Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Аналіз і дослідження методів забезпечення відмовостійкості засобами маршрутизації в інфокомунікаційних мережах
(тема)

Виконав:
студент 2 курсу, групи ІКІм-22-1
Недоступ Д.М.
(прізвище, ініціали)

Спеціальність: 172 Телекомунікації та радіотехніка
(код і повна назва спеціальності)
Тип програми: освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма: Інфокомунікаційна інженерія
(повна назва освітньої програми)

Керівник: проф. кафедри ІКІ ім. В.В. Поповського
Єременко О.С.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2024р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 172 Телекомунікації та радіотехніка
(код і повна назва)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Інфокомунікаційна інженерія
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2023р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Недоступу Даніілу Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Аналіз і дослідження методів забезпечення відмовостійкості засобами маршрутизації в інфокомунікаційних мережах
затверджена наказом по університету від «19» жовтня 2023 р. №1212 Ст
2. Термін подання студентом роботи до екзаменаційної комісії 20.01.2024 р.
3. Вихідні дані до роботи: методи математичного програмування; математичні моделі багатошляхової відмовостійкої маршрутизації з різнотипними метриками; засоби аналітичного моделювання процесів відмовостійкої маршрутизації (середовище Python IDLE, GEKKO Optimization Suite, Numpy, Scipy); вихідні дані для проведення моделювання (структура досліджуваної мережі, пропускна здатність каналів зв'язку, елементи мережі для реалізації схем захисту каналу та вузла).
4. Перелік питань, що потрібно опрацювати в роботі:
1) Визначити особливості побудови відмовостійких інфокомунікаційних мереж.
2) Проаналізувати сучасний стан та перспективи розвитку технологій забезпечення відмовостійкості засобами маршрутизації в інфокомунікаціях.
3) Провести огляд та порівняльний аналіз існуючих протоколів та алгоритмів відмовостійкої маршрутизації в інфокомунікаційних мережах.
4) Провести аналітичне моделювання та дослідження багатошляхової швидкої перемаршрутизації з різнотипними метриками з реалізацією схем захисту каналу та вузла.

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації (титульний слайд; опис проблеми, об'єкт, предмет і мета дослідження; актуальність забезпечення відмовостійкості інфокомунікаційних мереж; аналіз технологій забезпечення відмовостійкості засобами маршрутизації; математичні моделі багатошляхової швидкої перемаршрутизації; результати моделювання; висновки).

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	професор Єременко Олександра Сергіївна		15.01.2024

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	19.10.2023	Виконано
2	Збір матеріалів для дослідження	30.10.2023	Виконано
3	Розробка 1 розділу	05.11.2023	Виконано
4	Розробка 2 розділу	26.11.2023	Виконано
5	Розробка 3 розділу	10.12.2023	Виконано
6	Розробка 4 розділу	25.12.2023	Виконано
7	Оформлення кваліфікаційної роботи	15.01.2024	Виконано

Дата видачі завдання 19 жовтня 2023 року

Студент _____ Недоступ Д.М.
(підпис) (прізвище, ініціали)

Керівник роботи _____ проф. Єременко О.С.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 69 с., 31 рис., 9 табл., 16 джерел.

МЕРЕЖА, ВІДМОВОСТІЙКА МАРШРУТИЗАЦІЯ, ШВИДКА ПЕРЕМАРШРУТИЗАЦІЯ, КАНАЛ, ВУЗОЛ, РЕЗЕРВУВАННЯ, ЯКІСТЬ ОБСЛУГОВУВАННЯ.

Об’єкт дослідження – процес забезпечення відмовостійкості засобами маршрутизації в інфокомунікаційних мережах.

Предмет дослідження – методи відмовостійкої маршрутизації в інфокомунікаційних мережах.

Мета роботи – аналіз і дослідження методів відмовостійкої маршрутизації в інфокомунікаційних мережах.

Методи досліджень – аналіз, формалізація, моделювання та порівняння.

В роботі виконано комплексне дослідження методів відмовостійкої маршрутизації для стійкості мереж до зовнішніх факторів. Дослідження містило наступні етапи: аналіз актуальних перешкод і викликів, що запобігають реалізації відмовостійких систем, оцінка сучасного стану та перспектив розвитку технологій забезпечення відмовостійкості, а також дослідження сучасних підходів, моделей, методів та алгоритмів, за допомогою яких вирішується проблема забезпечення відмовостійкості інфокомунікаційних мереж. Також в роботі розв’язується задача відмовостійкої маршрутизації на основі потокових моделей швидкої перемаршрутизації з використанням схем резервування каналу та вузла. Проводиться дослідження та порівняльний аналіз побудови маршрутних рішень для основного та резервного шляхів за умови багатошляхової стратегії та різних метрик по аналогії з протоколами RIP та OSPF.

ABSTRACT

The report contains: 69 p., 31 fig., 9 table, 16 sources.

NETWORK, FAULT TOLERANT ROUTING, FAST REROUTING, LINK, NODE, RESERVATION, QUALITY OF SERVICE.

A research object is a process of ensuring fault tolerance by routing means in information and communication networks.

The subject of research is methods of fault-tolerant routing in information and communication networks.

The work aims to analyze and research the methods of fault-tolerant routing in information and communication networks.

Methods of research are analysis, formalization, modeling, and comparison.

The work presents a comprehensive study of fault-tolerant routing methods for network resilience to external factors. The study included the following stages: analysis of existing obstacles and challenges that prevent the implementation of fault-tolerant systems, assessment of the current state and prospects for the development of fault-tolerance technologies, as well as research of modern approaches, models, methods, and algorithms that solve the problem of ensuring the fault-tolerance of information and communication networks. The work also solves the problem of fault-tolerant routing based on flow-based fast reroute models using link and node protection schemes. A study and comparative analysis of the routing solutions for the primary and backup paths is carried out under the condition of a multi-path strategy and various metrics by analogy with the RIP and OSPF protocols.

ЗМІСТ

Перелік скорочень, умовних позначень, символів, одиниць і термінів ……. 8
Вступ …….. 9
1 Аналіз основ побудови відмовостійких інфокомунікаційних мереж ... 11
1.1 Визначення актуальності забезпечення відмовостійкості інфокомунікаційних мереж …….. 11
1.2 Використання маршрутизації як засобу забезпечення стійкості інфокомунікаційних мереж …….. 12
2 Аналіз сучасного стану та перспектив розвитку технологій забезпечення відмовостійкості засобами маршрутизації в інфокомунікаціях …….. 19
2.1 Визначення ролі відмовостійкості та якості обслуговування в інфокомунікаційних мережах ……... 19
2.2 Використання шестиступінчатої стратегії відмовостійкості в інфокомунікаційних мережах …….. 21
2.3 Перспективи розвитку підходів до вдосконалення відмовостійкої маршрутизації ……. 23
3 Огляд та порівняльний аналіз існуючих протоколів та алгоритмів відмовостійкої маршрутизації в інфокомунікаційних мережах …… 27
3.1 Класифікація засобів відмовостійкої маршрутизації в інфокомунікаційних мережах ……. 27
3.2 Огляд основних протоколів резервування шлюзу за замовчуванням …….. 30
3.3 Забезпечення відмовостійкої маршрутизації за допомогою технології Fast ReRoute …… 34
3.4 Аналіз моделей і методів відмовостійкої маршрутизації …….. 38
4 Дослідження та порівняльний аналіз потокових моделей швидкої перемаршрутизації ……... 43
4.1 Математичні моделі швидкої перемаршрутизації в інфокомунікаційних мережах …….. 43
4.2 Дослідження та аналіз потокових моделей швидкої перемаршрутизації ……... 46
Висновки …… 65

Перелік джерел посилання ……. 68

Додаток А Вихідний код програми проведення аналітичних розрахунків для моделі швидкої перемаршрутизації …… 70

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ІКМ – інфокомунікаційна мережа
КЗ – канал зв’язку
ПЗ – пропускна здатність
ТКМ – телекомунікаційна мережа
ARP – Address Resolution Protocol
ATM – Asynchronous Transfer Mode
BER – Bit Error Rate
DDoS – Distributed Denial-of-service attack
ECMP – Equal Cost MultiPaths
FHRP – First-Hop Redundancy Protocol
FRR – Fast ReRoute
LSP – Label Switched Path
LP – Link Protection
LFA – Loop Free Alternate
MPLS – Multi Protocol Label Switching
NP – Network Performance
NP – Node Protection
QoE – Quality of Experience
QoR – Quality of Resilience
QoS – Quality of Service
SDN – Software-defined Networking
SPOF – Single Point of Failure
TE – Traffic Engineering

ВСТУП

В інформаційно-комунікаційних мережах надійність і неперервність зв'язку є критичними факторами для забезпечення безперебійної роботи різних додатків і послуг. З поширенням мережних технологій і зростанням обсягу передачі даних вимоги до відмовостійкості стають ще більш актуальними. Тому аналіз і дослідження методів забезпечення відмовостійкості засобами маршрутизації в інфокомунікаційних мережах стає надзвичайно важливим завданням у галузі інфокомунікаційних технологій.

Однією з ключових складових стійкості мереж є методи маршрутизації, які визначають оптимальний шлях передачі даних у мережі. Вони відіграють вирішальну роль у забезпеченні ефективності та надійності мережі. Однак з підвищенням складності та об'єму даних, що обробляються мережами, та зі зростанням загроз кібербезпеці, стає складніше вирішувати проблему стікойсті мереж, тому завдання забезпечення відмовостійкості процесів маршрутизації стає дедалі актуальнішим.

Таким чином, аналіз і дослідження перспективних методів забезпечення відмовостійкості засобами маршрутизації в інфокомунікаційних мережах (ІКМ), а також вибір ефективної моделі відмовостійкої маршрутизації, її простота, наочність і достовірність отриманих з її допомогою результатів представляється важливою науковою та практичною задачею.

Метою роботи є аналіз і дослідження методів відмовостійкої маршрутизації в інфокомунікаційних мережах.

Для вирішення цієї задачі в першому розділі визначено основи побудови відмовостійких інфокомунікаційних мереж. Окреслено перешкоди та виклики, що запобігають реалізації відмовостійких систем. А також було підкреслено актуальність забезпечення відмовостійкості інфокомунікаційних мереж та запропоновано використання маршрутизації як засобу забезпечення стійкості інфокомунікаційних мереж.

У другому розділі роботи проведено аналіз сучасного стану та перспектив розвитку технологій забезпечення відмовостійкості засобами маршрутизації в ІКМ. Визначені ролі відмовостійкості та якості обслуговування в інфокомунікаціях. Проаналізовані переспективи розвитку підходів до вдосконалення стійкості

маршрутизації та приділено увагу використанню сучасної шестиступінчатої стратегії відмовостійкості мереж.

У третьому розділі проведено огляд та порівняльний аналіз існуючих протоколів та алгоритмів відмовостійкої маршрутизації в інфокомунікаційних мережах. Приведено класифікацію засобів відмовостійкої маршрутизації, розглянуті основні протоколи резервування шлюзу за замовчуванням та проаналізовано забезпечення відмовостійкої маршрутизації за допомогою технології FastReRoute. Також приділено увагу аналізу моделей і методів відмовостійкої маршрутизації в ІКМ.

Четвертий розділ роботи присвячено дослідженню та порівняльному аналізу потокових моделей швидкої перемаршрутизації. У межах оптимізаційної постановки задачі були представлені та описані математичні моделі швидкої перемаршрутизації з різними метриками за умови реалізації схем захисту (резервування) каналу та вузла в інфокомунікаційній мережі. На прикладі досліджуваного фрагменту мережі було проведено моделювання з використанням бібліотек Python NumPy та Scipy. З урахуванням різних метрик формування маршрутів було проведено дослідження щодо побудови маршрутних рішень для основного та резервного шляхів при зміні значення інтенсивності потоку та вибору елемента мережі (каналу або вузла), що підлягає захисту. Проведені дослідження дозволили зробити висновки відносно вибору метрики.

Окремі результати роботи доповідались на Міжнародних наукових конференціях. Кваліфікаційна робота пов'язана з дослідженнями у межах науково-технічної (експериментальної) розробки 0123U100128 "Розробка алгоритмічно-програмного забезпечення для кіберстійких інфокомунікаційних систем і мереж критичних інфраструктур", що ведеться на кафедрі інфокомунікаційної інженерії імені В.В. Поповського Харківського національного університету радіоелектроніки.

1 АНАЛІЗ ОСНОВ ПОБУДОВИ ВІДМОВОСТІЙКИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ

1.1 Визначення актуальності забезпечення відмовостійкості інфокомунікаційних мереж

Сьогодні інформаційно–комунікаційні технології відіграють провідну роль у цифровізації світу. Програмне забезпечення для бізнесу, охорони здоров’я, науки та соціальні мережі працюють через інтернет. Всі сервери дата-центрів по всьому світу підключені через глобальну мережу. Це все вимагає постійного підключення, безперебійного доступу, продуктивності та відмовостійкості інфокомунікаційної інфраструктури [1-3].

Навіть при сталому покращенні надійності сучасного комунікаційного обладнання, проблема забезпечення очікуваного рівня стійкості інфокомунікаційних мереж все ще залишається актуальною. Несправності елементів комунікаційної мережі неминучі. Вони можуть виникати з різних причин, таких як стихійні лиха (наприклад, урагани, землетруси), людські помилки (наприклад, обрив кабелю) або зловмисні атаки. Незважаючи на різноманітність причин, їх об’єднує одна спільна риса – їх неможливо усунути [2].

Через зростаючу залежність від комунікаційних мереж, обмін інформацією значно збільшується. Як наслідок, нові збої мережних каналів (або вузлів) призводять до значних втрат даних і прибутку. З постійним розширенням охоплення комунікаційних мереж для підтримки майже всіх видів діяльності нашого суспільства, очікується, що негативні наслідки збоїв лише посилюватимуться.

Кажучи про телекомунікаційну інфраструктуру, що включає як стаціонарні, так і мобільні мережі зв’язку, у тому числі стаціонарні та мобільні телефонні системи, вона грає важливу роль у забезпеченні швидкого обміну інформацією, навіть у віддалених районах. Ця інфраструктура стала необхідною складовою соціальної та економічної основи нашого повсякденного життя.

Зважаючи на розвиток Інтернету та широкосмугових з’єднань, що стали вкрай важливими завдяки останнім технологічним досягненням, телекомунікаційна інфраструктура набула нового статусу, ставши не лише засобом забезпечення традиційних телефонних послуг, але й основним середовищем для

поширення різноманітної інформації та надання різних послуг, наданих державою та приватними компаніями.

У випадку надзвичайних ситуацій, таких як природні катастрофи, телекомунікаційна інфраструктура використовується для надання засобів екстреного сповіщення та забезпечення зв’язку для основних адміністративних служб. Така інфраструктура має велике значення для забезпечення безпеки та добробуту громадян та здатності країни функціонувати в надзвичайних обставинах.

У період або після стихійних лих, голосові дзвінки по телефону та мобільній телефонній мережі найчастіше використовуються для підтвердження безпеки та обміну інформацією в зоні події. Однак велика кількість дзвінків може призводити до перевантаження мережі, що є важливою проблемою, яку можна вирішити за допомогою нових технологій та відповідної поведінки користувачів.

Також надзвичайно важливо відновлювати телекомунікаційну інфраструктуру після надзвичайних ситуацій. Кабелі, мобільні базові станції та локальні комутатори можуть зазнати значних пошкоджень, і відновлення інфраструктури вимагає використання всіх доступних засобів [4].

З погляду відмовостійкості та відновлення мережі, обговорені вище аспекти становлять ключові виклики. Запобігання та мінімізація перебоїв у зв’язку у разі пошкодження інфраструктури є двома головними цілями у сфері стійкості мережі.

Проблема забезпечення відмовостійкості інфокомунікаційних мереж стає все більш важливою в сучасному світі. Розвиток та вдосконалення інфраструктури зв'язку стають вимогою часу для забезпечення стабільності та надійності у надзвичайних ситуаціях, а також для забезпечення безперебійного функціонування суспільства.

1.2 Використання маршрутизації як засобу забезпечення стійкості інфокомунікаційних мереж

До основних глобальних причин відмов у інфокомунікаційних та телекомунікаційних мережах відносять катастрофи, вплив соціально-політичних і економічних факторів, відмови, що виникають в результаті первинних проблем, помилки операторів, загрози для мережної безпеки, а також проблеми, пов'язані з навколишнім середовищем. Крім того, серед технічних факторів, які спричиняють відмови в мережах, можна відзначити проблеми фізичного рівня, несправності та перевантаження мережного обладнання під час експлуатації, а також помилки в

конфігурації та оновленні термінального та мережного програмного забезпечення [5].

Інфокомунікаційні мережі стикаються з великою групою викликів, розпізнавання яких має вирішальне значення для проектування та планування мережі. Причину відмови можна визначити як характеристику або умову, яка може виникнути як подія, що впливає на нормальну роботу мережі [6].

До основних причин відмов мережі відносять:

– Великомасштабні катастрофи (Large–Scale Disasters) – можуть бути спричинені силами природи, включаючи землетруси або урагани, що призводять до значних порушень ліній зв'язку, а також комунікаційного обладнання (вузлів). Окрім наземних або метеорологічних причин, стихійні лиха можуть також бути наслідком космологічних подій, включаючи, наприклад, геомагнітні бурі. Іншим джерелом великомасштабних катастроф є людська діяльність. Такі антропогенні катастрофи можуть бути спричинені як зловмисними діями, так і наслідком ігнорування ранніх попереджень у роботі системи.

– Соціально-політичні та економічні виклики (Socio-Political and Economical Challenges) – включають навмисні дії (в тому числі терористичні акти), спрямовані на порушення нормальної роботи мережі, наприклад, як відповідь на політичні рішення або просто для досягнення переваги на економічних ринках.

– Залежні відмови (Dependent Failures) – стосуються викликів, які можуть призвести до каскаду відмов, наприклад, після відмови системи (або її частини), що надає послуги іншій системі. Прикладами можуть бути електромережі, що забезпечують електропостачання для Інтернету.

– Людські помилки (Human Errors) – передбачають незловмисні людські дії. Вони включають, наприклад, помилки неправильної конфігурації, що є результатом некомпетентності людини. Як наслідок, комунікаційні мережі можуть навіть зіткнутися з катастрофічними збоями.

– Зловмисні атаки (Malicious Attacks) – це ще одна група викликів, які стосуються навмисних дій, спрямованих на спричинення якомога більших збоїв, зазвичай спрямованих на найважливіші програмно-апаратні елементи мережної інфраструктури.

– Незвичайний трафік (Unusual Traffic) – може бути проблемою, якщо його обсяг перевищує обмеження (тобто верхню межу), які встановлені на етапі проектування мережі. Такий додатковий трафік може бути виявлений у мережі, наприклад, після виникнення катастрофічної події, яка не обов’язково порушує

саму мережну інфраструктуру, але призводить до значного збільшення кількості одночасних запитів на отримання інформації.

– Екологічні виклики (Environmental Challenges), у свою чергу, залежать від характеристик комунікаційного середовища. Вони пов'язані, наприклад, з аспектами мобільності в бездротових ad-hoc мережах (зокрема, із залежними від часу характеристиками бездротових з'єднань).

Класифікацію подій, що призводять до масових збоїв/перебоїв у комунікаційних мережах можна побачити на рис. 1.1.

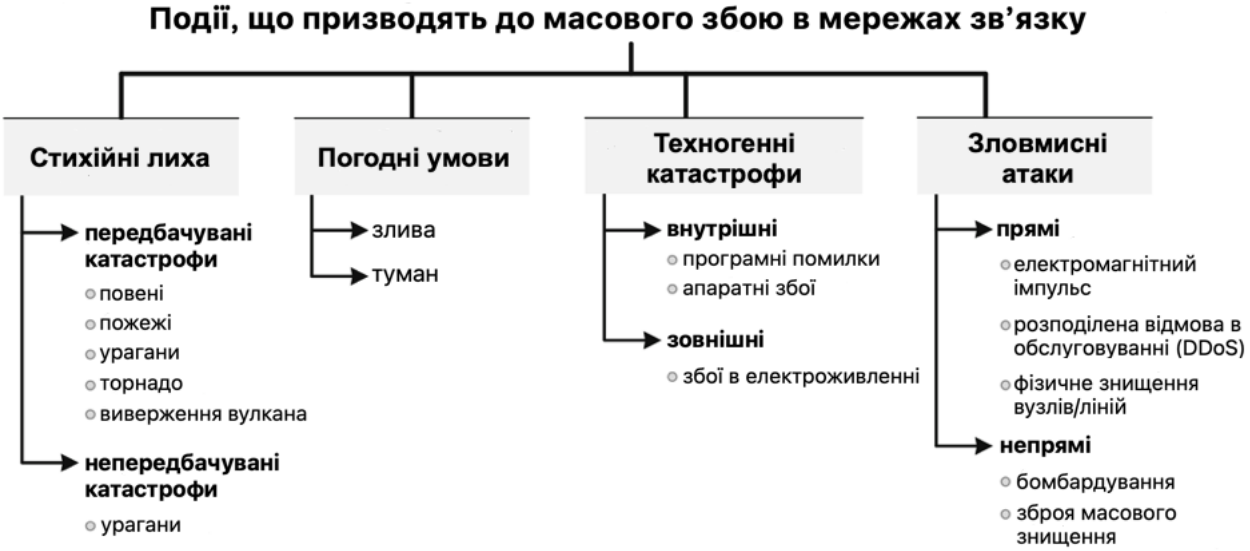

Рисунок 1.1 – Класифікація подій, що призводять до масових збоїв/перебоїв у комунікаційних мережах [7]

Незалежно від проблеми, найважливіші аспекти стосуються характеристик, які можна виміряти в просторі та в часі. Як показано в табл. 1.1, вплив збою на продуктивність комунікаційної мережі може відрізнятися від початкового масштабу та тривалості виклику. Наприклад, атака, яка є проблемою, пов'язаною з одним вузлом, може вплинути на продуктивність усієї мережі.

Будь-який мережний виклик можна класифікувати на основі детальних критеріїв, включаючи причину (природна, створена людиною або залежна від виклику), межі (внутрішні чи зовнішні), ціль (пряма чи побічна), задача (незловмисна або зловмисний), намір (ненавмисний або навмисний), здатність (випадковість або некомпетентність), розмір (апаратне забезпечення, програмне забезпечення, протоколи або трафік), домен (середовище), обсяг (вузли, зв'язки або область), значимість (незначна, велика або катастрофічна), стійкість (короткочасна,

довготривала або тимчасова) і повторення (одноразове, багаторазове або адаптивне) [6].

Таблиця 1.1 – Просторові та часові характеристики відмов мережі [6]

Тип відмови	Простір		Тривалість	
	Масштаб	Наслідки	Масштаб	Наслідки
Землетрус	100 км^2	100 км^2	Секунди	Дні
Пожежа	100 м^2	10 км^2	Години	Дні
Ураган	100 км^2	100 км^2	Години	Дні
Зловмисна атака	Сервер	Глобальний	Години	Години
Неправильна конфігурація	Сервер	Глобальний	Секунди	Хвилини
Пандемія	Глобальний	Глобальний	Дні	Місяці
Політичні причини	–	Регіональний/Глобальний	–	Роки
Відключення електроенергії	100 км^2	Регіональний	Хвилини	Години
Сонячна буря	1000 км^2	1000 км^2	Хвилини	Дні
Тероризм	100 км^2	Глобальний	Години	Години

Виявлення проблем у режимі реального часу є складним завданням, особливо коли вони мають низку спільних симптомів. Наприклад, збільшення трафіку може бути наслідком спроби атаки розподіленої відмови в обслуговуванні (DDoS) або просто законного перевантаження, спричиненого спалахом активності користувачів.

Для правильного розпізнавання викликів часто необхідний багатоетапний підхід (рис. 1.2). Він включає виявлення симптомів відмови (тобто, які можуть призвести до розпізнавання початку збою), визначення першопричини та визначення потенційного впливу на систему. Однак, щоб бути економічно ефективним, будь-яким діям з відновлення має передувати оцінка збою порівняно з вартістю відновлення. Механізми виявлення викликів, які зазвичай викликаються розподіленим способом, повинні бути якомога меншими, щоб не використовувати

ресурси без потреби (що є ключовою вимогою для мереж з обмеженими ресурсами) і не порушувати нормальну роботу мережі [6].

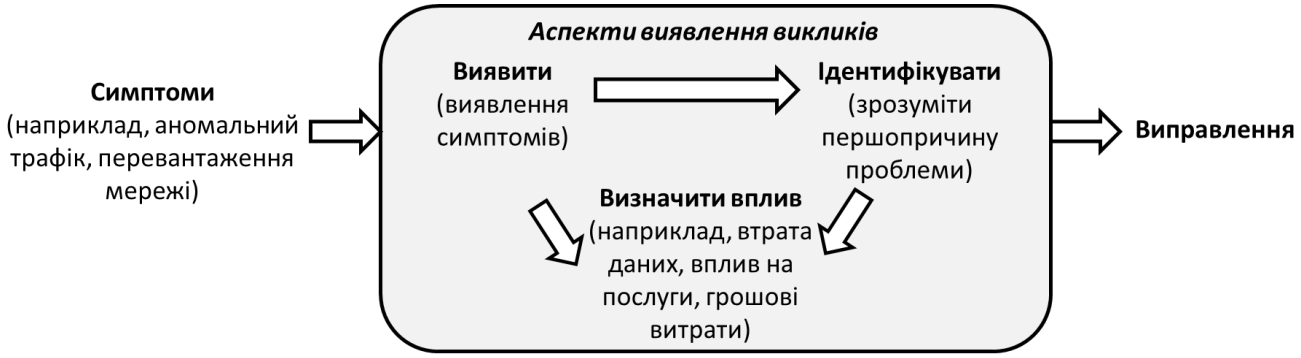

Рисунок 1.2 – Аспекти ідентифікації несправності мережі [6]

Проблема має бути виявлена в режимі реального часу або на фізичному рівні (наприклад, через втрату сигналу, втрату модуляції або втрату тактового сигналу) за допомогою розпізнавання погіршення сигналу (наприклад, збільшення частоти бітових помилок – BER), або погіршення якості обслуговування (вказується зниженням пропускної здатності або збільшенням затримки передачі). Після виявлення несправності важливо локалізувати точку несправності, щоб поширювати повідомлення про несправності, необхідні для усунення негативних наслідків несправності на продуктивність мережі. Повне повернення мережі зв'язку до нормального робочого стану може бути досягнуто пізніше, лише якщо усунути основні причини несправності [6].

Несправність, якщо її не усунути належним чином, може призвести до збою служби (або короткого збою).

Проблеми, що призводять до збоїв мережних каналів або вузлів, часто означають серйозні збої в маршрутизації запитів. Виникаюча проблема недоступності шляхів зв'язку додатково загострюється внаслідок безперервного експоненціального збільшення обсягу переданої інформації. Оскільки збої в шляхах зв’язку неминучі просто через нездатність запобігти значній підмножині викликів, необхідні відповідні модифікації схем маршрутизації, щоб зробити наскрізний зв’язок можливим у разі виникнення проблем.

У зв’язку з цим на сьогоднішній день надзвичайно актуальною є задача, пов’язана з побудовою так званих відмовостійких мереж (Resilient Networks), здатних забезпечити високий рівень якості обслуговування (Quality of Service, QoS) та відмовостійкості (Quality of Resilience, QoR).

Слід відзначити, що відмовостійкість мереж розглядається як окремий аспект забезпечення якості обслуговування і акцентує увагу на параметрах, пов'язаних з надійністю інфокомунікаційних мереж (ІКМ). Важливість якості стійкості до відмов (QoR) є надзвичайною, оскільки вона має вирішальне значення для нормального функціонування мереж і впливає на різноманітні технології, які забезпечують різнорівневу якість обслуговування (QoS) для кінцевих користувачів (рис. 1.3) [5].

Рисунок 1.3 – Співвідношення вимог щодо якості обслуговування та відмовостійкості [2]

Основні засоби забезпечення надійності телекомунікаційних мереж включають:

– інженерні стратегії для організації експлуатації, технічного обслуговування та ремонту обладнання в телекомунікаційній системі;

– засоби для діагностики (включаючи самодіагностику) та перевірки працездатності елементів мережі;

– протоколи для моніторингу та збору інформації про стан мережі;

– засоби для передбачення відмов елементів мережі та аналізу можливих несправностей;

– протоколи для резервного (дублюючого) забезпечення елементів мережі та її сегментів;

– механізми маршрутизації;

– розподіл навантаження в мережі;

– планування мережі з використанням структурного та функціонального резерву;

– методи переконфігурації мережі.

Отже, маршрутизація може використовуватися для забезпечення відмовостійкості інфокомунікаційних мереж, як під час активного вибору та використання найбільш надійних маршрутів (проактивний підхід), так і під час оперативного переключення потоків у разі відмови та резервування мережних компонентів (реактивний підхід) [2].

2 АНАЛІЗ СУЧАСНОГО СТАНУ ТА ПЕРСПЕКТИВ РОЗВИТКУ ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ ЗАСОБАМИ МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЯХ

2.1 Визначення ролі відмовостійкості та якості обслуговування в інфокомунікаційних мережах

Відмовостійкість – це здатність мережі або системи забезпечувати і підтримувати прийнятний рівень обслуговування в умовах різних збоїв і викликів (наприклад, атак) для нормальної роботи [7]. Для мережних топологій забезпечення відмовостійкості еквівалентно основному збереженню втрат, джиттера і затримок настільки успішно, наскільки це можливо для даного сервісу – і, звичайно, ці аспекти якості обслуговування (QoS) можуть бути скомпрометовані, якщо відбуваються збої/атаки і якщо механізми відмовостійкості недоступні для їх усунення. Крім топології, широкі аспекти рівня обслуговування, які повинні бути збережені, – це доступність і надійність обслуговування [7].

У майбутньому відмовостійкість мережних послуг буде особливо важливою, оскільки в багатьох випадках такі послуги все частіше будуть пропонуватися критично важливими додаткам/системам, і вони потребуватимуть гарантій, що виходять за рамки "best effort delivery" (найкраще обслуговування, але відсутність гарантій доставки пакетів), які спочатку вважалися прийнятними для додатків, що пропонувалися ранніми (і навіть більш пізніми) мережами.

Протягом останнього десятиліття і більше були спроби розробити вимоги, які будуть засновані на майбутніх мережних додатках, принципах та підходах – це змушує згадати історичні зусилля, включаючи дослідження, проведені за часів мереж з асинхронним режимом передачі (ATM), які були розвитком телекомунікаційних технологій, призначених для передачі даних в майбутньому. Зазвичай прийнято класифікувати додатки (в тому числі й ті, що передбачаються в майбутньому) за групами, які спрощують завдання визначення додаткової підтримки, яку повинна надавати мережа. Вони визначають ступінь, до якого згадані вище аспекти QoS будуть підтримуватися послугою. Новітні додатки, які передбачаються в майбутньому, вимагатимуть ретельного контролю затримок, а також синхронізації між значною кількістю потоків, щоб послуги могли бути скоординованими. Існуватиме цілий ряд рівнів деградації, дозволених групам

додатків, і вимоги до них потрібно буде ретельно відстежувати і контролювати перед обличчям викликів для мережних операцій. Таким чином, зростуть вимоги до забезпечення відмовостійкості в мережі і до різних транспортних послуг, що пропонуються [7].

У найближчому майбутньому прогнозується поява нових мережних послуг, таких як голографічні комунікації та зв'язок між транспортними засобами, які матимуть надзвичайно низькі вимоги до затримок, а також надзвичайно високу пропускну спроможність. Будь-який збій, який не вдасться відновити, буде значною втратою для мережних операторів. Тому відмовостійкість мережі є життєво важливою для підтримки QoS мережі, а також високої доступності та надійності нових, вимогливих послуг.

Визначення відмовостійкості мережі, наведене вище, включає в себе кілька суміжних дисциплін, які спрямовані на усунення несправностей і викликів.

1) Дисципліни, пов'язані з толерантністю до викликів, які стосуються проектування та інжинірингу стійких мереж.

2) Дисципліни, пов'язані з надійністю, які надають способи опису стійкості мережної системи.

Схему наведений дисциплін показано на рис. 2.1.

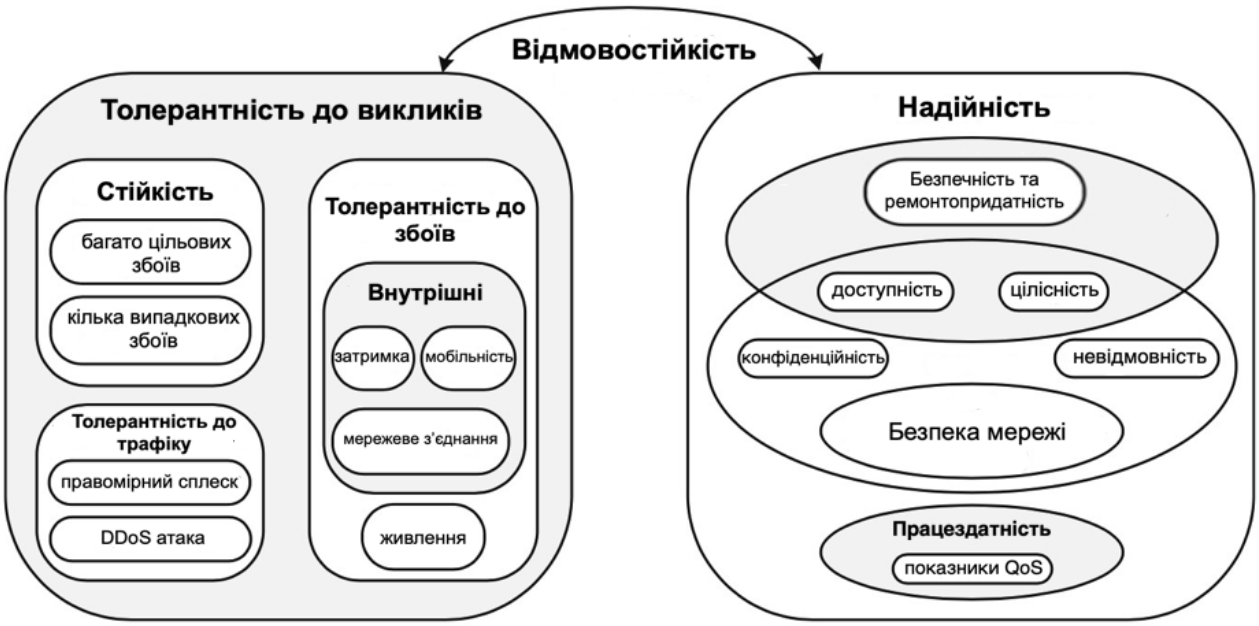

Рисунок 2.1 – Дисципліни, пов'язані з відмовостійкістю мережі та їх взаємозв'язок [7]

Дисципліна відмовостійкості має на меті забезпечити безперервне обслуговування (тобто запобігти збоям), коли існує невелика кількість некорельованих помилок. Це досягається за рахунок резервування апаратного та програмного забезпечення. Очевидно, що застосування надмірності для стійкості є важливим; однак, цього недостатньо для високо корельованих проблем. Необхідно застосовувати інші механізми суміжних дисциплін, наприклад стійкість системи.

Стійкість – здатність системи підтримувати оптимальний стан під час атак або великомасштабних стихійних лих [7]. Це завдання вимагає різноманітності для пом'якшення наслідків великомасштабних стихійних лих і атак. Різноманітність може застосовуватися в різних формах, залежно від завдання, яке потрібно вирішити. Наприклад, щоб забезпечити стійкість до стихійних лих, таких як зсуви або повені, можна застосувати географічне розмаїття мережних компонентів. У той же час, щоб пом'якшити певні типи кібератак, різноманітність системних реалізацій може бути використана для забезпечення того, щоб програмне забезпечення не містило такої ж уразливості, як та, яку використовує зловмисник. Таким чином, механізми стійкості, засновані на надмірності та різноманітності, добре підходять для боротьби з перебоями в мережі.

2.2 Використання шестиступінчатої стратегії відмовостійкості в інфокомунікаційних мережах

Навколо проблеми відмовостійкості мереж було проведено значну кількість досліджень. Однак, незважаючи на ці різноманітні зусилля, інфокомунікаційні системи проявляють меншу стійкість, ніж було б бажано.

Значним недоліком існуючих досліджень і розгорнутих систем є відсутність систематичного погляду на проблему стійкості, тобто погляду на те, як створити мережу, стійку до викликів, яка виходить за межі тих, що розглядаються в одній тематичній області.

Для вирішення даної проблеми, компанією ResumeNet була розроблена стратегія стійкості D2R2+DR (Defend, Detect, Remediate, Recover, Diagnose and Refine). В основі даної стратегії знаходяться циклічні процеси, які в реальному часі виявляють проблеми в роботі мережі та їх вплив на неї, а також аналізують показники (метрики), що можуть кількісно оцінити стан мережі [8].

Ілюстрацію циклічних процесів стратегії стійкості D2R2+DR можна побачити на рис. 2.2.

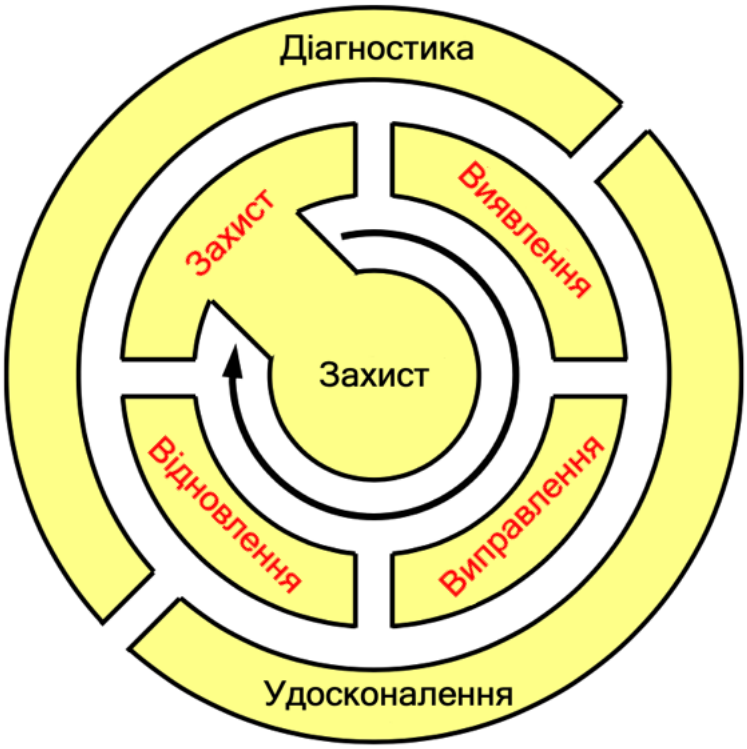

Рисунок 2.2 – Циклічні процеси стратегії стійкості D2R2+DR [7]

Усі індивідуальні процеси D2R2+DR мають визначену зону відповідальності та функціональне призначення.

1. Defend – аналіз мережі або мережної системи, яку потрібно захистити. Цей етап включає в себе проектування системи таким чином, щоб вона була стійкою до потенційних загроз. Це включає налаштування резервних та різноманітних компонентів, щоб система мала можливість автоматично переконфігуруватися в разі виникнення небажаних ситуацій. Ключовим етапом на цьому початковому етапі є проведення оцінки ризиків, щоб визначити слабкі місця системи, які можуть бути найбільш вразливими та які становлять найбільшу загрозу для її надійності в разі порушення.

2. Detect – другий етап полягає у якнайшвидшому виявленні аномалій за допомогою механізмів моніторингу, а саме виявлення, класифікація та аналіз проблем, які порушили оптимальний процес надання послуг.

3. Remediate – процес відновлення, включаючи автономні дії, для максимально швидкого відновлення надання послуг та зменшення збитків, спричинених зовнішніми або внутрішніми небажаними факторами.

4. Recover – етап відновлення, який необхідний для відновлення нормального функціонування мережі або мережної системи або досягнення максимально

можливого приближення до початкового стану після повного усунення несприятливого чинника (відмови, збою) або ворожої кібер-атаки.

5. Diagnose – етап діагностики та аналізу виправленої проблеми. Відбуваються процес оцінки її впливу на систему та визначення можливих заходів для запобігання подібним проблемам у майбутньому.

6. Refine – процес ухвалення рішень з метою запобігання діагностований та проаналізованій проблемі у майбутньому, наприклад як переконфігурація конкретних компонентів або зміна логіки окремих процесів.

Основною перевагою стратегії D2R2+DR є використання політик для керування поведінкою системи [8]. Оскільки проблеми, пов'язані з роботою інфокомунікаційної інфраструктури, можуть виникати несподівано та непередбачувано, вони потребують негайної реакції для відновлення прийнятного рівня обслуговування. Для згладжування цих проблем необхідні складні багатоетапні стратегії, які об'єднують різноманітні механізми моніторингу та виявлення, що впливають на роботу механізмів відновлення [8]. Таким чином, управління на основі політик виявляється досить ефективним для управління складними системами. Ці політики допомагають налаштовувати схеми відмовостійкості, дозволяючи описувати стратегії адаптації системи до зовнішніх або внутрішніх негативних впливів у реальному часі, що в свою чергу підвищує рівень її відмовостійкості.

Отже, у новій ері все більшого розгортання програмно-конфігурованих інфокомунікаційних мереж, ключові аспекти безпеки та відмовостійкості залишаються відкритими для подальшого вивчення. Деякі завдання, пов'язані з цими аспектами, вже були вирішені, проте вимоги нових областей надання послуг настільки настійливо вказують на необхідність перегляду питань забезпечення безпеки та відмовостійкості, що потребує подальшого вивчення і розвитку.

2.3 Перспективи розвитку підходів до вдосконалення відмовостійкої маршрутизації

Слід зауважити, що в сучасних мультисервісних телекомунікаційних мережах вже не достатньо просто забезпечити захист каналів, вузлів і шляхів для відмовостійкої маршрутизації. Необхідно також гарантувати якість обслуговування вздовж основних і резервних маршрутів. Це особливо важливо, оскільки більшість сучасних додатків вимагає QoS за різними параметрами, такими як пропускна

здатність, часові параметри та надійність. Наприклад, мультимедійні додатки можуть бути чутливими як до доступної пропускної здатності, так і до затримок у передачі пакетів тощо. Отже, вирішення завдань відмовостійкої маршрутизації вимагає захисту не одного показника якості обслуговування, а всієї групи параметрів якості обслуговування, як вздовж основних, так і резервних маршрутів [5].

Властивості реакції різних додатків на параметри якості обслуговування (QoS) можна побачити в табл. 2.1.

Таблиця 2.1 – Чутливість трафіка різних додатків до значень QoS-показників [2, 4]

Додаток	Надійність	Середня затримка	Джитер	Пропускна здатність
Електронна пошта	Висока	Низька	Низька	Низька
Передача файлів	Висока	Низька	Низька	Середня
Web доступ	Висока	Середня	Низька	Середня
Аудіо за вимогою	Низька	Низька	Низька	Середня
Відео за вимогою	Низька	Низька	Висока	Висока
Телефонія	Низька	Висока	Висока	Низька
Відеоконференція	Низька	Висока	Висока	Висока

На основі аналізу існуючих і майбутніх рішень щодо відмовостійкої маршрутизації можна класифікувати перспективні схеми захисту рівня якості обслуговування в телекомунікаційних мережах (табл. 2).

Перший тип, позначений як QoS^1–FRR, включає в себе рішення, спрямовані на швидке переключення з захистом одного параметра мережної продуктивності (Network Performance, NP). Наприклад, це можуть бути рішення, орієнтовані на забезпечення високої пропускної здатності, оскільки саме пропускна здатність є ключовим та одним із найважливіших показників якості обслуговування. Також існують досить ефективні одношляхові так і багатошляхові стратегії маршрутизації, які поєднують захист каналу, вузла або шляху з підтримкою пропускної здатності мережі.

Таблиця 2.2 – Схеми захисту рівня якості обслуговування в телекомунікаційних мережах [5]

Тип схем	Показники мережної продуктивності (Network Performance)		
	Пропускна здатність	Середня затримка	Ймовірність втрат пакетів
QoS[1]-FRR	+	–	–
QoS[2]-FRR	+	+	–
	+	–	+
QoS[3]-FRR	+	+	+

Також існує механізм швидкої перемаршрутизації, спеціально адаптований для програмно-конфігурованих мереж з централізованою архітектурою. Цей механізм передбачає, що контролер, який визначає основні та резервні маршрути, використовує ефективний сценарій спільного резервування пропускної здатності для резервних шляхів. Таким чином, ця пропозиція стосується резервування та спільного використання пропускної здатності, що сприяє більш ефективному використанню наявних мережних ресурсів [5].

Існує багато інших рішень щодо швидкої перемаршрутизації. Вони включають схему захисту пропускної здатності при розрахунку резервних маршрутів. У той час як умови захисту каналу та вузла під час реалізації багатошляхової маршрутизації представлені у лінійній формі. Крім того, було введено систему критеріїв оптимізації з встановленням ієрархії вагових коефіцієнтів у відповідних цільових функціях, що призвело до покращення продуктивності та масштабованості рішень щодо швидкої перемаршрутизації та зменшення їх обчислювальної складності.

Також слід звернути увагу на метод дворівневої швидкої перемаршрутизації з балансуванням навантаження для програмно-конфігурованих мереж. Цей метод включає в себе захист рівня якості обслуговування на основі єдиного показника – пропускної здатності. Він базується на прогнозуванні взаємодій дворівневої ієрархії розрахунків маршрутних змінних, які визначають основні та резервні шляхи та реалізують схеми захисту каналу, вузла та шляху, забезпечуючи баланс навантаження каналів зв'язку мережі для потоків, які передаються як основними, так і резервними маршрутами. Це відповідає концепції Traffic Engineering. Також було розроблено ефективне рішення, засноване на концепції TE, яке поєднує баланс

навантаження та швидку перемаршрутизацію з захистом каналу, вузла та пропускної здатності шляху, використовуючи розв'язання задачі лінійного програмування.

Також існує вдосконалений метод ієрархічно-координаційної міждоменної швидкої перемаршрутизації. Цей метод розроблено з метою забезпечення надійного захисту приграничних маршрутизаторів у ядрі мережі. Він включає розрахунок основних і резервних міждоменних шляхів, як для одношляхової, так і для багатошляхової маршрутизації. Метод ґрунтується на розкладенні потокової моделі маршрутизації та використанні принципу цільової координації. Його впровадження сприяє підвищенню масштабованості і стійкості маршрутних рішень [5].

Наступним рівнем складності щодо схем захисту рівня якості обслуговування в телекомунікаційних мережах є QoS^2–FRR. Ця схема передбачає забезпечення захисту рівня якості обслуговування на основі двох показників мережної продуктивності. Прикладом реалізації QoS^2–FRR є математична модель відмовостійкої QoS-маршрутизації в мультисервісних телекомунікаційних мережах. Ця модель дозволяє забезпечити захист рівня якості обслуговування за показниками пропускної здатності та середньої міжкінцевої затримки пакетів. Також слід звернути увагу на рішення в рамках схеми QoS^2–FRR, яке базується на нелінійній потоковій моделі для швидкої перемаршрутизації зі захистом двох показників мережної продуктивності: пропускної здатності та ймовірності втрат пакетів. Ця модель враховує обмеженості буфера черг на інтерфейсах маршрутизаторів, що дозволяє керувати навантаженням мережного ресурсу.

Далі перспективним напрямком у розвитку рішень щодо відмовостійкої маршрутизації є підтримка третього типу схем QoS^3–FRR. У цих схемах передбачається захист рівня якості обслуговування за допомогою розширеної множини показників мережної продуктивності, таких як пропускна здатність, середня міжкінцева затримка та ймовірність втрат пакетів.

3 ОГЛЯД ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ ІСНУЮЧИХ ПРОТОКОЛІВ ТА АЛГОРИТМІВ ВІДМОВОСТІЙКОЇ МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

3.1 Класифікація засобів відмовостійкої маршрутизації в інфокомунікаційних мережах

На сьогодні можна визначити категорії засобів відмовостійкої маршрутизації в ІКМ (рис. 3.1) [2] за:

– ступенем гарантування резервування (захисту) мережних компонентів;
– видом підтримуваної схеми захисту.;
– здатністю забезпечувати відмовостійкість на рівні якості обслуговування (QoS);
– місцем, де реалізована відмовостійка маршрутизація в мережі;
– вибором схеми резервування.

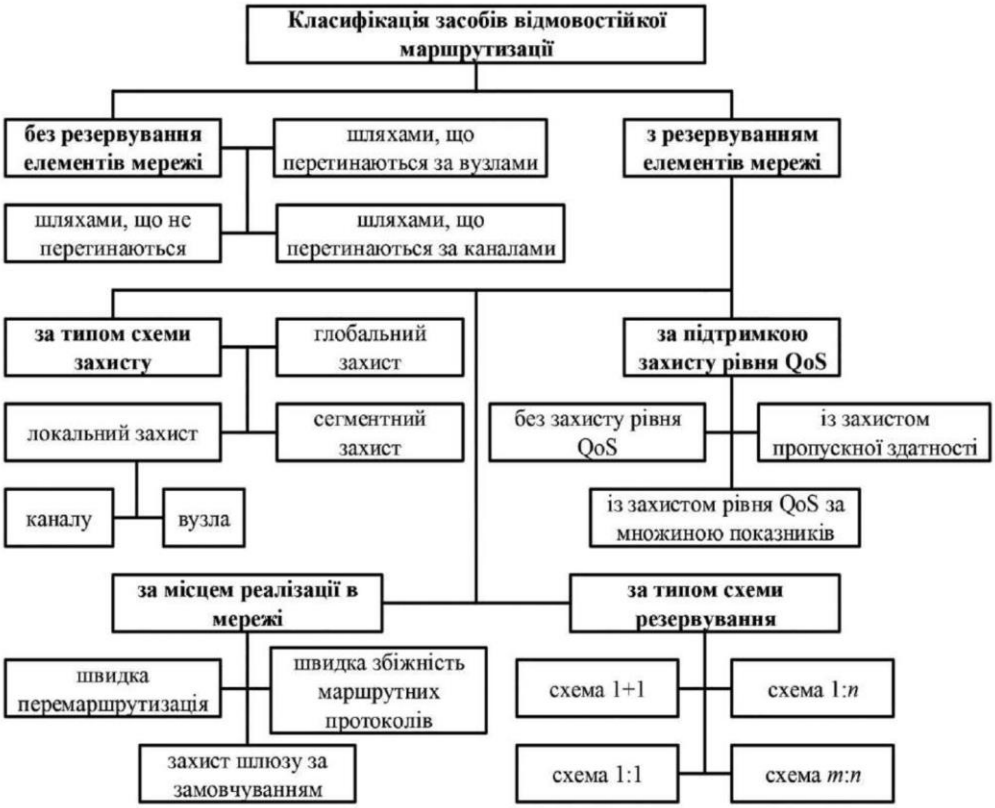

Рисунок 3.1 – Класифікація засобів відмовостійкості маршрутизації [2]

У випадку відсутності захисту (резервування) елементів мережі та впровадження багатошляхової маршрутизації можуть бути задіяні шляхи наступних класів. У шляхів, які не мають спільних вузлів або каналів, спільними є лише вузли відправника та отримувача. Якщо шляхи містять як мінімум один спільний вузол/канал, такі шляхи називаються такими, що перетинаються. В випадках якщо шляхи мають тільки спільні вузли, або спільні канали, такі шляхи називаються шляхами, що перетинаються за вузлами або шляхами, що перетинаються за каналами відповідно.

Класифікацію шляхів можна побачити на рис. 3.2.

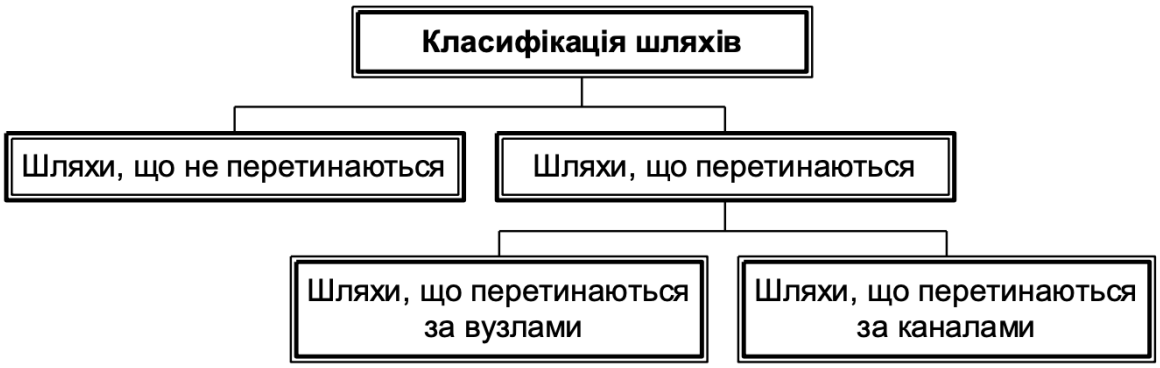

Рисунок 3.2 – Класифікація шляхів [2]

Залежно від типу схеми захисту, яка використовується в системі відмовостійкої маршрутизації, можна виділити три основних підходи: локальний захист (для каналів або вузлів), глобальний захист (для шляхів) і сегментний захист (для групи елементів мережі) [2].

1. Схема захисту каналу (link protection) полягає у створенні альтернативного маршруту, який обходить пошкоджений канал. При виявленні аварії маршрутизатор перенаправляє пакети через створений резервний маршрут. Передача пакетів через резервний маршрут триває до відновлення основного маршруту від відправника до отримувача.

2. Схема захисту вузла (node protection) застосовується при відмові маршрутизатора (node failure). У цьому випадку резервний маршрут не повинен включати пошкоджений вузол. Фактично ця схема зводиться до захисту всіх каналів, що приєднані безпосередньо до захищеного вузла.

3. Схема захисту маршруту (path protection) є глобальним методом захисту. При її реалізації основний і резервний маршрути можуть мати спільні вузли лише на рівні відправника і отримувача.

З урахуванням захисту якості обслуговування існують різні підходи до впровадження відмовостійкої маршрутизації. Ці підходи можна розділити на три основні категорії: перша – включає в себе захист без урахування рівня якості обслуговування, друга – це захист одного конкретного параметра якості обслуговування, зазвичай це пропускна здатність, і третя – це захист за допомогою багатьох параметрів якості обслуговування [2].

При реалізації захисту пропускної здатності відбувається відведення необхідного канального ресурсу, необхідного для успішної передачі пакетів як по основному, так і по резервному маршруту.

Схема захисту рівня якості (QoS) обслуговування стає актуальною, коли недостатньо простої доступності резервного шляху і важливо гарантувати, що цей шлях забезпечить необхідний обсяг пропускної здатності. Це особливо важливо для потоків пакетів, які чутливі до пропускної здатності, затримки та джитеру.

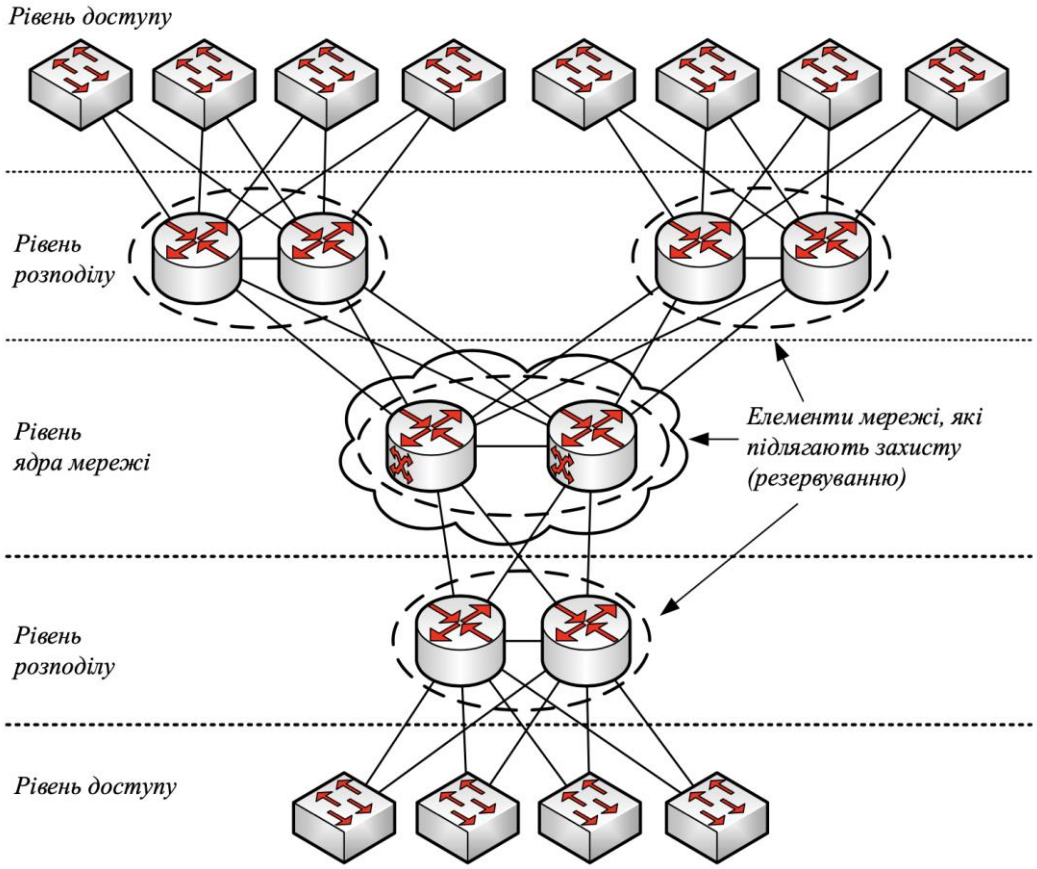

Рисунок 3.3 – Багаторівнева архітектура забезпечення відмовостійкості ІКМ [2]

За місцем реалізації, відповідно до багаторівневої архітектури сучасних ІКМ, задачі відмовостійкої маршрутизації можуть розв’язуватись як на рівні доступу, так і на рівні ядра ІКМ або транспортної мережі (рис. 3.3) [2].

На рівні доступу, завдання відмовостійкої маршрутизації полягає у захисті головного маршрутизатора (шлюзу за замовчуванням), який є точкою входу для певної мережі доступу. Це можливо здійснити в ситуації, коли мережі доступу мають можливість одночасно підключатися до кількох приграничних маршрутизаторів, і інтерфейси цих маршрутизаторів конфігуруються відповідним протоколом як віртуальний шлюз за замовчуванням. В IP-мережах до таких протоколів належать протоколи резервування шлюзу за замовчуванням – FHRP (First Hop Redundancy Protocol).

3.2 Огляд основних протоколів резервування шлюзу за замовчуванням

Використання механізму резервування в ІКМ запропонував себе як ефективний засіб підвищення доступності, продуктивності та відмовостійкості мережі, а також зменшення відмов спричиненою SPOF (Single Point of Failure), тобто єдиною точкою збою, відмова якої може спричинити до виходу з ладу всієї системи. Дана проблема може бути усунена за допомогою дублювання та додавання каналів зв’язку або інших мережних компонентів. Це дозволяє створити альтернативні резервні системи, включаючи обладнання, вузли, канали, маршрути з метою забезпечення надійності функціонування мережі під час можливих збоїв [9].

Однією з ключових стратегій для забезпечення надійності є впровадження резервного шлюзу за замовчуванням. Основна проблема, яка вирішується при використанні резервування, полягає в тому, що при відмові маршрутизатора або лінії зв'язку втрачається доступ до зовнішньої мережі. Тому необхідно мати альтернативний резервний маршрутизатор, щоб уникнути відключення мережі шлюзу в разі збою. Протоколи групи FHRP зазвичай надають функціонал, який спрощує налаштування та використання декількох шлюзів кінцевими пристроями. Вони також автоматично пересилають дані хостам на резервний маршрутизатор, не потребуючи ручного втручання в конфігурацію. Тому ці протоколи допомагають подолати обмеження, які зазвичай пов'язані із шлюзом за замовчуванням, і забезпечують надійне обслуговування.

До сімейства FHRP відносять наступні протоколи:

– Hot Standby Router Protocol (HSRP);
– Virtual Router Redundancy Protocol (VRRP);
– Gateway Load Balancing Protocol (GLBP);
– Common Address Redundancy Protocol (CARP);
– Extreme Standby Router Protocol (ESRP);
– Routed Split multi-link trunking (R-SMLT);
– NetScreen Redundancy Protocol (NSRP);
– Chassis Cluster Redundant Ethernet.

Hot Standby Router Protocol (HSRP) – протокол від компанії Cisco, який використовується для налаштування маршрутизаторів як членів групи та надає їм віртуальну IP-адресу (VIP) і віртуальну MAC-адресу. Ці параметри використовуються кінцевими пристроями для спілкування з маршрутизатором-шлюзом [9]. У групі HSRP маршрутизатор із найвищим пріоритетом визначається як активний маршрутизатор і відповідає за перенаправлення трафіку. Маршрутизатор із другим найвищим пріоритетом стає резервним маршрутизатором, який приймає на себе маршрутизацію пакетів у разі відмови активного маршрутизатора або за певних умов, визначених заздалегідь. Інші маршрутизатори у групі HSRP перебувають у режимі прослуховування.

Virtual Router Redundancy Protocol (VRRP) – це відмовостійкий open-source протокол, стандартизований IETF (Internet Engineering Task Force) [9]. Протокол використовується для забезпечення неперервної та надійної роботи мережі. У групі VRRP активний маршрутизатор, який керує VIP-шлюзом, називається головним (master) маршрутизатором, тоді як усі інші маршрутизатори VRRP є резервними маршрутизаторами. Використання VRRPv3 має свої переваги, оскільки цей протокол дозволяє значно швидше переключатися на резервні пристрої у випадку відмови, порівняно зі стандартними механізмами виявлення сусідніх пристроїв IPv6. VRRPv3 дозволяє резервному маршрутизатору стати основним (master) маршрутизатором всього за кілька секунд, і це відбувається без використання додаткового службового трафіку або участі хоста [9]. Ще однією перевагою використання VRRPv3 є поліпшення процесу резервування в мережі, оскільки цей протокол дозволяє використовувати кілька пристроїв як шлюзи за замовчуванням.

Таблиця 3.1 – Порівняння протоколів резервування шлюзу за замовчуванням [9]

Назва характеристики	HSRP	VRRP	GLBP
Застосування	Cisco Proprietary	IEEE Standard	Cisco Proprietary
Рік створення	1994	1998	2005
Стандарт	RFC 2281	RFC 5798	Ні
Балансування навантаження	Ні	Так	Так
IPv6	Так	Так	Так
Складність імплементації	Легка	Легка	Середня
IP багатоадресної мережі	HSRPv1- 224.0.0.2; HSRPv2 - 224.0.0.102	224.0.0.18	224.0.0.102
Діапазон підтримуваних груп	HSRPv1: 0-255 HSRPv2: 0-4095	0-255	0-1023
Активні маршрутизатори	Один активний, один пасивний	Один активний, один пасивний	Декілька активних
Віртуальний IP та MAC адреси	Одна віртуальна IP-адреса та одна віртуальна MAC-адреса	Одна віртуальна IP-адреса або реальна IP-адреса з маршрутизатора та одна віртуальна MAC-адреса	Одна віртуальна IP-адреса, багато різних віртуальних MAC-адрес
Таймер за замовчуванням	Повідомлення Hello: 3 секунди Час утримання: 10 сек	Повідомлення Hello: 1 секунди Час утримання: 3 сек	Повідомлення Hello: 3 секунди Час утримання: 10 сек
Аутентифікація	Так	Ні	Так

Common Address Redundancy Protocol (CARP) – протокол резервування шлюзу використовується для підвищення доступності мережі та забезпечення безперебійних послуг. CARP є безпечним протоколом, оскільки він використовує алгоритм HMAC (Hash-based message authentication code) SHA-1 (Secure Hash Algorithm 1), і його можна розгорнути як у мережах IPv4, так і IPv6 [9]. Протокол

застосовується серед групи пристроїв, які мають однакову IP-адресу в одній мережі. Ця група пристроїв відома як група резервування (redundancy group). У межах кожної групи один пристрій обирається як головний (master), і він обслуговує всі запити, що надходять на спільну IP-адресу, такі як запити ARP. У будь-який момент пристрій може бути членом декількох різних груп.

Для належної функціональності кожен вузол в CARP вимагає встановлення трьох основних параметрів. Перші два параметри – це база сповіщень (advertisement base - advbase) і відхилення бази сповіщень (advertisement skew - advskew). Обидва ці параметри впливають на інтервал часу, протягом якого вузол передає свої сповіщення [9]. Параметр “advskew” використовується для визначення, який вузол з групи резервування отримає статус головного (master) з обмеженням, де менше значення advskew вказує на вищий пріоритет для статусу головного вузла. Параметр “advbase” визначає час у секундах, протягом якого генеруються сповіщення CARP. Третім обов'язковим параметром є пароль, який використовується для аутентифікації сповіщень.

Приклад імплементації FHRP показаний на рис. 3.4.

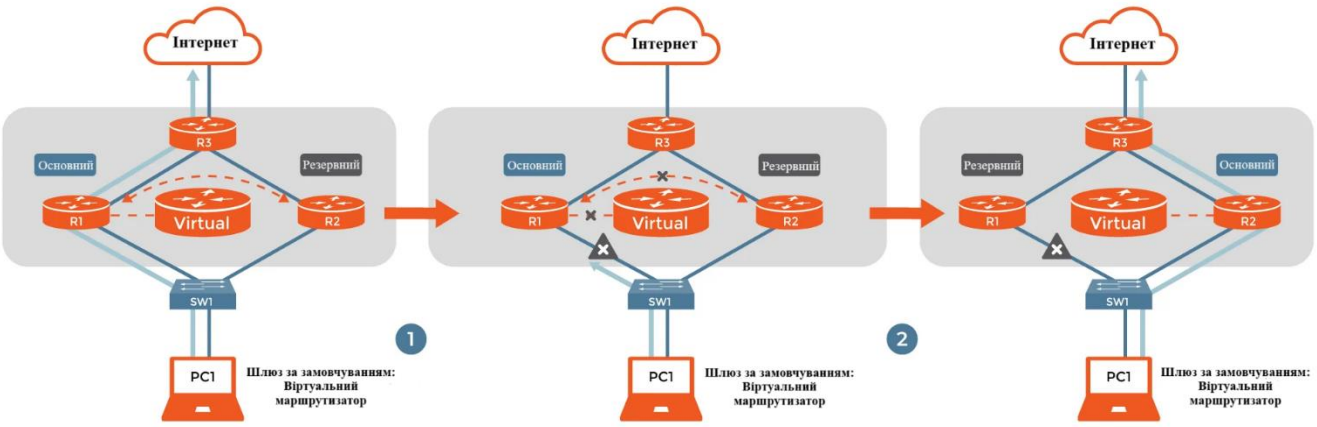

Рисунок 3.4 – Імплементація FHRP в інфокомунікаційній мережі [10]

Як можна побачити на рис. 3.4, коли маршрутизатор R2 виявляє збій на активному пристрої, він бере на себе активну роль. Він продовжує обробляти трафік даних з ПК1. В результаті, шлюз за замовчуванням залишається активним, і на кінцевих точках не виникає переривань та збоїв [10].

Gateway Load-Balancing Protocol (GLBP) – протокол дозволяє розподіляти навантаження пакетів серед множини резервних маршрутизаторів. GLBP гарантує можливість балансування навантаження для кількох маршрутизаторів шлюзів з

однаковою IP-адресою, але з різними MAC адресами. У GLBP усі маршрутизатори працюють як активні з метою запобігання руйнування всієї системи. Він підвищує продуктивність мережі, забезпечуючи балансування навантаження та IP резервування [10].

Отже, серед основних недоліків існуючих рішень щодо відмовостійкої IP-маршрутизації можна виділити наступні:

– не враховується потоковий характер мережного трафіку;

– обмежені можливості для балансування навантаження та вимагають адміністративної конфігурації;

– відсутня узгоджена стратегія вирішення взаємопов'язаних завдань вибору шлюзу за замовчуванням і маршрутизації в транспортній мережі.

Наприклад, згідно з табл. 3.1 для балансування навантаження за інтерфейсами шлюзів за замовчуванням можна використовувати такі механізми: Round Robin і Weighted в GLBP, а також Host-dependent в GLBP і VRRP.

Ці механізми балансування значно знижують швидкість реакції мережі на можливі збої та обмежують функціональність мережних рішень для захисту шлюзів (резервування). Навіть при оптимізації балансування навантаження для захисту шлюзу, немає гарантії того, що після вибору шлюзу за замовчуванням у транспортній мережі буде наявний маршрут з необхідною пропускною здатністю для забезпечення QoS. Це пов’язано з тим, що відомі рішення захисту шлюзу за замовчуванням не узгоджуються з рішеннями маршрутизації в транспортній мережі та вирішуються послідовно та незалежно один від одного.

3.3 Забезпечення відмовостійкої маршрутизації за допомогою технології Fast ReRoute

Функціонал відмовостійкої маршрутизації на рівні ядра мережі здійснюється за допомогою технологій швидкої конвергенції IGP/BGP та швидкої перемаршрутизації (Fast ReRoute), які застосовуються в IP та MPLS мережах. Розглядаючи технологію швидкої перемаршрутизації (Fast ReRoute), даний підхід використовується у мережах IP та MPLS для забезпечення захисту елементів транспортної мережі, таких як каналів, вузлів, шляхів та загальної пропускної здатності мережі [2].

Технологія MPLS FRR є механізмом забезпечення швидкого відновлення зв'язку в MPLS-мережах. Вона використовує маркування MPLS (Multiprotocol Label

Switching) для передачі трафіку та надає ефективні методи обходу відмовних вузлів чи каналів зв'язку. Стандартний режим роботи MPLS TE за замовчуванням полягає в обчисленні нового оптимального маршруту у випадку відмови каналу чи вузла в LSP (Label Switched Path) основного маршруту. Цей процес може бути занадто повільним для додатків, які чутливі до затримок [11-13].

Приклад стандартної логіки пошуку нового шляху в мережі MPLS при відмови каналу чи вузла показано на рис. 3.5.

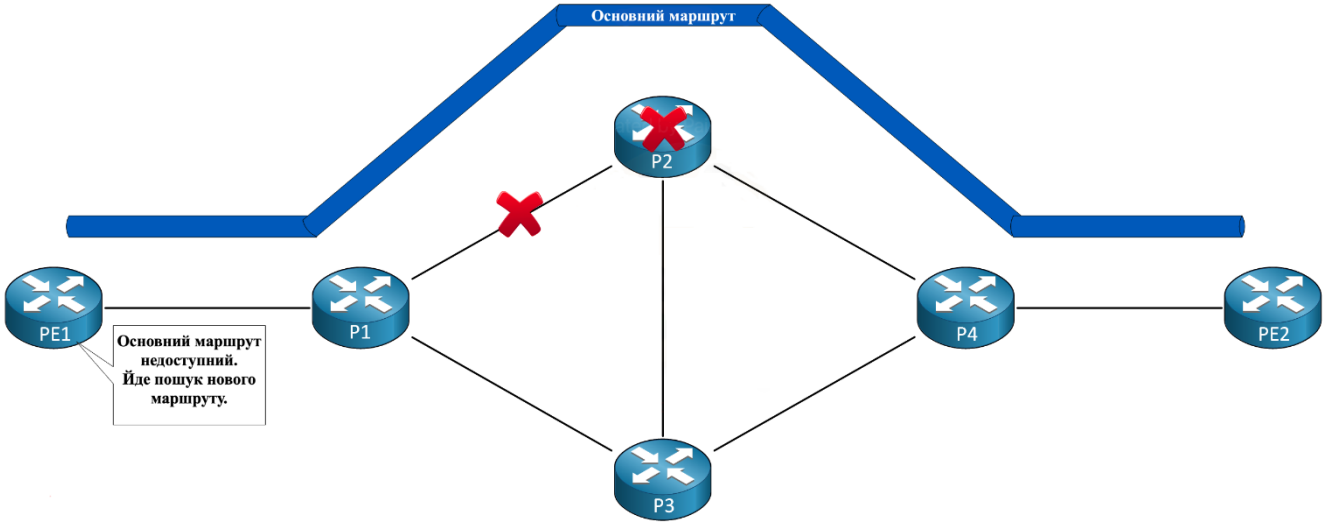

Рисунок 3.5 – Приклад пошуку нового маршруту в мережі MPLS при відмови каналу або вузла [13]

За допомогою швидкої перемаршрутизації маршрутів MPLS TE (MPLS TE Fast Reroute), у випадку відмови каналу зв’язку чи вузла в основному маршруті, трафік перенаправляється по заздалегідь визначеному резервному шляху, який не містить проблемний елемент мережі (канал або вузол). Це дозволяє досягнути часу відновлення менше ніж 50 мс [13].

Приклад логіки пошуку нового шляху в мережі MPLS при відмови каналу чи вузла з використанням швидкої перемаршрутизації показано на рис. 3.6.

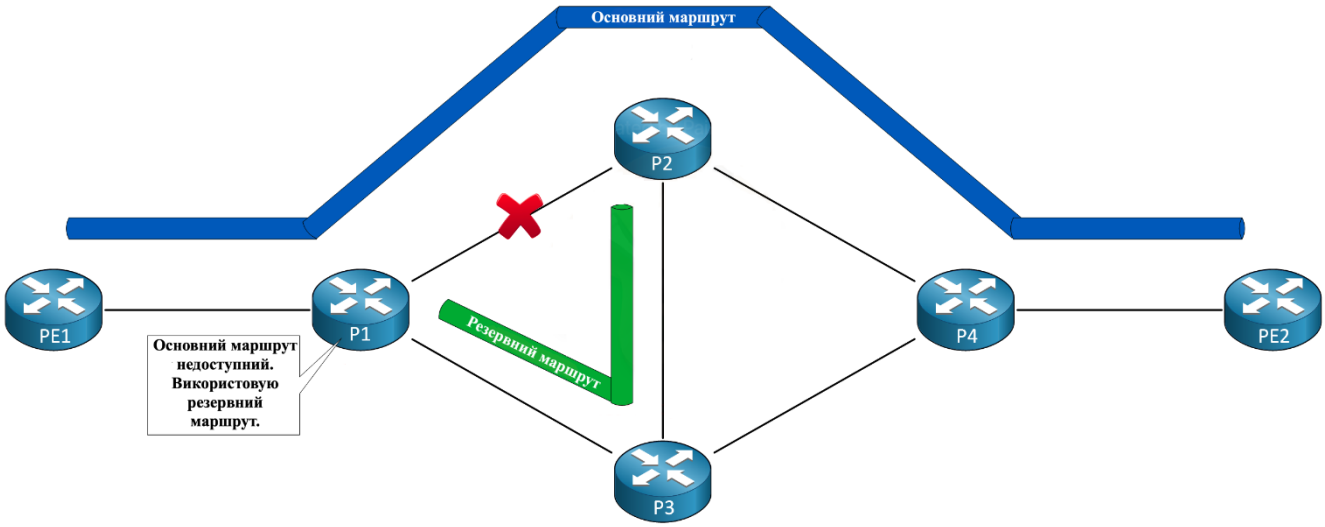

Рисунок 3.6 – Приклад пошуку нового маршруту в мережі MPLS при відмові каналу чи вузла з використанням швидкої перемаршрутизації [13]

MPLS TE Fast Reroute підтримує два механізми захисту – захист каналу (Link Protection, LP) та захист вузла (Node Protection, NP).

У випадку механізму захисту каналу (Link Protection), канал основного маршруту, який вийшов з ладу, маркується як захисний (Protected Link) та не буде враховуватись при розрахунку резервного маршруту.

Приклад розрахунку резервного маршруту за допомогою механізму захисту каналу (Link Protection) показано на рис 3.7.

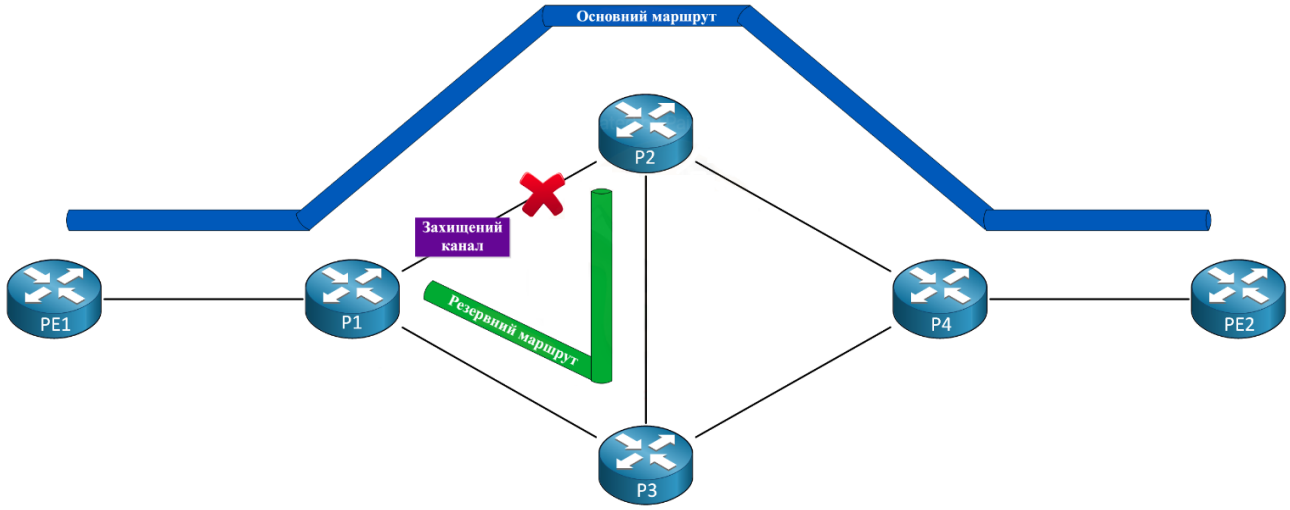

Рисунок. 3.7 – Розрахунок резервного маршруту за допомогою механізму захисту каналу [13]

У випадку механізму захисту вузла (Node Protection), при виведені з ладу вузла основного маршруту, вузол маркується як захисний, а також маркуються суміжні до нього канали. Розрахунок резервного маршруту не буде враховувати захищені вузли та канали.

Приклад розрахунку резервного маршруту за допомогою механізму захисту вузла (Link Protection) показано на рис 3.8.

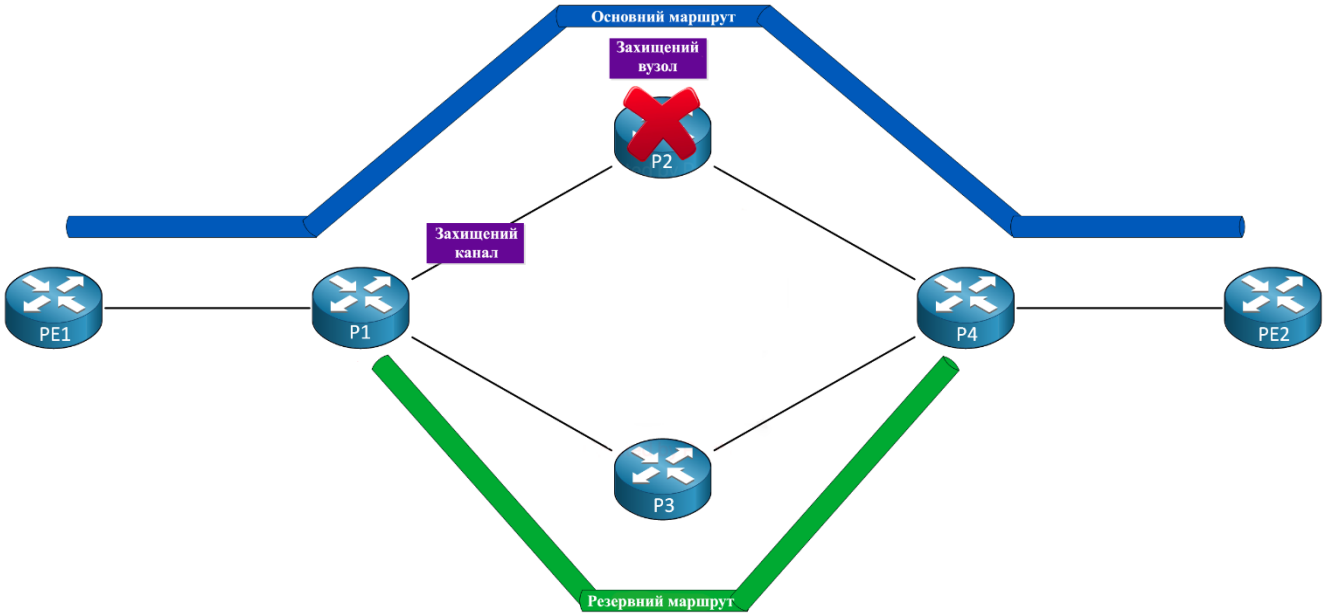

Рисунок 3.8 – Приклад розрахунку резервного маршруту за допомогою механізму захисту вузла [13]

Також слід зазначити, що технології IP/MPLS-мереж, а також більшість рішень, спрямованих на підвищення надійності мережі, базуються на впровадженні різноманітних схем резервування [2]:

– схема 1+1, де потік пакетів передається одночасно і основним, і резервним маршрутами;

– схема 1:1, при якій для кожного основного маршруту створюється відповідний резервний шлях, який не повинен містити проблемних елементів мережі (канал або вузол);

– схема 1:n, де формується один резервний шлях для n основних шляхів (резервне відновлення служб);

– схема m:n, при якій створюється m резервних шляхів для n основних шляхів.

Для підвищення відмовостійкості IP мереж використовується технологія IP FRR, яка багато в чому аналогічна технології Fast ReRoute, що функціонує в мережах MPLS-TE. Основною задачою IP FRR є знаходження альтернативного маршруту для передачі пакетів у випадку можливої відмови каналу або вузла мережі, при цьому уникаючи утворення мікропетель. При використанні швидкої перемаршрутизації застосовуються IP протоколи OSPF та IS-IS [2]. Якщо маршрутизатор має інформацію про декілька маршрутів із рівною метрикою (вартістю) (Equal Cost MultiPaths, ECMP) від відправника до отримувача, і деякі з них не пролягають через несправні канали або вузли, то такі шляхи можна використовувати як резервні. У випадку відсутності таких шляхів маршрутизатор автоматично звертається до безпосередньо підключеного сусіда, який має маршрут, що не включає аварійний канал або вузол до отримувача. Цей шлях через безпосередньо підключеного сусіда називається альтернативним маршрутом без петель (Loop Free Alternate, LFA) [2].

Важливо зазначити, що технологія швидкої маршрутизації (Fast ReRoute) не лише забезпечує швидке відновлення після відмов вузлів на каналів, але також також слугує як механізм для підвищення рівня QoS. Це забезпечує збалансований підхід до забезпечення високої надійності, швидкого відновлення та управління пріоритетами трафіку, що є важливим аспектом сучасних мереж.

3.4 Аналіз моделей і методів відмовостійкої маршрутизації

Відомо, що головним чином ефективність протоколів маршрутизації, в тому числі відмовостійкої, цілком залежить від теоретичних моделей і методів, на яких вони базуються. Отже актуальним представляється завдання проведення огляду перспективних теоретичних моделей та методів щодо відмовостійкої маршрутизації в телекомунікаційних мережах.

Завдяки існуючим рішенням відмовостійкості маршрутизації, вдалося сформулювати перелік ключових вимог, які повинні дотримуватись у перспективних рішеннях у цій сфері [2]. Основну увагу слід зосередити на математичних моделях та методах, на яких вони ґрунтуються:

– врахування потокового характеру трафіку, що є ключовою особливістю більшості мультимедійних послуг і важливим фактором для реалізації заходів забезпечення пропускної здатності та якості обслуговування в мережі;

– постановка задачі з орієнтацією на оптимізацію використання наявних мережних ресурсів;

– забезпечення високої масштабованості;

– підтримка базових схем захисту для мережних компонентів, таких як вузли, канали зв'язку, шляхи та пропускна здатність;

– узгоджене вирішення окремих завдань відмовостійкої маршрутизації, наприклад, захист шлюзу за замовчуванням, швидка перемаршрутизація тощо;

– розширення можливостей існуючих рішень для підтримки балансування навантаження, особливо у випадках багатошляхової стратегії маршрутизації та підтримки схем захисту для мультишляхового пересилання пакетів одного потоку;

– збезпечення прийнятної обчислювальної складності для рішень маршрутизації.

Умовно, рішення в області відмовостійкості маршрутизації можна класифікувати на наступні категорії: евристичні підходи, методи на основі графів та комбінаторики, рішення, спрямовані на оптимізацію потоків, відмовостійка маршрутизація в мережах, побудованих на підставі концепції SDN (Software-Defined Networking), і також методи, що використовують балансування навантаження в рамках концепції Traffic Engineering (TE) [2].

Серед евристичних алгоритмів відмовостійкої маршрутизації можна виділити адаптивний евристичний алгоритм відмовостійкої маршрутизації на основі використання графу (n, k)-зірки. Головною перевагою даного алгоритму є широкі властивості щодо масштабування. Ідея даного алгоритму полягає в збиранні інформації, яка використовується в процесі маршрутизації на графі n-зірки, для застосування на графі (n, k)-зірки ($S_{n,k}$) (рис. 3.9) [2].

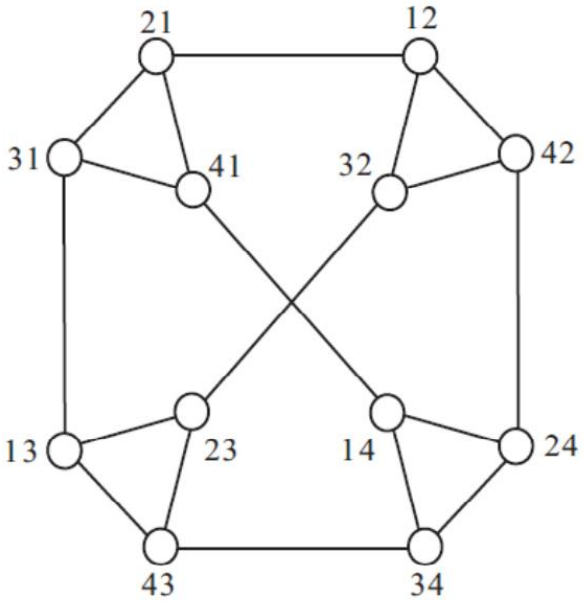

Рисунок 3.9 – Приклад графу (4, 2)-зірки ($S_{4,2}$) [2]

Також існує підхід використання ймовірнісного вектору безпеки (Probabilistic Safety Vector, PSV) та алгоритм маршрутизації з метою визначення надійного маршруту, застосовуючи PSV. Проте, ефективність PSV-маршрутизації погіршується зі збільшенням відсотку непрацездатних вузлів, особливо при перевищенні 25% непрацездатних вузлів. Для підвищення продуктивності маршрутизації в умовах великої кількості вузлів, які можуть вийти з ладу, був розроблений адаптивний метод для визначення порогу PSV. Використання маршрутизації PSV з динамічним порогом показує найкращі результати в порівнянні з іншими методами моделювання.

Наступним евристичним методом є метод для відмовостійкої маршрутизації у mesh-мережах. Цей метод базується на мурашиному алгоритмі для пошуку найкращого шляху, з урахуванням вузлів, які можуть вийти з ладу. Для вирішення завдання відмовостійкої маршрутизації в цьому алгоритмі використовувався алгоритм оптимізації мурашиної колонії, зокрема, з використанням кольорових феромонних мурах для подолання проблеми відновлення функціонування мережних елементів. Даний метод швидко реагує на відмови у мережі, надаючи можливість обирати оптимальний маршрут від відправника до отримувача в будь-який момент часу [2].

Подальшим алгоритмом відмовостійкої маршрутизації є алгоритм для ієрархічних дуальних мереж (Hierarchical Dual-Net, HDN), незалежно від обмеженої або довільної кількості вузлів, які можуть вийти з ладу. У цьому

контексті, HDN створено на основі симетричного графа, який має форму тривимірного тору або n-вимірного гіперкубу. Представлені алгоритми дозволяють знайти надійний маршрут від відправника до отримувача в ситуації, коли відома група вузлів, що можуть вийти з ладу.

Також слід звернути увагу на механізм швидкої перемаршрутизації в IP-мережах за допомогою неперетинаючих кістякових дерев з коренем. Цей підхід гарантує відновлення роботи після відмови до (k-1) каналів зв'язку в мережі, яка може бути представлена як k-реберний зв'язний граф. Слід зауважити, що будування неперетинаючих кістякових дерев (рис. 3.10) може бути виконане за час, пропорційний квадрату розміру мережі, і цей підхід забезпечує високу масштабованість [2].

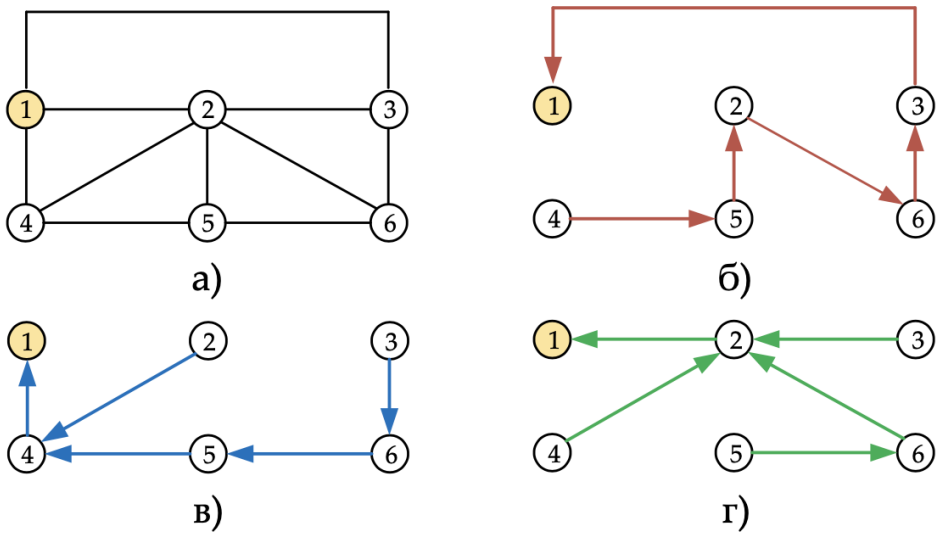

Рисунок 3.10 – Приклад дерев, які моделюють рішення задачі перемаршрутизації за шляхами, що не перетинаються за дугами: (а) мережа, (б) червоне дерево, (в) синє дерево і (г) зелене дерево [2]

Серед графових та комбінаторних рішень щодо відмовостійкості маршрутизації слід виділити алгоритми відмовостійкості маршрутизації для гіперкубових мереж на основі приблизних маршрутних імовірностей (approximate routable probabilities), які характеризують доступність для маршрутизації будь-якого вузла на певній відстані. Кожен вузол вибирає одного зі своїх сусідів для передачі повідомлення, враховуючи приблизні ймовірності маршруту.

Також, серед методів підвищення відмовостійкості телекомунікаційних мереж (ТКМ) є циркулянтні графи, які відзначаються високою гнучкістю у відношенні до кількості вузлів та зв’язності мережі (рис. 3.11) [2]. Також існує

модель для оцінки надійності з'єднання як у випадку відмови вузлів, так і в разі відмови каналів зв'язку в мережі. Даний алгоритм показує лінійний ріст надійності зі збільшенням зв'язності мережі в логарифмічному масштабі.

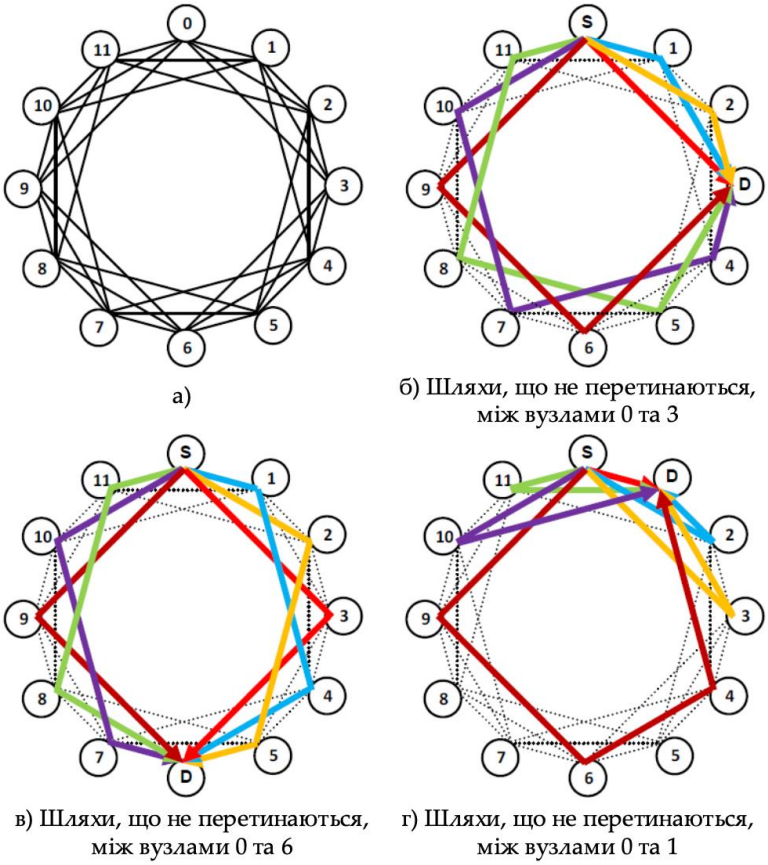

Рисунок 3.11 – Архітектура мережі на основі циркулянтного графа та приклади відмовостійкої маршрутизації за шляхами, що не перетинаються за вузлами [2]

Потокові моделі та методи запропонували себе як найбільш переспективні та ефективні рішення для відмовостійкості маршрутизації, оскільки, вони враховують потоковий характер трафіку, що передається в сучасних телекомунікаційних мережах, а також, як правило, формулюються у вигляді оптимізаційних задач, орієнтованих на оптимізацію використання мережних ресурсів, допускаючи реалізацію схем захисту пропускної здатності мережі.

Обирати метод відмовостійкої маршрутизації слід залежно від конкретних проблем і характеристик мережі. Важливо пам'ятати, що кращий підхід може залежати від розміру, складності та вимог що до стійкості мережі.

4 ДОСЛІДЖЕННЯ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ ПОТОКОВИХ МОДЕЛЕЙ ШВИДКОЇ ПЕРЕМАРШРУТИЗАЦІЇ

4.1 Математичні моделі швидкої перемаршрутизації в інфокомунікаційних мережах

Для швидшого реагування на можливі перебої в обслуговуванні пакетів, спричинені перевантаженням каналів і черг маршрутизаторів, все частіше застосовуються засоби відмовостійкої маршрутизації, такі як, наприклад, Fast ReRoute [14]. Швидка перемаршрутизація є складовою відмовостійкої маршрутизації, яка використовується на рівні ядра ІКМ і ґрунтується на впровадженні ресурсної надлишковості. Отже, для кожного потоку одночасно з визначенням основного шляху (мультишляху) передбачається розрахунок резервного шляху (мультишляху), який уникає проблемних елементів мережі (вузлів, каналів, сегментів), що підлягають захисту [2]. Це призводить до певних особливостей у самій структурі моделі швидкої перемаршрутизації в ІКМ. У зв'язку з цим пропонується до використання підхід щодо розв'язання задачі відмовостійкої маршрутизації на основі потокової моделі швидкої перемаршрутизації, що дозволяє впроваджувати вказані схеми резервування (захисту каналу, вузла та шляху) [14].

В описі потокової моделі швидкої перемаршрутизації в ІКМ варто зазначити наступні вихідні дані:

– кількість каналів зв'язку в мережі (n);
– кількість вузлів у мережі (m);
– вузол-відправник пакетів (s);
– вузол-отримувач пакетів (d);
– пропускні здатності каналів зв'язку ($c_{i,j}$);
– метрики каналів зв'язку для основного (f^o) та резервного (f^p) маршрутів;
– інтенсивність потоку, що надходить до мережі (r, пакетів за секунду, пак/с);
– схема захисту елемента мережі, що реалізується

Кількість каналів зв'язку в мережі (n) визначає розмірність вектора $\vec{x}$, координати $x_{i,j}$ якого характеризують долю потоку в каналі зв'язку між i-м і j-м вузлами. Зі свого боку розмірність вектора метрик $\vec{f}$ відповідає числу каналів у мережі (n), координати $f_{i,j}$ якого характеризують метрику відповідного каналу між i-м і j-м вузлами.

В процесі дослідження для реалізації багатошляхової маршрутизації на координати вектору $\vec{x}$ основного та резервного маршруту накладаються наступні обмеження [14]:

для основного маршруту

$$0 \le x_{i,j} \le 1; \tag{4.1}$$

для резервного маршруту

$$0 \le \bar{x}_{i,j} \le 1. \tag{4.2}$$

Фізичний зміст змінних (4.1)–(4.2) визначає можливість розгалуження потоку за шляхами мережі, тобто пакети можуть передаватися як одним, так і множиною шляхів.

Під час розв'язання маршрутної задачі необхідно забезпечити виконання умов збереження потоку для основного та резервного маршруту в кожному з мережних вузлів та мережі загалом [14]:

для основного маршруту

$$\begin{cases} \sum_{j:(i,j)} x_{i,j} - \sum_{j:(j,i)} x_{j,i} = 1 \ - \text{для вузла відправника;} \\ \sum_{j:(i,j)} x_{i,j} - \sum_{j:(j,i)} x_{j,i} = 0 - \text{для транзитних вузлів;} \\ \sum_{j:(i,j)} x_{i,j} - \sum_{j:(j,i)} x_{j,i} = -1 - \text{для вузла отримувача;} \end{cases} \tag{4.3}$$

для резервного маршруту

$$\begin{cases} \sum_{j:(i,j)} \bar{x}_{i,j} - \sum_{j:(j,i)} \bar{x}_{j,i} = 1 \ - \text{для вузла відправника;} \\ \sum_{j:(i,j)} \bar{x}_{i,j} - \sum_{j:(j,i)} \bar{x}_{j,i} = 0 - \text{для транзитних вузлів;} \\ \sum_{j:(i,j)} \bar{x}_{i,j} - \sum_{j:(j,i)} \bar{x}_{j,i} = -1 - \text{для вузла отримувача.} \end{cases} \tag{4.4}$$

Також важливо уникнути перевантаження каналів ІКМ за наступних умов, кількість яких відповідає кількості каналів у мережі:
для основного маршруту

$$r * x_{i,j} \leq c_{i,j} \ (i,j = \overline{1,n}, i \ \neq j); \tag{4.5}$$

для резервного маршруту

$$r * \bar{x}_{i,j} \leq c_{i,j} \ (i,j = \overline{1,n}, i \ \neq j); \tag{4.6}$$

Як було зазначено раніше, у процесі швидкої перемаршрутизації можуть підтримуватися кілька основних схем захисту елементів мережі: вузла, каналу, шляху та його пропускної здатності. Тому слід враховувати додаткові обмеження для реалізації схем захисту каналу та вузла на маршрутні змінні $\bar{x}_{i,j}$, що відповідають за визначення резервного шляху [2, 3].

У випадку багатошляхової маршрутизації додаткові обмеження для схеми захисту каналу мають вигляд:

$$0 \leq \bar{x}_{i,j} \leq \delta_{i,j}, \tag{4.7}$$

де

$$\delta_{i,j} = \begin{cases} 0, \text{за умови захисту каналу зв}'\text{язку } (i,j); \\ 1, \text{в іншому випадку.} \end{cases} \tag{4.8}$$

Виконання умов (4.7)–(4.8) гарантує, що канал (i,j), який вважається таким, що захищається, не буде враховуватись і застосовуватись резервним маршрутом.

Для схеми захисту вузла у випадку багатошляхової маршрутизації додаткові обмеження пов’язані з тим, що захисту підлягатимуть канали зв’яку, суміжні до вузла, який захищаться:

$$0 \leq \bar{x}_{i,j} \leq \delta_{i,j} \ \text{для каналів зв}'\text{язку, суміжних до вузла, що захищається,} \tag{4.9}$$

де $\delta_{i,j}$ – значення, вибір яких підпорядковується умові (4.8).

Для визначення значень маршрутних змінних $x_{i,j}$ та $\bar{x}_{i,j}$ під час розв'язання задачі відмовостійкої маршрутизації у мережі, потрібно мінімізувати наступну цільову функцію [14]:

$$F = \sum_{(i,j)} f_{i,j}^{o} x_{i,j} + \sum_{(i,j)} \bar{f}_{i,j}^{p} \bar{x}_{i,j}, \tag{4.10}$$

де $f_{i,j}^{o}$ – метрика каналу (i,j) для основного маршруту, $\bar{f}_{i,j}^{p}$ – метрика каналу (i,j) для резервного маршруту.

4.2 Дослідження та аналіз потокових моделей швидкої перемаршрутизації

Нехай структура ядра інфокомунікаційної мережі має топологію, зображену на рис. 4.1. Досліджуваний фрагмент мережі можна представити у вигляді, показаному на рис. 4.2. Дана топологія буде використовуватися для подальшого моделювання з використанням бібліотек Python NumPy та Scipy і порівняльного аналізу моделей швидкої перемаршрутизації та відповідних схем захисту каналу та вузла мережі.

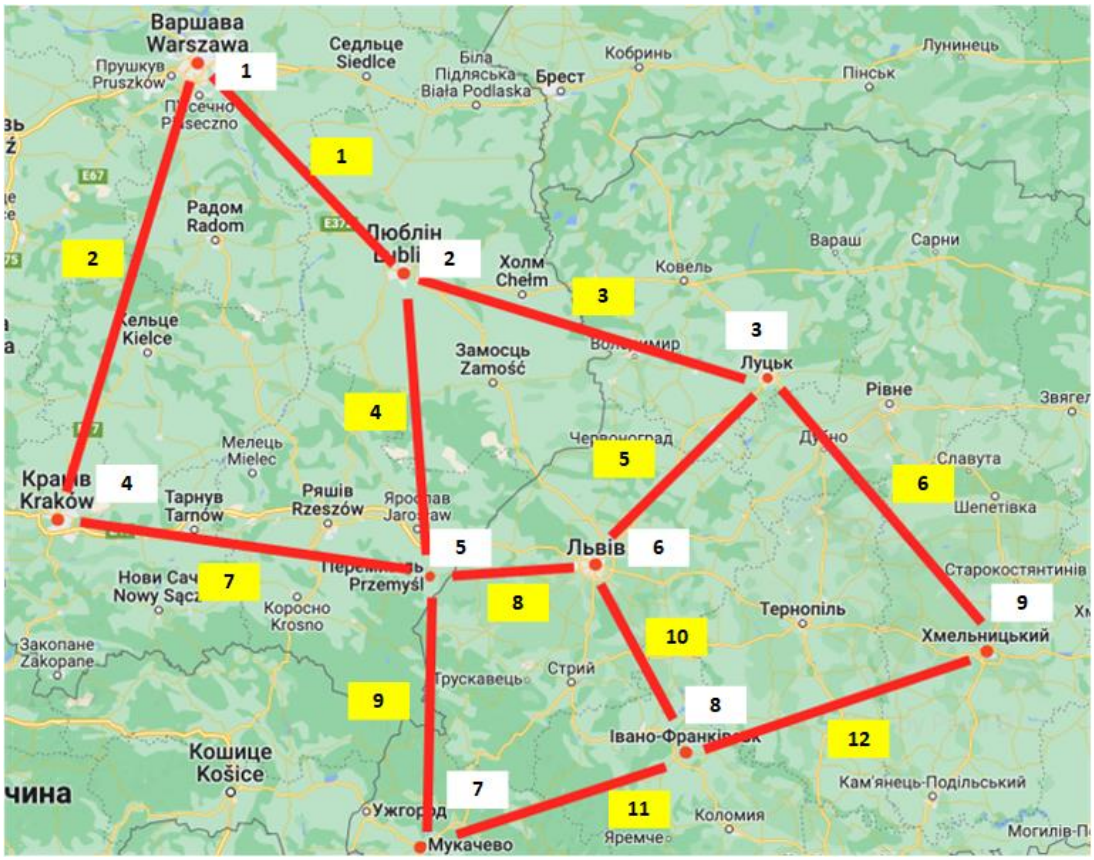

Рисунок 4.1 – Фрагмент ядра досліджуваної мережі

Структура ядра досліджуваної мережі (рис. 4.1) складається з 9 вузлів і 12 каналів зв’язку. Як вузол-відправник обрано перший маршрутизатор, а вузлом-отримувачем – восьмий. Також на рис. 4.2 зображено топологію мережі з урахуванням умовної пропускної здатності каналів зв’язку (табл. 4.1).

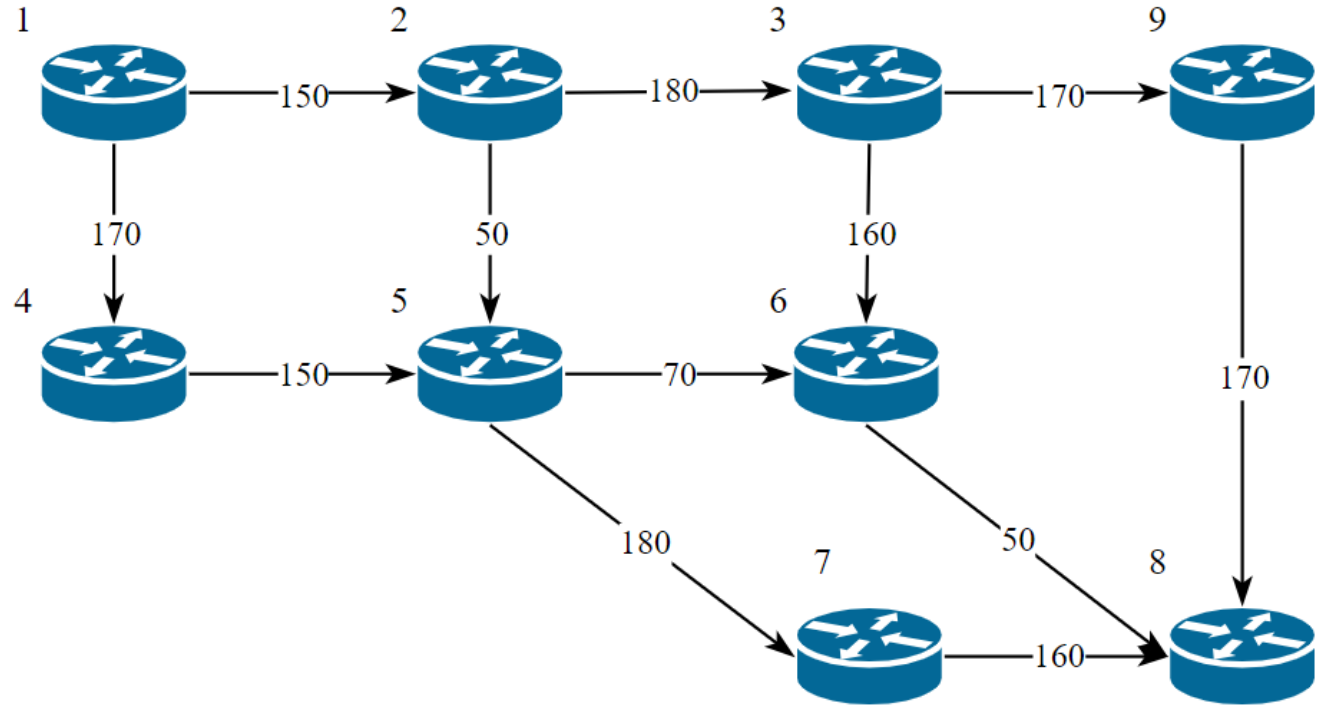

Рисунок 4.2 – Топологія ядра досліджуваної мережі

Таблиця 4.1 – Пропускні здатності каналів зв’язку

№	Канал зв’язку	Пропускна здатність каналу $c_{i,j}$, пак/с
1	(1,2)	150
2	(1,4)	170
3	(2,3)	180
4	(2,5)	50
5	(3,6)	160
6	(3,9)	170
7	(4,5)	150
8	(5,6)	70
9	(5,7)	180
10	(6,8)	50
11	(7,8)	160
12	(9,8)	170

Шуканий вектор $\vec{x}$ для структури мережі та її пропускних здатностей каналів зв'язку, які показані на рис. 4.2, набуває вигляду:

$$\vec{x} = \begin{bmatrix} x_{1,2} \\ x_{1,4} \\ x_{2,3} \\ x_{2,5} \\ x_{3,6} \\ x_{3,9} \\ x_{4,5} \\ x_{5,6} \\ x_{5,7} \\ x_{6,8} \\ x_{7,8} \\ x_{9,8} \\ \bar{x}_{1,2} \\ \bar{x}_{1,4} \\ \bar{x}_{2,3} \\ \bar{x}_{2,5} \\ \bar{x}_{3,6} \\ \bar{x}_{3,9} \\ \bar{x}_{4,5} \\ \bar{x}_{5,6} \\ \bar{x}_{5,7} \\ \bar{x}_{6,8} \\ \bar{x}_{7,8} \\ \bar{x}_{9,8} \end{bmatrix} \tag{4.11}$$

Вектор вагових коефіцієнтів $\vec{f}_{RIP}$, координатами якого є величини $f_{i,j}^{o}$ та $\bar{f}_{i,j}^{p}$, у разі використання метрики по аналогії з протоколом RIP виглядає наступним чином:

$$\vec{f}_{RIP} = \begin{bmatrix} f^o_{1,2} \\ f^o_{1,4} \\ f^o_{2,3} \\ f^o_{2,5} \\ f^o_{3,6} \\ f^o_{3,9} \\ f^o_{4,5} \\ f^o_{5,6} \\ f^o_{5,7} \\ f^o_{6,8} \\ f^o_{7,8} \\ f^o_{9,8} \\ \bar{f}^p_{1,2} \\ \bar{f}^p_{1,4} \\ \bar{f}^p_{2,3} \\ \bar{f}^p_{2,5} \\ \bar{f}^p_{3,6} \\ \bar{f}^p_{3,9} \\ \bar{f}^p_{4,5} \\ \bar{f}^p_{5,6} \\ \bar{f}^p_{5,7} \\ \bar{f}^p_{6,8} \\ \bar{f}^p_{7,8} \\ \bar{f}^p_{9,8} \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}. \quad (4.12)$$

Використання метрики (4.12) дозволить розрахувати основний і резервний маршрути, які будуть містити мінімальну кількість каналів зв’язку.

Також для розрахунків і порівняльного аналізу буде використовуватись метрика за аналогією з протоколом OSPF для обчислення маршрутів, найкращих з погляду пропускної здатності:

$$\vec{f}_{OSPF} = \begin{bmatrix} f^o_{1,2} \\ f^o_{1,4} \\ f^o_{2,3} \\ f^o_{2,5} \\ f^o_{3,6} \\ f^o_{3,9} \\ f^o_{4,5} \\ f^o_{5,6} \\ f^o_{5,7} \\ f^o_{6,8} \\ f^o_{7,8} \\ f^o_{9,8} \\ \bar{f}^{\,p}_{1,2} \\ \bar{f}^{\,p}_{1,4} \\ \bar{f}^{\,p}_{2,3} \\ \bar{f}^{\,p}_{2,5} \\ \bar{f}^{\,p}_{3,6} \\ \bar{f}^{\,p}_{3,9} \\ \bar{f}^{\,p}_{4,5} \\ \bar{f}^{\,p}_{5,6} \\ \bar{f}^{\,p}_{5,7} \\ \bar{f}^{\,p}_{6,8} \\ \bar{f}^{\,p}_{7,8} \\ \bar{f}^{\,p}_{9,8} \end{bmatrix} = \begin{bmatrix} 10^8/c_{1,2} \\ 10^8/c_{1,4} \\ 10^8/c_{2,3} \\ 10^8/c_{2,5} \\ 10^8/c_{3,6} \\ 10^8/c_{3,9} \\ 10^8/c_{4,5} \\ 10^8/c_{5,6} \\ 10^8/c_{5,7} \\ 10^8/c_{6,8} \\ 10^8/c_{7,8} \\ 10^8/c_{9,8} \\ 10^8/c_{1,2} \\ 10^8/c_{1,4} \\ 10^8/c_{2,3} \\ 10^8/c_{2,5} \\ 10^8/c_{3,6} \\ 10^8/c_{3,9} \\ 10^8/c_{4,5} \\ 10^8/c_{5,6} \\ 10^8/c_{5,7} \\ 10^8/c_{6,8} \\ 10^8/c_{7,8} \\ 10^8/c_{9,8} \end{bmatrix}. \quad (4.13)$$

Сформуємо умови збереження потоку (4.3) та (4.4) на вузлах ядра мережі, що досліджується, які є однаковими як для основних, так і для резервних маршрутів:

$$\begin{cases} x_{1,2} + x_{1,4} = 1; \\ -x_{1,2} + x_{2,3} + x_{2,5} = 0; \\ -x_{2,3} + x_{3,6} + x_{3,9} = 0; \\ -x_{1,4} + x_{4,5} = 0; \\ -x_{2,5} - x_{4,5} + x_{5,6} + x_{5,7} = 0; \\ -x_{3,6} - x_{5,6} + x_{6,8} = 0; \\ -x_{5,7} + x_{7,8} = 0; \\ -x_{3,9} + x_{9,8} = 0 \\ -x_{6,8} - x_{7,8} - x_{9,8} = -1. \end{cases} \quad (4.14)$$

$$\begin{cases} \bar{x}_{1,2} + \bar{x}_{1,4} = 1; \\ -\bar{x}_{1,2} + \bar{x}_{2,3} + \bar{x}_{2,5} = 0; \\ -\bar{x}_{2,3} + \bar{x}_{3,6} + \bar{x}_{3,9} = 0; \\ -\bar{x}_{1,4} + \bar{x}_{4,5} = 0; \\ -\bar{x}_{2,5} - \bar{x}_{4,5} + \bar{x}_{5,6} + \bar{x}_{5,7} = 0; \\ -\bar{x}_{3,6} - \bar{x}_{5,6} + \bar{x}_{6,8} = 0; \\ -\bar{x}_{5,7} + \bar{x}_{7,8} = 0; \\ -\bar{x}_{3,9} + \bar{x}_{9,8} = 0 \\ -\bar{x}_{6,8} - \bar{x}_{7,8} - \bar{x}_{9,8} = -1. \end{cases} \quad (4.15)$$

У векторно-матричному представленні система рівнянь прийме такий вигляд:

$$Aeq * \vec{x} = \vec{b}eq,$$

де згідно з (4.14) або (4.15)

$$Aeq = \begin{bmatrix} Aeq1 & 0 \\ 0 & Aeq1 \end{bmatrix},$$

$$\vec{b}eq = \begin{bmatrix} \vec{b}eq1 \\ \vec{b}eq1 \end{bmatrix}$$

при

$$Aeq1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & -1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 \end{bmatrix};$$

$$beq1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \end{bmatrix}. \quad (4.16)$$

Умови запобігання перевантаження каналів зв’язку для основного маршруту представлено системою нерівностей:

$$\begin{cases} r * x_{1,2} \le c_{1,2}; \\ r * x_{1,4} \le c_{1,4}; \\ r * x_{2,3} \le c_{2,3}; \\ r * x_{2,5} \le c_{2,5}; \\ r * x_{3,6} \le c_{3,6}; \\ r * x_{3,9} \le c_{3,9}; \\ r * x_{4,5} \le c_{4,5}; \\ r * x_{5,6} \le c_{5,6}; \\ r * x_{5,7} \le c_{5,7}; \\ r * x_{6,8} \le c_{6,8}; \\ r * x_{7,8} \le c_{7,8}; \\ r * x_{9,8} \le c_{9,8}. \end{cases} \quad (4.17)$$

Доповнимо систему умов перевантаження каналів зв’язку основного маршруту умовами для резервного маршруту:

$$\begin{cases} r * \bar{x}_{1,2} \le c_{1,2}; \\ r * \bar{x}_{1,4} \le c_{1,4}; \\ r * \bar{x}_{2,3} \le c_{2,3}; \\ r * \bar{x}_{2,5} \le c_{2,5}; \\ r * \bar{x}_{3,6} \le c_{3,6}; \\ r * \bar{x}_{3,9} \le c_{3,9}; \\ r * \bar{x}_{4,5} \le c_{4,5}; \\ r * \bar{x}_{5,6} \le c_{5,6}; \\ r * \bar{x}_{5,7} \le c_{5,7}; \\ r * \bar{x}_{6,8} \le c_{6,8}; \\ r * \bar{x}_{7,8} \le c_{7,8}; \\ r * \bar{x}_{9,8} \le c_{9,8}. \end{cases} \quad (4.18)$$

Система нерівностей (4.17) або (4.18) у векторно-матричній формі буде мати наступний вигляд:

$$A * \vec{x} \le \vec{b},$$

де

$$A = \begin{bmatrix} A1 & 0 \\ 0 & A1 \end{bmatrix},$$

$$\vec{b}eq = \begin{bmatrix} \vec{b}1 \\ \vec{b}1 \end{bmatrix},$$

$$A1 = \begin{bmatrix} r & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & r & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & r & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & r & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & r & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & r & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & r & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & r & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & r & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & r & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & r & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & r \end{bmatrix};$$

$$\vec{b}1 = \begin{bmatrix} c_{1,2} \\ c_{1,4} \\ c_{2,3} \\ c_{2,5} \\ c_{3,6} \\ c_{3,9} \\ c_{4,5} \\ c_{5,6} \\ c_{5,7} \\ c_{6,8} \\ c_{7,8} \\ c_{9,8} \end{bmatrix}. \quad (4.16)$$

Нехай захисту підлягатиме канал (2,3) фрагменту мережі, показаному на рис. 4.2. Також від першого до восьмого вузла передаватиметься потік з інтенсивністю r = 50 пак/с. Таким чином, в результаті розв'язання задачі лінійного програмування при застосуванні коду, реалізованого за допомогою Python та функціоналу бібліотек NumPy та Scipy (Додаток А), були отримані наступні маршрутні рішення.

З використанням метрики (4.12) був отриманий порядок маршрутизації для основного та резервного маршрутів, показаний на рис. 4.3.

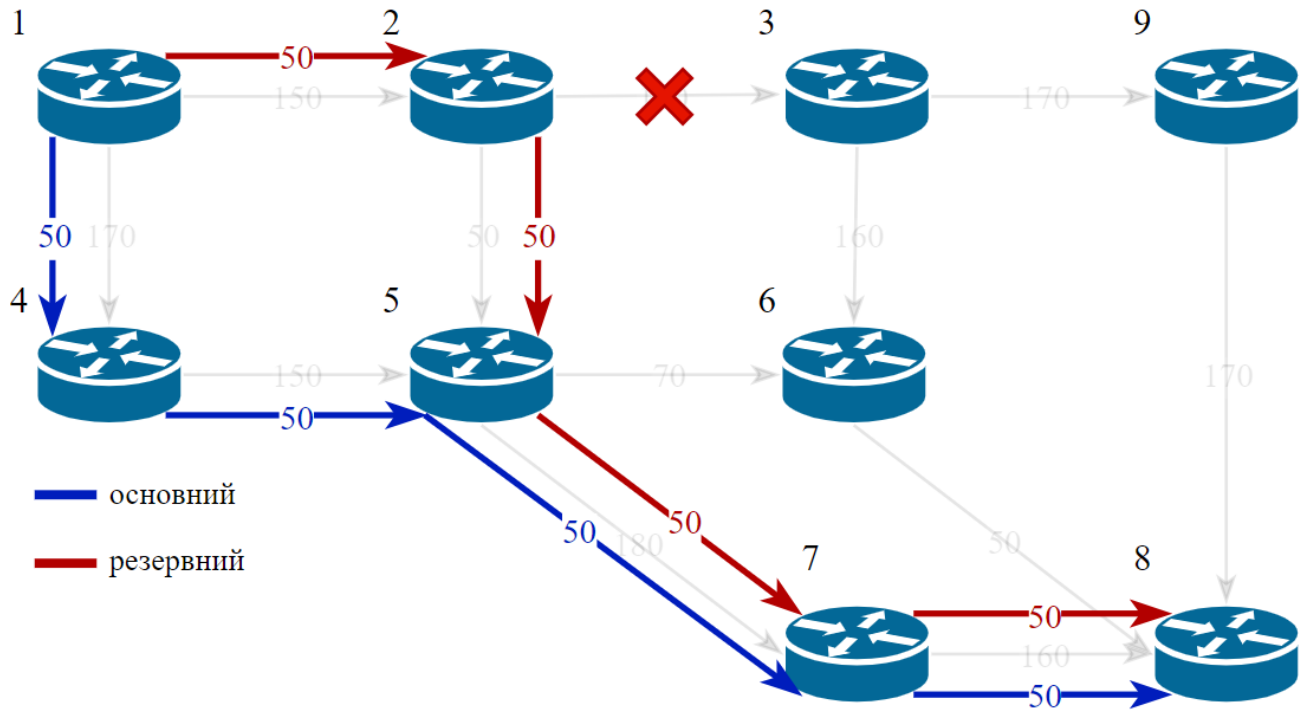

Рисунок 4.3 – Основний і резервний маршрути з метрикою (4.12) при інтенсивності потоку r = 50 пак/с та захисті каналу (2,3)

Водночас при використанні метрики (4.13) отримано маршрутні рішення, вказані на рис. 4.4.

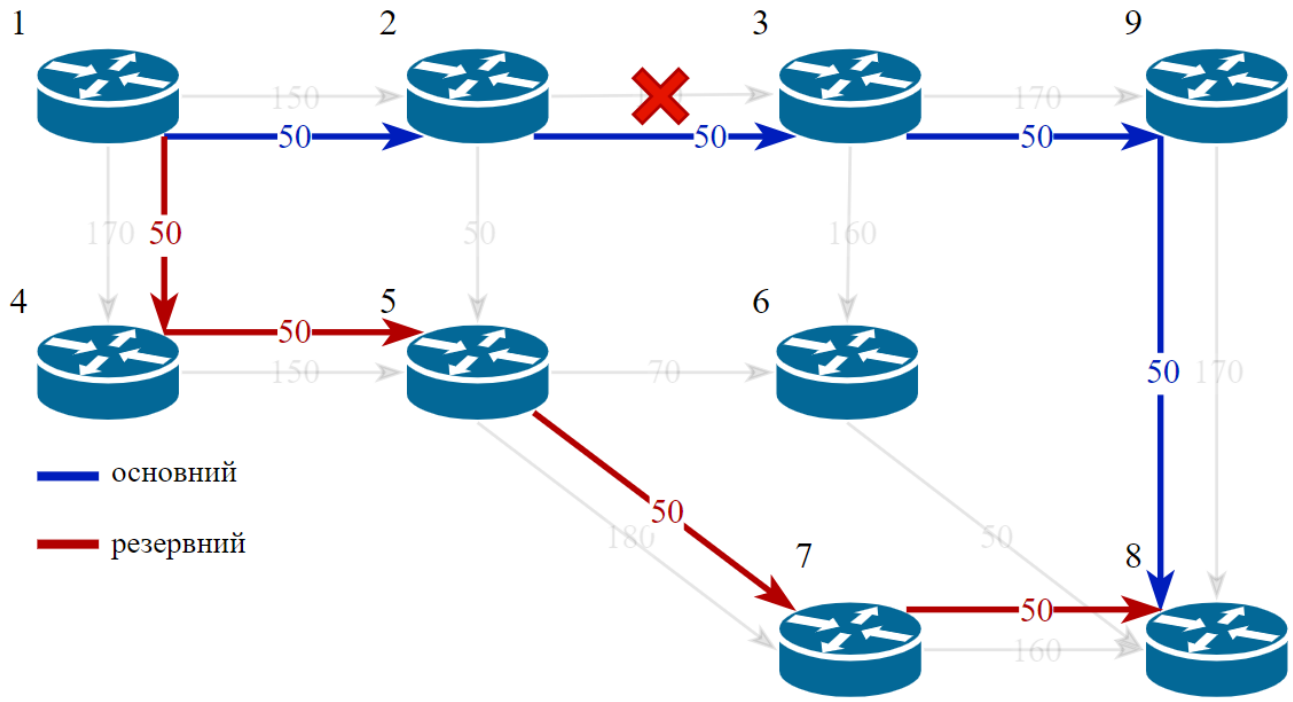

Рисунок 4.4 – Основний і резервний маршрути з метрикою (4.13) при інтенсивності потоку r = 50 пак/с та захисті каналу (2,3)

Аналіз отриманих результатів показав наступне. Метрика (4.12), що орієнтована на вибір найкоротшого маршруту за кількістю каналів зв'язку, сприяє формуванню основного і резервного маршрутів таким чином, щоб вони обидва оминали канал, який захищається. Бачимо, що основний і резервний маршрути відрізняються лише двома каналами між собою. Зі свого боку метрика (4.13) дозволяє розрахувати основний і резервний маршрути, що не перетинаються, та, крім того, обираються так, що пропускна здатність (ПЗ) основного і резервного маршрутів є максимальною (таблиця 4.2).

Таблиця 4.2 – Пропускні здатності та канали зв'язку основного та резервного маршрутів при інтенсивності потоку r = 50 пак/с та захисті каналу (2,3)

Тип маршруту	Маршрут			
	f_{RIP}	ПЗ, пак/с	f_{ospf}	ПЗ, пак/с
Основний	1→ 4 → 5 → 7 → 8	150	1→ 2 → 3 → 9 → 8	150
Резервний	1→ 2 → 5 → 7 → 8	50	1→ 4 → 5 → 7 → 8	150

Виконаємо аналогічні розрахунки маршрутів для швидкої перемаршрутизації для того ж самого потоку, але при захисті каналу (1,2) (рис. 4.5 і 4.6).

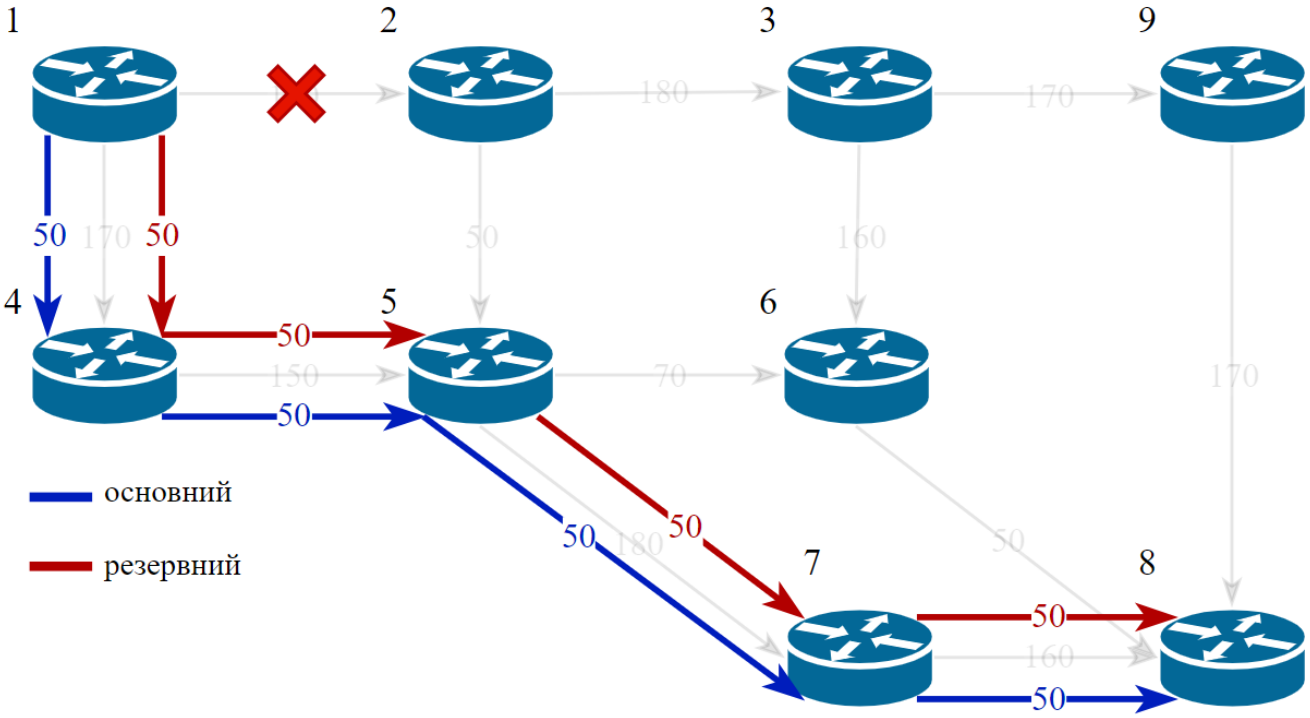

Рисунок 4.5 – Основний і резервний маршрути з метрикою (4.12) при інтенсивності потоку r = 50 пак/с та захисті каналу (1,2)

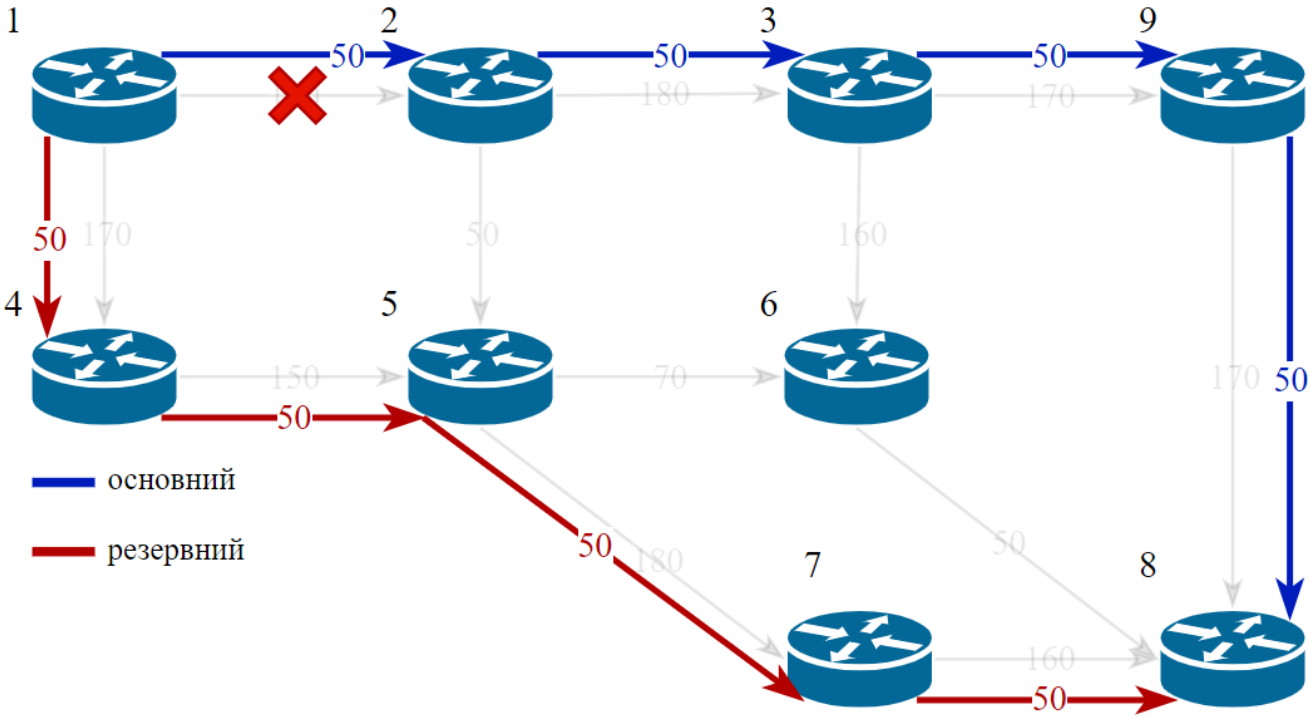

Рисунок 4.6 – Основний і резервний маршрути з метрикою (4.13) при інтенсивності потоку r = 50 пак/с та захисті каналу (1,2)

Використання метрики (4.12) призвело до повного співпадіння основного і резервного маршрутів, водночас метрика (4.13) дозволила отримати результат, аналогічний попередньому розрахунковому прикладу. Таким чином, робимо висновок, що метрика (4.13) сприяє обчисленню найбільш продуктивних як основного, так і резервного маршрутів.

Для подальшого аналізу збільшимо інтенсивність потоку до значення r = 160 пак/с та змінимо канал, який має бути захищений, на канал (2,3). Отриманий порядок маршрутизації для основного та резервного маршрутів з використанням метрики (4.12) показаний на рис. 4.7.

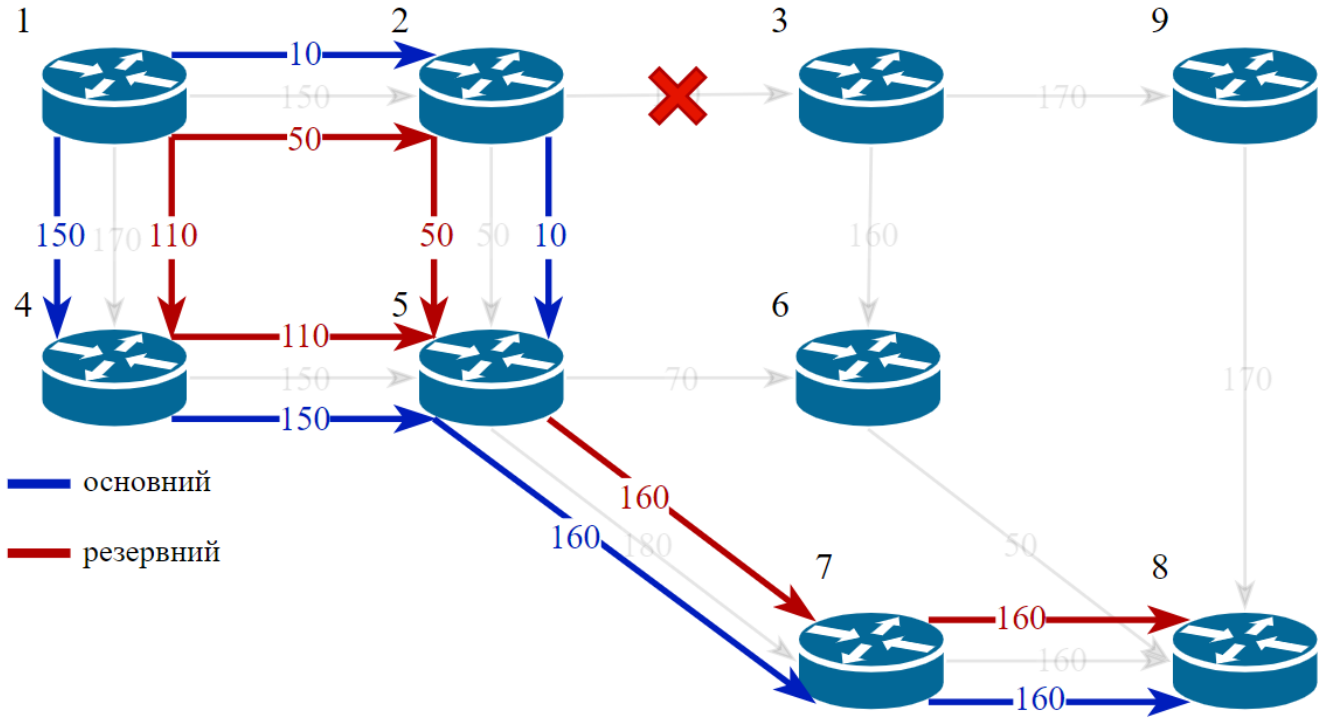

Рисунок 4.7 – Основний і резервний маршрути з метрикою (4.12) при інтенсивності потоку r = 160 пак/с та захисті каналу (2,3)

З результатів розрахунку маршрутів за метриками (4.12) та (4.13) можна побачити, що при збільшенні інтенсивності потоку до r = 160 пак/с обидві метрики використовують балансування навантаження та потік пакетів розподіляється за декількома шляхами. У випадку метрики (4.12), балансування навантаження для основного та резервного маршрутів, здійснюється за однаковими шляхами та оминають захисний канал. В той час метрика (4.13) має однаковий з метрикою (4.12) маршрут для резервного шляху, але основний маршрут розрахований з урахуванням максимальної пропускної здатності та пролягає через канал (2,3), який

підлягає захисту. Характеристика отриманих основного і резервного мультишляхів показано в таблиці 4.3.

Таблиця 4.3 – Пропускні здатності та канали зв'язку основного та резервного маршрутів при інтенсивності потоку r = 160 пак/с та захисті каналу (2,3)

Тип маршруту	Маршрут			
	f_{RIP}	ПЗ, пак/с	f_{ospf}	ПЗ, пак/с
Основний мультишлях	1) 1→ 4 → 5 → 7 → 8 2) 1→ 2 → 5 → 7 → 8	150 50	1) 1→ 2 → 3 → 9 → 8 2) 1→ 4 → 5 → 7 → 8	150 150
Резервний мультишлях	1) 1→ 4 → 5 → 7 → 8 2) 1→ 2 → 5 → 7 → 8	150 50	1) 1→ 4 → 5 → 7 → 8 2) 1→ 2 → 5 → 7 → 8	150 50

Тоді як при використанні метрики (4.13), отриманий порядок маршрутизації для основного та резервного маршрутів показаний на рис. 4.8. Слід зауважити, що сумарна пропускна зданість основного маршруту, отриманого на основі (4.13) дорівнює 300 пак/с, що у півтори рази вище за пропускну здатність основного маршруту з метрикою (4.12) – 200 пак/с (таблиця 4.3).

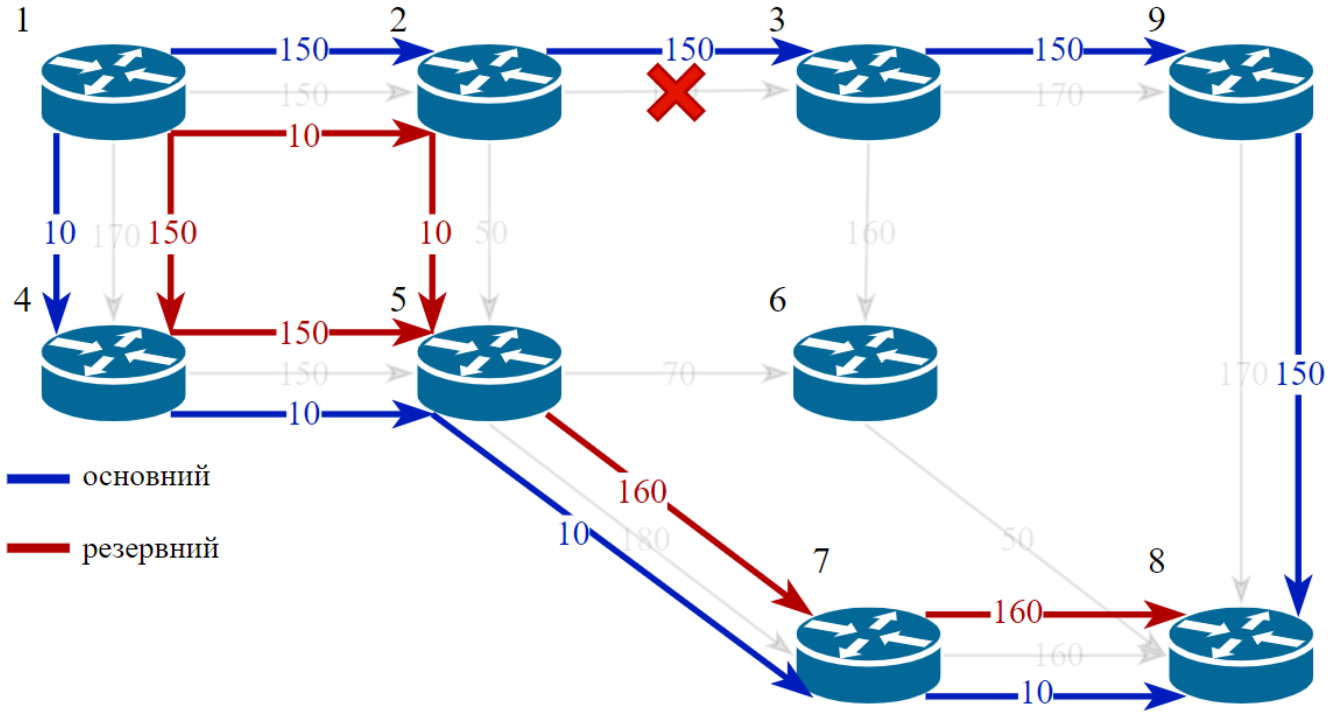

Рисунок 4.8 – Основний і резервний маршрути з метрикою (4.13) при інтенсивності потоку r = 160 пак/с та захисті каналу (2,3)

Для наступного досліджуваного прикладу збільшимо інтенсивність потоку до r = 200 пак/с та канал, який підлягатиме захисту, залишатиметься (2,3). Отримані маршрутні рішення для основного та резервного маршрутів з використанням метрик (4.12) та (4.13) співпадають та показані на рис. 4.9 та таблиці 4.4.

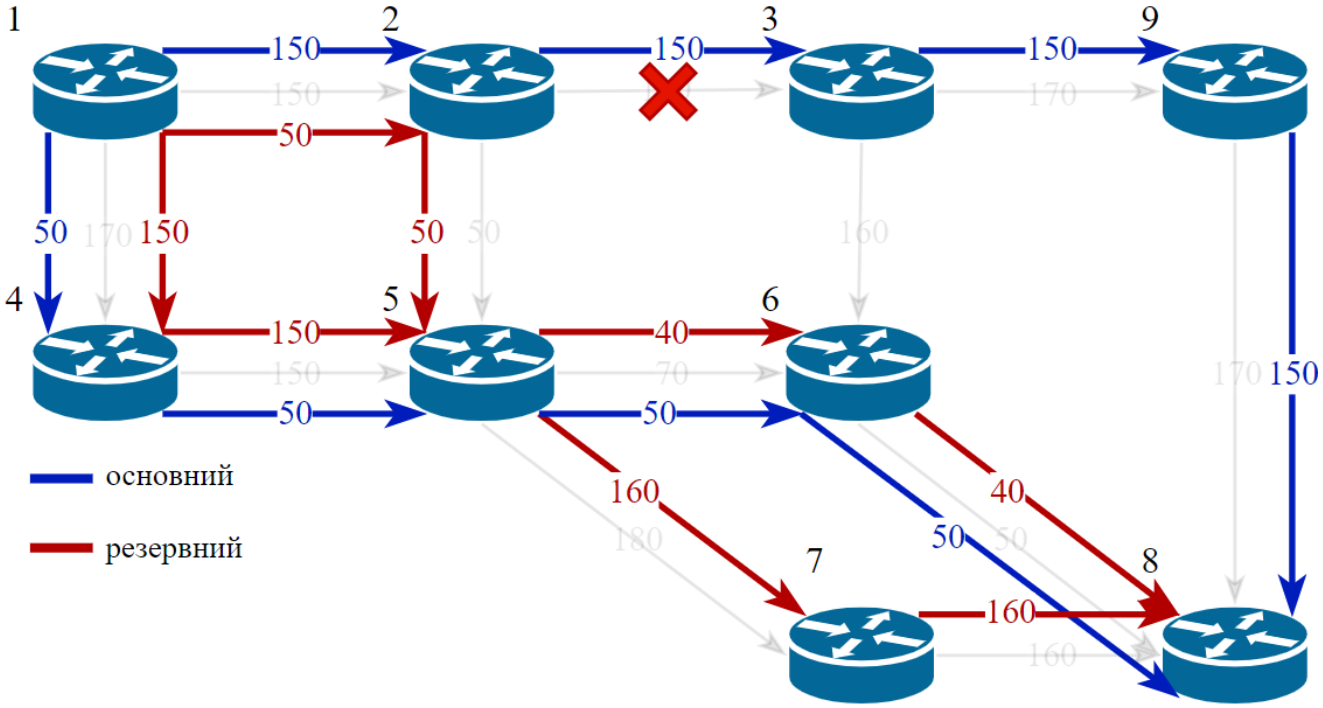

Рисунок 4.9 – Основний і резервний маршрути з метрикою (4.12 та 4.13) при інтенсивності потоку r = 200 пак/с та захисті каналу (2,3)

Таблиця 4.4 – Характеристика основного та резервного маршрутів при інтенсивності потоку r = 200 пак/с та захисті каналу (2,3)

Тип маршруту	Маршрут			
	f_{RIP}	Доля r, пак/с	f_{ospf}	Доля r, пак/с
Основний мультишлях	1) 1→ 2 → 3 → 9 → 8 2) 1→ 4 → 5 → 6 → 8	150 50	1) 1→ 2 → 3 → 9 → 8 2) 1→ 4 → 5 → 6 → 8	150 50
Резервний мультишлях	1) 1→ 4 → 5 → 7 → 8 2) 1→ 2 → 5 → 6 → 8 3) 1→ 2 → 5 → 7 → 8	150 40 10	1) 1→ 4 → 5 → 7 → 8 2) 1→ 2 → 5 → 6 → 8 3) 1→ 2 → 5 → 7 → 8	150 40 10

Отже, маршрутні рішення для обох метрик співпадають щодо основного та резервного шляхів, тому що інтенсивність потоку у 200 пак/с є максимально

можливою для данного фрагменту мережі та постановки оптимізаційної задачі. Також дослідження показало, що при інтенсивності меншій 150 пак/с за будь-якої метрики можливе використання єдиного шляху, а при інтенсивності більше 150 пак/с починається формування мультишляху. Проте основний і резервний мультишляхи формуються по-різному. Залежності кількості маршрутів в основному та резервному мультишляхах для метрики (4.13) від інтенсивності потоку, що передається, показано на рисунках 4.10 та 4.11. Для аналізу обрано метрику f_{ospf} (4.13), оскільки вона дозволяє отримувати найбільш продуктивні маршрутні рішенння.

Характер цих залежностей показує те, що основний мультишлях формується саме з найбільш продуктивних каналів зв'язку, а резервний формується на основі того мережного ресурсу, що залишається після формування основного. Проте очевидно, що не використовується високопродуктивний канал (3,6). Це говорить про те, що з погляду покращення балансування навантаження в мережі потрібно також використовувати принципи концепції Traffic Engineering, коли при формуванні мультишляхів враховується завантаженність каналів зв'язку.

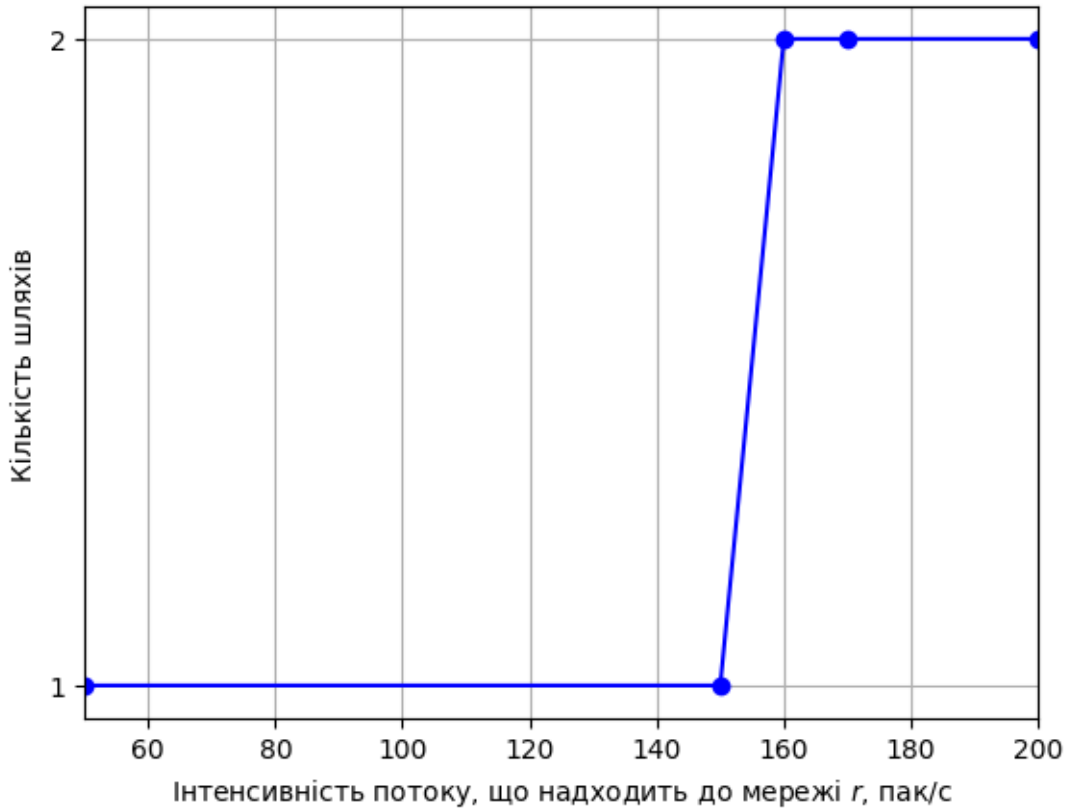

Рисунок 4.10 – Залежність кількості маршрутів в основному мультишляху для метрики (4.13) від інтенсивності потоку, що передається

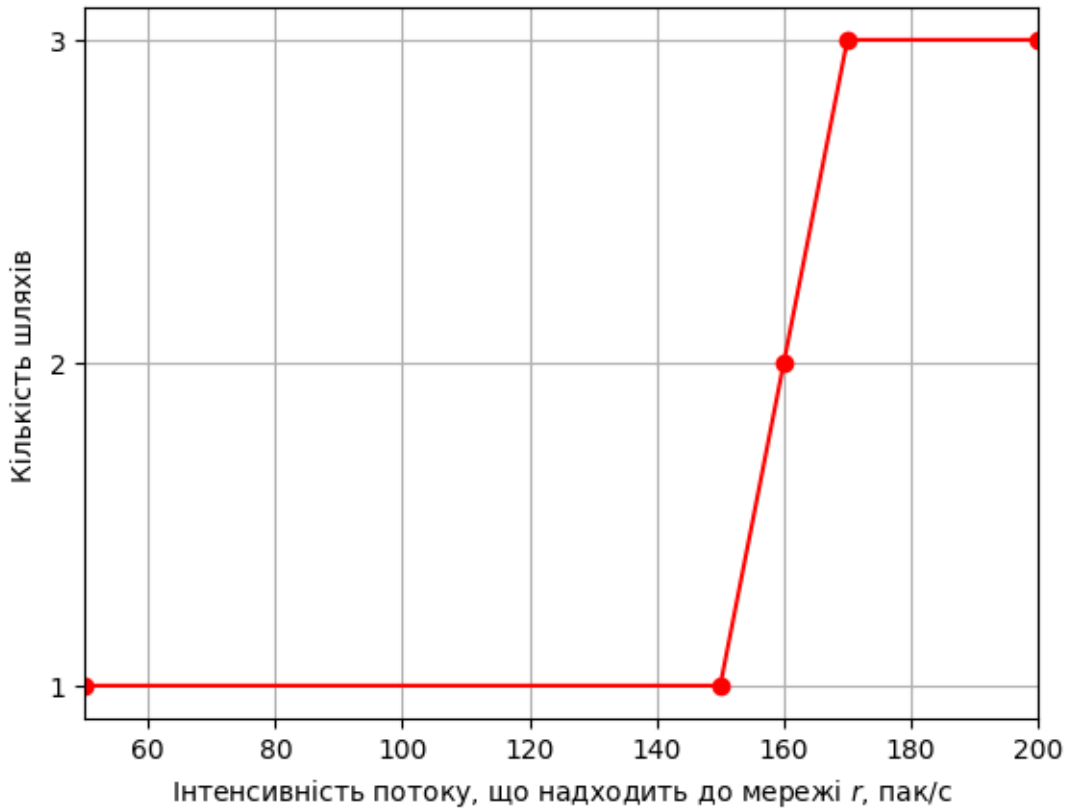

Рисунок 4.11 – Залежність кількості маршрутів у резервному мультишляху для метрики (4.13) від інтенсивності потоку, що передається

Далі буде розглянуто особливості реалізації схеми захисту вузла мережі (4.9). Для подальшого аналізу нехай захисту підлягає вузол 9 при інтенсивності потоку $r = 50$ пак/с. Отриманий порядок маршрутизації для основного та резервного маршрутів з використанням метрики (4.12) показаний на рис. 4.12. Слід зазначити, що захист вузла 9 по суті означає блокування щодо використання у резервному маршруті каналу (3,9) або (9,8).

Результати моделювання показали, що застосування метрики (4.12) знову призвело до співпадіння основного і резервного маршрутів, а метрика (4.13) дозволила отримати результат, аналогічний результату захисту каналів (1,2) та (2,3). Тобто обчислювались найбільш продуктивні основний і резервний маршрути.

Як можна побачити, при побудові маршрутних рішень за допомогою метрики (4.12), основний та резервний маршрут будуються в обхід захисного вузла та прилеглих до нього каналів. У випадку метрики (4.13) були отримані результати, аналогічні попереднім розрахунковим прикладам.

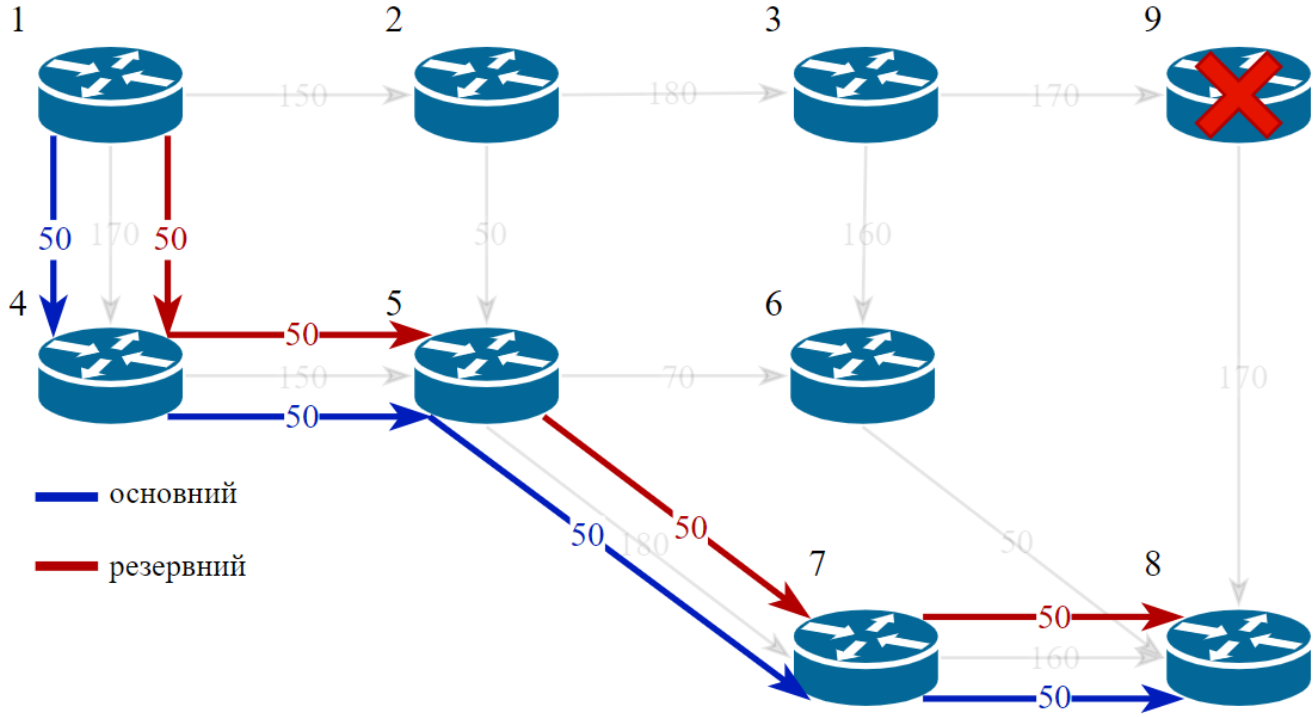

Рисунок 4.12 – Основний і резервний маршрути з метрикою (4.12) при інтенсивності потоку r = 50 пак/с та захисті вузла (9)

Розраховані маршрутні рішення з використанням метрики (4.13) показані на рис. 4.13.

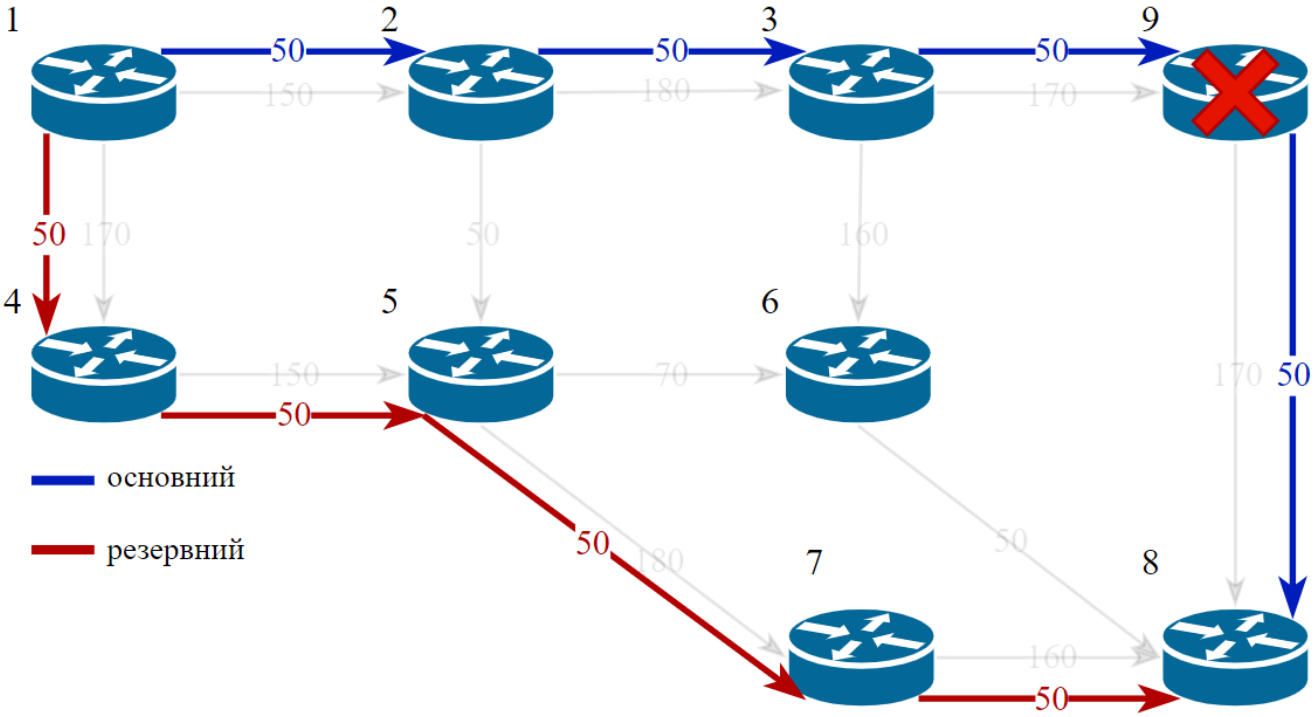

Рисунок 4.13 – Основний і резервний маршрути з метрикою (4.13) при інтенсивності потоку r = 50 пак/с та захисті вузла (9)

Для порівняння побудови маршрутних рішень виконаємо аналогічні розрахунки для швидкої перемаршрутизації, залишаючи вузол 9 таким, що захищається, та збільшуючи інтенсивність потоку до r = 200 пак/с. Отримані порядки маршрутизації для основного та резервного маршрутів з використанням метрик (4.12) та (4.13) показані на рис. 4.14 та рис. 4.15.

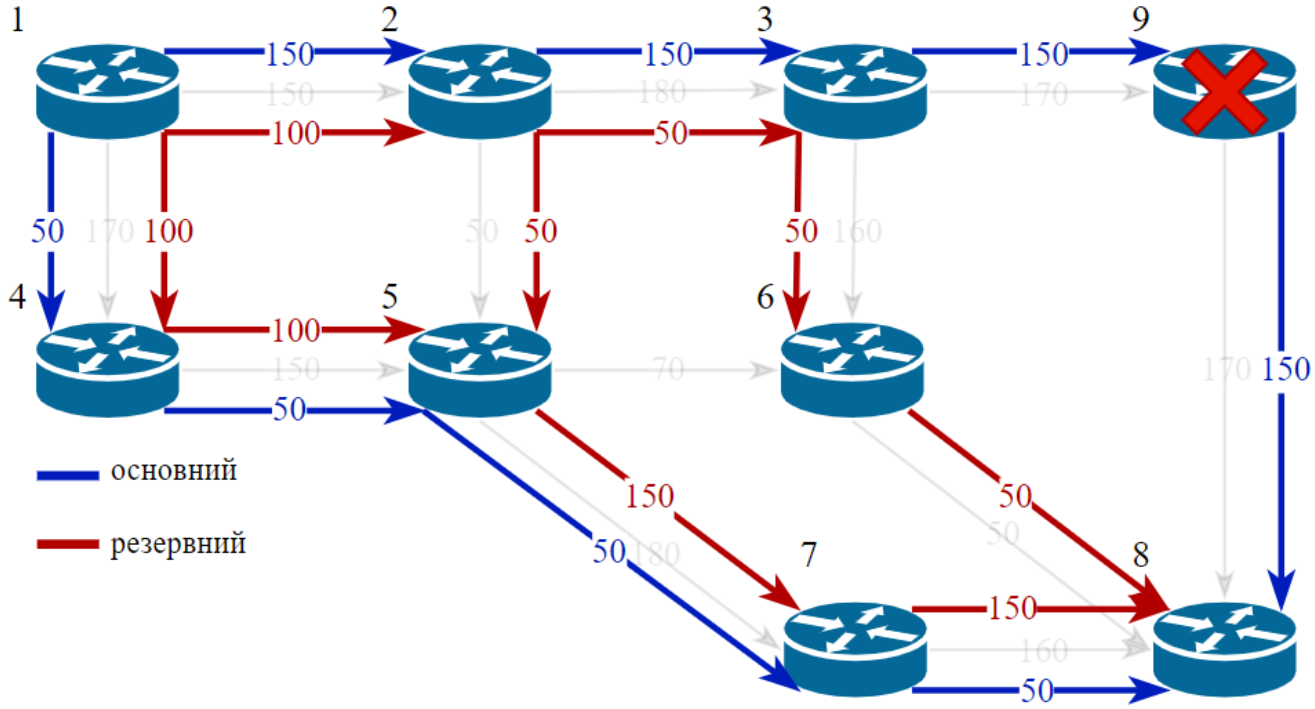

Рисунок 4.14 – Основний і резервний маршрути з метрикою (4.12) при інтенсивності потоку r = 200 пак/с та захисті вузла (9)

Таблиця 4.5 – Характеристика основного та резервного маршрутів при інтенсивності потоку r = 200 пак/с та захисті вузла 9

Тип маршруту	Маршрут			
	f_{RIP}	Доля r, пак/с	f_{ospf}	Доля r, пак/с
Основний мультишлях	1) 1→ 2 → 3 → 9 → 8 2) 1→ 4 → 5 → 7 → 8	150 50	1) 1→ 2 → 3 → 9 → 8 2) 1→ 4 → 5 → 7 → 8	150 50
Резервний мультишлях	1) 1→ 4 → 5 → 7 → 8 2) 1→ 2 → 5 → 7 → 8 3) 1→ 2 → 3 → 6 → 8	100 50 50	1) 1→ 4 → 5 → 7 → 8 2) 1→ 2 → 3 → 6 → 8	150 50

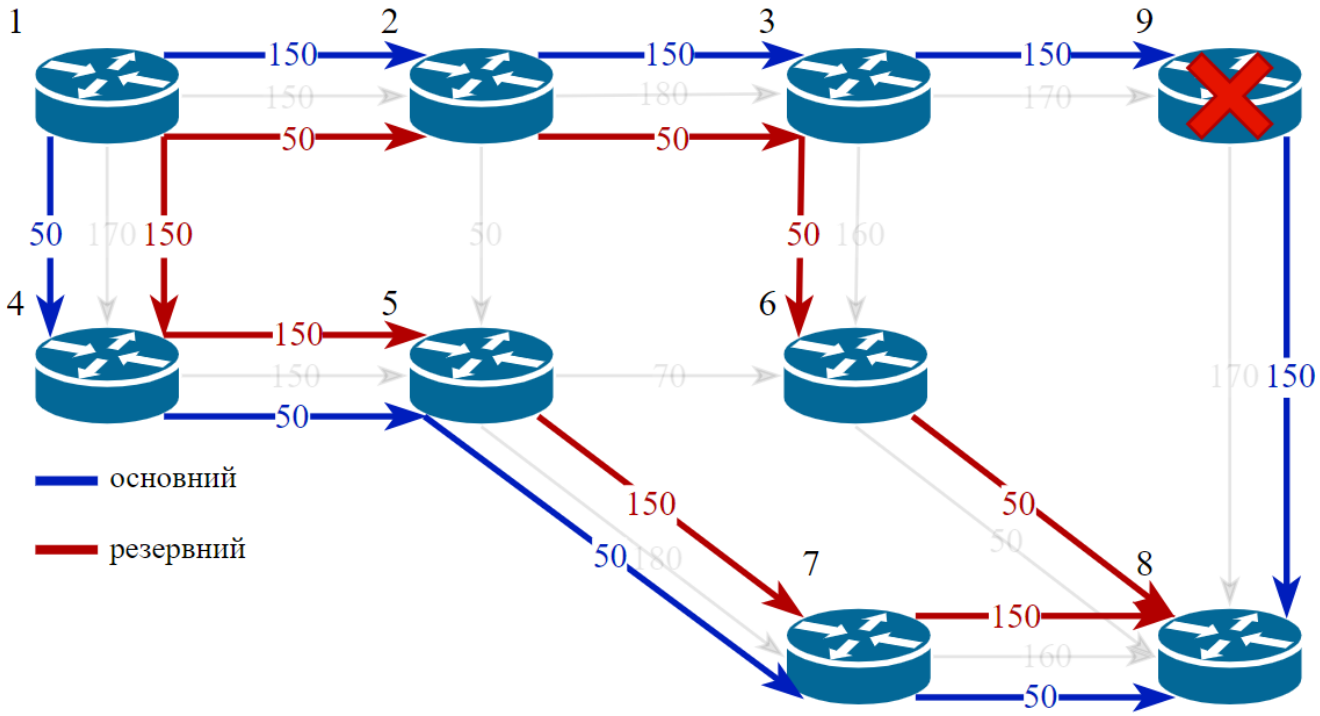

Рисунок 4.15 – Основний і резервний маршрути з метрикою (4.13) при інтенсивності потоку r = 200 пак/с та захисті вузла (9)

Згідно з рис. 4.14 та рис. 4.15, можна побачити, що при збільшенні інтенсивності потоку обидві метрики знов використовують балансування навантаження та потік пакетів розподіляється за декількома шляхами. У випадку метрики (4.12), розгалуження основного потоку відбувається за двома шляхами, в той час, як розгалуження резервного потоку охоплює 3 шляхи. Для метрики (4.13) основний маршрут залишається незмінним, але резервний маршрут повністю оминає сегмент мережі, що містить вузол 9, і формується за принципом включення найбільш продуктивних каналів зв’язку у маршрут.

ВИСНОВКИ

У кваліфікаційній роботі задачу щодо аналізу та дослідження перспективних методів забезпечення відмовостійкості засобами маршрутизації в інфокомунікаційних мережах, а також вибору ефективної моделі відмовостійкої маршрутизації вирішено у повному обсязі.

Зважаючи на результати дослідження, було визначено основи побудови відмовостійких інфокомунікаційних мереж та окреслено перешкоди та виклики, що запобігають реалізації відмовостійких систем. Було наголошено на актуальності забезпечення відмовостійкості ІКМ та запропоновано використання маршрутизації як засобу забезпечення стійкості інфокомунікаційних мереж.

Досліджено сучасний стан та перспективи розвитку технологій забезпечення відмовостійкості засобами маршрутизації в ІКМ. Визначено важливі ролі відмовостійкості та якості обслуговування в інфокомунікаціях. Проаналізовано перспективи розвитку підходів до вдосконалення стійкості маршрутизації та приділено увагу використанню сучасної шестиступінчатої стратегії відмовостійкості мереж.

Також проведено огляд та порівняльний аналіз існуючих протоколів та алгоритмів відмовостійкої маршрутизації в інфокомунікаційних мережах. Приведено класифікацію засобів відмовостійкої маршрутизації, розглянуті основні протоколи резервування шлюзу за замовчуванням та проаналізовано забезпечення відмовостійкої маршрутизації за допомогою технології FastReRoute. Приділено увагу аналізу моделей і методів відмовостійкої маршрутизації в ІКМ.

Експериментальну частину роботи присвячено дослідженню та порівняльному аналізу потокових моделей швидкої перемаршрутизації. У межах оптимізаційної постановки задачі були представлені та описані математичні моделі швидкої перемаршрутизації з різними метриками за умови реалізації схем захисту (резервування) каналу та вузла в мережі. На прикладі досліджуваного фрагменту мережі було проведено моделювання з використанням бібліотек Python NumPy та Scipy.

Технологічне завдання багатошляхової швидкої перемаршрутизації було сформульовано в оптимізаційній формі. Відповідні умови та обмеження для обчислення основного та резервного маршрутів представлені виразами (4.1)–(4.10), а також умови захисту каналу та вузла (4.7)–(4.9). Дослідження проводилось на

обраній топології (рис. 4.1), яка була використана для подальшого моделювання в середовищі Google Colab і програмної реалізації мовою Python. Для розрахунку основних і резервних маршрутів були використані метрики по аналогії з протоколами RIP та OSPF (4.12) та (4.13).

З урахуванням різних метрик формування маршрутів було проведено дослідження щодо побудови маршрутних рішень для основного та резервного шляхів при зміні значення інтенсивності потоку та вибору елемента мережі (каналу або вузла), що підлягає захисту. Проведені дослідження дозволили зробити висновки відносно вибору метрики та стратегії балансування навантаження.

При низькій інтенсивності потоку та механізму захисту каналу аналіз отриманих результатів показав наступне. Метрика (4.12), що орієнтована на вибір найкоротшого маршруту за кількістю каналів зв'язку, сприяє формуванню основного і резервного маршрутів таким чином, щоб вони обидва оминали канал, який захищається. Зі свого боку метрика (4.13) дозволяє розрахувати основний і резервний маршрути, що не перетинаються, та, крім того, обираються так, що пропускна здатність основного і резервного маршрутів є максимальною.

При збільшенні інтенсивності потоку, що передавався між вузлами отправником і отримувачем, обидві метрики сприяли формуванню мультишляхів, коли потік пакетів розподілявся за декількома шляхами. Таким чином, обрана стратегія багатошляхової маршрутизації сприяла і реалізації балансування навантаження під час швидкої перемаршрутизації.

Також дослідження показали, що при інтенсивності меншій 150 пак/с за будь-якої метрики можливе використання єдиного шляху, а при інтенсивності більше 150 пак/с починалось формування мультишляху. Проте основний і резервний мультишляхи формувались по-різному. Було отримано відповідні залежності кількості маршрутів в основному та резервному мультишляхах для метрики (4.13) від інтенсивності потоку, що передається.

Характер отриманих залежностей показав, що основний мультишлях формується саме з найбільш продуктивних каналів зв'язку, а резервний формується на основі того мережного ресурсу, що залишається після формування основного. Проте очевидно, що деякі високопродуктивні канали мережі не використовувались. Це говорить про те, що з погляду покращення балансування навантаження в мережі потрібно також використовувати принципи концепції Traffic Engineering (TE), коли при формуванні мультишляхів враховується завантаженність каналів зв'язку.

Результати дослідження побудови маршрутних рішень для основного та резервного шляхів за допомогою метрик (4.12) та (4.13) при схемі захисту вузла підтвердили динаміку отримуваних рішень для реалізації схеми захисту каналу.

Загальний висновок говорить про те, що в сучасних мультисервісних інфокомунікаційних мережах рекомендується використовувати стратегії багатошляхової відмовостійкої маршрутизації спільно з балансуванням навантаження на основі ТЕ. Крім того, потрібно забезпечувати захист (резервування) не тільки каналів, вузлів і шляхів для підвищення мережної відмовостійкості, але й резервування з гарантією якості обслуговування вздовж основних і резервних маршрутів (наприклад, захист пропускної здатності).

Окремі результати роботи доповідались на Міжнародних наукових конференціях, а саме [8, 15, 16]. Кваліфікаційна робота пов’язана з дослідженнями у межах науково-технічної (експериментальної) розробки 0123U100128 «Розробка алгоритмічно-програмного забезпечення для кіберстійких інфокомунікаційних систем і мереж критичних інфраструктур», що ведеться на кафедрі інфокомунікаційної інженерії імені В.В. Поповського Харківського національного університету радіоелектроніки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Khan N., Bin Salleh R., Koubaa A., Khan Z., Khan M.K., Ali I. Data plane failure and its recovery techniques in SDN: A systematic literature review. Journal of King Saud University-Computer and Information Sciences. 2023. Vol. 35(3). P. 176–201. DOI: https://doi.org/10.1016/j.jksuci.2023.02.001.

2. Лемешко О. В., Єременко О. С., Невзорова, О. С. (2020), Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість, Харків: ХНУРЕ, 308 с. DOI: https://doi.org/10.30837/978-966-659-282-1.

3. Лемешко О.В., Єременко О.С., Євдокименко М.О., Шаповалова А.С., Слейман Б. Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах : монографія. М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. Харків : ХНУРЕ, 2022. 198 с. DOI: https://doi.org/10.30837/978-966-659-378-1.

4. International Telecommunication Union. Requirements for Network Resilience and Recovery. 2014. 28 с.

5. Єременко О.С., Євдокименко М.О. Огляд теоретичних рішень щодо відмовостійкої маршрутизації в телекомунікаційних мережах. Проблеми телекомунікацій. 2018. №1(22), С. 25–42.

6. Rak J., Resilient Routing in Communication Networks (Computer Communications and Networks), 1st edition. Springer. 2015. 181 с.

7. Rak J., Hutchison D. (eds) Guide to Disaster-Resilient Communication Networks. Computer Communications and Networks. Springer, Cham. 2020. 813 p. DOI: https://doi.org/10.1007/978-3-030-44685-7.

8. Недоступ Д.М., Солом'яний М.В. Аналіз підходів забезпечення відмовостійкості архітектур Extended Cloud. Матеріали восьмої Міжнародної науково-технічної конференції «Проблеми електромагнітної сумісності перспективних безпроводових мереж зв'язку (ЕМС-2022)». Харків, ХНУРЕ, 2022. С. 39–40.

9. Єременко О.С., Мерсні А., Підвищення відмовостійкості елементів сучасних інфокомунікаційних мереж із застосуванням протоколів резервування шлюзу за замовчуванням. Проблеми телекомунікацій. 2020. №2(27). С. 68–81.

10. GLobal PivIT., The Ultimate Comparison Guide – FHRP Shootout: HSRP vs. VRRP vs. GLBP. url: https://ipcisco.com/lesson/first-hop-redundancy-protocols/.

11. IPCisco., First Hop Redundancy Protocols. https://ipcisco.com/lesson/first-hop-redundancy-protocols/.

12. Lemeshko O., Mersni A., Yeremenko O., Omowumi S.O., Volotka V., Al-Dulaimi A.M. Application prospects of first hop redundancy protocols for fault-tolerant SDN controllers: a survey. In Proc. 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). October 2021. IEEE, 2021. P. 416–420. IEEE. DOI: https://doi.org/10.1109/PICST54195.2021.9772141.

13. MPLS Traffic Engineering (TE) Fast Reroute (FRR). 2023. URL: https://networklessons.com/mpls/mpls-traffic-engineering-te-fast-reroute-frr.

14. Лемешко О.В., Невзорова О.С., Єременко О.С., Євсєєва О.Ю. Методичні вказівки до практичних занять з дисципліни «Управління та маршрутизація в ТКС» для студентів денної форми навчання спеціальності 6.050903 – Телекомунікації. Харків: ХНУРЕ, 2016. 64 с.

15. Nedostup D., Solomianyi M., Mamon R. End-to-End Network Resilience, Security, and QoS in SD-WAN. Інформатика, Математика, Автоматика IMA :: 2023: матеріали та програма Міжнародної наукової конференції молодих учених (м. Суми, 24-28 квітня 2023 р.). Суми : СумДУ, 2023. С. 39.

16. Недоступ Д.М., Солом’яний М.В. Стратегії відмовостійкості архітектур Extended Cloud на основі політик. XV Міжнародна науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» ПРІТС 2023: Збірник тез конференції. К.: КПІ ім. Ігоря Сікорського, 2023. С. 364.