ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно-інтегрованих технологій, автоматизації, електроінженерії та радіоелектроніки
(повне найменування інституту, назва факультету)

Автоматика та телекомунікації
(повна назва кафедри)

«До захисту допущено»

В.о. завідувача кафедри

_____

_____
(підпис) (ініціали, прізвище)

"___"_____2021 р.

Випускна кваліфікаційна робота

магістра
(освітньо-кваліфікаційний рівень)

на тему Дослідження моделей розподілення трафіку в інформаційно-телекомунікаційних мережах спеціального призначення

Виконав : студент 2 курсу, групи ТКРзм-19
(шифр групи)

спеціальності 172 Телекомунікації та радіотехніка
(шифр і назва напряму підготовки, спеціальності)

Валяєв І.С. _____
(прізвище та ініціали) (підпис)

Керівник к.т.н., доц. Воропаєва В.Я. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Покровськ – 2021 р.

ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно- інтегрованих технологій, автоматизації, електроінженерії та радіоелектроніки
(повне найменування інституту, назва факультету)

Автоматика та телекомунікації
(повна назва кафедри)

Захист відбувся_____
(дата)
з оцінкою _____
секретар ДЕК_____
(підпис)

Випускна кваліфікаційна робота

магістра
(освітньо-кваліфікаційний рівень)

на тему Дослідження моделей розподілення трафіку в інформаційно-телекомунікаційних мережах спеціального призначення

Виконав студент групи ТКРзм-19 _____ І.С. Валяєв
(підпис, дата) (ініціали, прізвище)

Керівник _____ В.Я. Воропаєва
(підпис, дата) (ініціали, прізвище)

В.о.зав. каф. автоматики та телекомунікацій _____ І.С.Лактіонов
(підпис, дата) (ініціали, прізвище)

Консультанти _____
(підпис, дата) (ініціали, прізвище)

_____.
(підпис, дата) (ініціали, прізвище)

_____.
(підпис, дата) (ініціали, прізвище)

Нормоконтролер _____ Д.О.Жуковська
(підпис, дата) (ініціали, прізвище)

Покровськ – 2021 р.

ДВНЗ «Донецький національний технічний університет»

Факультет комп'ютерно-інтегрованих технологій, автоматизації електроінженерії та радіоелектроніки
Кафедра автоматика та телекомунікації
Освітній ступінь магістр
Спеціальність 172 Телекомунікації та радіотехніка
(шифр і назва)

ЗАТВЕРДЖУЮ:
В.о. завідувача кафедри
_____ /Лактіонов І.С./
"____" _____20___року

З А В Д А Н Н Я
НА ВИПУСКНУ КВАЛІФІАЦІЙНУ РОБОТУ СТУДЕНТУ

Валяєву Ігорю Станіславовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження моделей розподілення трафіку в інформаційно-телекомунікаційних мережах спеціального призначення

керівник роботи: к.т.н., доц. Воропаєва Вікторія Яківна
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом від " " 20 року №

2. Строк подання студентом роботи

3. Вихідні дані до роботи: результати науково-дослідної роботи, магістерської практики.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

1) аналітичний огляд методів побудови мереж спеціального призначення;
2) аналітичний огляд параметрів трафіку мереж спеціального призначення;
3) розрахунок статистичних параметрів трафіку мережі спеціального призначення;
4) проведення імітаційного моделювання мережі спецального призначення.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1			
2			
3			
4			

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Проходження практики	01.02-14.02.2021	
2	Аналіз мереж спеціального призначення	01.02-14.02.2021	
3	Аналіз характеристик трафіку мереж спеціального призначення	15.02-21.03.2021	
4	Аналіз моделей мереж спеціального призначення	22.03-11.04.2021	
5	Розрахунок параметрів математичних моделей мереж для проведення імітаційного моделювання	12.04-25.04.2021	
6	Імітаційне моделювання мережі	26.04-05.05.2021	
7	Написання пояснювальної записки	06.05-10.05.2021	

Студент _____ **Валяєв І.С.**
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ **Воропаєва В.Я.**
(підпис) (прізвище та ініціали)

Лист зауважень

Посада П.І.Б.	Суть зауваження, оцінка та підпис

АНОТАЦІЯ

Валяєв І.С. Дослідження моделей розподілення трафіку в інформаційно-телекомунікаційних мережах спеціального призначення / Випускна кваліфікаційна робота на здобуття освітнього ступеня «магістр» за спеціальністю 172 «Телекомунікації та радіотехніка». – ДВНЗ ДонНТУ, Покровськ, 2021.

Робота містить 90 сторінок, складається з вступу, чотирьох розділів, висновків, переліку використаних джерел з 36 найменувань, 25 рисунків, 6 таблиць, 1 додаток

Магістерська робота направлена на дослідження моделей розподілення трафіку в вузлах мереж спеціального призначення для подальшого проектування подібних мереж з мінімальною затримкою та втратою даних.

В роботі проведено аналіз структури мереж спеціального призначення, описано технології, які використовуються для побудови мереж спеціального призначення, розглянуті статистичні властивості трафіку мереж спеціального призначення, розглянуті ймовірнісі характеристики вузла мережі спеціального призначення, проведено імітаційне моделювання функціонування вузла мережі спеціального призначення в умовах надходження самоподібного трафіку з подальшим вибором моделі яка забезпечує мінімальний час затримки трафіку та мінімальні втрати пакетів даних.

Практична цінність отриманих результатів полягає в можливості використання оптимальних моделей для проектування реальних мереж спеціального призначення та забезепечення розподілу трафіку в мережі з мінімальною затримкою та втратою даних.

Ключові слова: МРЕЖА, ПОСЛУГА, ТРАФІК, МОДЕЛЬ, ЗАТРИМКА, ВТРАТА ПАКЕТІВ, МЕРЕЖЕВИЙ ВУЗОЛ, МОДЕЛЮВАННЯ.

ABSTRACT

Research of traffic distribution models in information and telecommunication networks of special purpose / Graduation qualifying work for obtaining an educational degree "Master" in specialty 172 "Telecommunications and Radio Engineering" - SHEE DonNTU Pokrovsky, 2021.

The work contains 90 pages, consists of an introduction, four sections, conclusions, a list of sources used with 36 titles, 25 figures, 6 tables, 1 appendices

The master's thesis is aimed at studying the models of traffic distribution in the nodes of special purpose networks for further design of such networks with minimal delay and data loss.

The paper analyzes the structure of special purpose networks, describes the technologies used to build special purpose networks, considers the statistical properties of traffic of special purpose networks, considers the probabilistic characteristics of a special purpose network node, simulates the operation of a special purpose network node in self-similar traffic. further selection of a model that provides minimal traffic delay time and minimal data packet loss.The practical value of the obtained results lies in the possibility of using optimal models for the design of real special purpose networks and ensuring the distribution of traffic in the network with minimal delay and data loss.

Keywords: NETWORK, SERVICE, TRAFFIC, MODEL, DELAY, LOSS OF PACKAGES, NETWORK NODE, SIMULATION

ЗМІСТ

ВСТУП 9
1 ОСОБЛИВОСТІ ПОБУДОВИ МЕРЕЖ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ 11
1.1 Концептуальні положення побудови та розвитку мереж спеціального призначення 11
1.2 Технології побудови мереж спеціального призначення 13
1.3 Архітектура мереж спеціального призначення 20
Висновки до розділу 1 23
2 ДОСЛІДЖЕННЯ СТАТИСТИЧНИХ ВЛАСТИВОСТЕЙ ТРАФІКУ МЕРЕЖ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ 26
2.1 Методи аналізу статистичних властивостей трафіку 26
2.2 Аналіз часу очікування заявки в черзі для системи масового обслуговування загального виду 33
2.3 Аналіз часу очікування заявки в черзі під час обробки корельованого трафіку 36
2.3.1 Потоки з гіперекспоненціальним розподілом 37
2.3.2 Потоки з розподілом Ерланга 39
Висновки до розділу 2 41
3 АНАЛІЗ ФУНКЦІОНУВАННЯ ВУЗЛА МЕРЕЖІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ 43
3.1 Загальне вирішення задачі оцінювання середнього часу очікування в черзі для системи G/G/1 43
3.2 Аналіз характеристик системи масового обслуговування загального виду методом рандомізації 47
Висновки до розділу 3 54
4 ДОСЛІДЖЕННЯ ВУЗЛІВ МЕРЕЖІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ МЕТОДОМ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ 56

4.1 Огляд засобів моделювання мереж зв’язку 56
4.2 Характеристики симулятора NS2 58
4.3 Моделювання та обробка самоподібного трафіку симулятором NS2 62
Висновки до розділу 4 73
ВИСНОВКИ 75
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 77
ДОДАТОК А. Розділ охорони праці та пожежна безпека в науково-дослідницькому відділі 81

ВСТУП

Актуальність. Домінантним підходом розвитку сучасних мереж зв'язку є підхід, оснований на концепції створення мереж нового покоління, що базуються на мультисервісних мережах. Телекомунікаційні системи крім завдання встановлення і підтримування комунікацій, покликані вирішувати завдання управління, підтримуючи функціонування різних інформаційних систем. При цьому конвергенція сучасних інформаційних і телекомунікаційних технологій призводить до створення мереж спеціального призначення.

Управління трафіком в мережах спеціального призначення з метою забезпечення високої якості надання послуг (QoS) вимагає аналізу і вибору математичних моделей функціонування мережі. Ці моделі повинні бути динамічними і описувати основні процеси генерації повідомлень, що несуть певну інформацію від різноманітних джерел, процеси розподілу повідомлень і процеси переносу інформації між джерелом і одержувачами інформації. При цьому будь-які сучасні послуги, формують так званий термінальний потік, що надходить на відповідний вузол МСП.

Сукупність таких потоків утворює мережевий інформаційний потік, який завдяки впливу різних випадкових чинників має яскраво виражений стохастичний характер і може бути адекватно описаний методами теорії масового обслуговування. Такий потік, званий трафіком, обробляється в вузлі МСП також випадковим чином, тому що параметри трафіку і параметри стану вузла можуть бути відомі, як правило, на рівні завдання законів розподілу випадкових значень цих параметрів.

Аналіз структури потоків інфокомунікаційних систем нового покоління виявили, що досліджуваний трафік має чітку структуру типу VBR (variable bit rate), що призводить до поява черг і втрати пакетів. Тому завдання вибору

моделі управління мережею спеціального призначення і трафіком в цій мережі є актуальним.

Мета роботи і завдання дослідження. Мета роботи полягає в дослідженні вузлів мереж спеціального призначення при обробці самоподібного трафіку.

Мета роботи досягається послідовним вирішенням наступних **завдань:**

- аналіз існуючих моделей трафіку і методів його обробки, заснованих на класичній теорії масового обслуговування,

- аналіз методів математичного моделювання трафіку з використанням самоподібних випадкових процесів,

- аналіз методів аналізу систем масового обслуговування загального вигляду при обробці трафіку з незалежними часовими інтервалами,

- аналіз характеристик систем масового обслуговування загального вигляду при обробці самоподібного трафіку методом імітаційного моделювання.

Об'єкт дослідження. Інфокомунікаційні мережі спеціального призначення.

Предмет дослідження. Моделі систем масового обслуговування і методи аналізу характеристик функціонування вузлів МСП при обробці самоподібного трафіку.

Структура роботи. Робота включає зміст, вступ, чотири розділи основного тексту, висновок і бібліографічний список.

1 ОСОБЛИВОСТІ ПОБУДОВИ МЕРЕЖ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

1.1 Концептуальні положення побудови та розвитку мереж спеціального призначення

Останнім часом в різноманітних корпораціях та відомствах спеціального призначення, де широко використовуються процеси інформатизації для забезпечення роботи департаментів та відділів, вводять різноманітні інформаційні та інформаційно-довідкові системи, які реалізують різноманітні інформаційні технології. У зв’язку з швидким зростом інформатизації корпоративні інформаційні та інформаційно-довідкові системи стали трансформуватися в єдині інфокомунікаціонні мережі спеціального призначення (МСП). Подібні мережі надають широкий спектр інформаційних та телекомунікаційних послуг, які реалізуються за допомогою програмно-апаратних комплексів, що включають в себе різноманітні телекомунікаційні мережі. Таким чином забезпечується надання всім користувачам повного пакету послуг: обмін інформацією, передача та доставка інформації, обробка, зберігання, збереження та накопичення.

Існують різні мережі спеціального призначення, які відрізняються один від одного потребами в ресурсах, розмахом, структурою, можливостями, реальної пропускною спроможністю, безпекою та стійкістю.

З розвитком корпоративних мереж передачі мови та даних, в різні роки були створені проекти зі створення сучасних телекомунікаційних мереж, спрямованих на обмін даними і промовою, інтегруючих різні мережі передачі даних, документального обміну, телефонні і телеграфні мережі та призначені для об'єднання існуючих мереж на основі технологій ISDN, FR, IP і MPLS поверх SDH або ATM.

Поєднання цих технологій при використанні в мережах зв'язку дозволяє надавати користувачам широкий спектр послуг, дає можливість

нарощувати послуги і розширювати підтримувані мережеві технології, створюючи таким чином необхідні умови для побудови телекомунікаційної основи мереж спеціального призначення. Однак, в даний час при побудові МСП на основі концепцій мереж зв'язку наступного покоління (NGN) і глобальної інформаційної інфраструктури (GII), в залежності від особливостей їх застосування, від пропонованих вимог щодо забезпечення безпеки, такі мережі значно відрізняються від загального вигляду перспективної мережі зв'язку загального користування.

Під мережами спеціального призначення будемо розуміти комплекс інформаційно-комунікаційних систем, що надають великий набір інформаційних та телекомунікаційних послуг з гнучким управлінням, створення і персоналізацію нових послуг за допомогою стандартизації інформаційних і мережевих рішень, використовують універсальну транспортну мережу з розподіленою комутацією, надання інформаційних та телекомунікаційних послуг в кінцеві мережеві вузли і об'єднання з традиційними і існуючими мережами зв'язку [1].

Зазвичай в концепції побудови та еволюції будь-якої великої мережі електрозв'язку викладені рішення по формально ідентичним положенням [2]:

- призначення (основні функціональні завдання);
- структура (на всіх рівнях ієрархії);
- рекомендований комплекс технічних засобів (що має на увазі вибір
- технологій передачі, комутації та обробки інформації);
- перелік підтримуваних послуг;
- показники якості обслуговування трафіку;
- принципи сигналізації, синхронізації, тарифікації та технічної експлуатації.

Жорсткі вимоги до показників надійності і живучості МСП визначають вибір структури мережі. Наприклад, на рівні транзитного фрагмента МСП між вузлами комутації можна створювати кілька (не менше двох) незалежних

шляхів обміну інформацією. При цьому на рівні доступу, де часто використовується деревоподібна топологія, такий підхід навряд чи реалізуємо. структура МСП повинна забезпечувати функцію мобільності абонентів, що може бути реалізовано на основі системи супутникового зв'язку. Крім того, структура мережі повинна бути орієнтована на оперативне вирішення завдання управління ресурсами при перевантаженнях і відмовах.

Мережа спеціального призначення, як і будь-яка мережа зв'язку, в технічному відношенні повинна базуватися на певній сукупності апаратно-програмних засобів і лінійних споруд, існуючих на даний момент в розпорядженні проектувальників. Вимога забезпечення максимально можливої інформаційної безпеки може змусити розробників при проектуванні МСП використовувати «старі» технології передачі інформації. В роботі [2] наведено приклад того, як на Міжнародному телекомунікаційному форумі представником розвиненою в телекомунікаційному відношенні Південної Кореї була озвучена теза про те, що мережа загального користування буде розвиватися на базі концепції NGN, а мережа для потреб державного управління - на базі технології комутації каналів. Таку заяву можна розглядати як дезінформацію для конкурентів (і потенційних супротивників), тому що в даний час існують технології, що поєднують в собі переваги технологій комутації пакетів і комутації каналів.

1.2 Технології побудови мереж спеціального призначення

VPN (Virtual Private Network) – це технологія побудови приватної мережі, що забезпечує захищений зв'язок логічної мережі поверх приватної або публічної при використанні високошвидкісного інтернету [3]. Технологія VPN будується на «віртуальному» з'єднанні, маршрутизації через інтернет з приватної мережі організації до віддаленого вузла або робочої станції

співробітника. Така організація технології передбачає установку з'єднання з особливим сервером на базі мережі загального доступу за допомогою спеціальних програм. При цьому в існуючому з'єднанні з'являється закритий від сторонніх канал обміну інформацією, створений за рахунок сучасних алгоритмів шифрування. VPN – це з'єднання за схемою «точка-точка» всередині незахищеної мережі або поверх неї, яке організовується за допомогою захищеного тунелю для обміну інформацією між користувачами і сервером. Використовуючи метод тунелювання пакети даних передаються через загальнодоступну мережу як за звичайним двоточковим з'єднанням. Між кожною парою «відправник-одержувач» встановлюється тунель – безпечне логічне з'єднання, що дозволяє інкапсулювати дані одного протоколу в пакети іншого (рис.1.1).

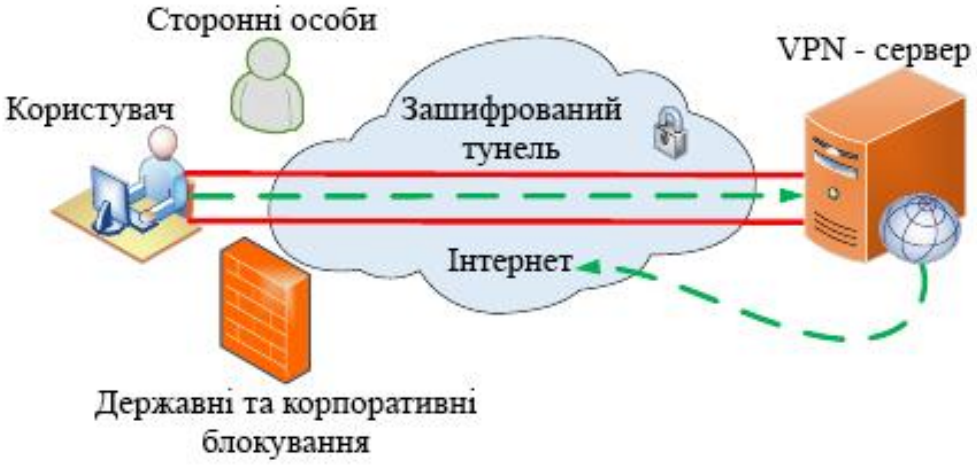

Рисунок 1.1 – Організація VPN мережі

Існує кілька видів VPN, які характеризуються на основі застосовуваних протоколів:

1) PPTP – тунельний протокол формату «точка-точка», за допомогою якого захищений канал накладається поверх звичайної мережі. З'єднання встановлюється за допомогою двох мережевих сесій: дані передаються через

PPTP по протоколу GRE, з'єднання ініціалізується та керується через порт TCP.

Таке з'єднання важко налагодити в мобільних мережах. На даний момент VPN-мережа, яка використовує такий вид протоколу, є найменш надійною. Тому застосовувати таку організацію VPN для мереж, де інформація повинна бути надійно захищена, не рекомендується.

2) L2TP – тунелювання 2-го рівня. Ця технологія являє собою покращений варіант, розроблений на основі протоколу PPTP і L2F. Такий тип тунелювання здійснюється за допомогою алгоритму шифрування IPSec, а також при об'єднанні основного і керуючого каналів в єдину сесію UDP.

Застосування такої технології є набагато безпечнішим.

3) SSTP - безпечне тунелювання сокетів на базі SSL. На базі цього протоколу створюються надійні зв'язки через HTTPS. Для працездатності протоколу потрібен відкритий 443 порт, що дозволяє налагоджувати зв'язок з будь-якої точки, навіть виходить за межі проксі [4].

VPN технологія представляє наступні можливості:

1) Використовуючи VPN реальний IP користувача змінюється на підставний, наприклад, що знаходиться за кордоном, і при використанні VPN цей користувач в мережі практично невидимий. Так, при заході на сайт або при передачі даних, видно, що IP-адреса наприклад, не з України, а з Фінляндії. Тому такому користувачеві не страшні ніякі блокування сайтів і обміну даними.

2) VPN використовує зашифроване з'єднання, при цьому ні провайдер, ні системний адміністратор мережі не дізнається з ким з'єднувався користувач. Наприклад, якщо виходити в мережу без VPN, то вся історія серфінгу по сайтах, на які заходить користувач, буде видна системному адміністратору і (або) провайдеру. При використанні VPN видно тільки те, що користувач дійсно підключений через VPN, а більше нічого не відомо. При цьому хакери при перехопленні даних не зможуть їх розпізнати через шифрування [5].

Застосовуючи спільно шифрування трафіку і підміну IP користувач стає повністю анонімним, а дані конфіденційними.

Технологія MPLS (Multiprotocol Label Switching) являє собою механізм передачі даних, який включає в себе різні властивості мереж з комутацією каналів поверх мереж з комутацією пакетів. Принцип технології полягає в спробі прискорити пересування IP-пакетів зберігаючи гнучкість IP мереж. З використанням MPLS з'являється більше можливостей для надання додаткових послуг [6]. MPLS може управляти трафіком на канальному рівні, а на мережевому рівні має властивості масштабованості і гнучкості протоколів, і тому MPLS зазвичай називають протоколом канально-мережевого рівня. Він був створений для багатофункціональної передачі даних користувачами мереж з комутацією каналів і мереж з комутацією пакетів.

Використання MPLS дає наступні можливості:

- об'єднання ATM і Frame Relay с IP;
- побудова віртуальних приватних мереж (VPN);
- прискорене транспортування пакетів всередині мережі найкоротшими стандартними маршрутами;
- вибір і пошук шляхів з урахуванням переданих даних (Traffic Engineering).

В основі роботи технології MPLS лежить передача трафіку по мережі з використанням інформації, що міститься в мітках, які приєднуються до IP пакетів. При передачі застосовуються технології другого рівня, які характеризуються передачею фреймів, при цьому мітки розташовуються між заголовками другого і третього рівня. А якщо використовувати такі технології, як ATM, засновані на передачі осередків, тоді мітки будуть знаходитися в полях ідентифікатора віртуального маршруту VPI і ідентифікатора віртуального каналу VCI.

Використання таких міток дозволяє маршрутизаторам і комутаторам, що підтримують технологію MPLS, вибрати наступний крок в маршруті пакету без виконання процедури пошуку адреси.

Технологія MPLS може бути застосована до будь-якого протоколу мережевого рівня, тобто MPLS є інкапсулює протокол, за допомогою якого можна транспортувати інформацію безлічі протоколів нижчих рівнів моделі OSI (рис. 1.2).

З рис. 1.2 випливає, що площина пересилання даних MPLS представлена в вигляді неповного рівня, яка розташовується в мережах IP, ATM або Frame Relay між другим і третім рівнями моделі OSI, але при цьому не підпорядковується цим рівнями. Таким чином, при організації MPLS одночасно на мережевому рівні і на рівні ланки даних створюється додатковий рівень, на якому відбувається комутація по мітках [7].

Рисунок 1.2 – площини MPLS

Metro Ethernet – багатофункціональна мережа великих розмірів. Ця технологія заснована на базі 1-10 гігабіт Ethernet і на мережевій архітектурі, що забезпечує швидке зростання сервісів, що вимагають великої смуги пропускання, таких як відео IP і мультимедійні додатки.

В даний час існують різні постачальники технології Metro Ethernet, що пропонують широкий спектр послуг. Тисячі абонентів користуються послугами Ethernet, та їх число з кожним днем зростає. Цих абонентів приваблюють переваги послуг Ethernet, в тому числі:

- простота використання;
- мінімальні витрати;
- гнучкість.

При розробці мереж Metro Ethernet в основі побудови лежить багаторівнева архітектура, що характеризується наступними властивостями:

- ієрархічність – представлення мережі декількома рівнями, кожен рівень відповідає за конкретні функції;
- модульність – рівні будуються на основі модулів, кожен модуль – це повноцінна функціональна одиниця, яка виконує функції відповідного рівня.

Можна виділити такі рівні архітектури мережі Metro Ethernet:

- ядро мережі – центральна частина, відповідає за високошвидкісну комутацію трафіку;
- рівень агрегації – відповідає за сполучну функцію та функцію агрегації трафіку абонентів;
- рівень доступу – являє собою функції підключення абонентів до мережі провайдера [8].

Мережі Metro Ethernet, що реалізуються у вигляді багаторівневої архітектури, забезпечують високу надійність функціонування, масштабованість і високу продуктивність.

Провайдери технології Metro Ethernet надають численні послуги для своїх клієнтів. Ця технологія пропонує великі можливості для впровадження нових послуг при появі «свіжих» сервісів, дозволяє швидко вводити їх в експлуатацію.

Корпоративні клієнти даної технології можуть отримати ряд послуг, таких як високошвидкісний доступ в інтернет, відеоспостереження, відеоконференції, послуги IP-телефонії, віртуальні приватні мережі, віддалене навчання та ін.

Так як клієнтами можуть бути державні і приватні організації, для них головним фактором у виборі технології мережі є забезпечення безпеки і конфіденційності мережі. Тому при будівництві та організації мережі Metro Ethernet провайдер повинен максимально використовувати всі засоби захисту. У сучасних пристроях для цього можуть бути використані наступні способи захисту:

- можливі списки доступу;
- використання стандарту 802.1x для аутентифікації користувачів;
- використання функції Dynamic Host Configuration Protocol (DHCP) snooping, яка дозволяє запобігти несанкціонованому доступу до мережі стороннього DHCP сервера;
- застосування численних способів для запобігання підробки MAC-адрес;
- використання різних комплексів для захисту, які розроблені виробниками (наприклад, розширення 802.1x компанії Cisco Systems і багато інших) [9].

1.3 Архітектура мереж спеціального призначення

Мережа спеціального призначення включає в себе 4 елементи:

- інформаційні пристрої, виконують функції зберігання та обробки даних, надають доступ до інформації;
- комунікаційна частина, відповідає за транспортування інформації між віддаленими пристроями, може бути реалізована у вигляді транспортної мережі і мереж доступу;
- власна інформація, представлена відеоінформацією, голосом, даними, прикладним програмним забезпеченням, за допомогою якого можна перетворювати повідомлення початкового вигляду (зображення, мова, відео) в електронний вигляд, який буде доступний для інших користувачів;
- спецкористувачі - джерела і передавачі інформації [10].

Взаємодію перерахованих елементів можна представити так, як показано на рис. 1.3.

Платформа підтримки додатків являє собою обчислювальні засоби, що працюють спільно з операційними системами і прикладним програмним забезпеченням, професійні процесори і кодеки.

В основі побудови архітектури мережі лежать транспортна мережа (зазвичай дворівнева), мережі доступу, вузли управління послугами, вузли інформаційних і телекомунікаційних служб.

В сучасних МСП дворівнева транспортна мережа є мультипротокольною і дає можливість перенесення різних видів інформації з використанням різних протоколів передачі (ATM, FR, IP-MPLS over ATM), тобто надає універсальну послугу перенесення, яка реалізує прозорість передачі інформації користувачів між мережевими закінченнями (мережами доступу) без будь-якого аналізу або обробки її змісту.

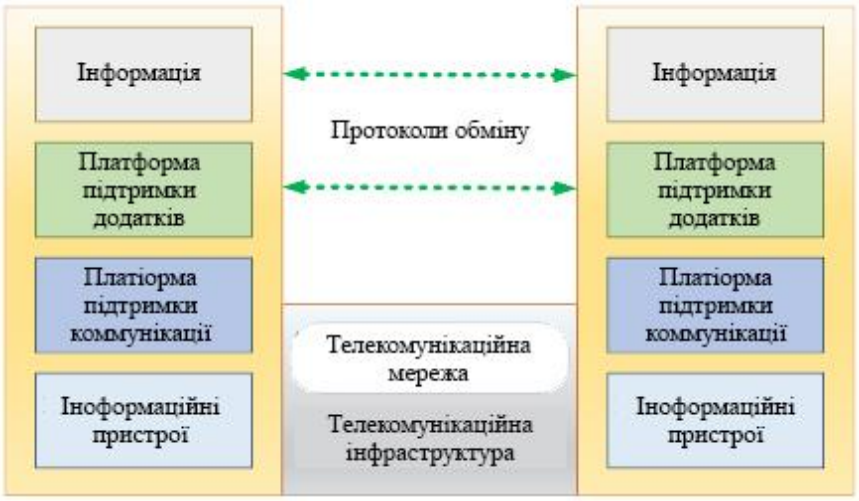

Рисунок 1.3 – Взаємодія основних елементів мережі спеціального призначення

У мережах спеціального призначення застосовується велика кількість програмно-апаратних засобів, необхідних для надання інформаційних та телекомунікаційних послуг. Ці засоби дають можливість обмінюватися даними, голосом, відео, здійснювати надання інформаційних послуг в будь-який час та з заданою якістю. За допомогою цих засобів можна також організувати кросмережеву взаємодію з користувачами інших мереж.

У мережах спеціального призначення при запиті або активізації послуги спецкористувачем, всі надані послуги характеризуються транзакціями. При санкціонованому доступі спецкористувач може отримати повне право на використання даної послуги.

Отримати доступ до послуг користувач може безпосередньо або за допомогою призначених для користувача додатків. Додатки повинні підтримуватися мережею, так, як і послуги. Зазвичай вони об'єднуються в пакети, щоб мати можливість надати для конкретного користувача необхідну послугу або дати доступ до додатка.

Сучасні мережі спеціального призначення надають великий спектр послуг, який може активно трансформуватися разом зі зміною доступних ресурсів. Для цього необхідно класифікувати певні компоненти послуг, але

при цьому кожен компонент послуги залежить від ресурсу, що використовується для її підтримки.

Загалом, МСП є поєднанням баз даних, засобів обробки інформації взаємодіючих мереж зв'язку та безлічі терміналів користувачів. При цьому доступ до інформаційних ресурсів МСП надається послугами нового типу, які отримали назву інфокомунікаційних послуг.

Інфокомунікаційні послуги МСП відрізняються від послуг традиційних мереж зв'язку технологічними особливостями побудови. Можна перерахувати такі технологічні особливості:

- інфокомунікаційні послуги відносяться до верхніх рівнів моделі взаємодії відкритих систем (ВВС), на відміну від послуг традиційних мереж, наданих на мережевому, транспортному, сеансовому і представницькому рівнях;
- інфокомунікаційні послуги припускають передачу мультимедійної інформації, для якої необхідна висока швидкість передачі і несиметричність вхідного і вихідного інформаційних потоків;
- більша частина інфокомунікаційних послуг передбачає присутність клієнтської частини і серверної; клієнтська частина реалізується в устаткуванні користувача, а серверна – в спеціально призначеному вузлі мережі, що має назву вузлом служб;
- для інфокомунікаційних послуг властиве різноманіття прикладних протоколів і можливості управління послугами з боку користувача;
- з метою надання інформаційно-комунікаційних послуг нерідко потрібні складні багатоточкові конфігурації мережевих з'єднань;
- для розпізнавання абонентів інфокомунікаційних послуг, в основному застосовується додаткова адресація в рамках даної інфокомунікаційної послуги [1].

Велика частина інфокомунікаційних послуг вважається «додатками», тобто їх працездатність розподілена поміж обладнанням «постачальника» послуги і термінальним обладнанням користувача. Тому функції термінального обладнання зобов'язані бути частиною інфокомунікаційної послуги, що слід брати до уваги при їх регламентації.

В її основі архітектури сучасної інфокомунікаційної мережі лежить універсальна транспортна мережа і мережі доступу, які функціонують на транспортному рівні та рівні управління комутацією і передачею.

Транспортна мережа містить:

- транзитні вузли, необхідні для перенесення інформації та комутації;
- кінцеві вузли, які дають можливість абонентам користуватися послугами транспортної мережі;
- контролери сигналізації, за допомогою яких відбувається обробка інформації сигналізації, регулювання викликами і з'єднаннями;
- шлюзи, необхідні для підключення традиційних мереж зв'язку;
- гнучкі багатопротокольні комутатори (softswitch).
- прикінцеві вузли транспортної мережі спеціального призначення можуть грати роль службових вузлів, таким чином вузли можуть мати розширені функції, що включають надання найпростіших телекомунікаційних послуг;
- для організації кінцевих вузлів можна застосувати технологію гнучкою комутації (softswitch), що дає можливість об'єднувати різні системи сигналізації.

Висновки до розділу 1

1. Під мережами спеціального призначення розуміється комплекс інформаційно-комунікаційних систем, що надають великий набір інформаційних і телекомунікаційних послуг з гнучким управлінням,

створення і персоналізацію нових послуг за допомогою стандартизації інформаційних і мережевих рішень, використовують універсальну транспортну мережу з розподіленою комутацією, надання інформаційних та телекомунікаційних послуг в кінцеві мережеві вузли і об'єднання з традиційними і існуючими мережами зв'язку.

2. В якості технологій побудови мереж зв'язку спеціального призначення можуть бути використані:

- технологія VPN, яка використовує протоколи тунелювання L2TP і SSTP, які дозволяють реалізовувати високий рівень безпеки сесій;
- технологія MPLS, що поєднує в собі можливості мереж, організованих за принципом «мережа з комутацією каналів поверх мережі з комутацією пакетів»;
- технологія Metro Ethernet, що дозволяє надавати послуги, які потребують великої смуги пропускання (відео по IP та мультимедійні додатки).

3. Архітектура мережі спеціального призначення характеризується чотирма елементами:

- інформаційними пристроями, які виконують функції зберігання та обробки даних, що надають доступ до інформації,
- комунікаційною частиною, що забезпечує транспортування інформації між віддаленими пристроями, яка реалізована у вигляді транспортної мережі іта мереж доступу,
- власне інформацією, яка надається відеоінформацією, голосом, даними, прикладним програмним забезпеченням, за допомогою якого можна перетворювати повідомлення початкового вигляду (зображення, мова, відео) в електронний вигляд, який буде доступний для інших користувачів;
- спецкористувачами – джерелами і передавачами інформації.

4. Інфокомунікаційні послуги МСП відрізняються від послуг традиційних мереж зв'язку технологічною побудовою. Особливості побудови:

- інфокомунікаційні послуги відносяться до верхніх рівнів моделі взаємодії відкритих систем (ВВС), на відміну від послуг традиційних мереж, які надаються на мережевому, транспортному, сеансовому і представницькому рівнях;
- інфокомунікаційні послуги припускають передачу мультимедійної інформації, для якої необхідна висока швидкість передачі і несиметричність вхідного і вихідного інформаційних потоків;
- більша частина інфокомунікаційних послуг передбачає присутність клієнтської частини і серверної; клієнтська частина реалізується в устаткуванні користувача, а серверна - в спеціально призначеному вузлі мережі, що має назву вузлом служб;
- інфокомунікаційні послуги характеризуються різноманіттям прикладних протоколів, можливістю управління послугами з боку користувача, а також складною конфігурацією мережевих з'єднань і використанням додаткової адресації для розпізнавання абонентів.

5. В якості моделі мережі спеціального призначення розглядається трьохрівнева модель, яка містить інфраструктурний, проміжний і базовий рівні, які представляють собою сукупність рівневих мереж. Кожен рівень можна розглядати як об'єднану двополюсну віртуальну мережу, відмітною ознакою якої є відсутність замкнутого внутрішнього трафіку.

2 ДОСЛІДЖЕННЯ СТАТИСТИЧНИХ ВЛАСТИВОСТЕЙ ТРАФІКУ МЕРЕЖ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

2.1 Методи аналізу статистичних властивостей трафіку

Рішення більшості завдань управління МСП, що забезпечують необхідний рівень якості функціонування інфокомунікаційної мережі, що надає комплекс необхідних інформаційних та телекомунікаційних послуг різним користувачам мережі в обов'язковому порядку вимагає формування досить суворого формалізованого опису самої МСП і процесів, що протікають в ній [11]. При цьому опис основних процесів, що відбуваються в мережі та викликають зміну її станів, має бути досить суворим і враховувати динаміку процесів.

Очевидно, основними процесами, що протікають в мережі, є процеси надходження, розподілу і перенесення інформації. Вимоги в сукупності з самою інформацією (повідомлення, дані, мова, відеоінформація, мультимедіа), що надходять від користувачів мережі на відповідні вузли МСП, утворюють термінальний потік, званий трафіком, а вся сукупність цих потоків визначає особливості мережевих інформаційних потоків в МСП, які в силу впливу цілого ряду випадкових факторів, носять явно виражений стохастичний характер.

При організації поточного управління мережі важливо вміти прогнозувати потоки інформації, що управляє і, зокрема, одну зі складових цих потоків – потоки інформації про стан МСП і її елементів (вузлів, трактів мережі, обладнання вузлів тощо). При цьому в якості математичної моделі трафіку і вузлів мережі успішно використовуються відповідні моделі систем масового обслуговування [12, 13, 14]. Обслуговування трафіку при цьому визначається відповідними параметрами, як правило, заздалегідь відомими

хоча б приблизно в частині законів розподілу випадкових значень цих параметрів.

На рис.2.1. зображено фрагмент трафіку, відображеного послідовністю пакетів, що надходять на вхід мережевого вузла,

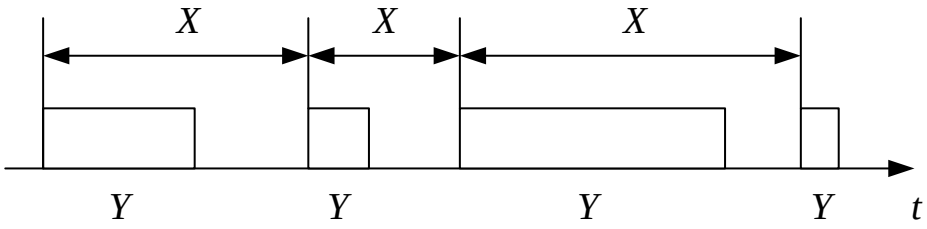

Рисунок 2.1 – Фрагмент трафіку

де *X* та *Y* – випадкові величини (з функціями розподілу *W(x)* та *W(y)*), що відображають інтервали часу між надходженням пакетів на вхід мережевого вузла та довжину пакета відповідно.

З позиції теорії масового обслуговування розподілу *W(x)* і *W(y)* визначають характеристики вузла мережі і методи розрахунку цих характеристик, серед яких найбільш важливими є середній час затримки пакета в пристрої та імовірність блокування пристрою. Слід зазначити, що класична теорія масового обслуговування передбачає незалежність елементів в послідовності *X* і *Y* [13, 15].

Найбільш простий спосіб аналізу трафіку полягає в оцінюванні кількості пакетів, які прийшли на вхід пристрою обробки, в послідовно фіксовані однакові проміжки часу. Якщо ці вимірювання відобразити в координатах «число пакетів - відліки часу», то отримана залежність буде випадковим часовим рядом (рис. 2.2), який називають трасою [14].

Чим менше вибрані для аналізу трафіку проміжки часу, тим ближче одержуваний тимчасової ряд буде до реалізації деякої випадкової функції.

На етапі початкового розвитку мереж (мала пропускна здатність, невелика кількість джерел, які одночасно посилають пакети по мережі,

відносно прості протоколи організації роботи мережі) задовільними моделями, що описують поведінку трафіку, були марковскі моделі, згідно яких випадковий час між пакетами і випадковий час обробки пакета описувалися показовими розподілами. Іншими словами, процес надходження пакетів і процес обробки пакетів володіли властивостями ординарності і відсутності післядії [15].

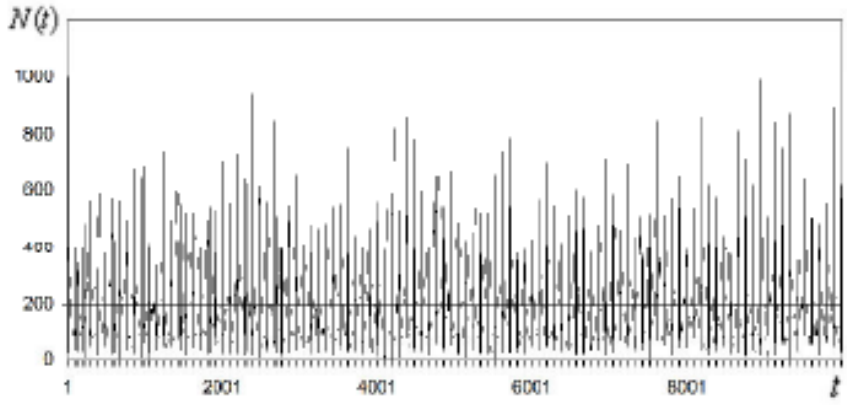

Рисунок 2.2 – Випадковий часовий ряд

По мірі розвитку мережевих технологій властивості трафіку ускладнювалися, і марковскі моделі перестали бути адекватним описом реального трафіку, тому що стали виявлятися кореляційні зв'язки інтервалів часу між пакетами, тобто коефіцієнти кореляції для сусідніх густо розташованих інтервалів часу між пакетами ставали відмінними від нуля. Аналогічні властивості стали проявлятися і для інтервалів часу обробки пакетів.

Більш того, на досить великому інтервалі часу часто відзначається деяка візуальна схожість траси з періодичним процесом. Не вдаючись в фізичні причини такої поведінки трафіку (від абсолютно випадкових на вигляд реалізацій до майже періодичних), можна сказати, що найбільш адекватною математичної теорією, яка описує реалізації трафіку, є теорія фракталів [14, 16].

Термін фрактал (від латинського слова fractus – дробовий), був запропонований американським математиком Бенуа Мандельброт в 1975 році для позначення нерегулярних самоподібних математичних структур.

Множина називається самоподібною, якщо вона складається з декількох компонент, подібних всій цій множині. Однак самоподоба – це хоча і необхідна, але далеко не достатня властивість фракталів.

Головна особливість фракталів полягає в тому, що їх співвідношення не укладається в звичні геометричні уявлення, засновані на поняттях топологічної розмірності. Тому використовується спеціальне поняття фрактальної розмірності, введене Хаусдорфом і Безіковичем [16].

Розмірність фрактальних об'єктів не є цілим числом, характерним для звичних геометричних об'єктів, і в більшості випадків фрактали нагадують об'єкти, які щільно займають реальний простір, але не використовують його повністю.

Фрактальну розмірність D зазвичай пов’язують з деяким параметром, який характеризує реалізацію часового ряду, що аналізується, та називається показником Херста:

$$H = 2 - D \tag{2.1}$$

Для гаусових розподілень часового ряду співвідношення (2.1) точне, для усіх інших розподілень – наближене.

Розрахунок показника Херста можна виконати за формулою, яка була запропонована Мандельбортом [16]:

$$\frac{R}{S} = (aN)^H \tag{2.2}$$

Звідки:

$$H = \frac{log\left(\frac{R}{S}\right)}{log\,(aN)} \tag{2.3}$$

де, R – розмах накопиченого відхилення,

S – середньоквадратичне відхилення ряду спостережень,

N – число інтервалів спостережень

a – деяка константа, $a > 0$.

$$S = \sqrt{\frac{1}{N} \cdot \sum_{i=1}^{N} \left(Y_i - Y\right)^2} \tag{2.4}$$

$$Y = \frac{1}{N} \cdot \sum_{i=1}^{N} Y_i \tag{2.5}$$

Розмах накопиченого відхилення є найбільш важливим елементом показника Херста та розраховується наступним чином:

$$R = max\left(\Delta Y_k\right) - min\left(\Delta Y_k\right) \tag{2.6}$$

де ΔY_k – накопичене відхилення ряду від середнього значення:

$$\Delta Y_k = \sum_{i=1}^{k} \left(Y_i - Y\right) \tag{2.7}$$

Відношення R/S Херст назвав нормованим розмахом.

З (2.3) при заданому N витікає:

$$log\left(\frac{R}{S}\right) = H \cdot logN + loga \tag{2.8}$$

Тому параметр H та константу a можна оцінити, зобразив графік залежності $log\ R/S$ від $log\ N$ та використовуючи отримані точки підібрати за методом найменших квадратів пряму лінію з нахилом H. Перетин отриманої прямої з осі ординат визначить значення $log\ a$. Інші методи оцінки параметра Херста наведені в [13].

Величина параметра Херста, який може приймати значення в інтервалі [0,1], говорить про наступне [15]:

1. Якщо $H = 0{,}5$, то досліджуваний часовий ряд є «броуновським рухом», відліки незалежні та мають гаусівське розподілення. Можна сказати, що в даному випадку попередні відліки часового ряду не впливають на наступні відліки.
2. Якщо $0 < H < 0{,}5$, то проявляється тенденція «повернення до середнього». Тобто кожен наступний відлік прагне бути протилежним попередньому. При цьому вважається, що часовий ряд зашумлений.
3. Якщо $H > 0{,}5$, то відліки не є незалежними. Попередні відліки впливають на наступні тим сильніше, чим більше H відрізняється від $0{,}5$. Виникає довгострокова пам’ять, при котрій простежується сильний вплив відліків один на одного.

Виходячи з цього, часовий ряд (рис. 2.2), що характеризує трафік в мережі, може мати фрактальні властивості.

Для використання методів класичної теорії масового обслуговування під час аналізу характеристик мережевих вузлів необхідно врахувати зв’язок самоподібних властивостей випадкового процесу з характеристиками часових інтервалів, зображених на рис. 2.1.

Розглянемо випадковий часовий ряд $X(t)$, що вимірюється в пакетах або байтах в момент часу t. Ряд $X(t)$ вважається стаціонарним в широкому смислі з кореляційною функцією $B(\tau)=B(|t_1-t_2|)$, де

$$B(t_1, t_2) = E\left[\left(X(t_1) - m\right) - X(t_2) - m\right] \quad (2.9)$$

де $m = E(X(t))$,

$\sigma^2 = B(0) = E(X(t) - m)^2$

Випадковий процес *X(t)* є строго самоподібним другого порядку з показником Херста $0 < H < 0{,}5$, якщо:

$$B(k) = \frac{\sigma^2}{2}\left[(k-1)^{2H} - 2k^{2H} + (k+1)^{2H}\right] \quad (2.10)$$

Самоподібність другого порядку означає, що кореляційна функція зберігає свій вид під час об'єднання часового ряду. При цьому початковий та об'єднаний ряди мають однакові розподілення ймовірностей.

Виходячи з вищесказаного можна охарактеризувати властивості самоподібного часового ряду:

1. Якщо $H > 0{,}5$, то відліки взаємозалежні, що спричиняє появу пам'яті процесу. При цьому кореляційна функція стає затухаючою та її можна апроксимувати наступним виразом:

$$B(k) = k^{2H-2} \cdot L(k) \quad (2.11)$$

де *L(k)* – повільно змінювана функція.

Можна показати, що довготривала залежність є причиною піковості трафіку, коли під час довгого проміжку часу швидкість надходження пакетів на мережевий вузол дорівнює пропускній спроможності каналу. Це може призвести до переповнення буферу пристрою, втраті пакетів та до затримки пакета на пристрої обробки [17].

2. Дисперсія вибраного середнього затухає повільніше, ніж величина, зворотна розміру вибірки *n*.

Для звичайного (не самоподібного) процесу $Z(t)$ дисперсія вибірки розміром n визначається як $\sigma^2(Z_i^{(n)}) = \sigma^2 n^{-1}$ для будь-якого i. Для вибірки самоподібного процесу $Y(t)$ дисперсія $\sigma^2(Y_i^{(n)})$ пропорційна $n^{(2H-2)}$ при $n \to \infty$. Це свідчить про те, що статистичні характеристики будь-якої вибірки будуть сходитися тим повільніше, чим ближче буде параметр H до 1.

2.2 Аналіз часу очікування заявки в черзі для системи масового обслуговування загального вигляду

Система масового обслуговування загального виду з одним обслуговуючим пристроєм в визначенні Кендалла представляється як *G/G/1*, при цьому перша позиція характеризує розподілення інтервалів часу між заявками, які поступають на обслуговування, а друга позиція визначає розподілення інтервалів часу обслуговування заявок. Для систем загального виду обидва розподілення довільні. Єдине обмеження, яке накладає класична теорія масового обслуговування, полягає в тому, що елементи обох послідовностей мають бути незалежні один від одного.

При цьому одна з найважливіших характеристик системи, середній час перебування заявки у черзі, може бути визначена шляхом вирішення рівняння Ліндлі [13], яке можна записати в вигляді:

$$W(x) = \int_0^{\infty} K(x - y(y))\, dW \qquad (2.12)$$

В даному записі W – інтегральна функція розподілення часу очікування заявки в черзі, функція K – ядро рівняння, яке записується як:

$$K(z) = \int_0^\infty B(z + x)\, a(x)\, dx \tag{2.13}$$

де B – інтегральна функція розподілення інтервалів часу обслуговування, a – диференціальна функція розподілення інтервалів між заявками, що поступають на обслуговування.

В роботі [13] наведено спектральний метод вирішення (2.12), який в якості першого кроку передбачає знаходження перетворення Лапласа *b(s)* та *a(s)* для диференційних функцій розподілення b та a інтервалів часу обслуговування заявок та інтервалів часу між надходженням заявок відповідно. Далі для виразу *a(-s)b(s)-1* необхідно знайти представлення:

$$a(-s)\, b(s) - 1 = \frac{\psi\,(s)}{\psi_{-}\,(s)} \tag{2.14}$$

в якому для функції в правій частині виразу повинні виконуватися наступні умови:

- функція $\psi_+(s)$ є аналітичною без нулів в області $Re(s)>0$;
- функція $\psi_-(s)$ є аналітичною без нулів в області $Re(s)<D$ при $D>0$;

Останньою операцією спектрального методу є визначення перетворення Лапласа $\Phi_+(s)$ функції, що відповідає відповідній густині розподілення $W(x)$ часу очікування в черзі:

$$\Phi\,(s) = \frac{\Delta}{\psi\,(s)} \tag{2.15}$$

де константа Δ визначається як:

$$\Delta = \lim_{s \to 0} \frac{\psi\,(s)}{s} \tag{2.16}$$

Відповідно перетворення Лапласа функції *W(x)* записується у вигляді:

$$W(s) = s \cdot \Phi(s) \tag{2.17}$$

В загальному вигляді наведений метод вирішення інтегрального рівняння Ліндлі для системи масового обслуговування типу *G/G/1* можна застосувати якщо для густини ймовірностей *a(τ)* та *b(τ)* використовувати апроксимацію сумою затухаючих експонент в вигляді [18]:

$$a(\tau) = \sum_{k=1}^{n} \left(a_k \cdot e^{-a_k \cdot \tau} \right) \qquad b(\tau) = \sum_{k=1}^{n} \left(b_k \cdot e^{-\beta_k \cdot \tau} \right)$$

що, відповідно, дозволить функції *a(s)* та *b(s)* представити в вигляді:

$$a(s) = \sum_{k=1}^{n} \frac{a_k}{s + a_k} \qquad b(s) = \sum_{k=1}^{n} \frac{b_k}{s + \beta_k}$$

та далі згідно (2.15) та (2.17):

$$W(s) = s\Phi(s) = \frac{s\Delta}{\psi(s)} = \frac{s\Delta \left(s - s_{i1}\right)\left(s - s_{i2}\right)\ldots\left(s - s_{ip}\right)}{\left(s - s_{j1}\right)\left(s - s_{j2}\right)\ldots\left(s - s_{jp}\right)}$$

де в загальному випадку *r* та *p* не перевищують *n+l*.

За знайденим розподіленням *W(x)* можна обчислити середній час очікування пакету в черзі як:

$$T_{cð} = \int_0^{\infty} x(x)\, dW$$

або скориставшись знанням характеристичної функції *W(s)*:

$$T_{cð} = -\frac{d}{ds} W(s) \qquad (2.18)$$

Часто при аналізі характеристики системи *G/G/1* використовується апроксимація $H_2/H_2/1$, яка дозволяє достатньо просто вирішити рівняння Ліндлі спектральним методом.

При аналізі трафіку з явно вираженими кореляційними властивостями послідовностей інтервалів часу обслуговування та інтервалів між заявками апроксимація $H_2/H_2/1$ також може бути використана, однак апроксимуючі послідовності з гіперекспоненціальним розподіленням H_2 має мати статистичні характеристики, які враховують кореляційні властивості початкових послідовностей таким чином, щоб залишились справедливими умови інтегрального рівняння Ліндлі для аналізу системи масового обслуговування.

2.3 Аналіз часу очікування заявки в черзі під час обробки корельованого трафіку

Аналіз корельованого трафіку, який обробляється системою масового обслуговування *G/G/1* можна провести з використанням інтегрального рівняння Ліндлі, якщо підібрати відповідні статистичні апроксимації потоків інтервалів часу між заявками та інтервалів часу обслуговування заявок. Апроксимуючі потоки називають оновлюючими потоками [17, 19-81, 23, 24]. Зазвичай використовують оновлюючі потоки з гіперекспоненціальним розподіленням миттєвих значень інтервалів часу (H_2) та потоки Ерланга.

2.3.1 Потоки з гіперекспонеціальним розподілом

Під оновлюючим процесом H мається на увазі процес, для якого $m_H=m_x$ та квадрат коефіцієнту варіації дорівнює індексу дисперсії початкового потоку, тобто $C^2_H=I_x$.

В роботі [21] показано, що для будь-якого оновлюючого процесу C^2_H можна відобразити у вигляді:

$$C_H^{\,2} = 1 + 2A_H \tag{2.19}$$

Якщо в якості оновлюючого процесу обирається сукупність з ймовірностями p та $(1-p)$ двох пуасоновських процесів з інтенисвностями γ_1 та γ_2, яка призводить до гіперекпоненціального розподілення зі щільністю:

$$w_H(\tau) = p \cdot \gamma_1 \cdot e^{-\gamma_1 \cdot \tau} + (1-p) \cdot \gamma_2 \cdot e^{-\gamma_2 \cdot \tau} \tag{2.20}$$

то перетворення Лапласа щільності ймовірностей розподілення H_2 буде мати вигляд:

$$w_H(s) = \frac{p \cdot \gamma_1}{\gamma_1 + s} + \frac{(1-p) \cdot \gamma_2}{\gamma_2 + s} \tag{2.21}$$

В роботі [21] показано, що параметри оновлюючого процесу мають бути визначені як:

$$\gamma_1 = \frac{1}{2}\left[\lambda_x + \alpha_H\left(1 + A_H\right) + \sqrt{\left(\lambda_x + a_H\left(1 + A_H\right)\right)^2 - 4 \cdot \lambda_x \cdot \alpha_H}\right]$$
$$\gamma_2 = \lambda_x + \alpha_H\left(1 + A_H\right) - \gamma_1 \tag{2.22}$$
$$p = \frac{\lambda_x + \alpha_H \cdot A_H - \gamma_2}{\left|\gamma_1 - \gamma_2\right|}$$

В виразах (2.22) присутні параметри A_H та a_H, які визначають властивості оновлюючого процесу. Встановити значення цих параметрів достатньо складно [17].

Функція піковості оцінює вплив потоку заявок з інтервалами часу між заявками на систему обслуговування, яка складається з безкінечного числа незалежних обслуговуючих пристроїв, кожен з яких має однакову інтенсивність обслуговування μ_B та розподіл часу обслуговування B. В роботі [23] показано, що у випадку коли B є показовим розподілом ймовірності з параметром μ_B, граничне значення функції $z_x(B)$ досягається при $\mu_B \to 0$ та може бути представлено у вигляді:

$$z_{xmax} = \frac{1 + C_x^2}{2} + C_x^2 \cdot \sum_{i=2}^{\infty} R_x(i) \qquad (2.23)$$

З іншої сторони у роботі [17] показано, що:

$$A_H = z_{xmax} - 1 \qquad (2.24)$$

Прирівнюючи z_{xmax} та z_{Hmax} можна визначити параметр A_H у вигляді:

$$A_H = \frac{C_x^2 - 1}{2} + C_x^2 \cdot \sum_{i=2}^{\infty} R_x(i) \qquad (2.25)$$

Для визначення параметра a_H припустимо, що щільність ймовірностей процесу H_2 та двофазного процесу, який складається з двох експоненціальних станів з інтенсивностями γ_1 та γ_2 та ймовірністю переходу p з одного стану в інший. Тоді згідно [17] можна записати:

$$\alpha_H = \frac{2\lambda_x}{2 \cdot A_H + 1} \qquad (2.26)$$

Отриманий набір параметрів дозволяє однозначно синтезувати щільність розподілення H_2.

2.3.2 Потоки з розподілом Ерланга

Для побудови оновлюючого процесу можна обрати сукупність не тільки двох пуасоновських процесів, що призводить до використання гіперекспоненціального розподілення H_2, але і сукупність процесів, миттєві значення яких підкорюються розподіленню Ерланга [19]. В роботі [22] показано, що необхідність такої апроксимації виникає коли для корельованого потоку значення індексу дисперсії може виявитися менше *0,5* *(I_x<0,5)*.

Розподілення Ерланга записується як:

$$w(x) = \frac{\lambda\,(\lambda x)^{k-1}}{(k-1)!} \qquad (2.27)$$

та параметри розподілення мають значення: $m_x=k/\lambda$, $\sigma^2_x=k/\lambda^2$. Розподілення Ерланга характеризує суму k незалежних випадкових величин, кожна з яких має експоненціальне розподілення з параметром λ. Графіки розподілення Ерланга наведені на рис. 2.3. Розподілення Ерланга співпадає з гама-розподіленням під час вибору параметра гама-розподілення у вигляді цілого числа.

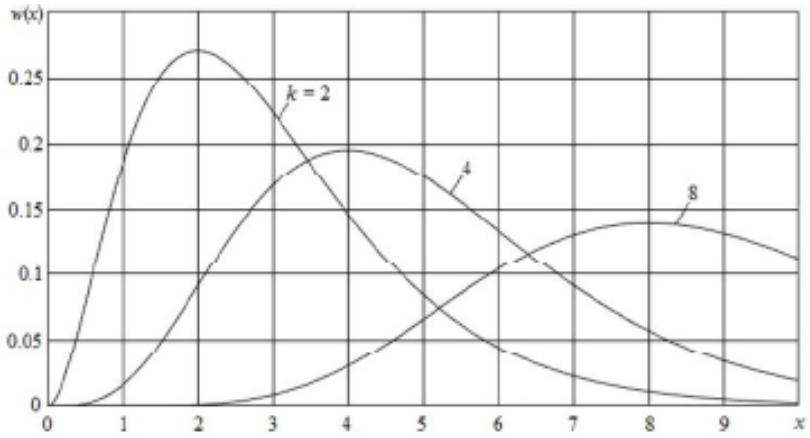

Рисунок 2.3 – Графіки розподілення Ерланга

Припустимо, що інтервали часу в оновлюючому процесі H, мають розподілення, яке визначається сукупністю розподілення Ерланга порядку k та експоненціального розподілення з параметром λ. Ваговим параметром під час реалізації сукупності є параметр, який позначено θ. Перетворення Лапласа від такої щільності ймовірностей має вигляд:

$$w_H(s) = \theta\left(\frac{\lambda}{\lambda + s}\right)^k + (1-\theta)\frac{\lambda}{\lambda + s} \tag{2.28}$$

Якщо прирівняти m_x до m_H та розрахувати m_2 (другий момент для X), то для фіксованого k можна записати:

$$m_H = m_x = \frac{\theta k + (1-\theta)}{\lambda} \tag{2.29}$$

$$m_2 = m_x^2\left(I_x + 1\right) = \frac{\theta k + (k+1) + 2(1-\theta)}{\lambda^2} \tag{2.30}$$

Тепер можна отримати два рівняння з двома невідомими для визначення λ та θ.

$$\lambda = \lambda_x[\theta k + (1-\theta)] \tag{2.31}$$

$$\theta = \frac{-\left[2\left(I_x + 1\right) - k(k+1) + 2\right] + \sqrt{\left[2\left(I_x + 1\right) - k(k+1) + 2\right]^2 - 4\left(I_x{}^2 - 1\right)(k-1)^2}}{2\left(I_x + 1\right)(k-1)^2} \quad (2.32)$$

з яких видно, що $\lambda \neq \lambda_H = \lambda_x$.

Якщо значення k невідомо, то його вибір, як показано в [19], може бути виконано шляхом вирішення задачі мінімізації середньоквадратичного відхилення. Вирішення задачі мінімізації виконується підбором параметрів λ та θ, після чого зі співвідношення (2.31) може бути знайдено значення k.

Висновки до розділу 2

1. Розглянуто методи аналізу статистичних властивостей трафіку. Показано, що адекватний опис трафіку, як випадкового процесу, сучасних (і проектованих) МСП може бути дано із застосуванням методів теорії фракталів з використанням самоподібних випадкових процесів. Введення в розгляд поняття «параметр Херста» дозволило класифікувати залежність відліків тимчасового ряду, що описує мережевий трафік.

2. Встановлено взаємозв'язок моделей трафіку, заснованих на заданні виду розподілу ймовірностей для випадкових величин, суть яких – інтервали часу між надходження на вхід мережевого вузла пакетів, з моделями у вигляді тимчасового ряду, тобто кількістю пакетів в одиницю часу. Дано опис властивостей самоподібного трафіку, що володіє вираженими кореляційними

властивостями, з використанням понять «індекс дисперсії інтервалів часу між подіями» і «індекс дисперсії числа подій». Показано, що обчислення часу очікування пакета в черзі вузла МСП при довільних розподілах ймовірностей інтервалів часу між пакетами і інтервалів обслуговування пакетів за умови їх незалежності може бути проведено на основі рішення інтегрального рівняння

Ліндлі. Наведено алгоритм вирішення рівняння Ліндлі спектральним методом. Обґрунтовано доцільність використання апроксимацій розглянутих розподілів ймовірностей сумами згасаючих експонент, зокрема – гіперекспоненціальними розподілами.

3. Наведено детальний аналіз часу очікування пакета в черзі при обробці корельованого трафіку. Розглянуто поняття оновлюючого випадкового процесу (потоку) з гіперекспоненціальним розподілом миттєвих значень, що дозволяє врахувати кореляційні властивості реального трафіку, що дозволило використовувати для аналізу часу очікування пакета в черзі рівняння Ліндлі. Показано важливу роль індексу дисперсії в формуванні оновлюючого потоку. Наведено необхідні розрахункові формули для отримання чисельного значення середнього часу очікування пакета в черзі.

4. Запропоновано апроксимація розглянутих розподілів ймовірностей корельованих тимчасових інтервалів, яка заснована на використанні розподілу Ерланга.

3 АНАЛІЗ ФУНКЦІОНУВАННЯ ВУЗЛА МЕРЕЖІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

3.1 Загальне вирішення задачі оцінювання середнього часу очікування заявки в черзі для системи G/G/1

У розділі 2 було показано, що трафік сучасних мереж, особливо на рівні доступу, володіє самоподібними властивостями, що характеризується яскраво
вираженими кореляційними зв'язками часових параметрів трафіку. Якщо такі тимчасові параметри як інтервали часу між заявками на обслуговування і інтервали часу обслуговування заявок незалежні, то аналіз роботи вузла мережі можна провести моделюючи його як систему масового обслуговування загального вигляду (*G/G/1*). При цьому одна з найбільш істотних характеристик роботи вузла – час очікування заявки в черзі, може бути отримана з вирішення інтегрального рівняння Ліндлі [13].

Одним з методів, що дозволяють врахувати невизначеність знання щодо параметрів розподілів, є інтервальний підхід [25, 26], при якому невизначені параметри задаються діапазоном своїх можливих значень. Ефективність такого підходу для аналізу марковської системи *M/M/1* продемонстрована в роботі [25]. При аналізі системи *G/G/1* будемо слідувати роботам [27, 28].

Розглянемо систему *G/G/1* з дисципліною обслуговування *FIFO*, в якій для визначеності використовуємо розподіл Парето (для значень інтервалів часу між заявками) і розподіл Вейбулла (для значень інтервалів часу обслуговування заявок). Таку систему можна позначити як *P/W/1*, маючи на увазі, що *P* означає розподіл Парето, а *W* - розподіл Вейбулла.

Запишемо дані розподілення у вигляді:

$$f_p(x) = \frac{\beta k^{\beta}}{x^{\beta+1}}, x \geq k \tag{3.1}$$

$$f_w(x) = \frac{\alpha}{\lambda} \cdot \left(\frac{x}{\lambda}\right)^{\alpha-1} e^{-\left(\frac{x}{\lambda}\right)^{\alpha}}, x \geq 0 \tag{3.2}$$

Припустимо, що $k=1$, $\lambda=1$, а параметр β відомий приблизно в деяких межах $[a,b]$. Найбільша невизначеність відносно параметра β буде характеризуватися рівномірною щільністю ймовірностей:

$$f(\beta) = \frac{1}{b-a} \tag{3.3}$$

Тому безумовна щільність ймовірностей для розподілення Парето буде мати вигляд:

$$f_{p'}(x) = \int_a^b f_p(x) \cdot f(\beta)\, d\beta = \frac{1}{b-a} \cdot \int_a^b \frac{\beta}{x^{\beta+1}}\, d\beta \tag{3.4}$$

Інтегруючи по частинам отримуємо:

$$f_{p'}(x) = \frac{1}{(b-a) \cdot (lnx)^2} \cdot \left[x^{-a-1} \cdot (1 + a \cdot lnx) - x^{-b-1} \cdot (1 + b \cdot lnx)\right] \tag{3.5}$$

Графік щільності при значеннях $a=1$, $b=3$ наведено на рис. 3.1.

Аналогічний результат можна отримати якщо припустити що параметр β з однаковою ймовірністю приймає значення $\beta=1,2,3$. При цьому, якщо з (3.1) позначити $f_p(x, \beta)=f_p(x)$, то замість (3.4) можна записати:

$$f_{p'}(x) = \sum_{i=1}^{n} \left(f_p\left(x, \beta_i\right) \cdot P\left(\beta_i\right) \right) = \frac{1}{N} \cdot \sum_{i=1}^{N} f_p\left(x, \beta_i\right) \qquad (3.6)$$

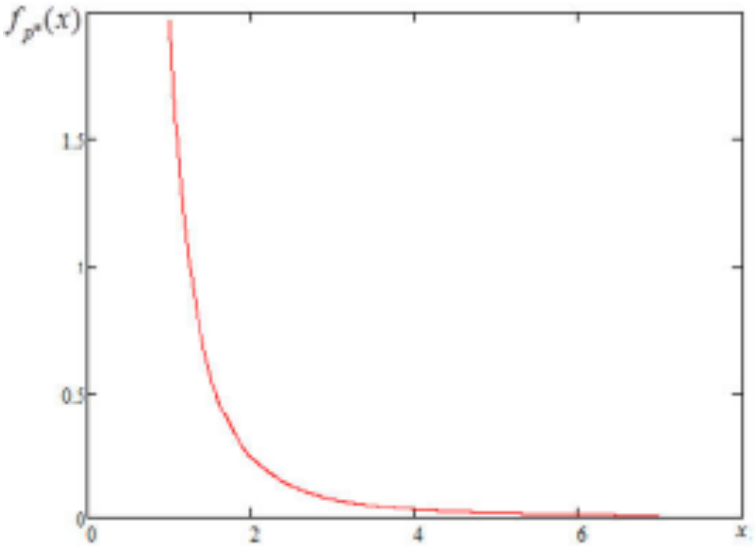

Рисунок 3.1 – Розподіл $f_{p*}(x)$

Аналогічно можна записати рівняння для розподілу Вейбулла:

$$f_{w'}(x) = \frac{1}{4} \cdot \left(e^{-x} + 2x \cdot e^{-x^2} + 3 \cdot x^2 \cdot e^{-x^3} + 4 \cdot x^3 \cdot e^{-x^4} \right) \qquad (3.7)$$

Графік щільності $f_{w*}(x)$, який побудовано згідно (3.7), наведено на рис 3.2.

Припустимо, що отримані необхідні апроксимації щільності $f_{p*}(x)$ та $f_{w*}(x)$ у вигляді:

$$f_{p'}(x) = \sum_{k=1}^{n} \left(p_k \cdot e^{-q_k \cdot x} \right) \qquad f_{w'}(x) = \sum_{k=1}^{l} \left(g_k \cdot e^{-h_k \cdot x} \right) \qquad (3.8)$$

де p_i, q_i, g_i, h_i – коефіцієнти апроксимації.

Тоді:

$$a(s) = \sum_{k=1}^{n} \frac{p_k}{s + q_k} \qquad b(s) = \sum_{k=1}^{l} \frac{g_k}{s + h_k} \tag{3.9}$$

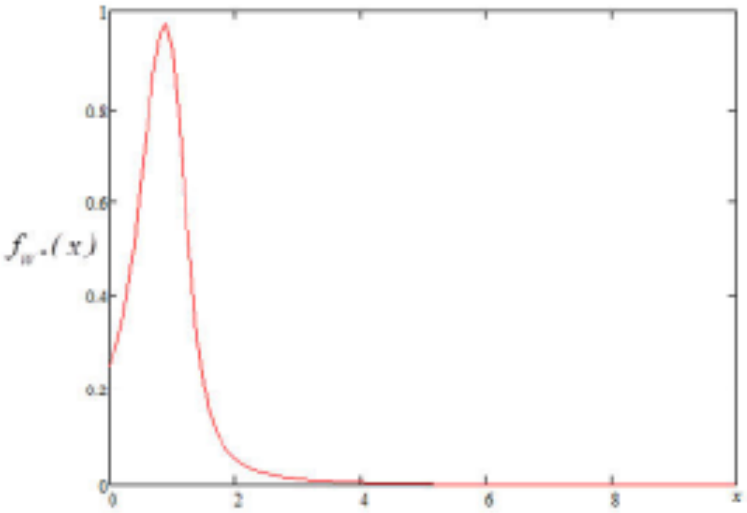

Рисунок 3.2 – Розподіл $f_{w^*}(x)$

Функція $\psi(s)$ відіграє ключову роль у визначенні часу очікування заявки в черзі, тому що через неї виражається перетворення Лапласа щільності ймовірностей питомого часу очікування. Характеристична функція при цьому, як показано в [29], записується у вигляді:

$$F(s) = \frac{K \cdot s(s - s_{i1})(s - s_{i2}) \ldots (s - s_{ir})}{(s - s_{j1})(s - s_{j2}) \ldots (s - s_{jz})} \tag{3.10}$$

Визначивши нулі та полюси функції $\psi(s)$ можна знайти характеристичну функцію часу очікування $F(s)$ при будь-яких значеннях n та l. Середній час очікування заявки у черзі може бути визначено за формулою (3.11).

$$T_{c\delta} = -\frac{d}{ds}F(s) \qquad (3.11)$$

Отже, завдання аналізу характеристик мережевого вузла, що моделюється системою масового обслуговування загального вигляду, може бути вирішена на основі інтервального підходу. Застосовуючи апроксимацію, використовуваних для опису роботи вузла мережі щільності ймовірностей, рядами згасаючих експонент, можна, вирішуючи рівняння Ліндлі спектральним методом, визначити один з найважливіших параметрів вузла мережі – час очікування заявки в черзі, при будь-яких імовірнісних властивостях оброблюваного трафіку.

3.2 Аналіз характеристик системи масового обслуговування загального виду методом рандомізації

Використаємо поняття оновлюючого процесу, введене в попередніх розділах, для аналізу показників системи загального вигляду методом рандомізації [30, 31].

В якості оновлюючого процесу використовується модель випадкового потоку що відображає статистичні властивості вихідного потоку. Дана модель, яка надається так званим узагальненим (рандомізованим) пуассоновим потоком (УПП), параметр якого є випадковою величиною з деякою функцією розподілу, описує ситуацію невизначеності параметрів вихідного потоку.

Для розгляду розподілу ймовірностей подій УПП, можна використати формулу (3.12) [4].

Вперше на можливість використання даного підходу для моделювання залежності між подіями не тільки всередині будь-якого інтервалу, а й між інтервалами, а також групування подій в пачки, вказав А.Я. Хинчин [32]. У

роботах [30, 31] наведені конкретні результати, отримані з використанням моделі (3.12).

$$\Omega\left(\vec{t},\vec{k}\right) = \int_0^{\infty} \prod_{i=1}^{n} \left(\frac{\lambda t_i^{k_i}}{k_i!} \cdot e^{-\lambda t_i} \right) dF \qquad (3.12)$$

де $F(\lambda)$ – функція розподілення випадкового параметра початкового пуассонового потоку.

Для окремого випадку гіперболічного розподілу числа подій на одному фіксованому інтервалі t, вираз (3.12) має вигляд:

$$\Omega_0(t) = \left(\frac{a}{a+t} \right)^{v} \qquad (3.13)$$

З використанням результатів роботи [32] в [31] показано, що функція розподілення інтервалів між подіями потоку може бути представлена у вигляді:

$$f(t) = \left(\frac{a}{a+t} \right)^{v+1} \qquad (3.14)$$

де a та v – параметри потоку подій.

Розглянемо деяку початкову систему з фіксованими параметрами. Замінимо початкову систему моделлю, функціонування якої залежить від деякого випадкового параметру a з відповідною функцією розподілу. При цьому робиться припущення, що модель відповідає виразу (3.12), тобто трафік що поступає на обробку замінюється рандомізованим пуассоновим потоком.

Позначимо для початкової системи через $q_i`(a)$ ймовірність того, що в момент надходження заявки на обробку в системі знаходиться i заявок. В роботі [30] показано, що для такої системи відповідні ймовірності визначаються виразом (3.15).

$$q_i = q_0 \cdot \int_{Z_a} \frac{q'_i(a)}{q'_0(a)}\, dF \qquad (3.15)$$

де Z_a – область визначення параметра a,

$F(a)$ – функція розподілу параметра a.

Значення q_0 в (3.15) визначається виходячи з умови нормування.

Формула (3.15) дозволяє отримати розподіл досліджуваної системи, якщо відомі розподіли ймовірностей станів початкової системи та функція розподілу випадкового параметра $F(a)$.

Розглянемо в якості прикладу систему $M/M/n$ з розміром буфера k. Якщо в якості випадкового параметра a взяти коефіцієнт завантаженості системи p, то можна отримати вираз для знаходження розподілу ймовірностей станів системи [13]:

$$q'_i(\alpha) = \begin{cases} \dfrac{\alpha^i}{i! \cdot q'_0(a)}, 0 \le i \le n \\ \dfrac{\alpha^i}{n! \cdot n^{i-n} \cdot q'_0(a)}, n \le i \le n+k \end{cases} \qquad (3.16)$$

Припустимо що випадковим є тільки параметр потоку, а час обслуговування залишається константою. Тоді з (3.15) та (3.16) отримуємо:

$$q_i = \begin{cases} \dfrac{q_0 \cdot \rho^{\,i} \cdot \Gamma(\nu + i)}{\Gamma(\nu)}, 0 \le i \le n \\ \dfrac{q_0 \cdot \rho^{\,i} \cdot \Gamma(\nu + i)}{n! \cdot n^{i-n} \cdot \Gamma(\nu)}, n \le i \le n + k \end{cases} \tag{3.17}$$

Якщо в системі один обслуговуючий пристрій *(n=1)*, то виходячи з (3.17) отримуємо:

$$q_{1+k} = \frac{\rho^{\,1+k} \cdot \Gamma(\nu + k)}{\Gamma(\nu) \cdot \left[\sum_{i=0}^{k+1} \frac{\left(\rho^{\,i} \cdot \Gamma(\nu + i) \right)}{\Gamma(\nu)} \right]^{-1}} \tag{3.18}$$

Формула (3.18) визначає ймовірність блокування системи, тобто характеризує ситуацію, коли заявка, що надійшла, отримує відмову в обслуговуванні.

З (3.17), для випадку коли $\nu = 1$ та $\Gamma(i+1) = i!$ можна записати (3.19) та якщо в (3.19) $n=1$, то отримуємо (3.20).

$$q_i = \begin{cases} i! \cdot \rho^{\,i} \cdot q_0, 0 \le i \le n \\ \dfrac{i! \cdot \rho^{\,i} \cdot q_0}{n! \cdot n^{i-n}}, n \le i \le n + k \end{cases} \tag{3.19}$$

$$q_i = \frac{i! \cdot \rho^{\,i}}{\sum_{j=0}^{k+1} \left(j! \, \rho^{\,j} \right)} \tag{3.20}$$

Для порівняння значення ймовірності блокування для класичної системи *M/D/1* з розміром буфера *k*:

$$P_{бл} = q'_{k+1} = \frac{\rho^{1+k}}{\sum_{i=0}^{k+1} \rho^{i}} \qquad (3.21)$$

Виходячи з розрахункових співвідношень можна порівняти ймовірність блокування для системи *M/D/1* та системи *G/D/1*. При цьому мається на увазі, що інтенсивність пуассонового потоку в системі *G/D/1* на кожному інтервалі між заявками приймає випадкове значення. Нижче наведені таблиці для ймовірностей блокування систем *M/D/1* та *G/D/1* при різних *p.*

Таблиця 3.1 – Ймовірність блокування при *p=0.25*

Система	*k*							
	0	1	2	3	4	5	6	7
G/D/1	0.200	0.091	0.064	0.060	0.069	0.094	0.142	0.222
M/D/1	0.200	0.048	0.012	0.002	0.001	0.000	0.000	0.000

Таблиця 3.2 – Ймовірність блокування при *p=0.3*

Система	*k*							
	0	1	2	3	4	5	6	7
G/D/1	0.231	0.122	0.099	0.106	0.064	0.108	0.293	0.413
M/D/1	0.231	0.065	0.019	0.006	0.002	0.000	0.000	0.000

Таблиця 3.3 – Ймовірність блокування при *p=0.5*

Система	*k*							
	0	1	2	3	4	5	6	7
G/D/1	0.333	0.250	0.273	0.353	0.469	0.584	0.672	0.713
M/D/1	0.333	0.143	0.067	0.032	0.016	0.008	0.004	0.002

Для значень *p=0.3* та *p=0.5* на рис. 3.3 наведено графіки залежності ймовірності блокування в залежності від довжини черги.

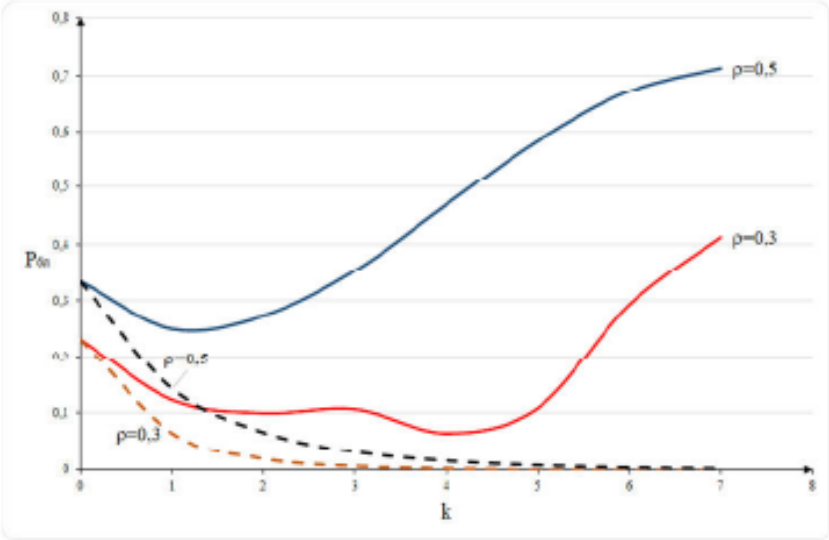

Рисунок 3.3 – Залежність $P_{бл}(k)$

З використанням (3.12) можна визначити вплив статичних зв'язків інтервалів часу обробки заявки в системі *M/M/1* на розмір черги при необмеженому розмірі вхідного буфера.

Нехай на вході системи *M/M/1* діє пуассоновий потік з параметром інтенсивності λ. Час обслуговування заявки τ є випадковою величиною з показовим законом розподілу та кожне випадкове значення τ реалізується так, що сума ймовірностей дорівнює 1. Таке припущення призводить до того, що розподілення часу обслуговування стає гіперекспоненційним.

Модель системи *M/M/1* [15, 31]:

$$q_i = q_0 \cdot \sum_{j=1}^{k} \left(p_j \cdot \rho_j{}^i\right), \rho_j = \lambda \cdot \tau_j$$

$$q_0 = \frac{1}{\sum_{j=1}^{k} \frac{p_j}{1-\rho_j}} \qquad (3.22)$$

Середня кількість заявок в системі:

$$E(i) = \sum_{i=0}^{\infty} iq_i = q_0 \cdot \sum_{j=1}^{k} \left[\frac{p_j \cdot \rho_j}{\left(1 - \rho_j\right)^2} \right] \qquad (3.23)$$

Для $k=2$ з (3.23) отримуємо:

$$i = \left(\frac{p_1}{1 - \rho_1} + \frac{p_2}{1 - \rho_2} \right)^{-1} \cdot \left[\frac{p_1 \cdot \rho_1}{\left(1 - \rho_1\right)^2} + \frac{p_2 \cdot \rho_2}{\left(1 - \rho_2\right)^2} \right] \qquad (3.24)$$

Згідно даної моделі формула (3.24) визначає середнє число заявок в системі, в якій інтервали часу обробки заявок не є незалежними.

Як об'єкт порівняння виберемо систему *M/G/1* з нескінченною чергою, в якій інтервали обслуговування заявок є послідовністю незалежних величин з гіперекспоненційним розподілом.

Середня кількість заявок в системі *M/G/1* визначається формулою Поллячека–Хинчина [13], в якій ключову роль відіграє значення другого моменту розподілу часу обслуговування. Використовуючи дану формулу спільно з останнім записом гіперекспоненційного розподілу, можна отримати:

$$i_H = \frac{\rho + p_1 \cdot p_2 \left(\rho_1 - \rho_2\right)^2}{1 - \rho} \qquad (3.25)$$

В таблиці 3.4. наведені результати розрахунків, які відносяться до системи *M/M/1*.

На рис. 3.4 показані графіки $i_H(\rho)$ та $i_M(\rho)$. Як видно з графіків, криві $i_H(\rho)$ та $i_M(\rho)$ практично зливаються одна з одною та знаходяться нижче $i(\rho)$, яка характеризує систему що аналізується.

Таблиця 3.4 – Середня довжина черги

	ρ							
	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8
i	0.170	0.273	0.428	0.647	1.012	1.621	3.422	12.140
i_H	0.130	0.234	0.406	0.649	0.970	1.384	2.217	3.960
i_M	0.111	0.250	0.428	0.667	1.000	1.500	2.330	4.000

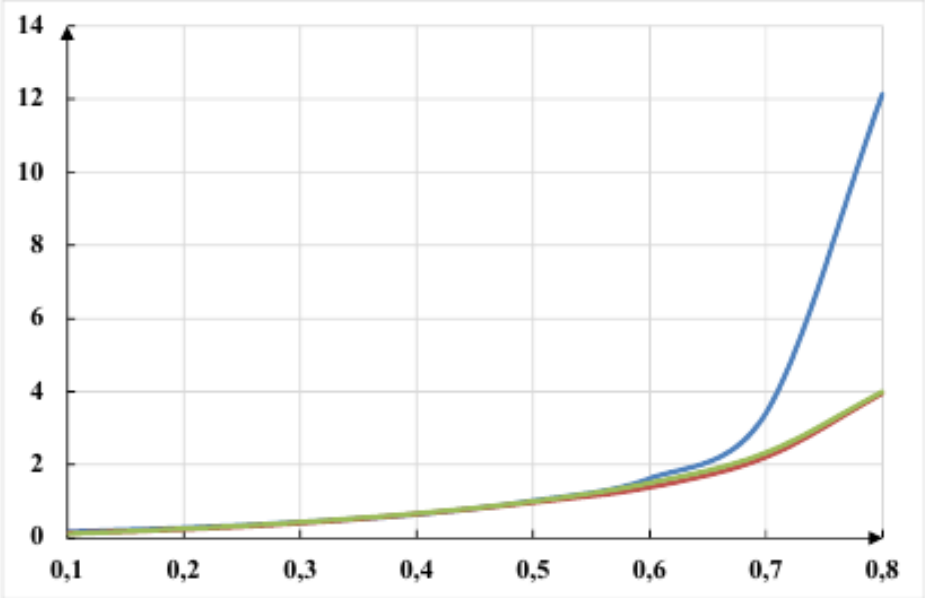

Рисунок 3.4 – Залежність середньої довжини черги від ρ

З результатів розрахунків, представлених в таблиці 3.4 і на графіках рис.3.4, виходить, що наявність статистичної залежності між інтервалами часу обслуговування істотно збільшує чергу заявок в буфері системи, що призводить до погіршення якості обслуговування в порівнянні з тим випадком, коли така залежність відсутня.

Висновки до розділу 3

1. Показано, що в разі, коли деякі параметри розподілів ймовірностей послідовностей інтервалів часу між пакетами і послідовностей інтервалів часу обслуговування відомі неточно, що характеризує невизначеність знання

щодо параметрів розподілів, при аналізі середнього часу очікування пакета в черзі можна використовувати інтервальний підхід, при якому невизначені параметри задаються діапазоном своїх можливих значень. При цьому в традиційному методі аналізу середнього часу очікування пакета в черзі (через рішення рівняння Ліндлі) невизначеність знання щодо неточно відомих параметрів долається усередненням розподілу із заданою (або обраною) ваговій функцією по інтервалу можливої зміни невідомого параметра.

2. На прикладі системи масового обслуговування виду *P/W/1* (де *P* означає розподіл Парето, а *W* – розподіл Вейбулла) показано, що після усереднення з невідомими параметрами задання визначення середнього часу очікування в черзі зводиться до використання рівняння Ліндлі і апроксимації усереднених розподілів сумами згасаючих експонент.

3. Використання в якості оновлюючого потоку рандомізованого пуассоновскького потоку дозволяє досліджувати ймовірносно-часові характеристики системи *G/D/1* при впливі на неї трафіку із випадковими взаємозалежними інтервалами часу між пакетами. Взаємозалежність інтервалів часу моделюється в рандомізованому пуассоновському потоці випадковою зміною параметра потоку.

4. Використання рандомізованого пуассоновского потоку дозволяє розраховувати ймовірність блокування системи *G/D/1*. Показано, що наявність кореляційних зв'язків інтервалів часу надходження потоку обмежує пропускну здатність системи, приводячи до швидкого зростання ймовірності блокування системи. Середня довжина черги при цьому різко збільшується при коефіцієнті завантаження системи вище значення 0,6.

4 ДОСЛІДЖЕННЯ ВУЗЛІВ МЕРЕЖІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ МЕТОДОМ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ

Викладені в розділах 2 і 3 матеріали по аналітичному дослідженню характеристик вузлів мультисервісних мереж зв'язку, якими є і мережі спеціального призначення, потребують експериментальної перевірки, яку доцільно здійснити з використанням спеціалізованих моделюючих платформ, що дозволяють відтворити на комп'ютері роботу не тільки вузла мережі при обробці реального трафіку, що володіє фрактальними властивостями, але і фрагментів дротових і бездротових мереж зв'язку.

4.1 Огляд засобів моделювання мереж зв’язку

Для створення надійно функціонуючої мережі зв'язку необхідно ще на етапі проектування знати потенційні характеристики вузлів мережі, тому що діапазон зміни розглянутих характеристик визначається апріорною варіацією параметрів оброблюваного трафіку.

Якість роботи мережі багато в чому обумовлена різними факторами, багато з яких носять випадкових характер і можуть не піддаватися суворому математичного аналізу. Основним інструментом аналізу при цьому може бути
імітаційне моделювання в комп'ютерних програмах-симуляторах без застосування реального обладнання.

На етапі побудові моделі виникає питання про вибір інструментарію. Критеріями створення ефективної моделі служать:

- детальна реалізація протоколів функціонування мереж;
- можливість написання і підключення власних модулів;

- можливість зміни параметрів моделювання під час проведення експериментів;
- платформна незалежність;
- розвинений графічний інтерфейс;
- ціна продукту.

Найбільш популярними середовищами імітаційного моделювання є:

1) The Network Simulator (NS-2) - об'єктно-орієнтований програмний продукт, ядро якого реалізовано на мові C ++. На базі NS2 можлива організація наочної демонстрації функціонування протоколів і мережевих механізмів.

2) OPNET Modeler Suite (OPNET) - засіб для проектування і моделювання локальних і глобальних мереж, комп'ютерних систем, додатків і розподілених систем. Включає наступні продукти: Netbiz (проектування і оптимізація обчислювальної системи), Modeler (моделювання і аналіз продуктивності мереж, комп'ютерних систем, додатків і розподілених систем), ITGuru (оцінка продуктивності комунікаційних мереж і розподілених систем).

3) OMNet ++ - розширюваний, модульний пакет, на основі компонентів бібліотеки C ++, який використовується для побудови моделей мереж, являє собою симулятор дискретних подій. В системі OMNeT++ закладена детальна реалізація протоколів, починаючи від мережевого рівня, можливість написання і підключення власних модулів, розвинений графічний інтерфейс.

У таблиці 4.1 представлені характеристики згаданих програмних продуктів.

NS2 розроблявся як програмне забезпечення з відкритим вихідним кодом (open source code software - OSS). Таке ПО поширюється безкоштовно - без будь-яких обмежень на право використання, модифікації та розповсюдження третіми особами. З цієї ж причини безкоштовні і завжди доступні on-line всі оновлення та доповнення продукту.

Ще однією властивістю програмного забезпечення є гнучка настройка відповідно до вимог конкретного користувача. Одною з характерних властивостей NS2 з точки зору гнучкості є мультіопераціонність. Повні версії, що включають всі функції, на даний момент працездатні під керуванням наступних операційних систем: SunOS, Solaris, Linux, FreeBSD, Windows [33].

Наведені дані дозволяють віддати перевагу мережному симулятору NS2.

Таблиця 4.1 – Характеристики імітаційних програмних продуктів

Продукт	Мова програмування	Наявність бібліотек	Візуалізація	Аналітичні функції	Трасування	Відкритий доступ
OPNET	C++	+	+	+	-	-
Omnet	C++	+	+	+	+	+
NS2	OTcl	+	+	+	+	+

4.2 Характеристики симулятора NS2

The Network Simulator (NS-2) - об'єктно-орієнтований програмний продукт, ядро якого реалізовано на мові C++. Як інтерпретатор використовується мова скриптів (сценаріїв) OTcl (Object oriented Tool Command Language). NS2 повністю підтримує ієрархію класів C ++ (звану в термінах NS2 компільованою ієрархією) і подібну ієрархію класів інтерпретатора OTcl. Використання двох мов програмування в NS2 пояснюється наступними причинами. З одного боку, для детального моделювання протоколів необхідно використовувати системну мову програмування, що забезпечує високу швидкість виконання і здатність маніпулювати досить великими обсягами даних. З іншого боку, для зручності

користувача і швидкості реалізації і модифікації різних сценаріїв моделювання привабливіше використовувати мову програмування більш високого рівня абстракції. Такий підхід є компромісом між зручністю використання і швидкістю. У NS2 як системноа мови використовується C ++, що дозволяє забезпечити:

- високу продуктивність;
- роботу з пакетами потоку на низькому рівні абстракції моделі;
- модифікацію ядра NS2 з метою підтримки нових функцій і протоколів.

В якості мови програмування високого рівня абстракції використовується мова скриптів OTcl, що дозволяє забезпечити ряд позитивних властивостей, властивих мові Tcl/Tk (тому що OTcl є об'єктно-орієнтованим розширенням мови Tcl):

- простота синтаксису;
- простота побудови сценарію моделювання;
- можливість з'єднання воєдино блоків, виконаних на системних мовах програмування і просту маніпуляцію ними.

У імітаційному моделюванні мережа є сукупністю мережевих об'єктів, які певним чином реагують на безліч подій. Мережеві об'єкти сповіщаються про ці події планувальником подій. У кожної події є набір атрибутів: час настання і мережевий об'єкт, до якого належить ця подія. Планувальник, виходячи з хронологічної таблиці, вибирає відповідні мережеві об'єкти і повідомляє про настання подій.

Основними компонентами моделювання NS2 є планувальник подій, мережеві об'єкти та події (at-події і пакети).

Основою моделювання в NS2 є планувальник подій (event scheduler). Основні користувачі планувальника подій – компоненти мережі, які моделюють затримку на обробку пакетів або яким потрібні таймери.

Планувальник подій реального часу використовується для емуляції, коли пакет моделювання взаємодіє з реальною мережею.

Інший варіант використання планувальника подій - це планування подій моделювання, такі як, наприклад, старт програми FTP, закінчення моделювання, генерація сценарію моделювання до запуску самого моделювання тощо.

Мережеві об'єкти можуть бути простими (черги, лінії затримки, мультиплексори/демультиплексори, агенти, додатки) і складовими, які утворюються шляхом об'єднання простих об'єктів (вузли, дуплексні лінії, локальні мережі 802.3 Ethernet, 802.11 Wi-Fi).

Вузол в NS2 є абстракцією мережевого рівня. Він може приймати пакети і класифікувати їх за адресою і портом, що є полями IP-заголовка.

Лінії зв'язку є складовими об'єктами (2 протилежно спрямовані симплексні лінії, які складаються з черги, Null-агента, лінії затримки і об'єкта). Якщо модель орієнтована на трасування подій, то ланка також буде містити об'єкти трасування.

Агенти в NS2 є абстракцією транспортного рівня і служать для того, щоб забезпечувати передачу пакетів між мережевими об'єктами. Для створення з'єднання з використанням протоколу TCP необхідна наявність двох агентів - TCP-передавачі: TCP, TCP/Tahoe, TCP/Reno, TCP/Vegas, і TCP-приймач: TCPSink. Передавач має можливість відповідати різним чином на сповіщення про отримання пакетів від адресатів. Приймач приймає пакети і відправляє сповіщення про отримання. При створенні з'єднання з UDP протоколом, повідомлення про отримання не передбачені, тому для передачі використовується UDP-агент, а для прийому - Null-агент, який приймає і знищує все пакети.

Додатки в NS2 відповідають за мережевий рівень. Додаток прикріплюється до агента і служить для створення трафіку. FTP, Telnet, CBR можна використовувати в якості додатків. FTP і Telnet моделюють трафік, характерний для реальних протоколів прикладного рівня. CBR є абстрактним генератором трафіку з постійним темпом видачі пакетів.

Типи черг задаються при створенні ланки передачі даних, до них відносяться:

- DropTail (аналог FIFO з відкиданням пакетів при переповненні черги);
- FQ (рівномірний розподіл пропускної спроможності між потоками);
- SFQ (рівномірний розподіл пропускної спроможності між обмеженою кількістю черг);
- DBR (обслуговування потоків в циклічному порядку з рівномірним розподілом пропускної спроможності між усіма класами);
- CBQ (розподіл пропускної здатності відбувається відповідно з класом пріоритету).

У NS2 пакети складаються з набору заголовків і поля даних. Формат заголовка пакета задається під час створення об'єкта Simulator. Для зручності користувача, всі пакети мають однаковий формат. Для прискорення процесу моделювання рекомендується вказувати які протоколи будуть використовуватися в моделі для того щоб виключити заголовки невикористовуваних протоколів з заголовка пакета.

У пакет NS2 входить засіб анімації результатів моделювання Nam[34], за допомогою якого можна спостерігати роботу мережі, її топологію, анімацію руху пакетів по каналах зв'язку або їх втрати, вести візуальний моніторинг стану черг і проводити аналіз даних.

Повна версія NS2 також містить візуалізатор Xgraph, за допомогою якого можна зобразити графічно отримані результати моделювання, що знаходяться у відповідному файлі, в який записуються дані в процесі симуляції.

У NS2 існує і математична підтримка, що дозволяє створювати різні види трафіку, як, наприклад, пуассоновского трафіку, самоподібного тощо.

Гнучка архітектура NS2 дає можливість її користувачам реалізовувати

власні математичні функції і закони на C ++.

У NS2 також реалізована можливість моделювання виникнення помилок (викривлення або втрата інформації) на канальному рівні, на рівні бітів або пакетів.

Є можливість реалізації власної моделі помилок.

4.3 Моделювання та обробка самоподібного трафіку симулятором NS2

Як зазначено в попередньому розділі, NS2 дозволяє описати для модельованої мережі топологію, конфігурацію джерел і приймачів трафіку, параметри з'єднань (смугу пропускання, затримку, ймовірність втрати пакетів) та інші параметри. При моделюванні є можливість управляти параметрами буферів, проводити моніторинг прийнятих, відправлених і втрачених пакетів, здійснювати збір статистики та ін. За допомогою генерації вихідних trace-файлів може бути отримана інформація про динаміку трафіку, стані з'єднань і об'єктів мережі, а також роботі протоколів.

Для генерації трафіку в системі NS2 призначені об'єкти типу Traffic. Вони створюються методами Traffic/type, де type – Expoo, Pareto або Trace.

Об'єкт Traffic/Pareto – ON/OFF генератор трафіку згідно з розподілом Парето (в NS2 є генератори інших розподілів – розподілу Вейбулла, гамма-розподілу). Проста ON/OFF модель передбачає, що джерела перемикаються між двома станами: ON – стан, в якому джерела генерують трафік з постійною швидкістю, OFF – стан, в якому трафік не генерується.

В роботі [35] наведено приклад генерації методом ON/OFF трафіку Парето з параметрами: пакети розміром 128 байт з постійною бітовою швидкістю 20000 біт/с протягом ON-періоду з середньою тривалістю в 500 мс. Середня тривалість OFF-періоду становить 1,5 с, параметр форми α дорівнює 1.2. Рисунок 4.1 пояснює створення генератора трафіку з розподілом Парето із заданими параметрами.

Для управління якістю обслуговування в маршрутизаторах *r1* і *r2* використовується алгоритм FIFO. Принцип роботи цього алгоритму заснований на процедурі відкидання всіх пакетів, які прийшли після досягнення заздалегідь встановленого максимального розміру черги. Ця процедура отримала назву «відкидання хвоста» (tail drop). Ефективність такої процедури досить низька, тому що про перевантаження стає відомо тільки при факті переповнення черги [13]. Таким чином, механізм FIFO не може зменшити реальний розмір черги, щоб знизити час затримки пакета.

```
set traffic [new Traffic/Pareto]
$traffic set packet-size_ 128
$traffic set burst-time_ 500ms
$traffic set idle-time_ 1.5s
$traffic set rate_ 20000.0
$traffic set shape_ 1.2
```

Рисунок 4.1 – Генератор трафіку Парето

З урахуванням співвідношення (4.1), справедливого для розподілу Парето, між параметром Херста H і параметром форми α можна стверджувати, що згідно рис. 4.1 буде згенеровано трафік з явними самоподібними властивостями *(H = 0.9)*.

$$H = \frac{3 - \alpha}{2} \tag{4.1}$$

Для аналізу ступеня впливу самоподібності трафіку на рівень втрати пакетів (packetloss) при негарантованій доставці даних (best-effort service) проведемо експеримент за схемою, що наведена на рис.4.2.

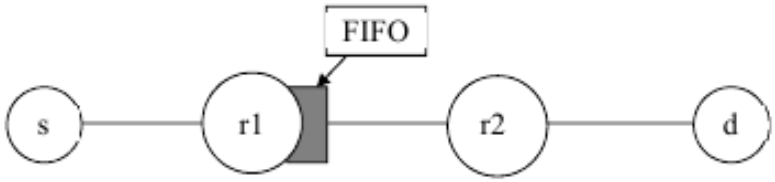

Рисунок 4.2 – Схема експерименту з негарантованої доставки даних

Під час генерації трафіку для випадкових інтервалів часу використовувався розподіл Парето із змінним параметром Херста. Значення параметра Херста змінювалося від 0,1 до 0,9. Для перетворення досліджуваних реалізацій в вид, необхідний для використання в якості джерела трафіку в NS2, використовувалася програма vega.tcl, розроблена F.Vega. Отримані таким чином самоподібні потоки, пакувалися в UDP-пакети і передавалися в сторону одержувача (*d*).

Для спостереження роботи алгоритму FIFO пропускна здатність віртуального каналу між маршрутизаторами (*r1* і *r2*) вибиралася менше швидкості потоку трафіку. Таким чином, частина трафіку губилася і при цьому спрацьовувала стандартна процедура управління чергою Tail Drop. Тривалість кожного експерименту – 3 години. Результати експерименту представлені на рис.4.3. пунктирною (згладженої) лінією.

Деякі додатки не здатні нормально функціонувати або ж функціонують вкрай неефективно у разі втрати пакетів.

Подібні додатки вимагають від мережі гарантії надійної доставки всіх пакетів.

Відкидання пакетів є неминучим явищем при негарантованій доставці трафіку. Слід також зазначити, що відкинуті пакети вказують на неефективне використання ресурсів мережі, частина яких була витрачена на доставку пакетів в точку, де вони були втрачені.

У моделі негарантованої доставки даних при використанні в якості алгоритму обслуговування черг стандартної процедури FIFO основною причиною відкидання пакету є переповнення буфера черги. Тому результат експерименту до певної міри може бути інтерпретований як ймовірність

блокування системи *G/D/1* с кінцевим розміром буфера за умови, що символ *G* в даному випадку означає розподіл Парето.

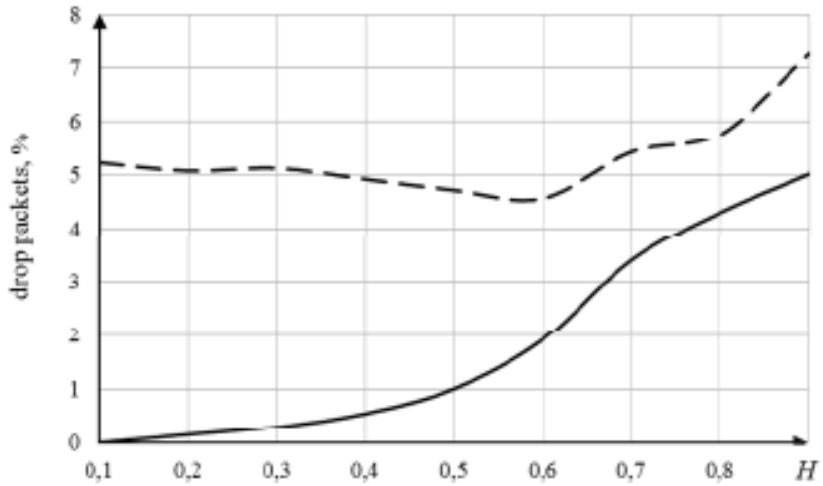

Рисунок 4.3 – Залежність кількості відкинутих пакетів від коефіцієнту Херста

З графіка рис.4.3 видно, що для значень *H* від 0,1 до 0,6 спостерігається плавне зменшення кількості відкинутих пакетів. Подальше збільшення параметра Херста призводить до значного зростання числа втрат пакетів. Мінімальний відсоток втрат спостерігається для H = 0,6 – 4,66%, максимальний відсоток – для H = 0,9 – 7,26%. Таким чином, збільшення втрат пакетів з ростом параметра Херста вказує на неефективність роботи алгоритму FIFO для потоків з самоподібностю.

За аналогічною схемою було проведено експеримент в моделі диференційованого обслуговування, коли якість обслуговування визначалася зваженим механізмом довільного раннього виявлення (WRED) [35]. У схемі рис.4.2 замість алгоритму FIFO слід в даному випадку записати алгоритм WRED. Плавне регулювання розміру черги алгоритмом WRED в даному експерименті характеризується наступними параметрами: при розмірі черги 10 пакетів ймовірність відкидання пакетів дорівнює 0, при зміні черги від 10

до 30 пакетів ймовірність відкидання пакетів лінійно зростає до величини 0,5 і далі стрибком приймає значення 1.

Результат експерименту представлений на рис.4.3 суцільною (згладженою) кривою. Порівняння кривих на рис.4.3 переконливо показує перевагу управління трафіком алгоритмом WRED.

Проаналізуємо ситуацію, пов'язану зі спільною передачею TCP і UDP трафіку. Для цього розглянемо схему, представлену на рис.4.4.

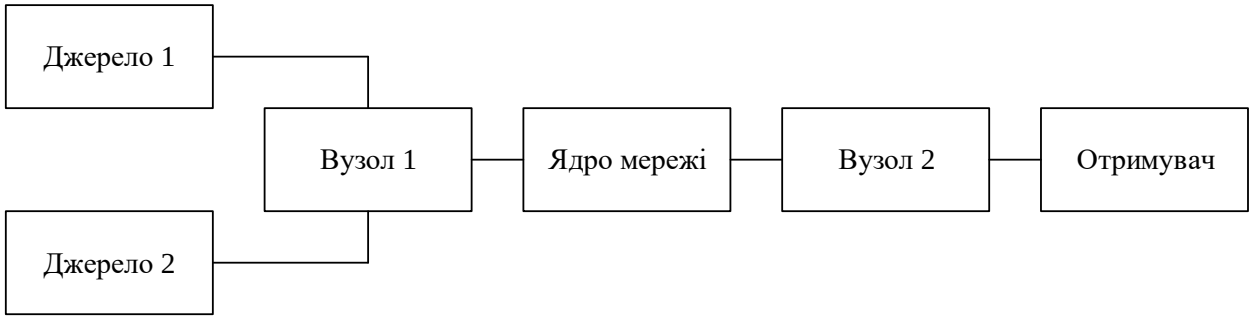

Рисунок 4.4 – Схема моделювання фрагменту мережі

Джерело 1 є генератором трафіку UDP з постійною швидкістю (CBR). Джерело 2 генерує трафік TCP по моделі ON/OFF з використанням розподілу Парето при різних значеннях параметра форми. Обробка результатів моделювання (трейс-файлу) здійснювалася за допомогою програми TraceGraph. З її допомогою було зібрано статистику, що показує величини затримки (мінімальну, середню, максимальну) і джитера між джерелом 2 і одержувачем. Даний експеримент дозволяє з'ясувати характер залежностей даних параметрів розміру пакета, швидкості потоку і параметра форми трафіку Парето. Результати наведені на рис. 4.5 – 4.7.

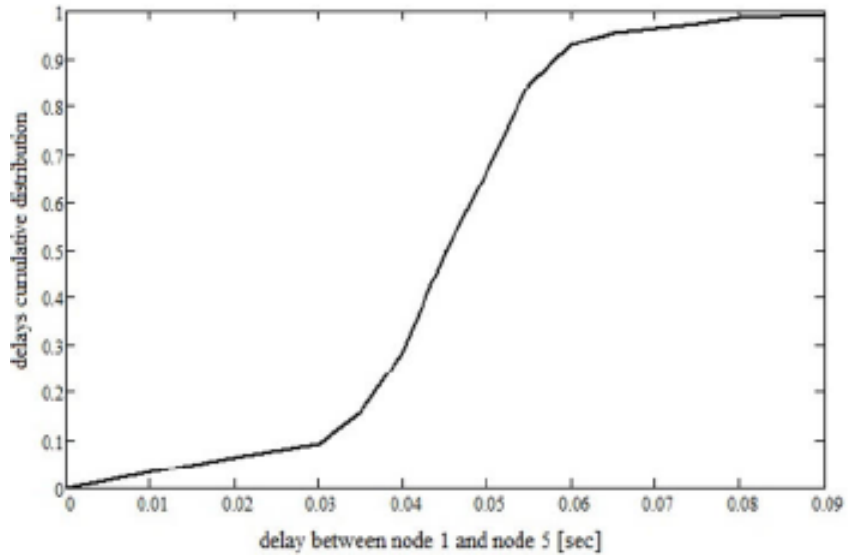

Рисунок 4.5 – Функція розподілу затримки: швидкість потоку 20 Мбіт/с, довжина пакета 1500 байт, параметр форми 3.5

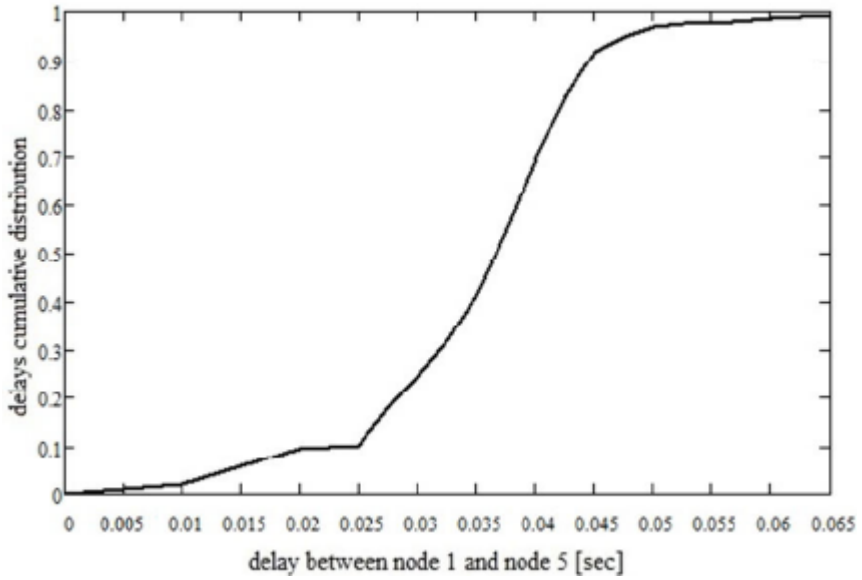

Рисунок 4.6 – Функція розподілу затримки: швидкість потоку 10 Мбіт/с, довжина пакета 1000 байт, параметр форми 1.5

З аналізу наведених графіків випливає, що для швидкості потоку 20 Мбіт/с і 10 Мбіт/с величини затримки розподілені досить рівномірно в діапазоні від 0,03 с до 0,07 с для різних довжин пакетів. При цьому параметр форми не робить помітного впливу на характеристику що аналізується.

Для швидкості потоку 5 Мбіт/с виявилося, що функція розподілу затримки має нерівномірний характер. Чим менше довжина пакета, тим менше

величина затримки. Параметр форми практично не впливає на дану характеристику.

Цікавим є аналіз залежності затримки між джерелом і одержувачем від часу відправлення пакетів (або, фактично, часу моделювання). Нижче на рис. 4.8 – 4.12 представлені ці залежності для різних варіацій модельованих параметрів.

З представлених результатів випливає, що затримка між одним з джерел і одержувачем має періодичний характер зі змінною «частотою» проходження і «амплітудою». Це пов'язано в першу чергу з генеруванням трафіку Парето ON/OFF періодами. На більш високих швидкостях потоку характер поведінки приблизно однаковий. На розкид значень затримок впливає параметр форми і довжина пакета.

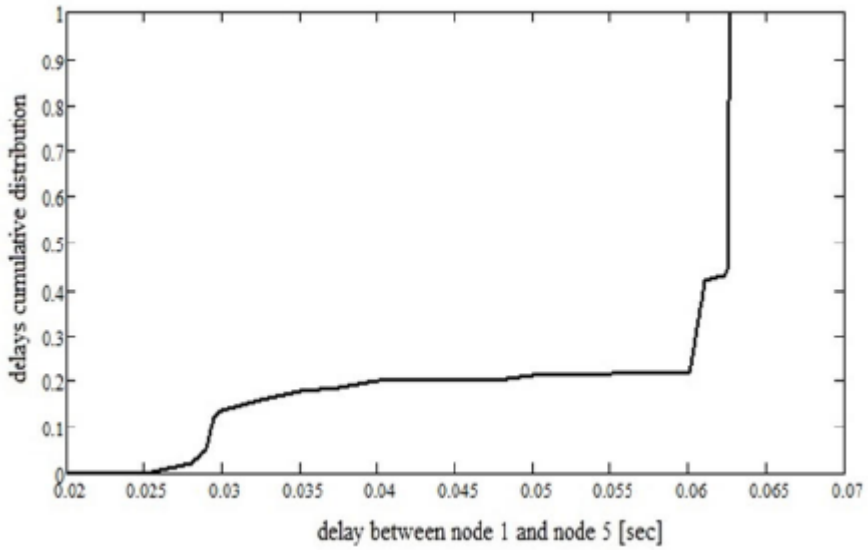

Рисунок 4.7 – Функція розподілу затримки: швидкість потоку 5 Мбіт/с, довжина пакета 1500 байт, параметр форми 1.5

Слід зазначити, що характер зміни затримки залежить від швидкості потоку. Якщо для швидкостей 20 Мбіт/с і 10 Мбіт/с відмінності в затримці

непомітні для ока, то при швидкості 5 Мбіт/с вони очевидні. Об'єктивну оцінку зазначених змін дає тільки статистична обробка результатів моделювання, наведена на рис. 4.5 - 4.7.

Узагальнюючи висновки по рис. 4.8 – 4.12 можна відзначити, що при збільшенні довжини пакета для однієї і тієї ж швидкості спостерігається не тільки збільшення величини затримки, але і розкид її значень між максимальним і мінімальним значеннями. Отже, при виборі довжини пакета необхідно керуватися типом переданого трафіку, його класом обслуговування і чутливістю до затримок. Крім того, для невеликого завантаження мережі (при малих швидкості передачі і довжині пакета) характерна сталість затримки протягом всього часу передачі пакетів.

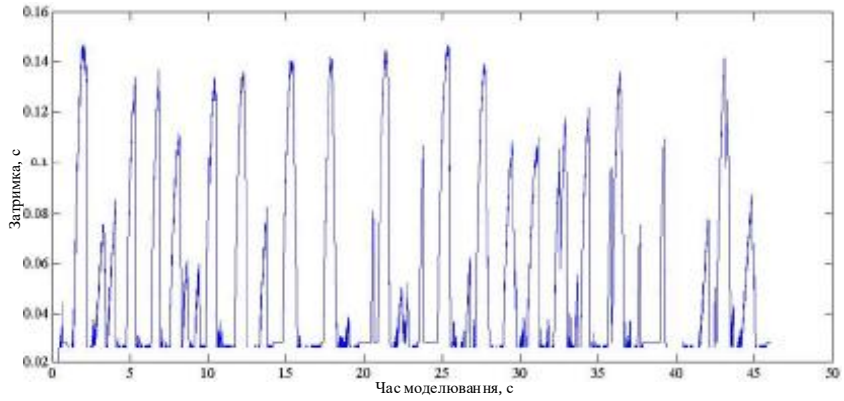

Рисунок 4.8 – Затримка між джерелом та отримувачем: швидкість потоку 20 Мбіт/с, довжина пакета 1500 байт, параметр форми 1.5

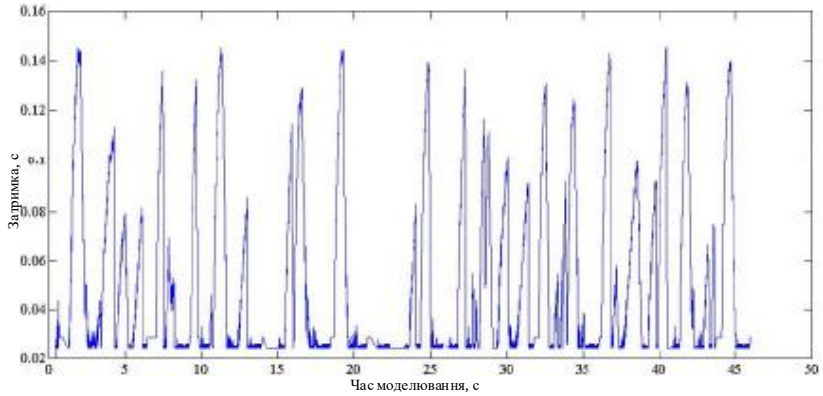

Рисунок 4.9 – Затримка між джерелом та отримувачем: швидкість потоку 20 Мбіт/с, довжина пакета 1500 байт, параметр форми 3.5

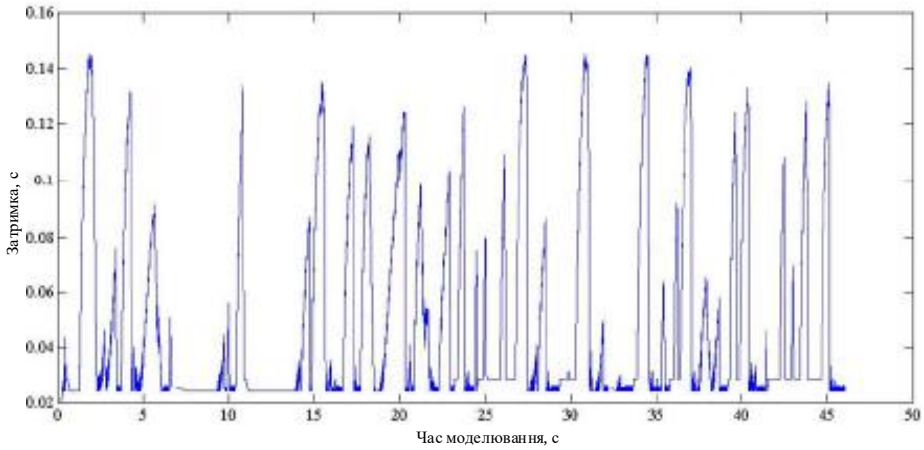

Рисунок 4.10 – Затримка між джерелом та отримувачем: швидкість потоку 10 Мбіт/с, довжина пакета 1500 байт, параметр форми 1.5

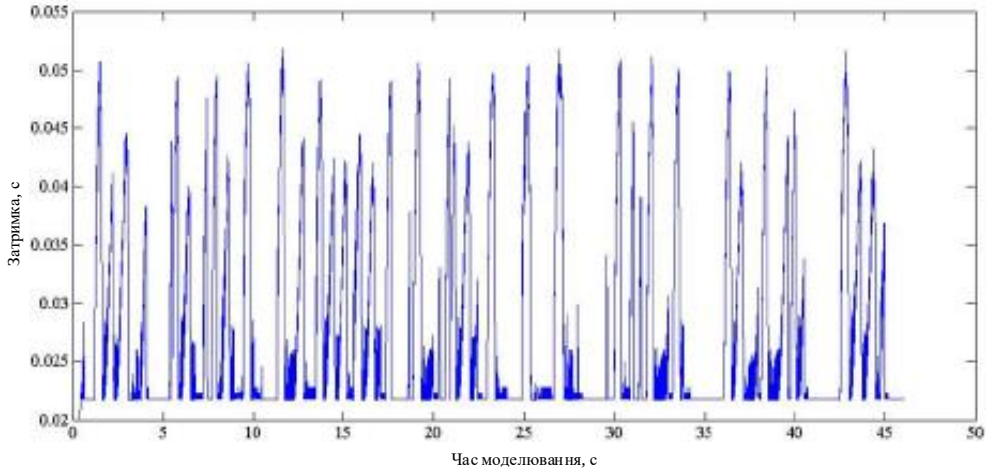

Рисунок 4.11 – Затримка між джерелом та отримувачем: швидкість потоку 10 Мбіт/с, довжина пакета 500 байт, параметр форми 1.5

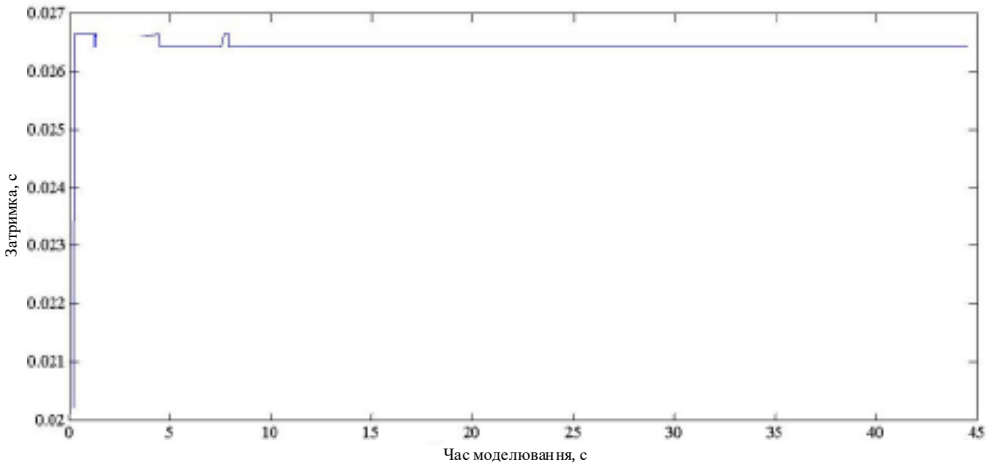

Рисунок 4.12 – Затримка між джерелом та отримувачем: швидкість потоку 5 Мбіт/с, довжина пакета 1000 байт, параметр форми 1.5

Промоделюємо роботу фрагмента мережі, представленого на рис. 4.13.

Для імітації ситуації в реальній мережі поряд з обробкою досліджуваного трафіку обробляється фоновий трафік. Фоновим для основного є поєднання CBR трафіку з постійною бітовою швидкістю і ON/OFF-трафіку з розподілом Парето.

Досліджуваний трафік передається між джерелом і одержувачем 1. Конкуруючий з даним потоком фоновий трафік передається від джерела до одержувача 2 і реалізується генерацією CBR і ON/OFF-трафіку. В якості основного потоку обробляється трафік IPTV. Даний трафік, зафіксований в реальній лінії зв'язку та імпортований в симулятор NS2.

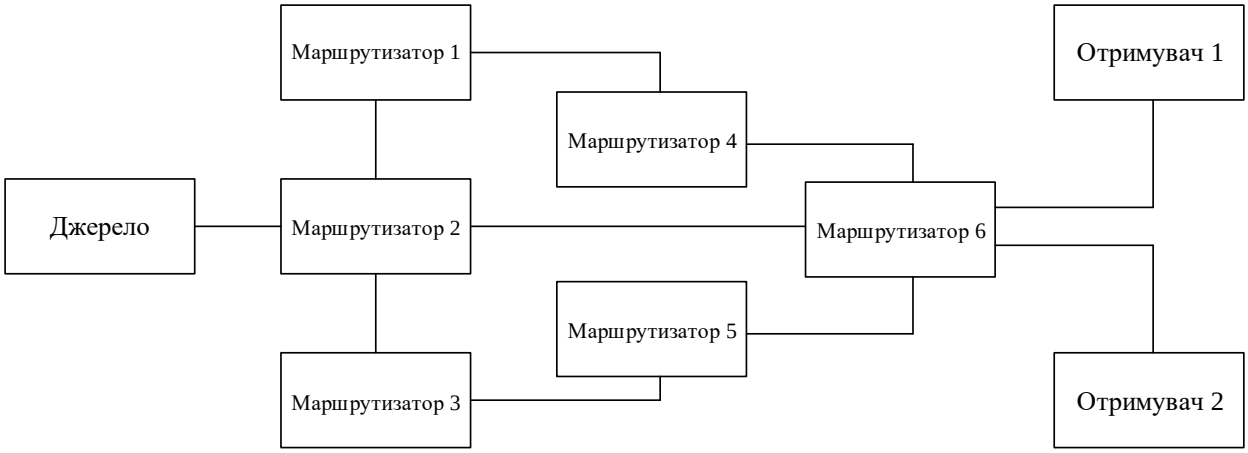

Рисунок 4.13 – Фрагмент мережі

Представлена схема дозволяє проаналізувати вплив кореляційних властивостей довжин пакетів (через задання параметра форми розподілу Парето, який задає значення параметра Херста і, отже, кореляційні властивості трафіку) на результати обробки трафіку одержувачем. В експерименті аналізувалися наступні параметри якості обслуговування: затримка, джитер і частка втрачених пакетів.

Для трафіку IPTV зміна затримки пакетів в часі і джитера в часі наведені на рис. 4.14 і 4.15, відповідно. Результати моделювання наведені в таблиці 4.2.

Аналіз результатів моделювання показав, що в процесі обробки трафіку ті параметри QoS, які традиційно використовуються для оцінки ефективності обробки потоків, мало відрізняються для різних моделей трафіку. Найбільш наближені значення параметрів QoS при обробці реального трафіку отримані для фонової моделі у вигляді ON/OFF процесу з розподіленийням Парето. При цьому такий параметр як ймовірність скидання пакету для корельованого трафіку значно перевищує допустимі значення по QoS.

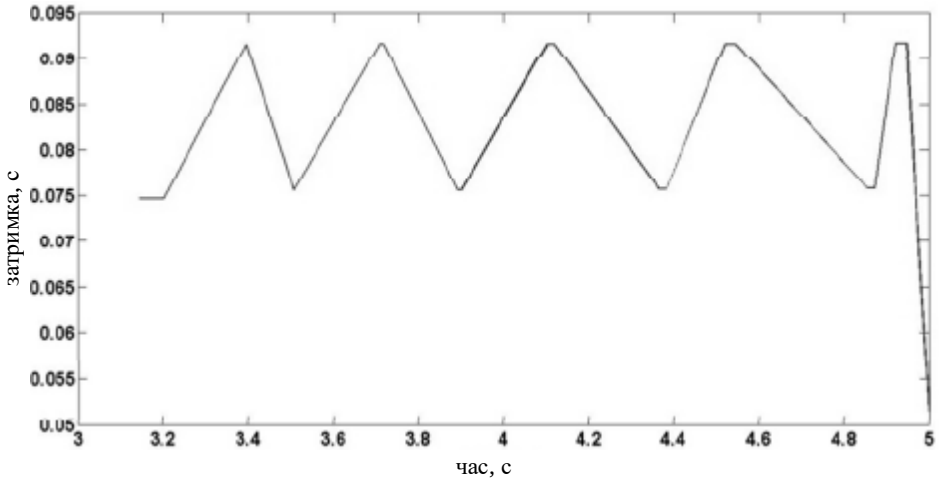

Рисунок 4.14 – Зміна затримки для трафіка мережі IPTV

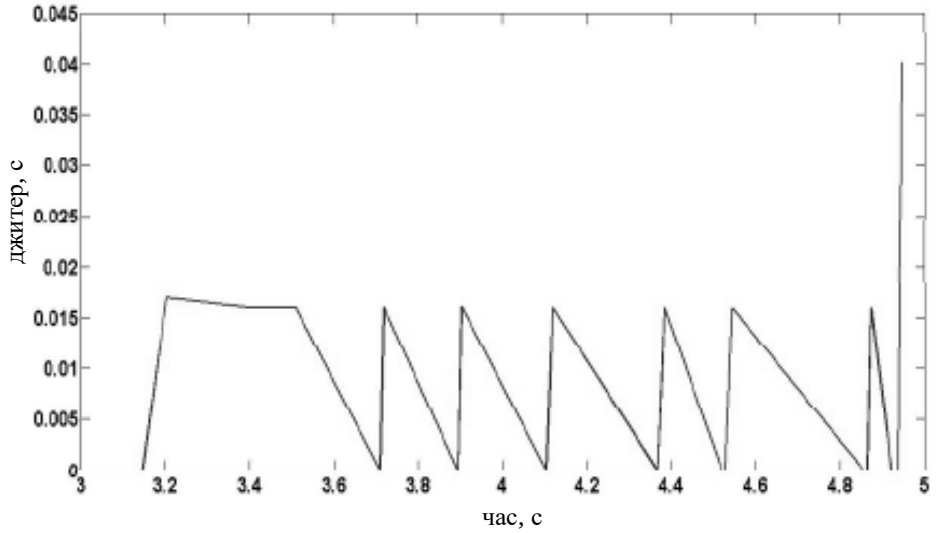

Рисунок 4.15 – Зміна джитера для трафіка мережі IPTV

Таблиця 4.1 – Результати моделювання

Параметри QoS	Тип трафіка		
	CBR	ON/OFF	IPTV
Delay, мс	80	91	82
Jitter, мс	5	0.51	8
Packet loss, %	0	5	0.3
Packet drop, %	6.5	0.3	12

Як зазначено в документах, що регламентують параметри якості обслуговування в операторських мережах [36], при передачі VoIP трафіку втрати пакетів не повинні перевищувати 0,25%, а при передачі потокового відео - не більше 1%.

Знання цих характеристик дає інформацію для поліпшення параметрів управління трафіком і підвищення рівня якості обслуговування в мережі.

Висновки до розділу 4

1. Для експериментальної перевірки теоретичних результатів, отриманих в розділах 2 і 3, здійснено вибір платформи моделювання фрагментів МСП.

У підсумку в якості платформи моделювання обраний вільно розповсюджуваний об'єктно-орієнтований програмний продукт NS2, ядро якого реалізовано на мові C ++.

2. Для аналізу ступеня впливу самоподібності трафіку на рівень втрати пакетів поставлений експеримент для моделі негарантованої доставки даних (з управлінням черги алгоритмом FIFO) і моделі диференційованого обслуговування (с управлінням чергою алгоритмом WRED).

При використанні розподілу Парето для інтервалів часу між пакетами і постійним часом обслуговування пакетів в моделі негарантованої доставки даних показано, що при збільшенні параметра Херста в інтервалі значень від 0.1 до 0.6 спостерігається збільшення кількості втрачених пакетів. Мінімальний відсоток втрат спостерігається для H = 0.6 – 4.66%,

максимальний відсоток – для H = 0.9 – 7.26%. Збільшення втрат пакетів з ростом параметра Херста вказує на неефективність роботи алгоритму FIFO для потоків з самоподібністю.

У моделі диференційованого обслуговування при H = 0.6 втрачається в середньому 2% пакетів, при H = 0.9 – 5%.

3. Моделювання варіанта спільної передачі TCP і UDP (CBR) трафіку показало, що затримка пакетів в фрагменті мережі в діапазоні швидкостей потоку від 20 Мбіт/с до 10 Мбіт/с в діапазоні від 0.03 с до 0.07 с при різних довжинах пакетів. Значення параметра форми розподілу Парето при цьому не робить істотного впливу на затримку.

Для швидкості потоку 5 Мбіт/с інтегральна функція розподілу затримки має нерівномірний характер, що характеризує можливо стрибкоподібний характер зміни затримки.

Залежність затримки між джерелом і одержувачем від часу відправлення пакетів має циклічний характер зі змінною «частотою» проходження і «амплітудою».

4. Розглянуто схему експерименту, в якій фоновий трафік конкурує з основним IPTV-трафіком та передається від джерела до одержувача і реалізується генерацією CBR і ON/OFF-трафіку. Аналіз зміни затримки пакетів і джитера показав, що в процесі обробки трафіку ті параметри QoS, які традиційно використовуються для оцінки ефективності обробки потоків мало відрізняються для різних моделей трафіку (IPTV, CBR і ON/OFF-трафіку).

Найбільш наближені значення параметрів QoS при обробці реального трафіку отримані для фонової моделі у вигляді ON/OFF процесу з розподілом Парето. При цьому, такий параметр, як ймовірність скидання пакету, для корельованого трафіку IPTV значно перевищує допустимі значення по QoS.

ВИСНОВКИ

Відповідно до мети кваліфікаційної роботи та поставленими завданнями дослідження в роботі отримані наступні результати:

1. Проведено аналіз існуючих моделей трафіку і методів його обробки, заснованих на класичній теорії масового обслуговування. При цьому встановлено, що в сучасних інформаційно-комунікаційних мережах трафік, як випадковий процес, володіє самоподібними властивостями, що характеризується явно вираженими кореляційними властивостями інтервалів часу між заявками і інтервалів часу обробки заявок у вузлах мережі.

2. У разі, коли послідовності зазначених інтервалів незалежні, для аналізу середнього часу очікування заявки в черзі системи масового обслуговування загального вигляду доцільно використовувати інтегральне рівняння Ліндлі, рішення якого спектральним методом може бути легко знайдено при апроксимації щільності ймовірностей тимчасових інтервалів рядами згасаючих експонент (зокрема, гіперекспоненційним або ерланговським розподілом).

3. Для обліку кореляційних властивостей тимчасових інтервалів в роботі використані моделі трафіку у вигляді оновлюючих процесів (процесів відновлення) з гіперекспоненційними розподілами. Облік кореляційних властивостей здійснюється через індекс дисперсії тимчасових інтервалів, який визначається сумою всіх значущих коефіцієнтів кореляції послідовності тимчасових інтервалів.

4. Для трафіку, що володіє самоподібними властивостями, запропонована методика оцінювання середнього часу очікування заявки в черзі для системи масового обслуговування загального вигляду, заснована на рішенні інтегрального рівняння Ліндлі спектральним методом з використанням моделі самоподібного трафіку у вигляді процесу відновлення

з гіперекспоніціональне розподілом миттєвих значень інтервалів часу між заявками.

5. Для оцінки впливу розміру черги на пропускну здатність системи масового обслуговування (або ймовірність блокування) використана модель самоподібного трафіку у вигляді рандомізованого пуассоновского потоку, у якого інтенсивність змінюється при зміні стану системи.

6. Для перевірки результатів, отриманих аналітичним шляхом, проведено імітаційне моделювання процесів передачі та обробки трафіку вузлами мережі з заданими характеристиками на симуляторі NS2. Моделювання показало якісний збіг теоретичних та експериментальних результатів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) Легков К.Е. Организация и модели функционирования современных инфокоммуникационных сетей специального назначения // T-Comm: Телекоммуникации и транспорт. – 2015. – Т. 9, №8. – С. 14-20.
2) Соколов Н.А. Системные аспекты построения и развития сетей электросвязи специального назначения [Электронный ресурс] / Н.А Соколов International Journal of Open Information Technologies ISSN. – 2014. – Т. 2, № 9.– С. 4–8.
3) Росляков А.В. Виртуальные частные сети: Основы построения и применения - М.: ЭкоТрендз, 2006, 304 с.
4) Что такое VPN? Суть технологии и области ее применения [Электронный ресурс]. – Режим доступа: https://www.syl.ru/article/145004/mod_chto-takoe-vpn-sut-tehnologii-i-oblasti-ee-primeneniya
5) Что такое VPN, зачем он нужен и как им пользоваться [Электронный ресурс]. – Режим доступа: http://hyiphunter.org/chto-takoe-vpn
6) Сатовский Б.Л. MPLS — технология маршрутизации для нового поколения сетей общего пользования [Электронный ресурс]: журнал о компьютерных сетях и телекоммуникационных технологиях / Сети и системы связи: Электрон. журн. – 2000. – Режим доступа: http://ccc.ru/magazine/depot/01_03/0303.htm
7) Гольдштейн А.Б., Гольдштейн Б.С. Технология и протоколы MPLS [Текст] / Научно-техн. изд. – СПб.: БХВ-Петербург, 2014. - 304 с.: ил.
8) Сети и телекоммуникации: учебник и практикум для академического бакалавриата / под ред. К.Е. Самуйлова, И.А. Шалимова, Д.С. Кулябова. - М.: Издательство Юрайт, 2016. - 363 с.
9) Ethernet в городских сетях [Электронный ресурс]. – Режим доступа:

http://mirznanii.com/a/308561/ethernet-v-gorodskikh-setyakh

10) Буренин А.Н., Легков К.Е., Нестеренко О.Е. К вопросу построения систем управления современными инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. – 2013. – Т. 6, №6. – С. 22–28.
11) Буренин А.Н., Легков К.Е. К вопросу математического описания потоков управляющей информации в процессе управления современной инфокоммуникационной сетью специального назначения // Наукоемкие технологии в космических исследованиях земли. 2013. №5.- С.8-12.
12) Клейнрок Л. Вычислительные системы с очередями / Пер. с англ. под ред. Б.С. Цыбакова. – М.: Мир, 1979, 600 с.
13) Клейнрок Л. Теория массового обслуживания / Пер. с англ. под ред. В.И. Неймана. - М.: Машиностроение, 1979, 432с.
14) Шелухин О.И., Тенякшев А.М., Осин А.В. Фрактальные процессы в телекоммуникациях / Под ред. О.И. Шелухина. - М.: Радиотехника, 2003, 480с.
15) Карташевский В.Г. Основы теории массового обслуживания. Учебник для вузов. - М.: Горячая линия-Телеком, 2013 – 130 с.
16) Федер Е. Фракталы.- М.: Мир, 1991. – 254 с.
17) Balcioglu B., Jagerman D.L., Altiok T., Melamed B. Mean Waiting Time Approximations in the G/G/1 Queue // Queueing Systems. 2004. 46. P. 481-506.
18) Метод аппроксимации произвольной плотности распределения суммами экспонент / Блатов И.А., Карташевский В.Г., Киреева Н.В. и др. // Вестник ВГУ. – 2013. – № 2. – С. 53-57.
19) Araghi M. A new renewal approximation for certain autocorrelated processes // Operations Research Letters, 36, 2008, P.133–139.
20) Araghi M.B. Incorporating Autocorrelated Service Nimes in the Analysis

of Delay Systems [Электронный ресурс]. – Режим доступа: https: www.researchgate.net/publication/228806763

21) Balcioglu B., Jagerman D.L., Altiok T. Approximate mean waiting time in a G/D/1 queue with autocorrelated times to failures // IIE Transactions, 2007, V.39, P. 985-996.
22) Balcioglu B., Jagerman D.L., Altiok T. Merging and Splitting Autocorrelated Arrival Processes and Impact on Queueing Performance // Performance Evaluation, 2008. Vol.65. P.653-669
23) Jagerman D.L., Melamed B. On Markovian traffic with applications to TES processes // J. Appl. Math. Stochastic Anal. 1994. 7(3). P. 373-396
24) Wolff R.W. Stochastic Modeling and the Theory of Queues / Prentice-Hall, Englewood Cliffs, NJ, 1989, 116 p.
25) Гончаренко В.А. Анализ реактивности узла вычислительной сети в условиях интервальной неопределенности // Изв. Вузов. Приборостроение, 2008, Т.51. №7. С. 34-39.
26) Кузнецов В.П. Интервальные статистические модели.- М.: Радио и связь, 1991, 352 с.
27) Букашкин С.А., Карташевский В.Г., Сапрыкин А.В. Анализ функционирования узла сети специального назначения в условиях неточного знания параметров трафика // Радиотехника. – 2017. - №4. – С. 93-97.
28) Букашкин С.А., Карташевский В.Г., Сапрыкин А.В. Анализ функционирования сетевого узла при неточном знании параметров трафика // 19-я международная конференция "Цифровая обработка сигналов и ее применение". – М., 2017. – С.230-234.
29) Решение уравнения Линдли спектральным методом для систем массового обслуживания общего вида / И.А. Блатов, В.Г. Карташевский, Н.В. Киреева, и др. // Электросвязь. №11. 2014. С.48-50.

30) Александров А.М. Один метод исследования систем массового обслуживания // Изв. АН СССР. Техническая кибернетика - 1971.- № 3. С. 105-115.
31) Александров А.М. Рандомизированные модели цифрового телетрафика // Электросвязь. № 6. 2010. С.41-44.
32) Хинчин А.Я. Математические методы теории массового обслуживания. - М.: Физматгиз, 1963. - 149 с.
33) Network Simulator 2 for Wireless [Электронный ресурс] – Режим доступа:http://www.winlab.rutgers.edu/~zhibinwu/html/network_simulator_2.htm
34) Кулябов Д.С., Ланеев Д.Е. Моделирование динамики взаимодействия WEB-сервера и пула клиентов в компьютерной сети в условиях атаки «Отказ в обслуживании» // Вестник Российского университета дружбы народов, серия «Прикладная и компьютерная математика».- Т.4. №1. 2005. С.164-178
35) Фомин В.В. Исследование алгоритма управления очередями WRED в модели дифференцируемого обслуживания // Инфокоммуникационные технологии. – 2010. т.8. № 2. – С. 27-31.
36) Архив документации на OpenNet.ru / Раздел «Cisco маршрутизаторы и коммутаторы». [Электронный ресурс] – Режим доступа: www.mpls-exp.ru/ispqoscisco.htm

ДОДАТОК А

Розділ охорони праці та пожежна безпека в науково-дослідницькому відділі

Площа приміщення науково-дослідницького відділу складає 40м^2. Діяльність науково-дослідницького відділу полягає у комп'ютерному проектуванні та моделюванні інформаційно-телекомунікаційних мереж спеціального призначення.

Діяльність працівників науково-дослідницького відділу напряму пов'язана з роботою на комп'ютерному обладнанні (ноутбук або стаціонарний комп'ютер) та користуванням мобільними телефонами. До основних шкідливих та небезпечних факторів виробничого середовища, пов'язаних з роботою на персональному комп'ютері відповідно ДСТУ 12.0.003-74 ССБТ «Загрозливі та шкідливі виробничі фактори», НПАОП 0.00–1.28-10 «Правила охорони праці при експлуатації ОМ» належать: напруга зорових органів та пов'язане з нею перевтомлення; значне навантаження на кисті рук та пальці; тривале знаходження в сидячій позі, що викликає застійні явища в організмі; випромінювання різного виду (рентгенівське, електромагнітне, інфрачервоне, статистичні поля); механічні шуми, пов'язані з роботою кулера, дискового приводу, оргтехніки; іонізація повітря; виділення в повітря робочого приміщення різних хімічних речовин (озон, триметілфосфат, біфеніли).

Мобільний телефон є також джерелом електромагнітного випромінювання, на яке організм певним чином реагує. Наукові досліди підтверджують негативний вплив таких пристроїв на мозок. Але вплив мобільного апарату на організм користувача і досі не є достатньо вивченим

До психологічно шкідливих факторів, які впливають на людину при роботі з комп'ютером можна віднести розумову напругу та нервово-емоційне перевантаження, які виникають внаслідок підвищеної концентрації уваги.

Усі ці фактори негативно впливають на здоров'я працівників відділу технічної підтримки та сприяють виникненню професійних захворювань:

комп’ютерний зоровий синдром; радіохвильова хвороба; синдром висихання рогівки ока; кистьовий тунельний синдром; захворювання шкіри; захворювання кишкового тракту; серцево-судинні захворювання.

Негативними наслідками регулярного використання мобільного телефону є ослаблення пам’яті, часті головні болі, зниження уваги, напруга в барабанних перетинках, порушення сну, дратівливість та ін.

Для зменшення шкідливого впливу негативних факторів виробничого середовища на працівників науково-дослідницького відділу необхідно вжити заходів щодо поліпшення їх умов праці. Розміщення робочих місць з ПК у підвальних приміщеннях та на цокольних поверхах заборонено. Кімната, у якій розташоване робоче місце з ПК повинна мати природне освітлення, яке здійснюється через світлові прорізи, орієнтовані переважно на північ чи північний схід. Віконні прорізи такого приміщення мають бути обладнані регульованими пристроями (жалюзі, завіски, зовнішні козирки). Також приміщення має бути обладнане системою опалення, кондиціонування повітря, або припливно-витяжною вентиляцією для забезпечення оптимальних показників мікроклімату. Загальний контур заземлення будівлі повинен бути виведений через розетку на кожне робоче місце з ПК. Забороняється для оздоблення інтер'єру приміщень з ПК застосовувати полімерні матеріали (деревинно-стружкові плити, шпалери, що миються, рулонні синтетичні матеріали, шаруватий паперовий пластик тощо), що виділяють у повітря шкідливі хімічні речовини. У приміщеннях, де розташовано монітори, потрібно виконувати заходи щодо боротьби зі статичним полем. Найбільш простим способом відповідно до рекомендацій є підтримка відносної вологості повітря на рівні 50-60%, заземлення усіх приладів, а також використання для підлоги антистатичного лінолеуму.

Площа на одне робоче місце з ПК відповідно ДСТУ 12.2.032-78, ССБТ «Робоче місце під час виконання робот сидячи. Загальні ергономічні вимоги» має становити не менше ніж 6,0 м^2, а об’єм не менше ніж 20,0 м^3. Відстань

від робочого місця з ПК до стіни з вікном повинна становити не менше ніж 1,5 м; від інших стін на відстані 1 м, а відстань між столами 1,5 м.

Для зменшення шкідливого впливу негативних факторів виробничого середовища робоче місце з ПК повинно відповідати наступним гігієнічним вимогам: екран та клавіатура повинні розташовуватись на оптимальній відстані від очей користувача, що становить 600...700 мм; висота робочої поверхні робочого столу має бути 800 мм; робочий стіл повинен мати простір для ніг заввишки не менше ніж 600 мм, завширшки не менше ніж 500 мм, завглибшки не менше ніж 450 мм, на рівні простягнутої ноги - ніж 650 мм.

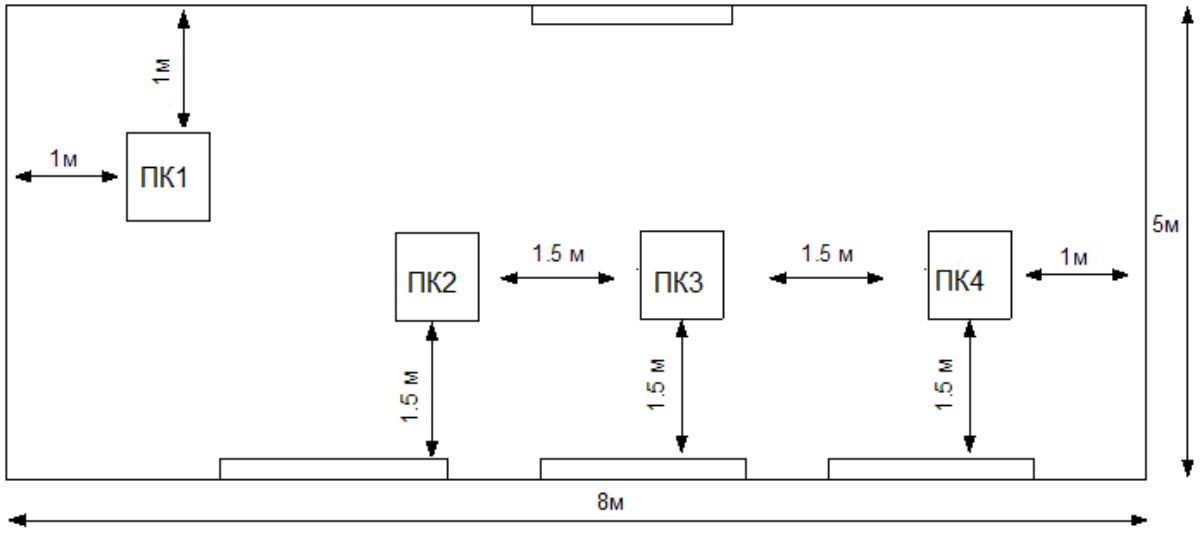

Рисунок А.1 – Розташування робочих місць з ПК у науково-дослідницькому відділі

Для зменшення негативного впливу мобільного апарату необхідно: скоротити до мінімуму час розмови по телефону; обирати мобільний телефон з мінімальним значенням SAR (Specific Absorbtion Rate) – одиниця виміру питомої величини поглинання випромінювання організмом людини. Максимальне значення SAR у Європі складає 2 Вт/кг.

У приміщенні науково-дослідницького відділу є джерела тепловиділення, тому необхідно визначити необхідний умови його вентилювання.

Повітрообмін по теплу визначаємо по формулі:

$$L = \frac{Q_{над}}{c \times p(t_в - t_н)}, \text{ м}^3/\text{год}, \quad (А.1)$$

де $Q_{над}$ - надлишкове виділення тепла в робочому приміщенні, ккал/год.;

с – теплоємкість повітря (0,237 ккал/кг°С);

р – обсягова вага повітря (1,226 кг/ м^3);

$t_в$ – температура витяжного повітря (30°С);

$t_н$ – температура приточного повітря (20°с).

Розрахуємо надлишкове надходження тепла за формулою:

$$Q_{над} = Q_{уст} + Q_{пер} + Q_{осв} + Q_{ср},$$

де $Q_{уст}$ – виділення тепла від устаткування;

$Q_{пер}$ – виділення тепла робітниками;

$Q_{осв}$ – надходження тепла від електричного освітлення;

$Q_{ср}$ – надходження тепла від сонячної радіації через вікна.

Визначимо виділення тепла від устаткування за формулою:

$$Q_{уст} = [(x_1 \cdot k_1) + (x_2 \cdot k_2) + (x_3 \cdot k_3) + (x_4 \cdot k_4)] \cdot K_а \cdot K_б \cdot 860,$$

де х1=4, х2=4, х3=1, х4=1 – кількість системних блоків, моніторів, принтерів, кондиціонерів відповідно;

к1=0.4, к2=0.15, к3=0.1, к4=1 – їх потужність, кВт/год;

$К_а$ - коефіцієнт установленої потужності (0,95);

$К_б$ - коефіцієнт одночасної роботи (1,0).

Розрахуємо:

$$Q_{уст} = \left[(4 \cdot 0.4) + (4 \cdot 0.15) + (1 \cdot 0.1) + (1 \cdot 1)\right] \cdot 0.95 \cdot 1 \cdot 860 = 2696 \text{ ккал/год.}$$

Визначимо виділення тепла від обслуговуючого персоналу за допомогою формули:

$$Q_{пер} = n \times g,$$

де n=4 – кількість працюючих;

g=100 ккал/год. – кількість тепла, що виділяє один працівник за годину (100 ккал/год.)

Розрахуємо:

$$Q_{пер} = 4 \cdot 100 = 400 \text{ ккал/год}$$

Визначимо надходження тепла від електричного освітлення за формулою:

$$Q_{осв} = E_м g_1 S,$$

де Ем – нормована освітленість для цієї зорової роботи приймаємо рівним 400 лк;

g1 - питоме тепловиділення на 1 м^2 підлоги при 1 лк освітленості (для люмінесцентних ламп - 0,05 ккал/год.).

S - площа приміщення, S=40 м^2.

Розрахуємо:

$$Q_{осв} = 400 \cdot 0.05 \cdot 40 = 800 \text{ ккал/год}$$

Визначимо надходження тепла від сонячної радіації через вікна по формулі:

$$Q_{ср} = F \cdot g_2 \cdot K_{осл},$$

де F=6.75(м^2) − площа віконних прорізів;

g_2 − кількість тепла, що надходить через 1 м^2 віконного прорізу (65 ккал/год.);

$К_{осл}$ − коефіцієнт ослаблення, приймаємо − 0,4.

Розрахуємо:

$$Q_{ср} = 6.75 \cdot 65 \cdot 0.4 = 176 \text{ккал/год.}$$

Визначимо кількість надлишкового тепла:

$$Q_{над} = 2696 + 400 + 800 + 176 = 4072 \text{ ккал/год.}$$

Визначимо витрати повітря в приміщенні:

$$L = \frac{4072}{0.237 \cdot 1.226 \cdot (30 - 20)} = 1404 \text{ м}^3\text{/год}$$

Існуюча в наявності система кондиціонування і вентилювання має продуктивність 1700 м3/год, що задовольняє необхідним нормативам.

Параметри мікроклімату на робочих місцях регламентуються ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень». Відповідно доданих санітарних норм температура повітря, швидкість руху повітря і відносна вологість у холодні періоди року повинна складати 21-23 градуса по Цельсію, 0,1 метра в секунду і 40-60 % відповідно. У теплі періоди року температура повітря повинна складати 22-24 градусів Цельсія, рухливість повітря 0,2 метра за секунду, вологість 40-60 %. Вище зазначені норми цілком відповідають фактичним даним приміщення науково-дослідницького відділу.

Найважливішою умовою роботи будь-якого підприємства є дотримання правил пожежної охорони. У приміщенні науково-дослідницького відділу основні міри для забезпечення пожежної безпеки визначає Інструкція про заходи пожежної безпеки для службових приміщень. Вона є обов’язковою

для виконання всіма співробітниками. В інструкції про засоби пожежної безпеки для службових приміщень забороняється:

- улаштовувати тимчасові електромережі, застосовувати саморобні плавкі вставки в запобіжниках, прокладати електричні проводи безпосередньо по пальній основі, експлуатувати світильники зі знятими ковпаками (розсіювачами), використовувати саморобні подовжувачі, що не відповідають вимогам Правил пристрою електроустановок; пристосовувати вимикачі, штепсельні розетки для підвішування одягу й інших предметів, обгортати електролампи і світильники, заклеювати ділянки електромережі пальною тканиною, папером; захаращувати підступи до засобів пожежогасіння, курити, проводити зварювальні й інші вогневі роботи без оформлення відповідного дозволу, застосовувати легкозаймисті рідини.

Первинні засоби пожежогасіння (зокрема вогнегасники) призначені для гасіння пожеж у початковій стадії їхнього розвитку силами персоналу об’єкта до прибуття штатних підрозділів пожежної охорони. Визначення видів та кількості вогнегасників слід проводити з врахуванням фізико-хімічних та пожежонебезпечних властивостей горючих речовин, площ і категорії виробничих приміщень за вибухопожежною небезпекою, а також класу можливої пожежі.

В моєму випадку науково-дослідницький відділ, де розташовані комп’ютери займає площу 40 м^2. Категорія приміщення за вибухопожежною та пожежною небезпекою – В, оскільки в ньому знаходяться тверді горючі матеріали (пластик). Клас можливої пожежі – А. Це приміщення, з огляду на мінімальне псування вимірювальної техніки під час гасіння пожежі бажано оснастити двома вуглекислотними вогнегасниками типу ВВ – 5.

Об’єктом розгляду на предмет визначення надзвичайних небезпек та їх наслідків є науково-дослідницький відділ університету. Однією із вірогідних загроз може бути раптове виникнення пожару внаслідок короткого замикання в електромережах або розрядів статистичної електрики, що може

привести до пошкодження і руйнування устаткування, комунікацій, виділення токсичних продуктів горіння.

Тому в університеті розроблено оперативний план гасіння пожежі, який визначає порядок дії персоналу при пожежі, порядок її гасіння, взаємодію з власним складом пожежних підрозділів, а також застосування схем и засобів пожежогасіння з урахуванням заходів безпеки.

Корпус повинен бути обладнаним мережею протипожежного водо забезпечення, установками виявлення та гасіння пожеж відповідно вимогам нормативно-технічних документів. Кожний працівник повинен чітко знати та виконувати вимоги ППБ та протиаварійний режим на об’єкті, уміти користуватися наявними вогнегасниками, іншими первинними засобами пожежогасіння і знати місце їхнього перебування.

Меблі та устаткування повинні розміщатися таким чином, щоб забезпечувався вільний евакуаційний прохід до дверей виходу з приміщення (шириною не менше 1 м). Евакуаційні шляхи і виходи необхідно постійно держати вільними, нічим не захаращувати. Засоби протипожежного захисту в приміщеннях потрібні триматися у справному стані.

У випадку виявлення пожежі слід: негайно повідомити державну пожежну охорону за телефоном «101», вказати при цьому адресу, кількість поверхів, місце виникнення пожежі, наявність людей, своє прізвище; повідомити про пожежу керівництву, а в нічний час черговому охоронцю; у разі можливості почати гасіння пожежі наявними засобами, організувати зустріч пожежних підрозділів.

При виникненні пожежі у початковій стадії його розвитку випромінюється тепло, накопичуються токсичні продукти згоряння, імовірні руйнування будівельних споруд. Тому слід як можна швидше провести евакуацію людей із палаючої будівлі. Показником ефективності евакуації є час, протягом якого працівники можуть при потрібності залишити окремі приміщення і будівлю в цілому. Безпека евакуації досягається тоді, коли час евакуації не перевищує час настання критичної фази розвитку пожежі, тобто

часу від початку пожежі до досягнення граничних для людини впливів факторів пожежі (критичних температур, ступені задимлення, зниження концентрації кисню и т.п.). Число евакуаційних виходів повинно бути не менш двох. Вони повинні розташовуватися розосереджено. Мінімальна відстань l між найбільш віддаленими один від одного евакуаційними виходами із приміщення визначається за формулою:

$$l = 1{,}5\sqrt{P},$$

де Р – периметр приміщення, м.

Двері на шляхах евакуації повинні відкриватися у напрямку виходу із будівлі (приміщення). У кожному приміщенні на видному місці повинен бути вивішений план евакуації при пожежі. При пожежі обов'язково необхідно враховувати небезпечні чинники і механізм їх дії на людину. При виникненні пожежі, після виклику пожежної охорони, необхідно попередити про це усіх, хто знаходиться поруч, після чого евакуюватися самому і по можливості допомогти евакуюватися іншим, особливо особам літнього віку і дітям, попереджаючи при цьому виникнення паніки. З метою обмеження циркуляції повітря, яке здатне збільшувати швидкість горіння, покидаючи приміщення, закрийте за собою усі двері, якщо це можливо. Якщо пожежа виникла в приміщенні над вами і безпосередньої загрози для вас не спостерігається, то бажано виконати заходи по зниженню можливих втрат від води яку проливають при гасінні пожежі. Для цього необхідно відключити всі електроприводи та прикрити їх поліетиленовою плівкою. Значно гірше, якщо пожежа виникла в приміщенні під вами – потрібно оцінити обстановку и якщо є впевненість, що ще не має сильної задимленості з високою температурою, потрібно негайно покинути приміщення, рухаючись до виходу по коридорам і сходовим кліткам. Користуватися ліфтом категорично забороняється, за винятком ліфтів, які спеціально призначені для

транспортування пожежної охорони. Шахта ліфта є шляхом для поширення диму і отруйних продуктів горіння, до того ж при пожежі ліфт часто відключають і можна опинитися в пастці при пожежі.

Якщо ви знаходитеся в приміщенні де немає пожежи, но відрізани вогнем, димом, високою температурою від головних шляхів евакуації, то в першу чергу необхідно заважити доступу диму и продуктів горіння в це приміщення. Для чого необхідно негайно закрити усі щілини у дверях та під ними змоченими водою ганчірками, рушниками, робочими халатами та інш.

Якщо приміщення все ж заповнено димом, необхідно підповзти до вікна, закрити при цьому рот та ніс змоченою тканиною, яка грає роль фільтру та в певної мірі захищає від продуктів горіння.

Рухатись у задимленій зоні поповзом або максимально пригнувшись, необхідно тому що більшість нагрітих газоподібних отруйних речовин та дим збираються у верхній зоні приміщення, окрім цього, в приміщенні при горінні температура на рівні очей людини у 6 разів вище за температуру на рівні полу, до того ж внизу завжди зберігається більша концентрація кисню. Коли ви опинились біля вікна трохи відкрийте його та дихайте через щілину, очікуючи прибуття пожежників. При їх прибутті негайно зверніть на себе увагу. Ніколи не стрибайте через вікно без відомої на це необхідності (кожний другий стрибок з 4-г поверху при пожежі смертельний).