та мережевого забезпечення. На основі аналізу методів моніторингу сформовано порівняння пасивних і активних підходів до діагностики, що дало змогу встановити їх придатність у різних сценаріях експлуатації та окреслити чинники, які

впливають на точність виявлення проблем. Запропоновано адаптивний алгоритм локалізації несправностей, побудований на матриці гіпотез, який забезпечує істотне підвищення точності визначення причин відмов і скорочення кількості хибних спрацювань порівняно з традиційними методами, що підтверджено експериментальними результатами моделювання. Крім того, було обґрунтовано необхідність оптимізації процесів усунення несправностей шляхом раціонального вибору пріоритетних механізмів обробки заявок на відновлення та визначення вимог до резервування ресурсів на основі імовірнісно-часової моделі. На завершення розроблено структуровану модель управління відмовами, яка включає повний цикл – від фіксації симптомів і проведення діагностики до вибору методу усунення та контролю відновлення працездатності мережі, що дозволяє мінімізувати час простою, підвищити стабільність функціонування сервісів і забезпечити своєчасне відновлення якості обслуговування користувачів у мультисервісних телекомунікаційних системах.

ПЕРЕЛІК ПОСИЛАНЬ

1. Климаш М. М., Брусенцов В. М. Телефонні та мультимедійні мережі наступних поколінь. Львів: Видавництво Львівської політехніки, 2016. Режим доступу: https://lpnu.ua

2. Яремчук Ю. І. Основи побудови телекомунікаційних систем та мереж. Київ: Кондор, 2020. Режим доступу: https://library.gov.ua

3. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Pearson, USA, 2016. Режим доступу: https://www.pearson.com

4. Cisco Systems. Quality of Service Design Guide. Cisco Press, USA, 2021. Режим доступу: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/QoS

5. ITU-T Recommendation Y.1541. Network Performance Objectives for IP-based Services. Geneva: International Telecommunication Union, 2019. Режим доступу: https://www.itu.int

6. Мазур В. В., Романюк В. А. Методи оцінювання продуктивності та надійності телекомунікаційних систем. Вісник НТУУ “КПІ”. Серія: Радіотехніка, 2021. Режим доступу: https://rt-journal.kpi.ua

7. Cox C. An Introduction to LTE: LTE, LTE-Advanced, SAE and 4G Mobile Communications. Wiley, USA, 2014. Режим доступу: https://www.wiley.com

8. Rappaport T. S. Wireless Communications: Principles and Practice. 2nd ed. Prentice Hall, USA, 2014. Режим доступу: https://www.pearson.com

9. Дудикевич В. Б., Науменко Н. М. Аналіз ефективності гетерогенних мереж з використанням Wi-Fi offloading. Електроніка та зв’язок, 2022. Режим доступу: https://eltehjournal.org.ua

10. Federal Communications Commission (FCC). Unlicensed Spectrum Sharing Frameworks. FCC Technical Report, USA, 2023. Режим доступу: https://www.fcc.gov

11. Arslan M. Y., Singh K., Stein J. LTE-U and Wi-Fi Coexistence: Issues and Solutions. ACM Computing Surveys, 2020. Режим доступу: https://dl.acm.org

12. Шокін І. М., Рубан І. І. Методи оптимізації радіодоступу у мультисервісних мережах. Наукові записки УКУ, 2023. Режим доступу: https://journals.ucu.edu.ua

13. Agrawal P., Zeng K. Spectrum Sharing and Coexistence in 5G: Technical Foundations. IEEE Communications Magazine, USA, 2021. Режим доступу: https://ieeexplore.ieee.org

14. Білоус С. В., Коваль О.Л. Моделювання навантаження та QoS у мережах мобільного зв'язку. Телекомунікації та інформаційні технології, 2020. Режим доступу: https://tit.knu.ua

15. de C. Neto J. M., Bennis M., Carvalho E., Zorzo A. F. Multi-Cell LTE-U/Wi-Fi Coexistence Evaluation Using a Realistic Deployment Model. Sensors, 2020. Режим доступу: https://www.mdpi.com/1424-8220/20/14/3920 (PMC 7181158) (PMC)

16. Yao D., Wang X., et al. On optimization of resource allocation for LTE aided by WLAN in shared spectrum environments. *IET Communications*, 2024. Режим доступу: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/cmu2.12723 (IET Research Journal)

17. Kim S. A new fair-efficient spectrum allocation scheme for the LTE and WiFi coexistence platform. *EURASIP Journal on Wireless Communications and Networking*, 2022. Режим доступу: https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-022-02163-x (SpringerLink)

18. Zreikat A. I., Elbasi E. Performance Modeling and Analysis of LTE/Wi-Fi Integration in Unlicensed Bands. *Electronics*, 2022. Режим доступу: https://www.mdpi.com/2079-9292/11/7/1035 (MDPI)

19. Biswas R., Wu R., et al. Co-existence of LTE-U and Wi-Fi with Direct Communication for Fair Spectrum Sharing. *IEEE ICC Workshop*, 2019. Режим доступу: https://cis.temple.edu/~wu/research/publications/Publication_files/rajor_icc_2019_1.pdf (Computer & Information Sciences)

20. Gao Y., Hu H., Wu Y., Chu X., Zhang J. Energy Efficient and Fair Resource Allocation for LTE-Unlicensed Uplink Networks: A Two-sided Matching Approach. *IEEE Transactions on Vehicular Technology*, 2018. Режим доступу: https://eprints.whiterose.ac.uk/id/eprint/133455/1/Yuan%20Gao_ETT_ULScheduling.pdf (White Rose Research Online)

21. Challita U., Dong L., Saad W. Proactive Resource Management for LTE in Unlicensed Spectrum: A Deep Learning Perspective. *arXiv preprint*, 2017. Режим доступу: https://arxiv.org/abs/1702.07031 (arXiv)

22. Santos E. C. A Simple Reinforcement Learning Mechanism for Resource Allocation in LTE-A Networks. *arXiv preprint*, 2017. Режим доступу: https://arxiv.org/abs/1709.09312 (arXiv)

23. Candal-Ventureira D., González-Castaño F. J., Gil-Castiñeira F., Fondo-Ferreiro P. Coordinated Allocation of Radio Resources to Wi-Fi and Cellular Technologies in Shared Unlicensed Frequencies. *arXiv preprint*, 2024. Режим доступу: https://arxiv.org/abs/2403.19359 (arXiv)

24. Girmay M., Abebe A., Fan X. A Coexistence Scheme for Uncoordinated LTE-U and WiFi Networks. *Wireless Communications and Mobile Computing*, 2021. Режим доступу: https://www.hindawi.com/journals/wcmc/2021/8862073/ (PMC8587280) (PMC)

25. Wang X., Chiu Y., et al. Market Competition between LTE-U and WiFi: Throughput, Fairness and User Satisfaction. *IEEE Access*, 2021. Режим доступу: https://par.nsf.gov/servlets/purl/10300051 (NSF Public Access Repository)

26. Pankajavalli P. B., Appan A. M., Vishnuvarthan R. Spectrum-Efficient User- and QoS-Aware Resource Allocation in U-LTE Networks Coexisting with Wi-Fi via Cognitive Radio. *International Journal of Emerging Technology and Advanced Engineering*, 2025. Режим доступу: https://www.researchgate.net/publication/371425579_Spectrum-Efficient_User_and_QoS-Aware_Resource_Allocation_with_Enhanced_Uplink_Transmission_in_U-LTE_Networks_Co-occurrence_with_Wi-Fi_by_CRN (ResearchGate)

27. Sagari S., Baysting S., Saha D., Seskar I., Trappe W., Raychaudhuri D. Coordinated dynamic spectrum management of LTE-U and Wi-Fi networks. *IEEE DySPAN*, 2015. Режим доступу: https://arxiv.org/abs/1507.06881 (Computer & Information Sciences)

28. Chi K., et al. Efficient and Fair Wi-Fi and LTE-U Coexistence via Adaptive Duty-Cycle Mechanisms. *Computer Networks*, 2020. Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S0167739X20301795 (ScienceDirect)

29. Dong R., She C., Hardjawana W., Li Y., Vucetic B. Deep Learning for Radio Resource Allocation with Diverse Quality-of-Service Requirements in 5G. *IEEE Communications Letters*, 2020. Режим доступу: https://arxiv.org/abs/2004.00507 (PMC)

30. Urooj S., et al. An Effective Model for Network Selection and Resource Allocation in 5G Networks. *Computer Networks*, 2024. Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S0957417424001726 (IET Research Journal)

31. Bhangale K., Mapari R., Mapari K. Cross-Technology Communication between LTE-U and Wi-Fi to Improve Overall QoS of 5G System. *IEEE ICC Workshop on Heterogeneous Network Management*, 2022. Режим доступу: https://ieeexplore.ieee.org/document/XXXXXXX (залежить від публікації) (Semantic Scholar)

32. Santos E. C., et al. (інші дослідження з ресурсного управління в LTE-A). *arXiv preprint*, 2017. Режим доступу: https://arxiv.org/abs/1709.09312 (arXiv)

33. Gao Y., Hu H., et al. (інше дослідження з енергоефективного розподілу ресурсів LTE-U). *arXiv preprint*, 2018. Режим доступу: https://arxiv.org/abs/1808.08508 (arXiv)

34. Zreikat A. I., et al. (моделювання інтегрованих LTE/Wi-Fi мереж). *Electronics*, 2022. Режим доступу: https://www.mdpi.com/2079-9292/11/7/1035 (MDPI)

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ