

О.В. Лемешко  
О.С. Єременко  
О.С. Невзорова

**ПОТОВОКІ МОДЕЛІ  
ТА МЕТОДИ МАРШРУТИЗАЦІЇ  
В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ:  
ВІДМОВОСТІЙКІСТЬ, БЕЗПЕКА,  
МАСШТАБОВАНІСТЬ**



**О.В. Лемешко, О.С. Єременко, О.С. Невзорова**

**ПОТОКОВІ МОДЕЛІ ТА МЕТОДИ МАРШРУТИЗАЦІЇ  
В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ:  
ВІДМОВОСТІЙКІСТЬ, БЕЗПЕКА, МАСШТАБОВАНІСТЬ**

**Монографія**

Харків 2020

УДК 621.391

*Рекомендовано Науково-технічною радою  
Харківського національного університету радіоелектроніки  
(протокол №1 від 15.02.2019)*

**Рецензенти:**

*Кіріченко Л.О.*, доктор технічних наук, професор, Харківський національний університет радіоелектроніки;

*Василишин В.І.*, доктор технічних наук, доцент, Харківський національний університет Повітряних Сил імені Івана Кожедуба

**Лемешко О.В., Єременко О.С., Невзорова О.С.** Потоківі моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість. – Харків: ХНУРЕ, 2020. – 308 с.

**ISBN 978-966-659-282-1**

Монографія присвячена питанням, пов'язаним із синтезом математичних моделей і методів маршрутизації, які б слугували подальшою теоретичною основою перспективних протоколів маршрутизації та технологічних засобів управління трафіком для підвищення якості обслуговування, відмовостійкості та масштабованості інфокомунікаційних мереж, а також рівня їх мережної безпеки.

Робота призначена для науково-педагогічних працівників, зокрема магістрантів, аспірантів і докторантів, які працюють у галузі інфокомунікацій та мережної безпеки.

ISBN 978-966-659-282-1

DOI: 10.30837/978-966-659-282-1

© О.В. Лемешко, О.С. Єременко,  
О.С. Невзорова, 2020

## ЗМІСТ

Перелік скорочень.....	7
Вступ.....	9
Розділ 1. Роль і місце маршрутизації в сучасних інфокомунікаційних мережах.....	12
1.1. Мета та завдання інфокомунікаційних мереж у сучасному суспільстві ...	12
1.2. Огляд технологічних засобів забезпечення якості обслуговування в ІКМ .....	15
1.3. Класифікація маршрутних рішень в ІКМ .....	19
1.4. Вимоги, які висуваються до перспективних маршрутних рішень .....	29
1.5. Напрями вдосконалення протоколів маршрутизації в ІКМ.....	30
1.6. Узагальнена структура потокової моделі маршрутизації в ІКМ .....	33
1.7. Опис базових поточкових моделей маршрутизації в ІКМ.....	36
1.7.1. Потокова модель одноадресної маршрутизації в ІКМ .....	36
1.7.2. Потокова модель багатоадресної та ширококомовної маршрутизації в ІКМ .....	38
1.7.3. Основні варіанти критеріїв оптимальності маршрутних рішень в ІКМ .....	40
Висновки до першого розділу.....	42
Перелік джерел посилання до вступу та першого розділу .....	43
Розділ 2. Поточкові моделі та методи відмовостійкої маршрутизації в інфокомунікаційних мережах.....	52
2.1. Маршрутизація як засіб забезпечення відмовостійкості ІКМ .....	52
2.2. Класифікація засобів відмовостійкої маршрутизації в ІКМ .....	55
2.3. Аналіз моделей і методів відмовостійкої маршрутизації в ІКМ .....	67
2.4. Система поточкових моделей відмовостійкої маршрутизації без резервування елементів ІКМ.....	78
2.4.1. Синтез та дослідження потокової моделі багатошляхової маршрутизації в ІКМ шляхами, що не перетинаються .....	79
2.4.2. Синтез та дослідження потокової моделі багатошляхової маршрутизації в ІКМ шляхами, що перетинаються за вузлами .....	83
2.5. Потокова модель швидкої перемаршрутизації в ІКМ.....	86

2.6. Формалізація умов забезпечення захисту вузла, каналу, маршруту та пропускної здатності під час швидкої перемаршрутизації в ІКМ .....	87
2.7. Дослідження оптимальності рішень щодо швидкої перемаршрутизації в ІКМ .....	90
2.7.1. Формування критерію оптимальності рішень щодо швидкої перемаршрутизації на основі метрик .....	90
2.7.2. Характеристика оптимізаційних задач швидкої перемаршрутизації на основі метрик та методів їх розв'язання .....	93
2.7.3. Обґрунтування вибору вагових коефіцієнтів у критерії оптимальності рішень щодо швидкої перемаршрутизації в ІКМ .....	94
2.7.4. Білінійний критерій оптимальності рішень щодо швидкої перемаршрутизації в процесі реалізації схеми захисту шляху .....	98
2.7.5. Приклади розв'язання задачі швидкої перемаршрутизації багатоадресних потоків в ІКМ .....	102
2.8. Рішення щодо швидкої перемаршрутизації з балансуванням навантаження в ІКМ .....	105
2.8.1. Синтез та дослідження дворівневого методу одношляхової швидкої перемаршрутизації з балансуванням навантаження в ІКМ .....	106
2.8.2. Синтез та дослідження лінійної оптимізаційної моделі багатошляхової швидкої перемаршрутизації з балансуванням навантаження в ІКМ .....	119
2.9. Поточкова модель відмовостійкої маршрутизації із захистом шлюзу за замовчуванням .....	127
2.9.1. Графова модель відмовостійкої маршрутизації в ІКМ .....	127
2.9.2. Поточкова модель відмовостійкої маршрутизації в ІКМ .....	129
2.9.3. Дослідження схеми захисту шлюзу за замовчуванням у разі використання різних стратегій маршрутизації в ІКМ .....	133
Висновки до другого розділу .....	136
Перелік джерел посилання до другого розділу .....	139
 Розділ 3. Моделі та методи безпечної маршрутизації в інфокомунікаційних мережах.....	149
3.1. Характеристика засобів мережної безпеки в інфокомунікаціях.....	149
3.2. Аналіз методів безпечної маршрутизації в ІКМ.....	154
3.3. Удосконалення методу безпечної маршрутизації повідомлень шляхами, що не перетинаються: проактивний підхід.....	156
3.3.1. Метод безпечної маршрутизації повідомлень шляхами, що не перетинаються в ІКМ .....	156

3.3.2. Дослідження методу безпечної маршрутизації повідомлень шляхами, що не перетинаються .....	159
3.4. Метод безпечної маршрутизації повідомлень шляхами, що перетинаються: проактивний підхід .....	164
3.5. Аналіз запропонованого методу безпечної маршрутизації повідомлень шляхами, що перетинаються .....	169
3.5.1. Дослідження методу безпечної маршрутизації повідомлень шляхами, що перетинаються, у разі використання єдиного композитного шляху .....	169
3.5.2. Дослідження методу безпечної маршрутизації повідомлень у разі використання двох різнотипних шляхів, що не перетинаються .....	173
3.6. Метод безпечної швидкої перемаршрутизації повідомлень композитними шляхами: проактивний і реактивний підходи .....	177
3.7. Дослідження методу безпечної швидкої перемаршрутизації повідомлень композитними шляхами .....	181
Висновки до третього розділу .....	184
Перелік джерел посилання до третього розділу .....	187
 Розділ 4. Потоків моделі та методи ієрархічної маршрутизації в інфокомунікаційних мережах .....	192
4.1. Аналіз відомих теоретичних і протокольних рішень щодо ієрархічної маршрутизації в ІКМ .....	192
4.2. Потоків модель і метод ієрархічно-координаційної внутрішньодоменної маршрутизації в інфокомунікаційній мережі SDN/MPLS .....	204
4.2.1. Декомпозиційна модель ієрархічно-координаційної внутрішньодоменної маршрутизації в програмно-конфігурованій інфокомунікаційній мережі SDN/MPLS .....	205
4.2.2. Розв'язання задачі ієрархічно-координаційної внутрішньодоменної маршрутизації на основі метрик в інфокомунікаційній мережі SDN/MPLS .....	207
4.2.3. Дослідження процесів ієрархічно-координаційної внутрішньодоменної маршрутизації одноадресних потоків на основі метрик в інфокомунікаційній мережі SDN/MPLS .....	210
4.2.4. Розв'язання задачі ієрархічно-координаційної внутрішньодоменної маршрутизації одноадресних потоків з балансуванням навантаження в інфокомунікаційній мережі SDN/MPLS-TE .....	224

4.2.5. Дослідження процесів ієрархічно-координаційної внутрішньодоменної маршрутизації одноадресних потоків з балансуванням навантаження в інфокомунікаційній мережі SDN/MPLS-TE .....	226
4.2.6. Дослідження процесів ієрархічно-координаційної внутрішньодоменної маршрутизації багатоадресних потоків в інфокомунікаційній мережі SDN/MPLS-TE .....	231
4.2.7. Структура методу ієрархічно-координаційної внутрішньодоменної маршрутизації в інфокомунікаційній мережі SDN/MPLS .....	242
4.3. Синтез і дослідження математичної моделі та методу ієрархічно-координаційної міждоменної маршрутизації в програмно-конфігурованій ІКМ .....	245
4.3.1. Декомпозиційна модель міждоменної маршрутизації в програмно-конфігурованій ІКМ, що складається з множини послідовно з'єднаних доменів .....	245
4.3.2. Метод ієрархічно-координаційної міждоменної маршрутизації в програмно-конфігурованій ІКМ.....	252
4.3.3. Дослідження запропонованого методу ієрархічно-координаційної міждоменної маршрутизації в програмно-конфігурованій ІКМ .....	256
4.3.4. Трирівневий метод ієрархічно-координаційної маршрутизації в багатодоменній ІКМ.....	266
4.4. Синтез і дослідження математичної моделі та методу ієрархічної міждоменної швидкої перемаршрутизації в ІКМ .....	274
4.4.1. Декомпозиційна модель ієрархічної міждоменної швидкої перемаршрутизації в ІКМ .....	275
4.4.2. Умови захисту приграничних маршрутизаторів під час ієрархічно-координаційної міждоменної швидкої перемаршрутизації в ІКМ .	279
4.4.3. Метод ієрархічно-координаційної міждоменної швидкої перемаршрутизації в ІКМ .....	281
4.4.4. Дослідження методу ієрархічно-координаційної міждоменної швидкої перемаршрутизації в ІКМ .....	284
Висновки до четвертого розділу .....	289
Перелік джерел посилання до четвертого розділу .....	295
Висновки .....	303

## ПЕРЕЛІК СКОРОЧЕНЬ

БШМ	багатошляхова маршрутизація
ГІІ	глобальна інформаційна інфраструктура
ІКМ	інфокомунікаційна мережа
КЗ	канал зв'язку
КВ	канал зв'язку
ОШМ	одношляхова маршрутизація
ОС	операційна система
ПЗ	пропускна здатність
МД	мережа доступу
ТМ	транспортна мережа
AS (Autonomous System)	автономна система
ATM (Asynchronous Transfer Mode)	асинхронний режим передачі
BGP (Border Gateway Protocol)	протокол приграничного шлюзу
BR (Border Router)	приграничний маршрутизатор
DiffServ (Differentiated Services)	диференційовані послуги
ECMP (Equal Cost Multipath)	механізм вибору маршруту залежно від його вартості
EIGRP (Enhanced Interior Gateway Routing Protocol)	удосконалений протокол маршрутизації внутрішнього шлюзу
EGP (Exterior Gateway Protocol)	протокол маршрутизації зовнішнього шлюзу
FRR (Fast ReRoute)	швидка перемаршрутизація
GLBP (Gateway Load Balancing Protocol)	протокол балансування навантаження шлюзу за замовчуванням
HSRP (Hot Standby Router Protocol)	протокол маршрутизатора гарячого резерву
IntServ (Integrated Services)	інтегровані послуги
IP (Internet Protocol)	протокол міжмережної взаємодії
IPDV (IP packet delay variation)	варіація затримки передачі (джитер) IP-пакета
IPER (IP packet error ratio)	коефіцієнт помилок IP-пакетів
IPLR (IP packet loss ratio)	коефіцієнт втрат IP-пакетів
IPTD (IP packet transfer delay)	середня затримка передачі IP-пакета
IGP (Interior Gateway Protocol)	протокол внутрішнього шлюзу
IGRP (Interior Gateway Routing Protocol)	протокол маршрутизації внутрішнього шлюзу



IPsec (Internet Protocol Security)	набір протоколів для забезпечення безпеки даних, які передаються за допомогою протоколу IP
IS-IS (Intermediate System – to – Intermediate System)	протокол маршрутизації «проміжна система – проміжна система»
ITU (International Telecommunication Union)	Міжнародний союз телекомунікацій
LAN (Local Area Network)	локальна мережа
LFA (Loop Free Alternate)	механізм запобігання створення петель уздовж резервного маршруту
MILP (Mixed integer linear programming)	змішане цілочисельне лінійне програмування
MINLP (Mixed Integer Nonlinear Programming).	змішане цілочисельне нелінійне програмування
MPLS (Multiprotocol Label Switching)	багатопротокольна комутація за мітками
MRT (Maximally Redundant Trees)	механізм побудови максимально надлишкових дерев
NGN (Next Generation Network)	мережа наступного покоління
NLP (Nonlinear Programming)	нелінійне програмування
OSI (Open Systems Interconnection)	еталонна модель взаємодії відкритих систем
OSPF (Open Shortest Path First)	відкритий протокол маршрутизації за найкоротшим шляхом
PNNI (Private Network – to – Network Interface)	приватний міжмережний інтерфейс
RIP (Routing Information Protocol)	інформаційний протокол маршрутизації
RSVP (Resource Reservation Protocol)	протокол резервування ресурсів
SDN (Software Defined Network)	програмно-конфігурована мережа
SLA (Service Level Agreement)	угода про рівень надання послуг
SCR-LDP (Signalling Constraint-based Routed Label Distribution Protocol)	сигнальний протокол розподілу міток
TE (Traffic Engineering)	інжиніринг трафіку
QoE (Quality of Experience)	якість обслуговування, яка сприймається
QoS (Quality of Service)	якість обслуговування
VRRP (Virtual Router Redundancy Protocol)	протокол резервування віртуального маршрутизатора
WAN (Wide Area Network)	територіально розподілена мережа

## ВСТУП

Стрімкий розвиток і постійне вдосконалення інфокомунікацій у напрямку впровадження технологій мереж майбутнього (Future Networks, FN) є ключовим пріоритетом у забезпеченні конкурентоздатності національної економіки та обороноздатності України загалом [1–13], що потребує подальшої інтеграції в провідні європейські та світові інституції в галузі зв'язку, використання міжнародних інфокомунікаційних стандартів з широкою їх адаптацією під умови та потреби сьогодення нашої країни. Слід зазначити, що, крім вимог до рівня якості обслуговування (Quality of Service, QoS), які вже стали класичними функціями сучасних інфокомунікаційних мереж (ІКМ), на перший план виходить функціонал щодо забезпечення високого рівня відмовостійкості та мережної безпеки [14–19]. Це особливо важливо для функціонування мереж в умовах постійних деструктивних (випадкових та антагоністичних) впливів. Саме вони приводять до суттєвої зміни як структурних, так і функціональних параметрів і властивостей ІКМ: її топології, пропускної здатності, керованості, стійкості тощо.

Як показав проведений аналіз [20–43], ключовим технологічним інструментарієм забезпечення якості обслуговування, відмовостійкості та мережної безпеки є протокольні засоби маршрутизації та управління трафіком загалом в ІКМ, до рівня ефективності функціонування яких з кожним роком висуваються все більш жорсткі вимоги, особливо щодо обчислювальної складності та масштабованості отримуваних мережних рішень. У галузі управління трафіком у ІКМ наука і практика постійно накопичує, поповнює та оновлює теоретичні та технологічні рішення, які стосуються різноманітних мережних платформ, широкого спектра наданих послуг зв'язку та вимог користувачів щодо якості обслуговування, зокрема відмовостійкості, безпеки та масштабованості тощо. Найбільш перспективними рішеннями в цій галузі є програмно-конфігуровані мережі (Software-Defined Networking, SDN), кіберстійкі мережі (Technical Cyber Resilience, TCR), інжиніринг трафіку (Traffic Engineering, TE), віртуалізація мережних функцій (Network Function Virtualization, NFV), самоорганізовані мережі (Self-Organized Networks, SON), мережі на основі хмарних технологій (Cloud Networking), інформаційно орієнтовані мережі (Information-Centric Networking, ICN), маршрутизація з підтримкою якості обслуговування (QoS-based Routing), відмовостійка маршрутизація (Fault-Tolerant Routing), безпечна маршрутизація (Secure Routing) [44–61].

Значний внесок у розроблення базових мережних концепцій, їх теоретичне обґрунтування та розвиток здійснили такі іноземні фахівці, як R. Gallager, D. Tipper, T. Gomes, L. Martins, J. Rak, J. Tapolcai, Y. Seok, а також вітчизняні вчені В.В. Поповський, П.П. Воробієнко, Ю.І. Лосєв, Л.Н. Беркман, В.А. Романюк, І.В. Стрелковська, М.М. Климаш, Б.Ю. Волочій, О.І. Романов, О.Ю. Євсєєва та ін. У галузі підтримки безпеки інформаційно-комунікаційних рішень активно працюють українські науковці В.О. Хорошко, О.Г. Оксіук, С.В. Толюпа, Г.Ф. Конахович, Ю.О. Кулаков та багато інших.

Незважаючи на високий науковий та прикладний рівень досягнутих у сфері маршрутизації в ІКМ результатів, до перспективних мережних рішень усе ж висувається низка важливих концептуальних вимог, які подекуди мають суперечливий характер:

- покращення якості обслуговування в ІКМ на підставі забезпечення ефективного балансування навантаження відповідно до вимог концепції Traffic Engineering;

- комплексне врахування вимог щодо відмовостійкості мережі з підтримкою на алгоритмічно-програмному рівні наявних і новітніх схем перемаршрутизації та захисту елементів мережі, їх пропускнуої здатності та рівня QoS загалом як на рівні доступу (Fault-Tolerant Routing), так і на рівні ядра мережі (Fast ReRouting);

- підвищення рівня мережної безпеки під час передачі різноманітних конфіденційних даних, зокрема сесійних ключів, інформації щодо автентифікації, критично важливих для користувача повідомлень тощо;

- оптимізація використання доступного мережного ресурсу, підвищення масштабованості отриманих мережних рішень, оснований зокрема на реалізації стратегій ієрархічної маршрутизації та управління трафіком в ІКМ загалом.

Варто зазначити, що фундаментом наявних та перспективних протоколів маршрутизації були й залишаються відповідні математичні моделі та методи. Саме рівень їх інформативності та адекватності повністю визначає результативну ефективність технологічних рішень щодо маршрутизації в ІКМ. Отже, мета цієї монографії полягає в подальшому розвитку теорії управління трафіком шляхом удосконалення наявних та синтезу нових математичних моделей і методів маршрутизації, які б слугували подальшою теоретичною основою перспективних протоколів маршрутизації та технологічних засобів управління трафіком для підвищення якості обслуговування, відмовостійкості та мережної безпеки в ІКМ.

Основу монографії становлять результати науково-прикладних досліджень, отриманих протягом останніх п'яти років авторським колективом – співробітниками кафедри інфокомунікаційної інженерії ім. В.В. Поповського Харківського національного університету радіоелектроніки. Монографія містить чотири розділи. Перший розділ присвячений питанням визначення ролі та місця завдань маршрутизації в сучасних ІКМ шляхом огляду технологічних засобів забезпечення якості обслуговування, класифікації маршрутних рішень та формулювання вимог, які висуваються до них, а також визначення основних напрямів удосконалення протоколів маршрутизації в ІКМ. Також у розділі описані базові математичні моделі одно- та багатоадресної/широкомовної маршрутизації в ІКМ, які, ґрунтуючись на запропонованій узагальненій структурі потокової моделі маршрутизації, підлягають подальшому вдосконаленню та розвитку в наступних розділах цієї роботи.

У другому розділі запропоновано теоретичні рішення щодо відмовостійкої маршрутизації, які містять відповідні потокові моделі та методи як без резервування елементів ІКМ, так і з підтримкою основних схем захисту (резервування) елементів мережі – шлюзу за замовчуванням, каналу, вузла, шляху та пропускної здатності мережі загалом. Запропоновані рішення адаптовані під різні типи мереж (IP/MPLS або SDN) і стратегії маршрутизації – одношляхової та багатошляхової; одноадресної і багатоадресної/широкомовної маршрутизації.

У третьому розділі описані моделі та методи безпечної маршрутизації фрагментованої доставки конфіденційних повідомлень множиною шляхів, що можуть допускати певний тип перетинання. Представлені моделі та методи безпечної маршрутизації та безпечної перемаршрутизації охоплюють як проактивні, так і реактивні рішення, орієнтовані на забезпечення заданих значень імовірності компрометації конфіденційних повідомлень, що передаються в ІКМ.

У четвертому розділі наведені потокові моделі та методи ієрархічно-координаційної маршрутизації в ІКМ. Ці рішення охоплюють варіанти організації як внутрішньодоменної маршрутизації «від джерела», яка є характерною, наприклад, для MPLS-мереж, так і міждоменної маршрутизації в мережах, що для підвищення своєї масштабованості розбиваються на множину пов'язаних між собою доменів (підмереж). Крім того, у розділі запропоновано математичну модель та метод ієрархічної міждоменної швидкої перемаршрутизації в ІКМ.

# РОЗДІЛ 1

## РОЛЬ І МІСЦЕ МАРШРУТИЗАЦІЇ

### В СУЧАСНИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

#### 1.1. Мета та завдання інфокомунікаційних мереж у сучасному суспільстві

Відповідно до сучасних тенденцій розвитку світової цивілізації технологічною основою інформаційного суспільства має стати глобальна інформаційна інфраструктура – ГІІ (Global Information Infrastructure, GII), яка могла б забезпечити можливість вільного доступу до інформаційних ресурсів кожного жителя планети. У свою чергу, матеріальною й одночасно системоутворювальною основою ГІІ є інфокомунікаційні мережі [62], без яких стає проблематичним широке впровадження досягнень науки та техніки в сфері промислового виробництва, бізнесу, освіти, медицини, культури й оборони країни.

ІКМ настільки інтегровані в ГІІ (рис. 1.1), що в багатьох випадках їх функції не вдається чітко розділити. У зв'язку з цим топологію та завдання ІКМ доцільно розглядати через структуру і функції ГІІ. Така спорідненість відбивається і в термінології, яка використовується у визначенні ГІІ і ІКМ.

Так, наприклад, відповідно до рекомендації Міжнародного союзу телекомунікацій (International Telecommunications Union, ITU-T) Y.100 «General overview of the Global Information Infrastructure standards development» і Y.101 «Global Information Infrastructure terminology: Terms and definitions» термін ГІІ визначено як «сукупність мереж, апаратури кінцевого користувача, інформації та людських ресурсів, яка може бути використана для доступу до корисної інформації, для зв'язку користувачів один з одним, роботи, навчання, отримання розважальної інформації в будь-який час і в будь-якому місці за умови прийнятної вартості за деякою глобальною шкалою».

Результативним кроком у реалізації на практиці ідей концепції глобальної інформаційної інфраструктури слід вважати створення мережі наступного покоління (Next Generation Network, NGN). В основу побудови NGN покладено ідею створення універсальної мережі, яка дозволяє переносити будь-який вид інформації (мова, дані, відео, аудіо, зображення тощо), а також забезпечувати можливість надання найбільш широкого спектра інфокомунікаційних послуг. ITU-T уже почав стандартизацію мереж нового покоління в межах проекту

глобальної інформаційної інфраструктури, що привело до розроблення низки рекомендацій щодо ГП серії Y. В описі функціональної моделі NGN з точки зору функцій регулювання, контролю та передачі слід керуватися також рекомендаціями ITU-T Y.110, X.200, G.805 і G.809. Відповідно до змісту вимог рекомендацій ITU-T Y.100, Y.110, Y.130 і Y.140 або Y.140.1 базовими принципами NGN є такі:

- переважна реалізація режиму комутації пакетів з відділенням одна від одної функцій перенесення інформації та комутації, функцій управління викликом і функцій управління послугами;

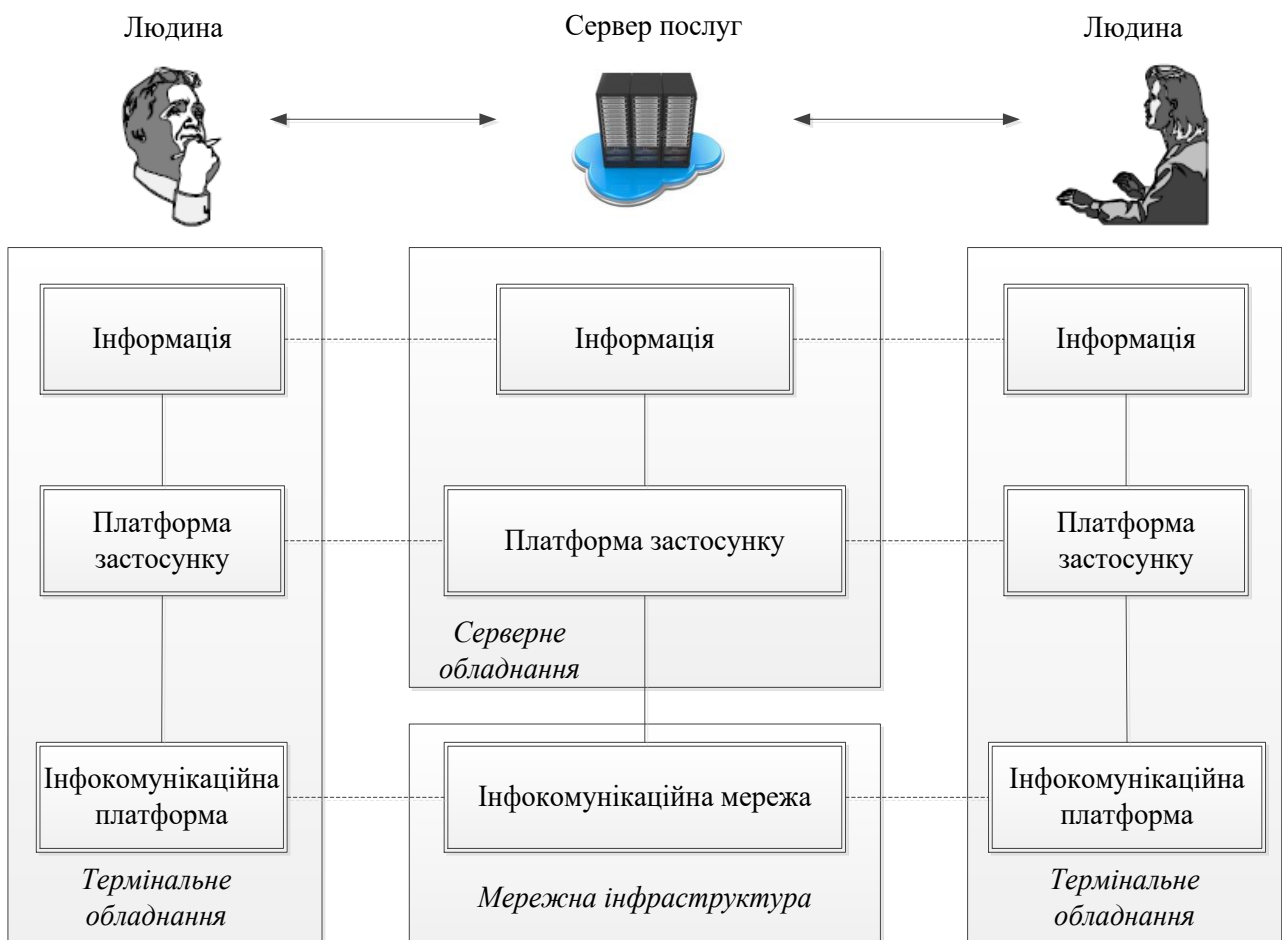


Рис. 1.1. Основні складники ГП (рекомендація ITU-T Y.110)

- взаємодія з наявними мережами зв'язку (телефонні мережі загального користування, мережі передачі даних, мережі рухомого зв'язку) за допомогою відкритих інтерфейсів і шлюзів;

- забезпечення відкритого та вільного доступу до мереж і постачальників послуг, що конкурують;

– підтримка універсальної мобільності, що дозволяє окремим абонентам користуватися й управляти послугами незалежно від технології доступу та типу застосовуваного терміналу;

– забезпечення надання множини інфокомунікаційних послуг (мультисервісу) із заданими показниками якості обслуговування (QoS);

– інтеграція послуг фіксованого та рухомого зв'язку;

– підтримка як вже наявного, так і нового термінального обладнання та пристроїв, зокрема аналогових телефонних апаратів, факсимільних апаратів, обладнання ISDN (Integrated Services Digital Network), стільникових телефонів різних стандартів, терміналів IP-телефонії, кабельних модемів тощо.

Відповідно до особливостей структурної та функціональної побудови NGN належать до складних організаційно-технічних систем, тому для забезпечення максимально можливих показників продуктивності та масштабованості вони будуються за принципами ієрархічності та багаторівневості. З огляду на рекомендації ITU-T у NGN виділяється два основних функціональних рівні – транспорту та послуг. Однак на практиці також застосовується більш детальна архітектура, що розширює тлумачення ITU та складається з чотирьох рівнів (рис. 1.2) [36, 63, 64].

Нульовий рівень – рівень термінальних пристроїв – містить множину терміналів, за допомогою яких користувачі взаємодіють з інфокомунікаційним середовищем, запитуючи та отримуючи ту чи іншу послугу. На першому рівні за допомогою інфокомунікаційних технологій рівня доступу термінали можуть обмінюватися інформацією один з одним напряму або через комутатори локальних мереж (Local Area Network, LAN). Для забезпечення територіально віддаленої інформаційної взаємодії користувачів або звернення до різних серверів послуг використовуються рішення другого рівня – рівня транспорту, основаного на технологіях транспортних мереж IP/MPLS. Саме на рівні транспорту функціонують територіально розподілені мережі (Wide Area Network, WAN), у межах яких здебільшого і визначається рівень якості обслуговування. Технологічні та протокольні засоби третього та четвертого рівнів NGN (рис. 1.2) відповідають за адміністративне управління мережними процесами, пов'язаними з наданням послуг, технічною експлуатацією, ремонтом, адмініструванням та плануванням мережі тощо.

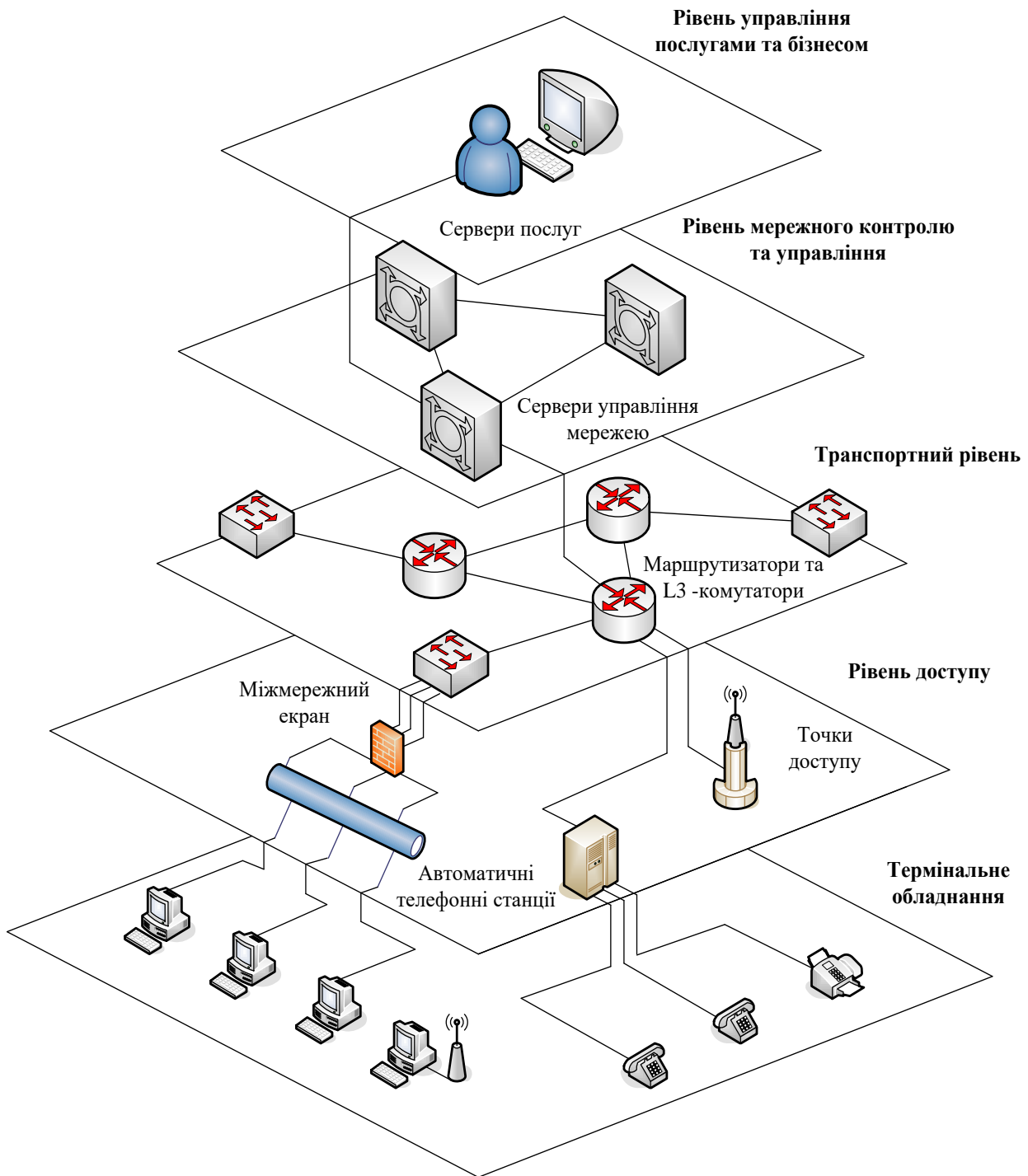


Рис. 1.2. Варіант багаторівневої архітектури NGN

## 1.2. Огляд технологічних засобів забезпечення якості обслуговування в ІКМ

Основним завданням сучасних ІКМ є надання широкого спектру послуг із забезпеченням необхідного рівня якості обслуговування. У сучасних ІКМ функції щодо забезпечення якості обслуговування реалізуються, як правило,



у межах тієї чи іншої мережної архітектури. До подібного роду архітектур, які застосовуються в IP/MPLS-мережах, належать такі [19–21, 25, 36, 63–65]:

- архітектура інтегрованих послуг (Integrated Services, IntServ), орієнтована насамперед на забезпечення гарантій якості обслуговування;
- архітектура диференційованих послуг (Differentiated Services, DiffServ), основана на пріоритетному обробленні пакетів різних служб і застосунків;
- архітектура MPLS DiffServ Aware Traffic Engineering, заснована на інтеграції DiffServ і концепції Traffic Engineering для MPLS-мереж [66];
- обслуговування «за можливістю» – best effort (BE) services.

Для кількісної оцінки рівня якості обслуговування вводяться числові характеристики, які в подальшому будуть називатися QoS-показниками. Залежно від того, між якими точками мережі вимірюються ці показники, їх поділяють на показники якості обслуговування, що сприймається на рівні користувача (Quality of Experience, QoE), та показники мережної продуктивності (Network Performance, NP), що оцінюються, як правило, на рівні границь транспортної мережі.

Показники мережної продуктивності умовно поділяються на три типи: показники пропускної здатності (швидкісні показники), часові показники та показники надійності. До швидкісних показників належить мінімальна, середня та максимальна швидкість передачі пакетів, часові показники представлені середньою затримкою та джитером (варіацією затримки) пакетів, а показники надійності, як правило, пов'язані з рівнем (імовірністю) втрат пакетів. На числові значення показників QoE, які представлені відповідними оцінками MOS (Mean Opinion Score) [29, 67–69], крім показників мережної продуктивності, також впливають характеристики мереж доступу та термінального обладнання.

Важливо зазначити, що трафік, який циркулює в інтересах того чи іншого мережного застосунку, по-різному чутливий до значень перелічених QoS-показників (табл. 1.1). Проте, як видно з табл. 1.1, для надання більшості послуг необхідно забезпечувати заданий рівень якості обслуговування одночасно за декількома різнотипними QoS-показниками.

Відповідно до змісту рекомендації ITU-T Y.1540 у табл. 1.2 наведені гранично допустимі значення основних QoS-показників, визначених для IP-мереж, залежно від типу використовуваного мережного застосунку. Варто зазначити, що ці QoS-вимоги стали основою для створення восьми класів мережної якості обслуговування (табл. 1.2). Зокрема клас 5, наприклад, не містить жодного граничного значення, що передбачає можливість їх динамічного формування на основі поточного запиту [27, 28].

Таблиця 1.1

## Чутливість трафіку різних застосунків до значень QoS-показників

Застосунок	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

Таблиця 1.2

Гранично допустимі значення основних QoS-показників в IP-мережах  
(відповідно до рекомендації ITU-T Y.1540)

Класи QoS	Застосунки (приклади)	Показник QoS				
		IPTD	IPDV	IPLR	IPER	IPRR
Клас 0	Застосунки реального часу, чутливі до джитеру, з високою взаємодією (VoIP)	100 мс	50 мс	$10^{-3}$	$10^{-4}$	<i>H</i>
Клас 1	Застосунки реального часу, чутливі до джитеру, інтерактивні (VoIP)	400 мс	50 мс	$10^{-3}$	$10^{-4}$	<i>H</i>
Клас 2	Дані транзакцій, високоінтерактивні застосунки (сигналізація)	100 мс	<i>H</i>	$10^{-3}$	$10^{-4}$	<i>H</i>
Клас 3	Дані транзакцій, інтерактивні застосунки	400 мс	<i>H</i>	$10^{-3}$	$10^{-4}$	<i>H</i>
Клас 4	Застосунки з низькими втратами (короткі транзакції, об'ємні дані, потокове відео)	1 с	<i>H</i>	$10^{-3}$	$10^{-4}$	<i>H</i>
Клас 5	Традиційні застосунки типових IP-мереж	<i>H</i>	<i>H</i>	<i>H</i>	<i>H</i>	<i>H</i>
Клас 6	—	100 мс	50 мс	$10^{-5}$	$10^{-6}$	$10^{-6}$
Клас 7	—	400 мс	50 мс	$10^{-5}$	$10^{-6}$	$10^{-6}$

IPTD – затримка передачі IP-пакета, яка містить затримки поширення та оброблення в черзі; IPDV – міжкінцева варіація затримки (джитер); IPLR – допустима ймовірність втрат IP-пакетів; IPER – допустима ймовірність прийому пакетів з помилками; IPRR – допустима ймовірність зміни порядку надходження IP-пакетів; *H* – параметр не визначено.

Важливо зазначити, що в табл. 1.2 йдеться про вимоги до міжкінцевих (end-to-end) показників якості обслуговування, значення яких традиційно залежить від ефективності вирішення завдань щодо управління трафіком та розподілу мережного ресурсу. Основні мережні ресурси ІКМ можна класифікувати так [36, 63–65]:

- *канальний ресурс*, до якого насамперед належить пропускна здатність каналів зв'язку мережі;
- *буферний ресурс*, основу якого становить буферна ємність черг на інтерфейсах маршрутизаторів мережі;
- *обчислювальний ресурс* (обчислювальна потужність) мережних вузлів (комутаторів, маршрутизаторів тощо) і серверів послуг;
- *інформаційний ресурс*, до якого належить мережний трафік, що циркулює в ІКМ, зміст баз даних про стан мережі, різномірна керівна інформація, наприклад, маршрутні таблиці;
- *програмний ресурс*, основу якого становлять безпосередньо мережні протоколи та інші програми, що входять до складу спеціального програмного забезпечення мережних вузлів.

З точки зору практики, реалізацією функцій щодо забезпечення якості обслуговування та управління трафіком у процесі розподілу зазначеного вище мережного ресурсу займаються технологічні засоби класифікації та маркування пакетів, управління доступом, профілювання трафіку, механізми управління чергами на маршрутизаторах мережі, а також протоколи маршрутизації, сигналізації та резервування мережних ресурсів.

З огляду на підтримку мультисервісності в ІКМ завдання щодо маркування пакетів пов'язані з призначенням пріоритету пакетів відповідно до запитуваного рівня якості обслуговування. Зокрема значення пріоритету відіграє ключову роль у вирішенні інших важливих завдань управління трафіком. Так, наприклад, в управлінні чергами (з точки зору їх організації, обслуговування та обмеження довжини) пріоритет обслуговування впливає на обсяг виділеного кожній з них канального ресурсу [65]. Для забезпечення гарантій якості обслуговування необхідно задіяти технологічні засоби резервування мережних ресурсів, до основних з яких належать протоколи RSVP (в IP-мережах) і LDP (у MPLS-мережах) [40, 41].

Виходячи з того, що нині особливо затребувані гарантії якості обслуговування «з кінця в кінець» (end-to-end) [24, 25], то ключова роль в управлінні трафіком, звичайно ж, відводиться маршрутизації, що як процес мережного рівня еталонної моделі взаємодії відкритих систем (EMBCC)

відповідає за розрахунок і використання одного або множини шляхів від відправника до отримувача пакетів, оптимальних у межах обраних критеріїв (метрик).

### 1.3. Класифікація маршрутних рішень в ІКМ

На цей час існує досить широка множина маршрутних рішень, які відрізняються принципами роботи, рівнем ефективності та сферою ймовірного використання. Зважаючи на наявність деяких спільних рис у цих рішеннях, у загальному випадку має місце така класифікація маршрутних протоколів та методів (рис. 1.3):

- за рівнем адаптивності маршрутних рішень (частотою оновлення маршрутних таблиць) виокремлюють статичну, квазістатичну та динамічну маршрутизацію;
- за способом збирання інформації про стан мережі – дистанційно-векторну маршрутизацію та маршрутизацію на основі стану каналів (зв'язків);
- за місцем формування маршрутів – маршрутизацію покрокову (hop-by-hop) та «від джерела» (on source);
- за типом використаної маршрутної метрики – маршрутизацію за структурною метрикою та маршрутизацію за функціональною метрикою;
- за кількістю врахованих параметрів мережі – маршрутизацію на основі скалярної, композитної (складної) або векторної метрики;
- за типом врахованих параметрів мережі – маршрутизацію за показниками якості обслуговування та маршрутизацію за показниками мережної безпеки;
- за кількістю отримувачів пакетів – одноадресну, багатоадресну та широкомовну маршрутизацію;
- за кількістю використаних шляхів – одно- та багатошляхову маршрутизацію;
- за способом формування маршрутних таблиць (маршрутів) – централізовану, розподілену та змішану маршрутизацію;
- за способом обчислення шляхів – маршрутизацію з попереднім обчисленням шляхів або без передобчислення маршрутів;
- за рівнем забезпечення відмовостійкості мережі – із захистом та без захисту (резервування) елементів мережі (каналу, вузла, шляху, мережного сегмента) та/або її пропускної здатності.

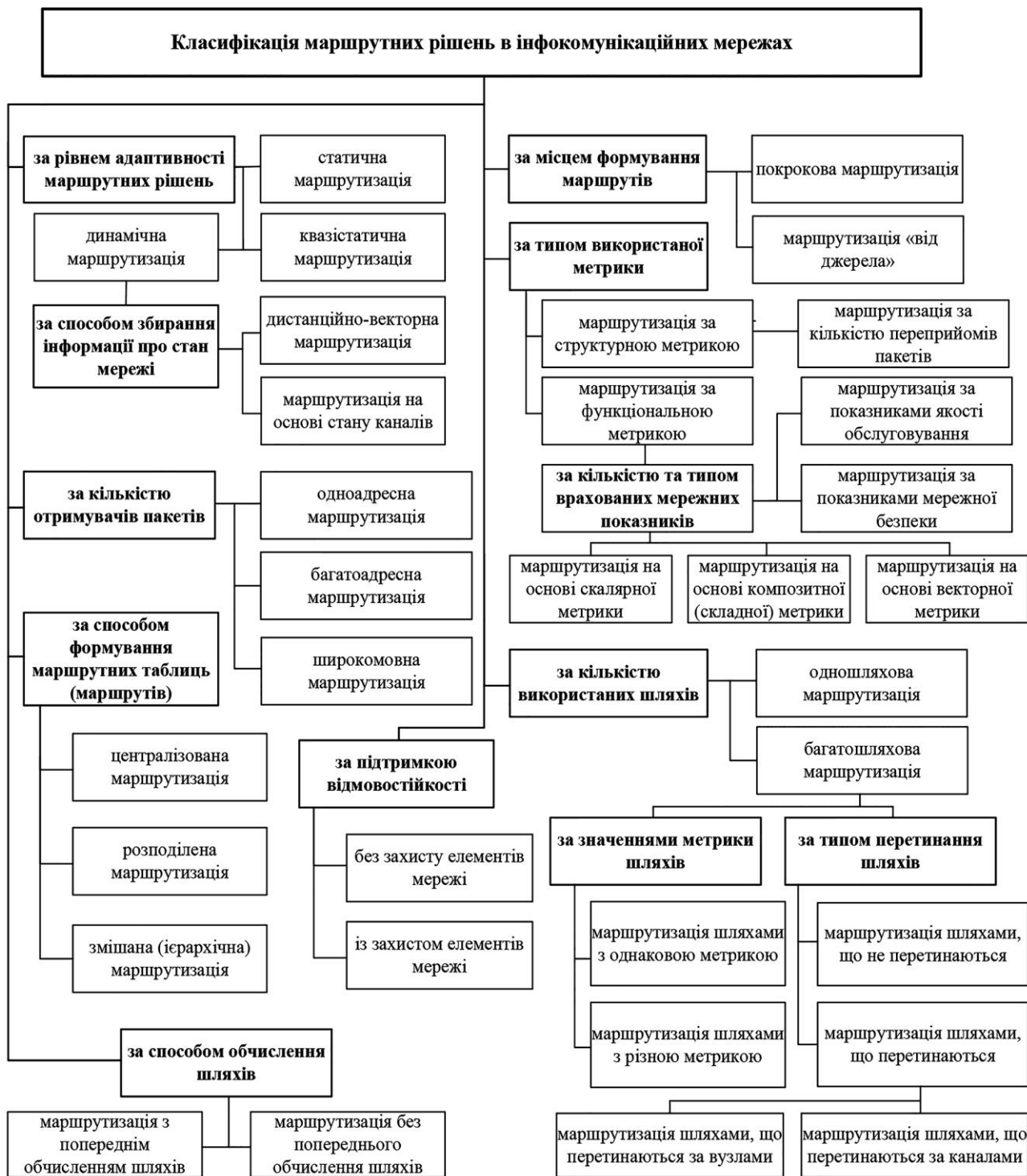


Рис. 1.3. Класифікація маршрутних рішень в ІКМ

За частотою оновлення маршрутних таблиць, спричиненого адаптацією до зміни стану мережі, виокремлюють статичну, квазістатичну та динамічну маршрутизацію. За умови статичної маршрутизації автоматична адаптація маршрутних рішень до зміни як структурних, так і функціональних параметрів ІКМ практично не можлива, оскільки зміст маршрутних таблиць визначається адміністративно та вноситься до маршрутизаторів переважно вручну.

Відсутність необхідності в збиранні інформації про стан мережі призводить до втрати оперативності реакції системи маршрутизації на можливе перевантаження чи вихід з ладу мережного обладнання, проте мінімізує обсяг створеного службового навантаження та не потребує високої обчислювальної потужності маршрутизаторів, оскільки не потрібно перераховувати маршрути. За умови квазістатичної маршрутизації передбачається зміна маршрутів та, відповідно, маршрутних таблиць, але не в реальному часі, а, як правило, також під час адміністративних налаштувань.

У сучасних умовах функціонування ІКМ лише динамічна маршрутизація може забезпечити найбільш високий рівень адаптації маршрутних рішень, які реалізуються за допомогою відповідних протоколів, здатних автоматично збирати та аналізувати інформацію про стан мережі та розраховувати маршрути в реальному часі (десятки секунд). Переважна більшість наявних протоколів динамічної маршрутизації [37, 43], наприклад, IGRP/EIGRP, OSPF, IS-IS, PNNI тощо, здатні адаптуватися до зміни як топологічних параметрів мережі (кількості маршрутизаторів та каналів зв'язку, порядку їх з'єднання), так і функціональних (пропускної здатності каналів зв'язку, затримок та рівня втрат пакетів на інтерфейсах маршрутизаторів). Протокол маршрутизації RIP під час розрахунку шляхів може враховувати оновлену інформацію лише про топологію ІКМ.

У свою чергу протоколи динамічної маршрутизації умовно поділяються на два класи, що відрізняються за способом збирання інформації про стан ІКМ. Для дистанційно-векторної маршрутизації, відповідно до якої працюють, наприклад, протоколи RIP (Routing Information Protocol), IGRP (Interior Gateway Routing Protocol) та BGP (Border Gateway Protocol), характерно, що в процесі оновлення інформації про стан мережі сусідні маршрутизатори періодично (30–90 с) обмінюються повними копіями своїх маршрутних таблиць. Однак вважається, що більш доцільним є використання протоколів маршрутизації на основі стану каналів [37, 43], за допомогою яких мінімізується обсяг переданої службової інформації про стан ІКМ, тому що на вимогу розсилаються лише зміни у змісті маршрутних таблиць за принципом «кожен з кожним». Це сприяє оперативному формуванню більш адекватної карти мережі на кожному з маршрутизаторів і зниженню ймовірності заиклення пакетів, що характерно для протоколів дистанційно векторної маршрутизації. До маршрутних протоколів стану каналів класу належать OSPF (Open Shortest Path First), IS-IS (Intermediate System – to – Intermediate System) та PNNI (Private Network – to – Network Interface) [37, 43]. Варто зазначити, що в

дистанційно-векторних протоколах маршрутизації для розрахунку шуканого оптимального шляху, як правило, використовується алгоритм Беллмана–Форда, а в протоколах стану каналів – алгоритм Дейкстри. У протоколі EIGRP (Enhanced IGRP), що поєднує в собі принципи як дистанційно-векторної маршрутизації, так і стану каналів, використовується алгоритм DUAL [65].

У сучасних IP-мережах, основаних на дейтаграмному режимі пакетної комутації, використовуються переважно протоколи покрокової маршрутизації. У разі покрокової маршрутизації кожен маршрутизатор ІКМ наділений функціями розрахунку шляху проходження пакетів, тобто шлях, який розрахував приграничний маршрутизатор, може бути змінений (уточнений) кожним наступним транзитним маршрутизатором. Реалізація покрокової маршрутизації сприяє більш ефективній адаптації маршрутних рішень під зміни стану мережі, але в низці випадків може призвести до створення циклів (петель) у маршрутах проходження пакетів. За умови маршрутизації «від джерела», яка переважно використовується в АТМ і MPLS-мережах, орієнтованих на віртуальні з'єднання, функціями формування шляхів наділені лише приграничні маршрутизатори. Тобто всі пакети передаються до маршрутизатора-отримувача пакетів лише тим маршрутом (віртуальним шляхом), який визначив приграничний маршрутизатор. Усі транзитні маршрутизатори тільки проводять комутацію пакетів відповідно до шляхів, розрахованих на приграничних маршрутизаторах. Хоча маршрутизація «від джерела» менш оперативно реагує на зміни в структурі та завантаженості мережі, проте істотно знижує ймовірність зациклення пакетів і спрощує функції щодо контролю за міжкінцевими показниками якості обслуговування.

Залежно від кількості отримувачів пакетів розрізняють одноадресну, багатоадресну та широкомовну маршрутизацію. У разі одноадресної маршрутизації пакети передаються між заданою парою вузлів «джерело–отримувач». На рис. 1.4, а показано приклад одноадресного шляху, коли перший маршрутизатор – відправник, а п'ятий – отримувач пакетів. За умови широкомовної маршрутизації пакети одного і того ж потоку передаються від маршрутизатора-джерела відразу до всіх інших маршрутизаторів мережі (рис. 1.4, б). У випадку багатоадресної маршрутизації пакети передаються одночасно декільком, але, на відміну від широкомовної маршрутизації, не всім маршрутизаторам ІКМ. На рис. 1.4, в продемонстровано приклад багатоадресного шляху від першого маршрутизатора до другого та п'ятого маршрутизаторів ІКМ. На практиці використання того чи іншого виду маршрутизації загалом визначається типом наданої інфокомунікаційної послуги.

Сучасні маршрутні протоколи обирають шлях, оптимальний у межах обраних критеріїв, які в цьому випадку називаються маршрутними метриками. Маршрутні рішення можуть класифікуватися за типом використаної маршрутної метрики, значення якої вздовж обраного шляху має бути мінімальним. У загальному випадку під час маршрутизації може застосовуватися структурна або функціональна метрика. Структурна метрика визначається особливостями топологічної побудови ІКМ. Найпростішим випадком маршрутизації є використання структурної метрики, пов'язаної з мінімізацією кількості переприйомів (hops) пакетів, як, наприклад, реалізовано в протоколі RIP. Застосування функціональної метрики ґрунтується на врахуванні функціональних параметрів елементів мережі. За умови маршрутизації за показниками якості обслуговування (QoS-маршрутизації) метрикою може бути функція від пропускної здатності та завантаженості каналів зв'язку, маршрутизаторів і шляхів загалом, а також від значень затримок і втрат пакетів у них. У разі безпечної маршрутизації метрика має враховувати показники мережної безпеки, наприклад, імовірність компрометації пакета, вузла, каналу та шляху.

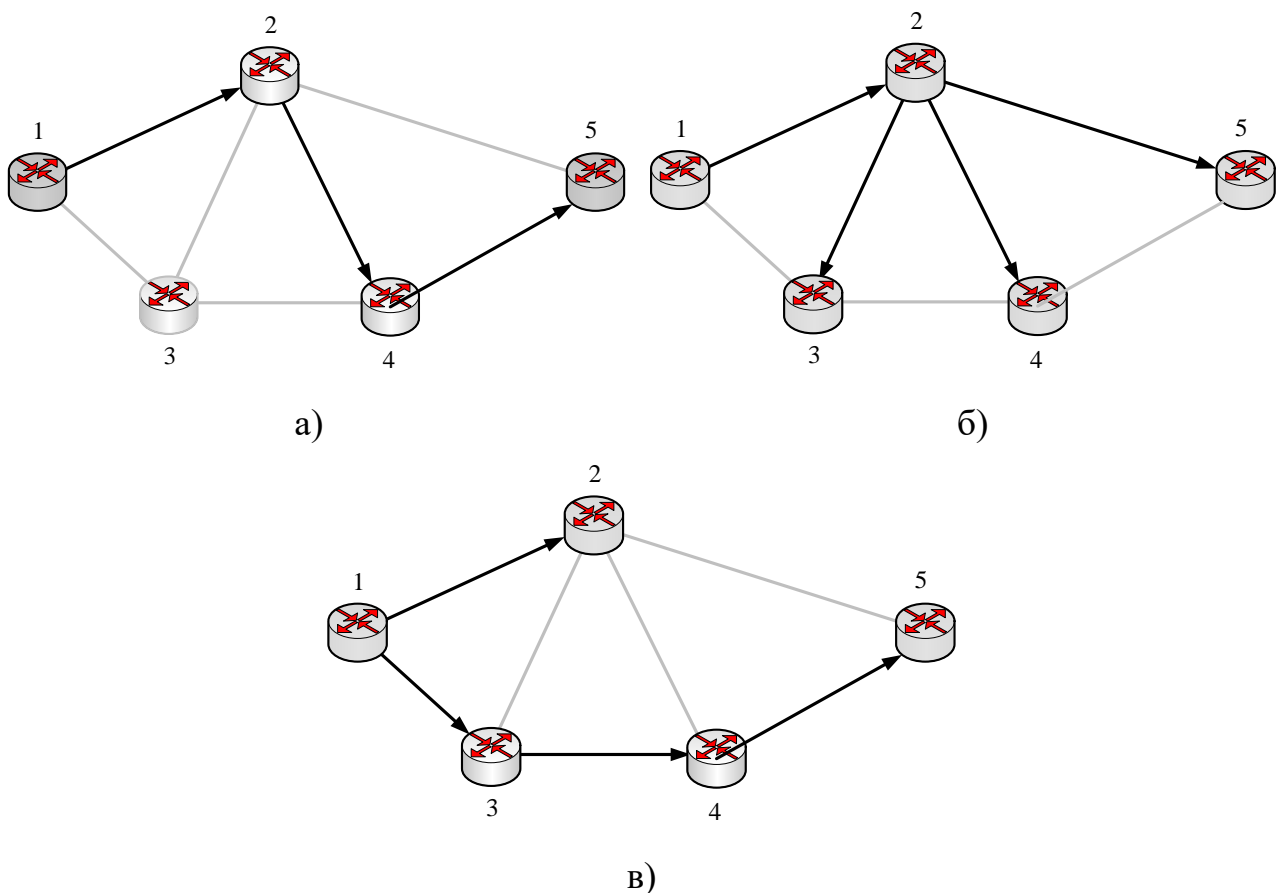


Рис. 1.4. Приклади маршрутизації в мережі:  
а – одноадресної; б – широкомовної; в – багатоадресної



За кількістю врахованих параметрів мережі виокремлюють маршрутизацію на основі скалярної, композитної (складної) або векторної метрики. Більшість наявних рішень, представлених протоколами маршрутизації, використовують скалярні метрики. Частіше за все скалярні метрики характеризують функцію від одного з QoS-показників, як, наприклад, у протоколі OSPF, або показника мережної безпеки. Якщо маршрутна метрика є згорткою множини показників, то така метрика називається композитною (складною). Композитна метрика використовується, наприклад, у протоколах IGRP/EIGRP або IS-IS. Проте застосування композитної метрики лише сприяє поліпшенню значень множини QoS-показників, які згортаються, але гарантій щодо числових значень цих показників та їх відповідності встановленим вимогам (табл. 1.2) не надається. Тому більш перспективними є маршрутні рішення, які використовують векторний підхід, коли з кожним каналом та маршрутизатором, а в результаті й маршрутом, пов'язано одночасно декілька метрик (вектор метрик). Це дозволить забезпечити виконання вимог одночасно за множиною QoS-показників та показників мережної безпеки вздовж розрахованого оптимального шляху.

За умови одношляхової маршрутизації всі пакети одного й того ж потоку передаються за одним єдиним маршрутом, що, як правило, визначається на приграничному маршрутизаторі. На рис. 1.5, а подано приклад маршрутизації цього типу, коли між першим та п'ятим маршрутизаторами використовується один шлях: 1→2→5. Однак практично всі наявні протоколи маршрутизації в IP, ATM та MPLS-мережах [37, 43] підсилили свій функціонал з точки зору підтримки функцій балансування навантаження одночасно за множиною шляхів. На маршрутизаторах компанії Cisco навіть у разі статичної маршрутизації підтримується багатошляхова маршрутизація.

Реалізація багатошляхової маршрутизації хоча і призводить до ускладнення процесу розрахунку, але сприяє забезпеченню більш збалансованого навантаження каналів і підвищенню якості обслуговування в ІКМ загалом. Так, на рис. 1.5, б показано приклад багатошляхової маршрутизації, коли між першим та п'ятим маршрутизаторами використовуються вже два шляхи: 1→2→5 та 1→3→4→5.

У свою чергу багатошляхова маршрутизація може бути різних типів. Вона, наприклад, поділяється на маршрутизацію за шляхами з однаковою або різною метрикою. Наприклад, протокол RIP підтримує балансування навантаження за шляхами з однаковою метрикою, а протоколи IGRP та EIGRP – за шляхами з різними значеннями метрики, проте це потребує

додаткових адміністративних налаштувань. Крім того, у випадку багатошляхової маршрутизації використані шляхи можуть перетинатись або не перетинатись. Два шляхи не перетинаються, якщо вони не містять спільних мережних елементів (маршрутизаторів і каналів), крім маршрутизаторів джерела та отримувача пакетів. Наприклад, маршрути  $1 \rightarrow 2 \rightarrow 5$  та  $1 \rightarrow 3 \rightarrow 4 \rightarrow 5$  (рис. 1.5, б) не перетинаються.

Маршрути, що перетинаються, можуть мати спільні маршрутизатори та (або) канали зв'язку. У першому випадку маршрути перетинаються за вузлами, а в другому – за каналами. Так маршрути  $1 \rightarrow 2 \rightarrow 5$  та  $1 \rightarrow 3 \rightarrow 2 \rightarrow 4 \rightarrow 5$  (рис. 1.5, в) перетинаються за вузлом, яким є другий маршрутизатор, а маршрути  $1 \rightarrow 2 \rightarrow 5$  та  $1 \rightarrow 2 \rightarrow 4 \rightarrow 5$  (рис. 1.5, г) перетинаються за каналом, що з'єднує перший та другий маршрутизатори. Як показано на наведених прикладах, маршрути, що перетинаються за каналами, завжди перетинаються і за вузлами, оскільки шляхи  $1 \rightarrow 2 \rightarrow 5$  та  $1 \rightarrow 2 \rightarrow 4 \rightarrow 5$ , крім спільного каналу, мають і спільний вузол – другий маршрутизатор.

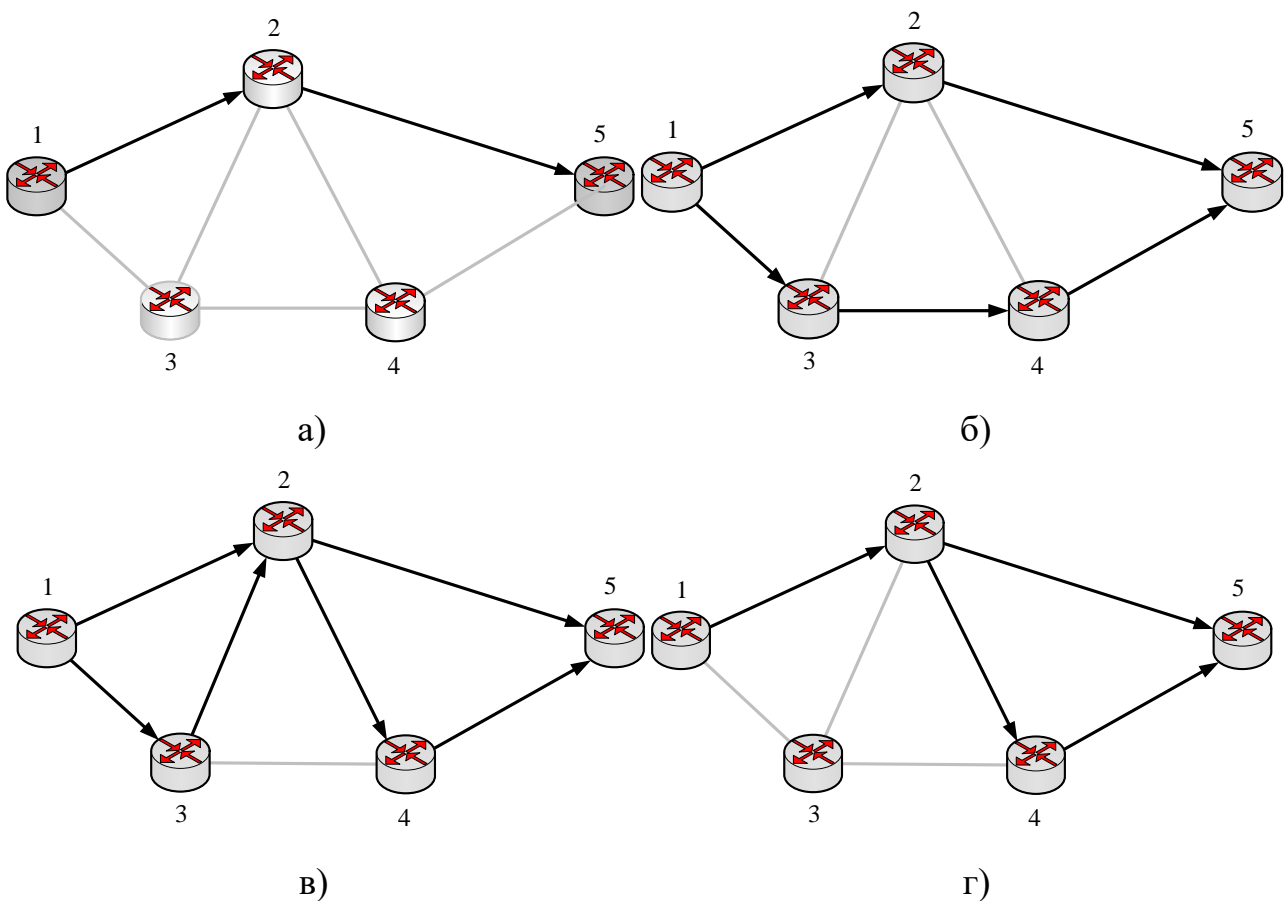


Рис. 1.5. Приклади маршрутизації в мережі:  
а – одношляхової; б, в, г – багатошляхової

За способом формування маршрутних таблиць розрізняють централізовану, розподілену (децентралізовану) та змішану маршрутизацію. За умови централізованої маршрутизації за розрахунок маршрутів і формування маршрутних таблиць для всіх вузлів мережі відповідає один центральний маршрутизатор, який ще може називатися сервером або контролером маршрутів (рис. 1.6). Яскравим прикладом централізованої маршрутизації є використання технології SDN, коли вирішення завдань щодо збирання, оброблення інформації про стан мережі та розрахунок маршрутів покладається на контролер мережної операційної системи [39, 45, 50, 54]. Функціональна централізація сприяє підвищенню якості розрахованих маршрутів з точки зору запобігання можливого перевантаження мережі, але негативно впливає на рівень надійності (відмовостійкості) та масштабованості маршрутних рішень в ІКМ великої розмірності, а також сприяє підвищенню вимог до обчислювальної потужності сервера (контролера) маршрутів.

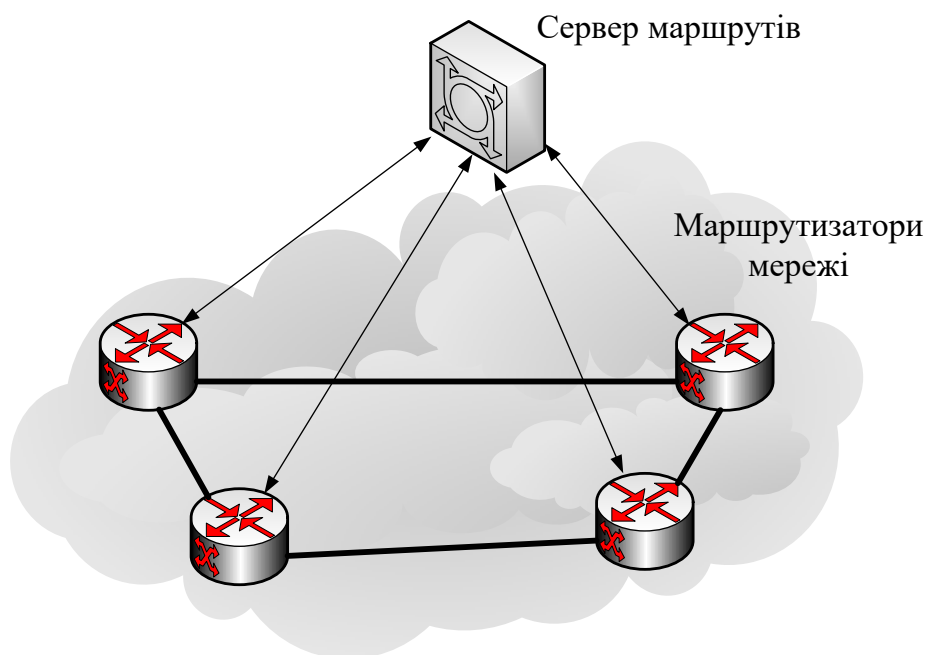


Рис. 1.6. Приклад організації централізованої маршрутизації

У процесі децентралізованої маршрутизації (рис. 1.7) функції визначення маршрутів розподіляються між множиною маршрутних серверів, у ролі яких можуть бути й маршрутизатори ІКМ. В архітектурі SDN, наприклад, кожен із множини маршрутних серверів може відповідати за розрахунок маршрутів в окремих підмережах ІКМ (рис. 1.8). У MPLS-мережі за розрахунок шляхів «з кінця в кінець» (Label Switching Path, LSP) відповідають лише приграничні маршрутизатори (Label Edge Router, LER), а транзитні вузли

(Label Switching Router, LSR) лише пересилають пакети вздовж цих шляхів, не змінюючи їх. Граничним випадком децентралізації подібних рішень є реалізація IP-маршрутизації, під час якої кожен IP-маршрутизатор сам для себе формує маршрутну таблицю.

Децентралізація маршрутних рішень, як правило, сприяє суттєвому підвищенню масштабованості та надійності мережі, проте негативно позначається на рівні якості обслуговування. Так, відсутність координованості в роботі різних приграничних маршрутизаторів LER у MPLS-мережі в процесі розрахунку шляхів може призвести до перевантаження каналного та буферного ресурсу, а у випадку реалізації IP-маршрутизації підвищується ймовірність зациклення пакетів (count to infinity), що спричинить зростання міжкінцевих затримок та ймовірності втрат пакетів.

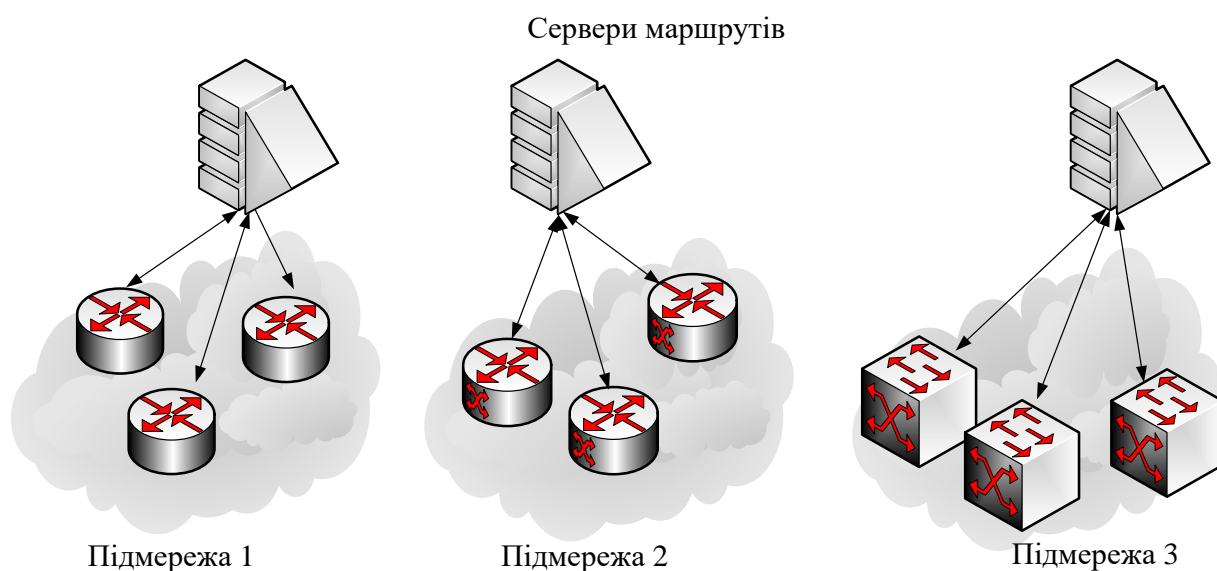


Рис. 1.7. Приклад організації розподіленої (децентралізованої) маршрутизації

Для мінімізації недоліків і реалізації основних переваг централізованої та децентралізованої (розподіленої) маршрутизації на практиці все частіше застосовуються принципи змішаної маршрутизації, що, як правило, матеріалізуються у вигляді протоколів ієрархічної маршрутизації. Для подібних протоколів, до яких належать EGP/BGP, OSPF, IS-IS і PNNI, характерна, по-перше, декомпозиція ІКМ на підмережі, а по-друге, введення структурної та функціональної ієрархії маршрутизаторів, що відповідають за маршрутизацію як безпосередньо всередині підмереж, так і між підмережами (рис. 1.8).

Залежно від типу використаної в мережі інфокомунікаційної технології підмережі можуть називатися автономними системами (Autonomous System, AS), доменами або кластерами.

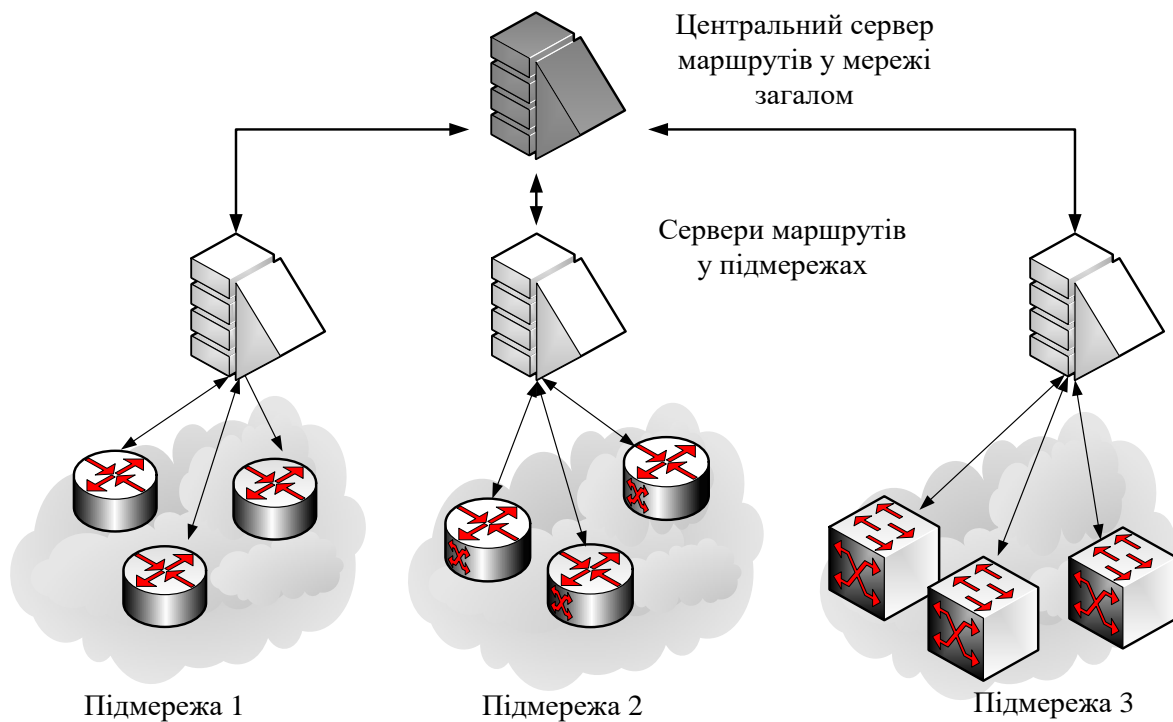


Рис. 1.8. Приклад організації ієрархічної маршрутизації

За способом обчислення шляхів розрізняють маршрутизацію з їх попереднім обчисленням (precomputation routing) і без попереднього визначення маршрутів. У першому випадку на маршрутизаторі шляхи можуть обчислюватися завчасно, тобто до надходження самих пакетів, які потребують маршрутизації. У цьому випадку для пакетів, що надійшли на маршрутизатор, може обиратися вже наявний шлях або шляхи, які відповідають установленним вимогам, зокрема і щодо рівня QoS. У другому випадку необхідний шлях (шляхи) розраховується на маршрутизаторі під потреби конкретного потоку пакетів, які на нього надходять.

Перспективною тенденцією в розвитку маршрутних рішень є забезпечення їх відмовостійкості. Це обумовлено тим, що сучасні протоколи маршрутизації здатні реагувати на зміни в стані мережі протягом десятків секунд, тому що таймер перерахунку маршрутних таблиць міститься в цих межах. Однак в ядрі мережі використовуються гігабітні або навіть терабітні швидкості передачі, тому за умови виходу з ладу або перевантаження елемента мережі перерахунок шляху, елемент якого відмовив, призведе до досить великих втрат пакетів. Тому в межах відмовостійкої маршрутизації

передбачається введення та використання ресурсної надлишковості, коли одночасно з основним розраховується й резервний маршрут (маршрути). Зокрема резервний маршрут не повинен перетинатися з основним за тим елементом мережі (маршрутизатором або каналом зв'язку), який у процесі відмовостійкої маршрутизації підлягає захисту. Реалізація відмовостійкої маршрутизації дозволяє в реальному часі (десятки мілісекунд) реагувати на можливий вихід з ладу мережного обладнання, тоді як у звичайних маршрутних протоколах час реагування відповідає десяткам секунд.

#### 1.4. Вимоги, які висуваються до перспективних маршрутних рішень

Як показав проведений аналіз, до маршрутних рішень, що застосовуються або плануються до використання на практиці, висувається низка системних вимог (рис. 1.9), перелічених нижче.

1. Оптимальність. Протокол маршрутизації має визначити оптимальний, тобто «найкращий» маршрут у межах обраного критерію оптимальності (метрики), що, як правило, пов'язаний з рівнем QoS та ефективністю мережі загалом. Крім того, збіжність до оптимального рішення повинна бути максимально швидкою.

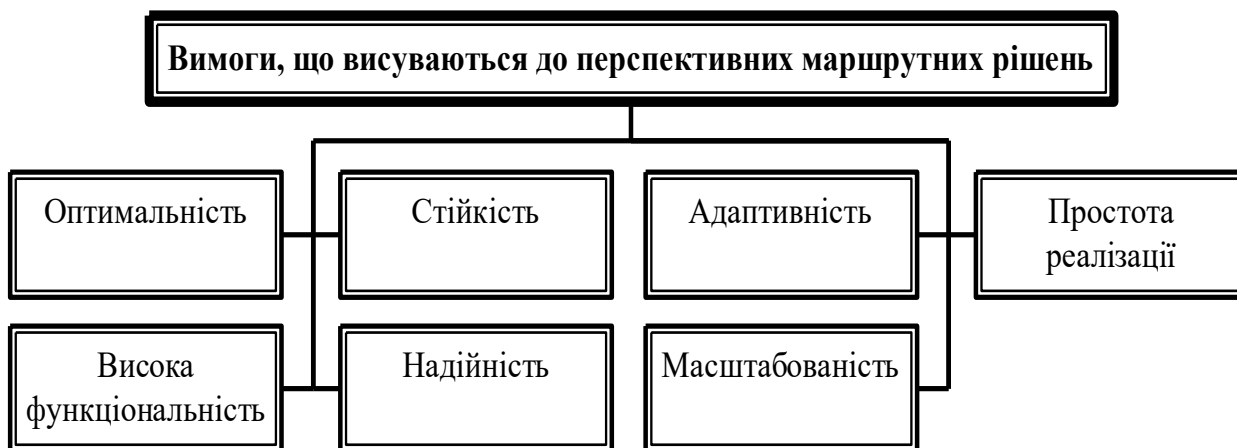


Рис. 1.9. Вимоги, що висуваються до перспективних маршрутних рішень

2. Стійкість. Маршрутне рішення має забезпечувати задану ефективність мережі в умовах невеликих коливань як її внутрішніх параметрів – структурних та (або) функціональних показників, так і характеристик зовнішніх впливів, наприклад, параметрів трафіку, що надходить до ІКМ.

3. Адаптивність. Протокол маршрутизації має оперативно адаптуватися (автоматично переналаштовуватися) до зміни стану мережі – її топології,

пропускної здатності каналів, завантаженості черг маршрутизаторів, характеристик трафіку та QoS-вимог.

4. Надійність. Протокольні рішення повинні гарантувати доступність маршрутів навіть в умовах відмов мережного обладнання, перевантаження, збоїв програмного забезпечення маршрутизаторів тощо.

5. Висока функціональність. У перспективні протокольні рішення мають бути закладені широкі функціональні можливості щодо їхнього налаштування під конкретний тип наданої інфокомунікаційної послуги та стан мережі. Це може проявлятися, наприклад, в обґрунтованому визначенні кількості та типів використаних шляхів і маршрутних метрик.

6. Масштабованість. Під масштабованістю в подальшому буде розумітися властивість маршрутного рішення забезпечувати задану ефективність функціонування мережі в умовах розширення її територіальної розподіленості та переліку наданих послуг, зростання кількості мережних елементів (маршрутизаторів і каналів зв'язку), збільшення загальної кількості користувачів і відповідної кількості й типів потоків пакетів.

7. Простота алгоритмічно-програмної та апаратної реалізації. Упровадження перспективного маршрутного протоколу не має призводити до створення надто великого обсягу службового трафіку та обчислювального навантаження на процесор маршрутизатора.

Перелічені вимоги мають суперечливий характер, оскільки, наприклад, забезпечення високого рівня функціональності маршрутних рішень обов'язково призведе до ускладнення програмної реалізації того чи іншого маршрутного рішення. У свою чергу розширення переліку структурних і функціональних параметрів, щодо яких здійснюється адаптація процесу маршрутизації, неодмінно викличе зростання обсягу службового навантаження про стан мережі. У зв'язку з цим на теперішній час не існує єдиного універсального маршрутного протоколу, який би повною мірою задовольняв зазначеним вище вимогам. Тому залежно від структури мережі, її завантаженості та рівня QoS-вимог вибір того чи іншого протоколу маршрутизації здійснюється адміністративно.

### **1.5. Напрями вдосконалення протоколів маршрутизації в ІКМ**

У процесі вдосконалення того чи іншого протоколу маршрутизації варто враховувати таку функціональну трирівневу ієрархію маршрутних рішень: модель, метод (алгоритм) і протокол маршрутизації. У цьому випадку основою довільного маршрутного рішення є адекватна математична модель

маршрутизації, яка може бути представлена математичними виразами, наприклад, алгебраїчними [70–73], диференціальними [74–80], інтегральними [80, 81], тензорними [82–85] рівняннями стану мережі. На виході тієї чи іншої математичної моделі, як правило, формулюється оптимізаційна задача щодо розрахунку шляху (шляхів) і балансування навантаження. Для розв’язання поставленої оптимізаційної задачі використовується обґрунтований з точки зору обраного показника ефективності (наприклад, обчислювальної складності) математичний метод (алгоритм). У свою чергу програмна реалізація послідовності дій, визначених у межах обраного математичного методу, є основою відповідного протоколу маршрутизації.

Так, наприклад, якщо математичну модель ІКМ представити зваженим орієнтованим графом, то технологічна задача маршрутизації може бути зведена до оптимізаційної задачі пошуку найкоротшого шляху на графі (рис. 1.10). Для розв’язання цієї задачі можуть бути використані, наприклад, математичні методи (алгоритми) Дейкстри, Беллмана–Форда, Флойда–Уоршелла [36–38]. На практиці алгоритми Дейкстри покладені в основу більшості маршрутних протоколів стану каналів – OSPF, IS-IS, PNNI, а алгоритм Беллмана–Форда застосовується дистанційно-векторними протоколами RIP та IGRP.



Рис. 1.10. Приклад трирівневої ієрархії маршрутних рішень

Відомі приклади, коли протокол маршрутизації вдосконалювався без перегляду чи модифікації обчислювального методу (алгоритму), на якому він базувався. Це, як правило, супроводжується зміною версії відповідного протоколу. Так, наприклад, друга версія протоколу RIP відрізняється від першої лише множиною програмних удосконалень, які стосуються зміни порядку розсилань оновлень між маршрутизаторами, підтримки масок змінної довжини тощо. Ключові ж моменти, пов’язані з типом використаної метрики та обраним алгоритмом маршрутизації, у цих версіях залишилися незмінними.



У свою чергу зміна методу (алгоритму) маршрутизації завжди веде до істотної модифікації наявного або навіть створення нового маршрутного протоколу. Так, наприклад, удосконалення протоколу дистанційно-векторної маршрутизації IGRP, яке супроводжувалося зміною алгоритму маршрутизації (з алгоритму Беллмана–Форда на DUAL), привело фактично до створення нового протоколу EIGRP змішаного типу, у якому частина функцій характерна для дистанційно-векторної маршрутизації, а частина – для протоколів стану каналів. Варто зазначити, що найбільш істотне вдосконалення протоколу маршрутизації можливо забезпечити лише на рівні зміни математичної моделі маршрутизації, що призведе також і до обов'язкового перегляду типу використаного методу маршрутизації.

Проте графові моделі та комбінаторні алгоритми пошуку найкоротшого шляху, які покладені в переважну більшість наявних протоколів маршрутизації, не відповідають сучасним вимогам. Це насамперед стосується таких обмежень:

- у формуванні маршрутної метрики переважно враховуються лише номінальні значення параметрів ІКМ, а не реально доступні обсяги мережного ресурсу, наприклад, пропускної здатності каналів зв'язку;

- для розрахунку найкоротшого шляху використовується скалярна метрика, яка, у кращому випадку, є згортою декількох параметрів мережі, функціонально пов'язаних з основними QoS-показниками. Це значно ускладнює забезпечення якості обслуговування одночасно за декількома різнорідними QoS-показниками, що є нагальною вимогою для надання сучасних, насамперед мультимедійних, сервісів;

- під час визначення шуканого маршруту не враховуються характеристики потоків (їхня кількість, інтенсивність, довжина пакетів та ін.), що значно ускладнює подальше балансування навантаження в мережі та в кінцевому випадку може спричинити перевантаження каналів зв'язку. Тому в сучасних ІКМ фактично рішення проблеми перевантаження каналів і мережі загалом перекладається на протоколи транспортного рівня EMBVC.

У зв'язку з цим усе більше уваги науковців різних країн світу приділяється синтезу та дослідженню поточкових моделей і методів маршрутизації, що використовують теорію графів, як правило, на етапі структурного опису ІКМ, а для моделювання безпосередньо процесів маршрутизації та балансування навантаження застосовують той чи інший математичний апарат, який з різним рівнем адекватності здатний урахувати статистичні параметри потоків пакетів, дисципліни їх обслуговування на маршрутизаторах та оптимального розподілу за каналами мережі. Для цього під

час досліджень активно використовується функціонал теорії диференціальних та інтегральних рівнянь, теорії марковських випадкових процесів і систем (мереж) масового обслуговування (теорії черг), методів фрактального аналізу, теорії оптимального управління та методів дослідження операцій тощо [78–80].

### **1.6. Узагальнена структура потокової моделі маршрутизації в ІКМ**

За результатами проведеного аналізу основних підходів до математичного моделювання маршрутних задач [86–88] була визначена узагальнена структура потокової моделі маршрутизації в ІКМ (рис. 1.11), яка представлена множиною умов 1÷9.

Основою більшості поточкових моделей маршрутизації є умови збереження потоку в мережних вузлах (маршрутизаторах) та в ІКМ загалом (умови першого типу). Зміст цих умов стосується того, що інтенсивність потоку на вході в мережу і на виході з мережі повинна залишатися незмінною. Форма подібних умов багато в чому залежить від типу стратегії маршрутизації – одно- або багатошляхової, одно- або багатоадресної. Умови другого типу, доповнюючи попередні умови, відповідають за забезпечення зв'язності кожного конкретного одно- або багатоадресного маршруту, щоб пакети того чи іншого потоку могли передаватися від маршрутизатора-джерела до маршрутизатора-отримувача (отримувачів).

Для підвищення рівня якості обслуговування в ІКМ, забезпечення керованості процесом боротьби з її перевантаженням та подекуди надання узгодженості вирішень завдань маршрутизації та управління каналним ресурсом маршрутну модель необхідно доповнити умовами відсутності перевантаження каналів зв'язку мережі (умови третього типу). Відсутність у структурі графових моделей маршрутизації подібних умов на практиці нерідко призводило до перевантаження каналів зв'язку, які утворюють так званий «найкоротший шлях» в обраній метриці, що особливо характерно у випадку зростання навантаження на мережу.

Залежно від вимог щодо стратегії маршрутизації, що використовується в ІКМ, модель може містити умови реалізації одно- або багатошляхової маршрутизації пакетів (умови четвертого типу). Окремим випадком є умови реалізації *K*-шляхової стратегії маршрутизації [89], коли кількість використаних шляхів наперед відома та задається у вихідних даних. Проте загальна кількість розрахованих шляхів може визначатися й адаптивно – залежно від навантаження мережі та вимог щодо рівня якості обслуговування.

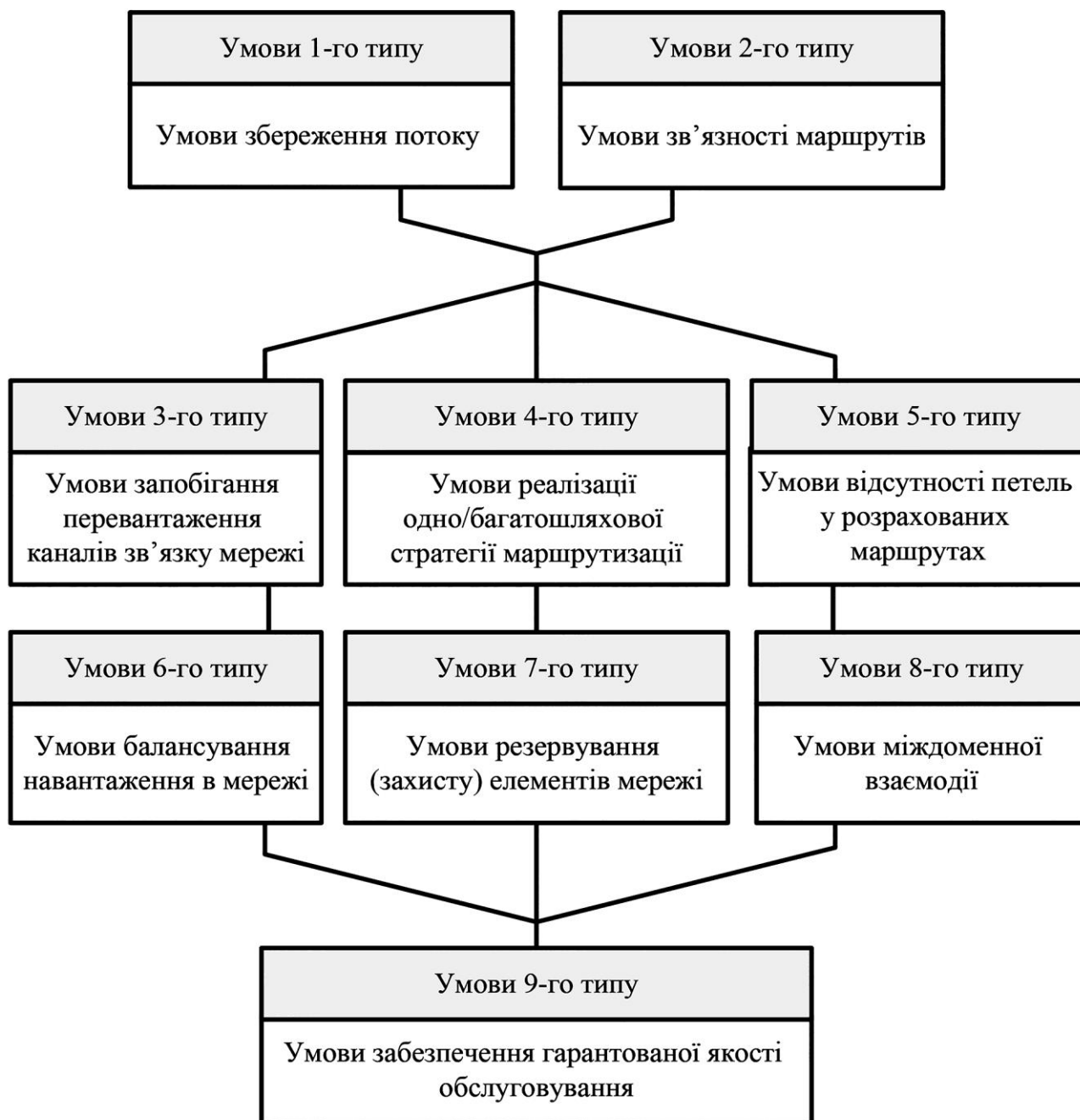


Рис. 1.11. Узагальнена структура потокової моделі маршрутизації в ІКМ

У загальному випадку в потоковій моделі маршрутизації має бути передбачене місце умовам відсутності петель у розрахованих маршрутах (умови п'ятого типу), щоб на протокольному рівні не перекладати функції щодо їх усунення на додаткові засоби боротьби із зацикленням пакетів, основаних, наприклад, на методах «розщеплення горизонту», тимчасової відмови від прийому повідомлень, примусових оголошень або на методі корегування скасування маршруту [65]. Подібні умови можуть задаватися в явній або неявній формі.

Для забезпечення збалансованого завантаження (використання) доступних мережних (буферного та каналного) ресурсів, згідно з вимогами концепції Traffic Engineering, до структури потокової моделі вводяться умови шостого типу. Їх виконання, як правило, також орієнтує на покращення значень основних QoS-показників – середнього затримання пакетів, джитеру, імовірності втрат пакетів та продуктивності ІКМ загалом.

Важливе місце в реалізації відмовостійкої маршрутизації в потоковій моделі займають умови резервування (захисту) елементів мережі та її пропускну здатності (умови сьомого типу). Як правило, виконання цих умов передбачає розрахунок шляхів, що не перетинаються за одним або множиною елементів мережі, які захищаються. Граничним випадком є варіант пошуку маршрутів, що не містять спільних каналів і маршрутизаторів, крім маршрутизаторів відправника та отримувача (отримувачів).

У математичному описі процесів ієрархічної маршрутизації в мультидоменних мережах до структури потокової моделі вводяться умови міждоменної взаємодії (умови восьмого типу), що відповідають за погоджене використання мережного ресурсу, який розміщується або між сусідніми доменами, або належить одночасно декільком мережним доменам. Так, наприклад, у використанні протоколу маршрутизації OSPF границя між доменами проходить через маршрутизатори, які є спільними для двох сусідніх доменів, а в протоколі IS-IS – через канали зв'язку, що з'єднують приграничні маршрутизатори різних доменів.

Ключове місце в структурі математичної моделі маршрутизації мають умови забезпечення гарантованої якості обслуговування (умови дев'ятого типу), виконання яких дозволяє не тільки покращити той чи інший QoS-показник, але й гарантувати, що числове значення цього показника буде міститися у наперед заданому діапазоні. У процесі досліджень можливі декілька основних варіантів формулювання подібних умов. Ці умови можуть вводитись як для оцінки міжкінцевих QoS-показників для кожного з потоків пакетів окремо, так і для аналізу усереднених значень для мережі загалом. Крім того, умови дев'ятого типу можуть бути сформульовані для кожного окремого QoS-показника, а можуть функціонально пов'язувати між собою декілька основних показників якості обслуговування. Варто зазначити, що в загальному випадку отримання в аналітичному вигляді умов забезпечення гарантованої якості обслуговування одночасно за кількома показниками QoS є досить складною науковою задачею. У відомих рішеннях цієї задачі [82–85] подібні умови вдалося отримати в нелінійному вигляді,

що критично позначається на обчислювальній складності та масштабованості кінцевих рішень.

Запропонований на рис. 1.11 перелік умов у структурі математичної моделі маршрутизації не є вичерпним і може бути доповнений низкою інших умов, пов'язаних, наприклад, з підвищенням стійкості та (або) робастності маршрутних рішень до можливих стохастичних змін структури ІКМ, характеристик мережного трафіку тощо. Наведені умови залежно від особливостей визначення оптимізаційної задачі маршрутизації можуть становити основу як критерію (критеріїв) оптимальності кінцевих рішень, так і обмежень, що накладаються на маршрутні змінні. Відповідно до особливостей постановки задачі маршрутизації та вимог до рівня адекватності їх математичного опису умови 1÷9 приймають форму рівнянь або нерівностей, які у свою чергу можуть бути представлені як лінійними, так і нелінійними виразами. Подібний підхід загалом відповідає змісту концепції маршрутизації на основі обмежень (Constraint-based Routing).

## 1.7. Опис базових поточкових моделей маршрутизації в ІКМ

У цьому підрозділі будуть представлені поточкові моделі одноадресної, багатоадресної та ширококомовної маршрутизації в ІКМ, які в наступних розділах роботи використовуватимуться як базові для синтезу нових і вдосконалення наявних моделей і методів відмовостійкої (у другому розділі), безпечної (у третьому розділі) та ієрархічної (у четвертому розділі) маршрутизації.

### 1.7.1. Поточкова модель одноадресної маршрутизації в ІКМ

Нехай структура мережі описується графом  $\Gamma = (R, E)$ , у якому  $R = \{R_i; i = \overline{1, m}\}$  – це множина вершин, що моделюють маршрутизатори, а  $E = \{E_{i,j}; i, j = \overline{1, m}; i \neq j\}$  – множина дуг, що представляють канали зв'язку в ІКМ. Тоді  $|E| = n$  визначає кількість каналів зв'язку в ІКМ. Зокрема кожній дузі  $E_{i,j} \in E$  поставимо у відповідність її пропускну здатність  $\varphi_{i,j}$ .

Позначимо через  $K^o$  підмножину одноадресних потоків. Тоді, як показано в роботах [70, 71], присвячених моделюванню задач одноадресної маршрутизації, для кожного  $k$ -го потоку відомі такі вихідні дані:

$\lambda^k$  – середня пакетна швидкість (інтенсивність), яка вимірюється в пакетах за секунду ( $1/c$ );

$s_k$  та  $d_k$  – вузол-відправник та вузол-отримувач пакетів  $k$ -го одноадресного потоку відповідно.

Тоді порядок одноадресної маршрутизації в мережі визначають маршрутні змінні  $x_{i,j}^k$ , кожна з яких характеризує долю (частину)  $k$ -го потоку, що протікає в каналі зв'язку (КЗ) між  $i$ -м та  $j$ -м вузлами (маршрутизаторами) мережі. Виходячи з фізичного змісту введених маршрутних змінних, залежно від реалізованої стратегії маршрутизації на них накладаються умови виду

$$x_{i,j}^k \in \{0;1\} \quad (1.1)$$

або

$$0 \leq x_{i,j}^k \leq 1. \quad (1.2)$$

Уведення умов (1.1) відповідає за реалізацію в ІКМ одношляхової стратегії маршрутизації. Для виконання умови (1.2) буде підтримуватися багатошляхова маршрутизація (не забороняючи одночасно використання й одношляхових рішень), за якої змінні  $x_{i,j}^k$  можуть приймати крайні зі своїх можливих значень – нуль або одиницю (1.1). Множина застосованих шляхів надалі буде називатися мультишляхом.

Крім того, під час розрахунку маршрутних змінних мають виконуватися умови збереження потоку на маршрутизаторах мережі [70, 71]:

$$\left\{ \begin{array}{l} \sum_{j:E_{i,j} \in E} x_{i,j}^k - \sum_{j:E_{j,i} \in E} x_{j,i}^k = 1, k \in K^o, R_i = s_k, \\ \sum_{j:E_{i,j} \in E} x_{i,j}^k - \sum_{j:E_{j,i} \in E} x_{j,i}^k = 0, k \in K^o, R_i \neq s_k, d_k, \\ \sum_{j:E_{i,j} \in E} x_{i,j}^k - \sum_{j:E_{j,i} \in E} x_{j,i}^k = -1, k \in K^o, R_i = d_k. \end{array} \right. \quad (1.3)$$

У разі виконання умов (1.3) гарантується відсутність втрат пакетів на кожному маршрутизаторі та в мережі загалом, а також забезпечується зв'язність розрахованих маршрутів між відправником та отримувачем пакетів  $k$ -го потоку.

Для запобігання перевантаження каналів зв'язку ІКМ необхідно забезпечити виконання таких умов [70, 71]:

$$\sum_{k \in K^o} \lambda^k x_{i,j}^k \leq \varphi_{i,j}, \quad E_{i,j} \in E, \quad (1.4)$$

кількість яких відповідає кількості каналів зв'язку в мережі.

### 1.7.2. Потокова модель багатоадресної та ширококомовної маршрутизації в ІКМ

Позначимо через  $K^{\bar{o}}$  підмножину багатоадресних потоків, тоді з кожним  $k$ -м багатоадресним потоком також будуть пов'язані параметри  $\lambda^k$  та  $s_k$ , а також

$$d_k^* = \{d_k^1, d_k^2, \dots, d_k^{m_k}\}, \quad (1.5)$$

що є множиною вузлів-отримувачів, де  $m_k$  – їхня загальна кількість для  $k$ -го багатоадресного потоку. Наприклад, на рис. 1.12 вершиною-відправником  $s_1$  багатоадресного потоку є перша вершина ( $R_1$ ), а множина  $d_1^* = \{d_1^1, d_1^2, d_1^3\}$  представлена вершинами  $R_5$ ,  $R_8$  та  $R_9$ .

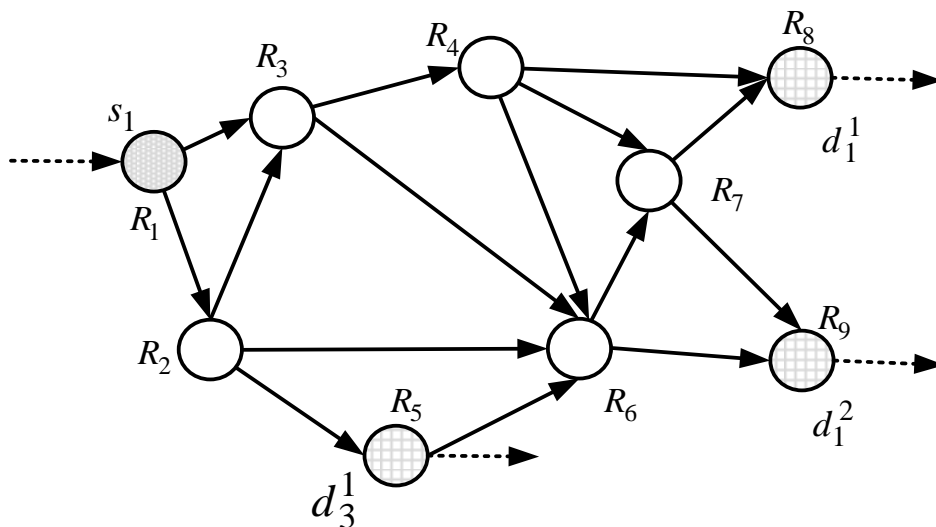


Рис. 1.12. Приклад графового опису вихідних даних для задачі багатоадресної маршрутизації

В описі поточної моделі ширококомовної маршрутизації множина вузлів-отримувачів пакетів дещо розширяється порівняно з (1.5)

$$d_k^{**} = \{d_k^1, d_k^2, \dots, d_k^{m-1}\}, \quad (1.6)$$

тобто вона містить усі вершини, крім  $s_k$ .

Тоді внаслідок розв'язання задачі багатоадресної маршрутизації необхідно розрахувати множину булевих змінних, вид яких збігається з формою (1.1), але за умови  $k \in K^{\bar{o}}$ . Загальна кількість маршрутних змінних, що відповідають за реалізацію багатоадресної маршрутизації, визначається добутком кількості каналів зв'язку на кількість потоків в ІКМ.

У разі багатоадресної маршрутизації на маршрутні змінні (1.1) накладається низка обмежень, пов'язаних з реалізацією умов збереження потоку в мережі [90–92]:

$$\sum_{j: E_{i,j} \in E} x_{i,j}^k \geq 1, \text{ якщо } k \in K^{\bar{b}}, R_i = s_k, \quad (1.7)$$

а також

$$\sum_{j: E_{i,j} \in E} x_{i,j}^k = 1, \text{ якщо } k \in K^{\bar{b}}; R_j \in d_k^*. \quad (1.8)$$

Умова (1.7) вводиться для вузла-відправника, а її виконання орієнтує на те, що від цього вузла потік, який надходить до мережі на обслуговування, буде переданий хоча б одному суміжному вузлу. Умови (1.8) спрямовані на забезпечення доставки пакетів потоку на кожний вузол-отримувач, зокрема відповідно до фізики процесу багатоадресної маршрутизації потік має надходити на ці вузли лише від одного суміжного вузла.

Для кожного транзитного вузла  $R_j \in R$ , яким може бути довільний маршрутизатор, крім вузла-відправника, додатково вводяться такі умови:

$$\sum_{i: E_{i,j} \in E} x_{i,j}^k \geq x_{j,p}^k \text{ якщо } k \in K^{\bar{b}}; R_j \notin s_k, \quad (1.9)$$

виконання яких робить можливим появу пакетів на будь-якому з вихідних від транзитного вузла інтерфейсів ( $E_{j,p} \in E$ ) лише в тому випадку, коли цей потік надходить на цей вузол хоча б через один вхідний інтерфейс ( $E_{i,j} \in E$ ).

Якщо на структурі мережі можливе утворення контурів (циклів), то в разі виконання умов (1.7)–(1.9) не завжди буде забезпечуватися зв'язність окремих каналів у багатоадресний маршрут. Для запобігання утворенню контурів у модель вводяться умови (за кількістю базисних контурів у мережі) вигляду [90–92]:

$$\sum_{E_{i,j} \in E_{\pi}^q} x_{i,j}^k < |E_{\pi}^q|, \quad (1.10)$$

де  $E_{\pi}^q$  – множина дуг графа, які створюють відповідно до своєї орієнтації  $q$ -й контур ( $\pi$ );

$|E_{\pi}^q|$  – потужність множини базисних контурів  $E_{\pi}^q$ , яка дорівнює цикломатичному числу графа  $\Gamma = (R, E)$ , що описує структуру ІКМ.



Виконання умов (1.10) гарантує, що кількість задіяних у процес багатоадресної маршрутизації дуг, які створюють той чи інший контур, завжди менша від загальної кількості дуг у цьому контурі, тобто розрахований маршрут не містить контурів. Для недопущення перевантаження каналів зв'язку багатоадресними потоками необхідно виконати умови (1.4), але якщо  $k \in K^{\bar{b}}$ .

Унаслідок розв'язання задачі ширококомовної маршрутизації також необхідно розрахувати множину булевих маршрутних змінних  $x_{i,j}^k$  (1.1), на які накладаються обмеження, аналогічні до (1.4), (1.7), (1.8) та (1.10), зі збереженням раніше вкладеного в них фізичного змісту. Водночас варто врахувати, оскільки умова (1.8) стосується всіх вузлів мережі (крім вузла-відправника), тобто  $R_j \in d_k^{**}$ , то в разі моделювання процесу ширококомовної маршрутизації відсутня необхідність у додатковому введенні умов (1.9), тому що в кожному вузол мережі (1.6) за замовчуванням надходить потік заданої інтенсивності  $\lambda^k$ .

### 1.7.3. Основні варіанти критеріїв оптимальності маршрутних рішень в ІКМ

Важливо зазначити, що в загальному випадку ІКМ має змішану топологію, яка допускає декілька можливих варіантів розв'язання маршрутних задач. Тому актуальним є вибір найбільш ефективного рішення, оптимального в межах обраного критерію. Вибір критерію оптимальності маршрутних рішень є ключовим моментом у завершенні формалізації моделей як одно-, так і багатоадресної маршрутизації. Від його форми та змісту безпосередньо залежить ефективність організації процесу маршрутизації з точки зору, по-перше, підвищення якості обслуговування за показниками середньої затримки, джитеру та ймовірності втрат пакетів; по-друге, визначення порядку використання та завантаженості каналів мережі в розрахованих маршрутах; і, по-третє, забезпечення збалансованого завантаження каналів і буферних ресурсів мережі. Крім того, традиційно вибір критерію оптимальності має повністю відповідати фізичному змісту розв'язуваної оптимізаційної задачі, меті проведеного дослідження, а також бути достатньо простим для отримання шуканих рішень у числовому вигляді. Для розрахунку оптимальних шляхів як приклад може використовуватися лінійний критерій [86–88]

$$\sum_{k \in K^0 \cup K^{\bar{b}}} \sum_{E_{i,j} \in E} c_{i,j}^k x_{i,j}^k \Rightarrow \min, \quad (1.11)$$

де  $c_{i,j}^k$  – маршрутна метрика, яка характеризує структурно-функціональні параметри каналу зв'язку  $E_{i,j} \in E$  та кількісно відображає умовну вартість використання даного КЗ. Чим вище числове значення зазначеної метрики, тим нижча ймовірність включення цього каналу в шуканий одноадресний та (або) багатоадресний маршрут.

Наприклад, якщо  $c_{i,j}^k = 1$ , то оптимальний шлях буде складатися з мінімальної кількості каналів зв'язку. У випадку, коли  $c_{i,j}^k = 1/\varphi_{i,j}$ , перевага у виборі оптимального шляху (шляхів) буде надаватися каналам з максимальною пропускнуою здатністю.

Використання критерію (1.11) з умовами-обмеженнями (1.1)–(1.4) у разі одноадресної маршрутизації та (1.1), (1.4), (1.7)–(1.10) у випадку багатоадресної маршрутизації дозволяє сформулювати задачу маршрутизації в оптимізаційному вигляді. Лінійність критерію та обмежень дає змогу використовувати для отримання шуканих рішень досить ефективно з обчислювальної точки зору методи лінійного програмування [80]. Окремо варто зауважити, що для розв'язання задачі одношляхової маршрутизації, коли маршрутні змінні мають булевий характер (1.1), оптимізаційна задача набуває форми задачі класу булевого програмування.

У роботах [93, 94] пропонується квадратичний критерій оптимальності, який має такий вигляд

$$\sum_{k \in K^o \cup K^b} \sum_{E_{i,j} \in E} x_{i,j}^k c_{i,j}^k x_{i,j}^k \Rightarrow \min. \quad (1.12)$$

Його застосування, на відміну від лінійного аналога (1.11), сприяє більш збалансованому використанню каналів зв'язку мережі, хоча й дещо підвищує обчислювальну складність алгоритмічної реалізації маршрутних рішень.

Проте для забезпечення балансування навантаження відповідно до вимог концепції Traffic Engineering, як показано в роботах [70–73], пропонується змінити форму запису умов запобігання перевантаження каналів зв'язку (1.4) на вирази, що мають вигляд:

$$\sum_{k \in K^o} \lambda^k x_{i,j}^k \leq \alpha \varphi_{i,j}, \quad E_{i,j} \in E, \quad (1.13)$$

де  $\alpha$  – додатково введена керуюча змінна, яка характеризує верхній динамічно керований поріг завантаженості каналів зв'язку. На неї відповідно до її фізичного змісту накладається таке обмеження:

$$0 \leq \alpha \leq 1. \quad (1.14)$$

Для підвищення якості обслуговування в ІКМ цю змінну необхідно мінімізувати, визначаючи тим самим вид критерію оптимальності рішень щодо маршрутизації та балансування навантаження в мережі [70–73]

$$\alpha \rightarrow \min. \quad (1.15)$$

У розв'язанні сформульованої оптимізаційної задачі отримане мінімальне значення змінної  $\alpha$  відповідно до умов (1.13) і (1.14) кількісно відповідає коефіцієнту використання найбільш завантаженого каналу. Як показано в роботах [73, 95], незаперечною перевагою моделі (1.13)–(1.15) також є те, що за умови збільшення навантаження на мережу значення змінної  $\alpha$  зростає лінійно, сприяючи тим самим прогнозованій (без різких коливань) зміні основних показників якості обслуговування – середньої затримки, джитеру та ймовірності втрат пакетів.

У використанні критерію (1.15) і модифікованих умов запобігання перевантаження (1.13) технологічна задача багатошляхової маршрутизації (1.2) приймає вигляд оптимізаційної задачі лінійного програмування. Але у разі одношляхової (1.1) та багатоадресної/широкомовної маршрутизації оптимізація вже зводиться до розв'язання задачі змішаного цілочисельного лінійного програмування (Mixed integer linear programming, MILP). Клас оптимізаційної задачі змінився, тому що необхідно розрахувати не тільки множину булевих змінних (1.1), але й одну додатково введenu керуючу змінну  $\alpha$ , яка є позитивним дійсним числом (1.14). Критерій оптимальності (1.15) та додатково введені обмеження (1.13) і (1.14) мають лінійний характер.

## Висновки до першого розділу

1. Як показав проведений у розділі аналіз, ключовою проблемою в сучасних мультисервісних ІКМ, що розвиваються в напрямі створення мереж наступного покоління, є проблема забезпечення якості обслуговування. Зокрема з розширенням переліку наданих інфокомунікаційних послуг, постійним зростанням гетерогенності мереж і різнорідності трафіку, що циркулює в мережі, ця проблема стає все гострішою, потребуючи теоретично обґрунтованого й узгодженого опрацювання множини мережних задач щодо управління трафіком в ІКМ. У зв'язку із затребуваністю якості обслуговування «з кінця в кінець» усе більше уваги приділяється саме протоколам маршрутизації, які, крім того, повинні забезпечувати оптимальність, адаптивність, надійність, стійкість, масштабованість і простоту реалізації маршрутних рішень в ІКМ (рис. 1.9).

2. Установлено, що вдосконалення того чи іншого маршрутного рішення може здійснюватися на рівні протоколу, використаного обчислювального методу (алгоритму) розрахунку або математичної моделі маршрутизації. У цьому випадку найбільш обґрунтоване та ефективне вдосконалення протоколу маршрутизації можна забезпечити лише на рівні заміни математичної моделі або методу маршрутизації. Графові моделі та комбінаторні алгоритми пошуку найкоротшого шляху, які покладені в основу більшості наявних протоколів маршрутизації, мають досить обмежені функціональні можливості щодо одночасного врахування декількох метрик, підтримки балансування навантаження за множиною шляхів тощо. У зв'язку з цим актуальним науковим і прикладним напрямом дослідження є розроблення та вдосконалення потокових моделей і методів маршрутизації, які порівняно з графовими рішеннями більш повно враховують як топологічні параметри мережі, так і характеристики потоків – їхню інтенсивність, нестационарність, довжину пакета тощо.

3. Для реалізації принципів системного підходу під час синтезу нових або вдосконалення наявних маршрутних рішень на рівні математичної моделі запропонована їй узагальнена структура (рис. 1.11). Структура потокової моделі маршрутизації представлена системою умов, що враховують як особливості структурно-функціональної побудови самої ІКМ, так і ключові аспекти та атрибути стратегій маршрутизації, які описуються за допомогою цієї моделі. Подібна система умов, які становлять основу обраної потокової моделі, повністю визначає фізичний зміст і математичну форму оптимізаційної задачі щодо маршрутизації в ІКМ як на рівні виду використаного критерію оптимальності маршрутних рішень, так і типу врахованих обмежень на керуючі (маршрутні) змінні.

4. Відповідно до описаної узагальненої структури потокової моделі маршрутизації у розділі представлені базові математичні моделі одноадресної, багатоадресної та ширококомовної маршрутизації в ІКМ, які в наступних розділах роботи використовуватимуться як основа для синтезу нових і вдосконалення наявних моделей і методів відмовостійкої (у другому розділі), безпечної (у третьому розділі) та ієрархічної (у четвертому розділі) маршрутизації.

### **Перелік джерел посилання до вступу та першого розділу**

1. ITU-T Rec. Y.3001. Future Network Vision: Objectives and Design Goals. May 2011. 26 p. URL: <https://www.itu.int/rec/T-REC-Y.3001-201105-I>.

2. ITU-T Rec. Y.3031. Identification framework in future networks. May 2012. 24 p. URL: <https://www.itu.int/rec/T-REC-Y.3031-201205-I/en>.
3. ITU-T Rec. Y.3015. Functional architecture of network virtualization for future networks. April 2016. 30 p. URL: <https://www.itu.int/rec/T-REC-Y.3015-201604-I/en>.
4. Hutchison D., Galis A., Gavras, A. The Future Internet-LNCS 7858. Springer-Verlag Berlin Heidelberg. 2013. 401 p. DOI: 10.1007/978-3-642-38082-2.
5. ETSI TS 103 195-2 V1.1.1. Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 2: An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management. May 2018. 149 p. URL: [https://www.etsi.org/deliver/etsi\\_ts/103100\\_103199/10319502/01.01.01\\_60/ts\\_10319502v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/103100_103199/10319502/01.01.01_60/ts_10319502v010101p.pdf).
6. ETSI TS 103 194 V1.1.1. Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Scenarios, Use Cases and Requirements for Autonomic/Self-Managing Future Internet. October 2014. 67 p. URL: [https://www.etsi.org/deliver/etsi\\_ts/103100\\_103199/103194/01.01.01\\_60/ts\\_103194v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/103100_103199/103194/01.01.01_60/ts_103194v010101p.pdf).
7. Про телекомунікації: Закон України від 18.11.2003 № 1280-IV. Відомості Верховної Ради України. 2004. № 12. Ст. 155.
8. Про інформацію: Закон України від 02.10.1992 № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 650.
9. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994. № 80/94-ВР. Відомості Верховної Ради України. 1994. № 31. Ст. 286.
10. Про схвалення Концепції розвитку телекомунікацій в Україні: Розпорядження Кабінету Міністрів України від 07.06.2006 № 316-р. Дата оновлення: 27.12.2008. URL: <http://zakon3.rada.gov.ua/laws/show/316-2006-%D1%80/page> (дата звернення: 14.03.2018).
11. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України від 15.05.2013 № 386-р. URL: <http://zakon2.rada.gov.ua/laws/show/386-2013-%D1%80> (дата звернення: 14.03.2018).
12. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17.01.2018 № 67-р. URL: <http://zakon3.rada.gov.ua/laws/show/67-2018-%D1%80> (дата звернення: 14.03.2018).
13. Про Рекомендації парламентських слухань на тему: «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору

України»: Постанова Верховної Ради України від 31.03.2016 № 1073-VIII. Відомості Верховної Ради. 2016. № 17. Ст. 191.

14. ITU-T Rec. Y.3051. The basic principles of trusted environment in information and communication technology infrastructure. March 2017. 16 p. URL: <https://www.itu.int/rec/T-REC-Y.3051-201703-I/en>.

15. Chaparadza R., Wodczak M., Meriem T.B., De Lutiis P., Tcholtchev N., Ciavaglia L. Standardization of resilience & survivability, and autonomic fault-management, in evolving and future networks: an ongoing initiative recently launched in ETSI. Design of Reliable Communication Networks (DRCN) 2013: Proceedings of the 9th International Conference. Budapest, Hungary, 4–7 March, 2013. IEEE, 2013. P. 331–341.

16. ITU-T Rec. Y. 2614. Network reliability in public telecommunication data networks. August 2008. 20 p. URL: <https://www.itu.int/rec/T-REC-Y.2614-201108-I/en>.

17. ITU-T Rec. Y.2701. Security requirements for NGN release 1. April 2007. 44 p. URL: <https://www.itu.int/rec/T-REC-Y.2701-200704-I/en>.

18. ITU-T Rec. Y.2704. Security mechanisms and procedures for NGN. January 2010. 58 p. URL: <https://www.itu.int/rec/T-REC-Y.2704-201001-I/en>.

19. ITU-T Rec. Y.2705. Minimum security requirements for the interconnection of the Emergency Telecommunications Service (ETS). March 2013. 24 p. URL: <https://www.itu.int/rec/T-REC-Y.2705-201303-I/en>.

20. ITU-T Rec. E.800. Definition of terms related to Quality of Service. September 2008. 30 p. URL: <https://www.itu.int/rec/T-REC-E.800-200809-I>.

21. ITU-T Rec. G.1000. Communications Quality of Service: A framework and definitions. January 2001. 16 p. URL: <https://www.itu.int/rec/T-REC-G.1000-200111-I/en>.

22. ITU-T Rec. E.802. Framework and methodologies for the determination and application of QoS parameters. February 2007. 38 p. URL: <https://www.itu.int/rec/T-REC-E.802-200702-I>.

23. ITU-T Rec. E.860. Framework of a service level agreement. June 2002. 30 p. URL: <https://www.itu.int/rec/T-REC-E.860-200206-I/en>.

24. ITU-T Rec. Y.1542. Framework for achieving end-to-end IP performance objectives. June 2010. 30 p. URL: <https://www.itu.int/rec/T-REC-Y.1542-201006-I/en>.

25. ITU-T Rec. Y.1291. An architectural framework for support of Quality of Service in packet networks. May 2004. 30 p. URL: <https://www.itu.int/rec/T-REC-Y.1291-200405-I/en>.

26. ITU-T Rec. E.803. Quality of service parameters for supporting service aspects. December 2011. 52 p. URL: <https://www.itu.int/rec/T-REC-E.803-201112-I/en>.
27. ITU-T Rec. Y.1540. Internet protocol data communication service – IP packet transfer and availability performance parameters. July 2016. 57 p. URL: <https://www.itu.int/rec/T-REC-Y.1540-201607-I/en>.
28. ITU-T Rec. Y.1541. Network performance objective for IP-based services. December 2011. 66 p. URL: <https://www.itu.int/rec/T-REC-Y.1541-201112-I/en>.
29. ITU-T Rec. G.1011. Reference guide to quality of experience assessment methodologies. July 2016. 26 p. URL: <https://www.itu.int/rec/T-REC-G.1011-201607-I/en>.
30. ITU-T Rec. E.804. Quality of service aspects for popular services in mobile networks. February 2014. 446 p. URL: <https://www.itu.int/rec/T-REC-E.804-201402-I/en>.
31. ITU-T Rec. 1545.1. Framework for Monitoring the Quality of Service of Internet Protocol network services. March 2017. 24 p. URL: <https://www.itu.int/rec/T-REC-Y.1545.1-201703-I/en>.
32. Cholda P., Tapolcai J., Cinkler T., Wajda K., Jajszczyk A. Quality of resilience as a network reliability characterization tool. *IEEE network*. 2009. Vol. 23, No. 2. P. 11–19. DOI: 10.1109/MNET.2009.4804331.
33. Tipper D. Resilient network design: challenges and future directions. *Telecommunication Systems*. 2014. Vol. 56, No. 1. P. 5–16. DOI: 10.1007/s11235-013-9815-x.
34. Rak J. *Resilient Routing in Communication Networks (Computer Communications and Networks)*, 1st edition. Springer, 2015. 181 p.
35. Mauthe A., Hutchison D., Cetinkaya E.K., Ganchev I., Rak J., Sterbenz J.P., Gunkelk M., Smith P., Gomes T. Disaster-resilient communication networks: Principles and best practices. *Resilient Networks Design and Modeling (RNDM) 2016: Proceedings of the 8th International Workshop*. Halmstad, Sweden, 13–15 September, 2016. IEEE, 2016. P. 1–10. DOI: 10.1109/RNDM.2016.7608262.
36. Телекомунікаційні системи та мережі. Структура та основні функції / В.В. Поповський та ін. Вид. 2-ге, випр. та допов. Харків: СМІТ. 2018. Т. 1. URL: <http://www.znanius.com/3534.html>.
37. Medhi D., Ramasamy K. *Network Routing, Second Edition: Algorithms, Protocols, and Architectures (The Morgan Kaufmann Series in Networking)* 2nd Edition. Cambridge, MA, USA: Elsevier Inc., 2018. 1018 p.
38. Misra S., Goswami S. *Network Routing: Fundamentals, Applications, and Emerging Technologies* 1st Edition. Wiley, 2017. 536 p.

39. White R., Tantsura J.E. Navigating Network Complexity: Next-generation routing with SDN, service virtualization, and service chaining. AddisonWesley Professional, 2015. 320 p.
40. Barreiros M., Lundqvist P. QoS-Enabled Networks: Tools and Foundations. 2nd Edition. Wiley Series on Communications Networking & Distributed Systems, Wiley, 2016. 254 p.
41. Szigeti T., Hattingh C., Barton R., Briley K. End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks. 2nd Edition. Cisco Press, 2013. 1040 p.
42. Tiso J., Teare D. Designing Cisco Network Service Architectures (ARCH): Foundation Learning Guide. Cisco press. 2011. 733 p.
43. Cisco Networking Academy (Ed.). Routing Protocols Companion Guide. Pearson Education. 2014. 792 p.
44. ITU-T Rec. Y.3071. Data aware networking (information centric networking) – Requirements and capabilities. March 2017. 18 p. URL: <https://www.itu.int/rec/T-REC-Y.3071-201703-I/en>.
45. ITU-T Rec. Y.3300. Framework of software-defined networking. June 2014. 22 p. URL: <https://www.itu.int/rec/T-REC-Y.3300-201406-I/en>.
46. ITU-T Rec. Y.2720. NGN identity management framework. January 2009. 34 p. URL: <https://www.itu.int/rec/T-REC-Y.2720-200901-I>.
47. ITU-T Rec. Y.2770. Requirements for deep packet inspection in next generation networks. December 2012. 38 p. URL: <https://www.itu.int/rec/T-REC-Y.2770-201211-I/en>.
48. Quality of service regulation manual. 2017. ITU. 176 p. URL: [https://www.itu.int/pub/D-PREF-BB.QOS\\_REG01-2017](https://www.itu.int/pub/D-PREF-BB.QOS_REG01-2017).
49. Barona López L.I., Valdivieso Caraguay Á.L., Sotelo Monge M.A., García Villalba L.J. Key technologies in the context of future networks: operational and management requirements. Future Internet. 2017. Vol. 9, No. 1. P. 1–15. DOI: <https://doi.org/10.3390/fi9010001>.
50. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. 1st Edition. Pearson Education Inc., 2016. 510 p.
51. Monge A.S., Szarkowicz K.G. MPLS in the SDN Era: Interoperable Scenarios to Make Networks Scale to New Services. 1st ed. O'Reilly Media, 2016. 920 p.
52. Schneier B. Data and Goliath: The hidden battles to collect your data and control your world. WW Norton & Company, 2015. 398 p.
53. Stallings W. Cryptography and Network Security: Principles and Practice. 7th Edition. Pearson, 2016. 768 p.



54. Xia W., Wen Y., Foh C.H., Niyato D., Xie H. A survey on software-defined networking. *IEEE Communications Surveys & Tutorials*. 2015. Vol. 17, No. 1. P. 27-51. DOI: 10.1109/COMST.2014.2330903.
55. Björck F., Henkel M., Stirna J., Zdravkovic J. Cyber resilience-fundamentals for a definition. *New Contributions in Information Systems and Technologies*. 2015. Vol. 353. Springer, Cham. P. 311–316. DOI: [https://doi.org/10.1007/978-3-319-16486-1\\_31](https://doi.org/10.1007/978-3-319-16486-1_31).
56. Fink G.A., Griswold R.L., Beech Z.W. Quantifying cyber-resilience against resource-exhaustion attacks. *Resilient Control Systems (ISRCS) 2014: Proceedings of the 7th International Symposium, Denver, CO, USA, 19–21 August, 2014*. IEEE, 2014. P. 1–8. DOI: 10.1109/ISRCS.2014.6900093.
57. Choras M., Kozik R., Bruna M.P.T., Yautsiukhin A., Churchill A., Maciejewska I., Eguinoa I., Jomni A. Comprehensive approach to increase cyber security and resilience. *Availability, Reliability and Security (ARES) 2015: Proceedings of the 10th International Conference. Toulouse, France, 24–27 August, 2015*. IEEE, 2015. P. 686–692. DOI: 10.1109/ARES.2015.30.
58. Musman S. Assessing prescriptive improvements to a system's cyber security and resilience. *Systems Conference (SysCon) 2016: Proceedings of the Annual IEEE Conference. Orlando, FL, USA, 18–21 April, 2016*. IEEE, 2016. P. 1–6. DOI: 10.1109/SYSCON.2016.7490660.
59. Galinec D., Steingartner W. Combining cybersecurity and cyber defense to achieve cyber resilience. *Informatics 2017: Proceedings of the IEEE 14th International Scientific Conference. Poprad, Slovakia, 14–16 November, 2017*. IEEE, 2017. P. 87-93. DOI: 10.1109/INFORMATICS.2017.8327227.
60. Rak J., Papadimitriou D., Niedermayer H., Romero P. Information-driven network resilience: Research challenges and perspectives. *Optical Switching and Networking, 2017*. Vol. 23, Part 2. P. 156–178. DOI: <https://doi.org/10.1016/j.osn.2016.06.002>.
61. Поповский В.В. Основы теории телекоммуникационных систем. LAPLAMBERT Academical Publishing. 2018. 565 с.
62. Rec ITU. Y. 110. Global information infrastructure principles and framework architecture. 1998. 47 с.
63. Багатоканальний електрозв'язок та телекомунікаційні технології: підручник: у 2 ч. / О.В. Лемешко та ін.; за ред. В.В. Поповського. Харків: СМІТ, 2010. Ч. 1. 470 с.

64. Багатоканальний електрозв'язок та телекомунікаційні технології: підручник: у 2 ч. / О.В. Лемешко та ін.; за заг. ред. В.В. Поповського. Харків: СМІТ, 2010. Ч. 2. 482 с.
65. Vegesna S. IP Quality of Service (Cisco networking fundamentals). Cisco press. 2001. 232 p.
66. Osborne E.D., Simha A. Traffic engineering with MPLS. Cisco Press, 2002. 608 p.
67. ITU-T Recommendation G.107: The E-model: a computational model for use in transmission planning. Geneva. 2015. 30 p.
68. ITU-T Recommendation G.1030 Estimating end-to-end performance in IP networks for data applications. Geneva. 2014. 30 p.
69. ITU-T Recommendation G.1070 Opinion model for video-telephony applications. Geneva. 2015. 32 p.
70. Wang Y., Wang Z. Explicit routing algorithms for Internet Traffic Engineering. Proc. of 8th International Conference on Computer Communications and Networks. Paris, 1999. P. 582–588.
71. Seok Y., Lee Y., Kim C., Choi Y. Dynamic Constrained Multipath Routing for MPLS Networks. IEEE International Conference on Computer Communications and Networks. 2001. №3. P. 348–353.
72. Seok Y., Lee Y., Choi Y., Kim C. Dynamic Constrained Traffic Engineering for Multicast Routing. Proc. Wired Communications and Management. 2002. Vol. 2343. P. 278–288.
73. Лемешко А.В., Вавенко Т.В. Усовершенствование потоковой модели многопутевой маршрутизации на основе балансировки нагрузки. Проблемы телекомунікацій. 2012. № 1 (6). С. 12–29. URL: [http://pt.journal.kh.ua/2012/1/1/121\\_lemeshko\\_multipath.pdf](http://pt.journal.kh.ua/2012/1/1/121_lemeshko_multipath.pdf).
74. Segall A. The modeling of adaptive routing in data communications networks. IEEE Trans. on communications. 1975. Vol. 25, № 1. P. 85–95.
75. Поповский В.В., Лемешко А.В., Евсеєва О.Ю. Динамическое управление ресурсами ТКС: математические модели в пространстве состояний. Наукові записки УНДІЗ. 2009. № 1(9). С. 3–26.
76. Лемешко О.В., Євсеєва О.Ю., Симоненко Д.В. Модель динамічного балансування мережних ресурсів у телекомунікаційній мережі. Системи обробки інформації. 2008. Вип. 5(72). С. 71–74.
77. Yeremenko O., Lemeshko O. QoS Ensuring over Probability of Timely Delivery in Multipath Routing. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education. ICCSEEA 2018.

Advances in Intelligent Systems and Computing, Springer, Cham. 2018. Vol. 754. P. 244–254. DOI: [https://doi.org/10.1007/978-3-319-91008-6\\_25](https://doi.org/10.1007/978-3-319-91008-6_25)

78. Методи наукових досліджень в телекомунікаціях: навч. посіб.: у 2 т. / за ред. В.В. Поповського. Харків: СМІТ, 2013. Т. 1. 390 с.

79. Методи наукових досліджень в телекомунікаціях: навч. посіб.: у 2 т. / за ред. В.В. Поповського. Харків: СМІТ, 2013. Т. 2. 330 с.

80. Математичні основи теорії телекомунікаційних систем / за заг. ред. В.В. Поповського. Харків: СМІТ, 2006. 564 с.

81. Гуревич И.М. Динамическая модель сети связи // Теория телетрафика в системах информатики. Москва: Наука, 1989. С. 54–64.

82. Policy-based QoS management model for multiservice networks / O.V. Lemeshko, S.V. Garkusha, O.S. Yeremenko, A.M. Hailan. International Siberian Conference on Control and Communications (SIBCON), 21–23 May 2015, Omsk, Russia. Publisher: IEEE. P. 1–4.

83. Lemeshko A.V., Evseeva O.Yu., Garkusha S.V. Research on Tensor Model of Multipath Routing in Telecommunication Network with Support of Service Quality by Greate Number of Indices. Telecommunications and RadioEngineering, 2014, Vol. 73. No 15. P. 1339–1360.

84. Lemeshko O., Yeremenko O. Dynamic Presentation of tensor model for multipath QoS-routing. Modern Problems of Radio Engineering, Telecommunications and Computer Science. Proceedings of the international Conference TCSET'2016. – Lviv–Slavske, Ukraine, February 23–26, 2016: Publishing House of Lviv Polytechnic, 2016. P. 601–604.

85. Lemeshko O., Yevdokymenko M., Naors Y. Anad Alsaleem. Development of the tensor model of multipath QoE-routing in an infocommunication network with providing the required Quality Rating. Eastern-European Journal of Enterprise Technologies. 2018. Vol. 5. Issue 2 (95). P. 40–46. DOI: <https://doi.org/10.15587/1729-4061.2018.141989>.

86. Обзор и сравнительный анализ основных моделей и алгоритмов многопутевой маршрутизации в мультисервисных телекоммуникационных сетях. / В.В. Поповский и др. Прикладная радиоэлектроника. 2005. Том. 4. Вып. № 4. С. 372–382.

87. Лемешко О.В., Дробот О.А., Симоненко Д.В. Результати порівняльного аналізу поточкових моделей маршрутизації в телекомунікаційних мережах. Збірник наукових праць Харківського університету Повітряних Сил. 2007. Вип. 1(13). С. 66–69.

88. Евсева О.Ю., Гаркуша С.В. Обзор технологических и теоретических решений в области маршрутизации на основе качества обслуживания. Проблемы телекомунікацій. 2012. № 3 (8). С. 24 – 46. URL: [http://pt.journal.kh.ua/2012/3/1/123\\_evseeva\\_review.pdf](http://pt.journal.kh.ua/2012/3/1/123_evseeva_review.pdf).

89. Вишневский В.М. Теоретические основы проектирования компьютерных сетей. Москва: Техносфера, 2003. 512 с.

90. Lemeshko O.V., Arous K.M., Yeremenko O.S. Fault-Tolerant Unicast, Multicast and Broadcast Routing Flow-Based Models. Scholars Journal of Engineering and Technology. 2015. 3(4A). P. 343–350.

91. Лемешко А.В., Арус К.М. Модель отказоустойчивой маршрутизации многоадресных и широковещательных потоков в MPLS-сети. Системы обробки інформації. 2013. № 9 (116). С. 160–163.

92. Лемешко А.В., Арус К.М. Потокковые модели многоадресной и широковещательной маршрутизации в телекоммуникационных сетях. Проблемы телекомунікацій. 2013. № 1(10). С. 38–45. URL: [http://pt.journal.kh.ua/2013/1/1/131\\_lemeshko\\_multicast.pdf](http://pt.journal.kh.ua/2013/1/1/131_lemeshko_multicast.pdf).

93. Лемешко А.В., Ахмад М. Хайлан. Многоуровневое управление трафиком в сети MPLS–TE DiffServ на основе координационного принципа прогнозирования взаимодействий. Проблемы телекомунікацій. 2010. № 1(1). С. 35–44. URL: [http://pt.journal.kh.ua/2010/1/1/101\\_lemeshko\\_traffic.pdf](http://pt.journal.kh.ua/2010/1/1/101_lemeshko_traffic.pdf).

94. Лемешко А.В., Добрышкин Ю.Н., Дробот О.А. Результаты исследования модели управления трафиком с учётом задаваемых приоритетов для многопродуктового и многополюсного случаев. / Проблемы телекомунікацій. 2010. № 2(2). С. 33–41. URL: [http://pt.journal.kh.ua/2010/2/2/102\\_lemeshko\\_results.pdf](http://pt.journal.kh.ua/2010/2/2/102_lemeshko_results.pdf).

95. Разработка и анализ диакоптического метода междоменной маршрутизации с балансировкой нагрузки в телекоммуникационной сети / А.В. Лемешко и др. Проблемы телекомунікацій. 2018. № 1(22). С. 3–24. URL: [http://pt.journal.kh.ua/2018/1/1/181\\_lemeshko\\_diacoptic.pdf](http://pt.journal.kh.ua/2018/1/1/181_lemeshko_diacoptic.pdf).

## РОЗДІЛ 2

### ПОТОКОВІ МОДЕЛІ ТА МЕТОДИ ВІДМОВОСТІЙКОЇ МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

У розділі пропонується система теоретичних рішень щодо розв'язання задач відмовостійкої маршрутизації в ІКМ, представлених відповідними математичними моделями та методами, які можуть бути покладені в основу перспективних маршрутних протоколів. Нові та вдосконалені математичні моделі та методи охоплюють два основні варіанти організації відмовостійкої маршрутизації – без та з резервуванням елементів ІКМ. Маршрутні рішення без резервування елементів ІКМ ґрунтуються на реалізації багатопляхової маршрутизації без введення надлишковості в обсяги використаного мережного ресурсу, коли в разі відмови одного або декількох шляхів мережний трафік міг ще передаватися множиною працездатних маршрутів. Тому при розв'язанні задач відмовостійкої маршрутизації в цьому випадку накладаються додаткові обмеження на характер перетинання множини розрахованих шляхів, щоб відмова одного шляху мінімально впливала на працездатність інших маршрутів.

Моделі та методи відмовостійкої маршрутизації з резервуванням елементів ІКМ вводять надлишковість у використання мережного ресурсу. Тобто одночасно з множиною основних шляхів також розраховується і множина резервних маршрутів, на використання яких майже миттєво (50–60 мс) [1, 2] перемикаються потоки пакетів у разі відмови того чи іншого елемента мережі: шлюзу за замовчуванням, каналу, вузла або шляху, що підлягають захисту. У зв'язку з цим на рівні транспортної мережі подібні відмовостійкі рішення належать до засобів швидкої перемаршрутизації (Fast ReRoute, FRR). Запропоновані в розділі рішення для підвищення рівня QoS орієнтовані як на реалізацію вимог концепції Traffic Engineering (TE-FRR) щодо забезпечення збалансованого використання доступного мережного ресурсу, так і на захист рівня QoS за показником пропускної здатності (швидкості передачі пакетів).

#### **2.1. Маршрутизація як засіб забезпечення відмовостійкості ІКМ**

Незважаючи на постійне зростання надійності сучасного комунікаційного обладнання, проблема забезпечення заданого рівня відмовостійкості ІКМ також стоїть досить гостро. До основних глобальних причин відмов в ІКМ належать

масштабні катастрофи, соціально-політичні та економічні чинники, вторинні відмови, людський чинник (помилки людини-оператора), загрози мережній безпеці, екологічні проблеми тощо [3–12]. Крім того, серед основних технологічних чинників, що викликають відмови в обслуговуванні в мережі, виокремлюють збої фізичного рівня та перевантаження мережного обладнання в процесі його експлуатації, помилки під час конфігурації та оновлення термінального або мережного програмного забезпечення (рис. 2.1, табл. 2.1) [3–6]. У зв'язку з цим на сьогоднішній день надзвичайно актуальним є завдання, пов'язане з побудовою так званих відмовостійких мереж (Resilient Networks), здатних забезпечити високий рівень якості обслуговування та відмовостійкості (Quality of Resilience, QoR) [3, 4].

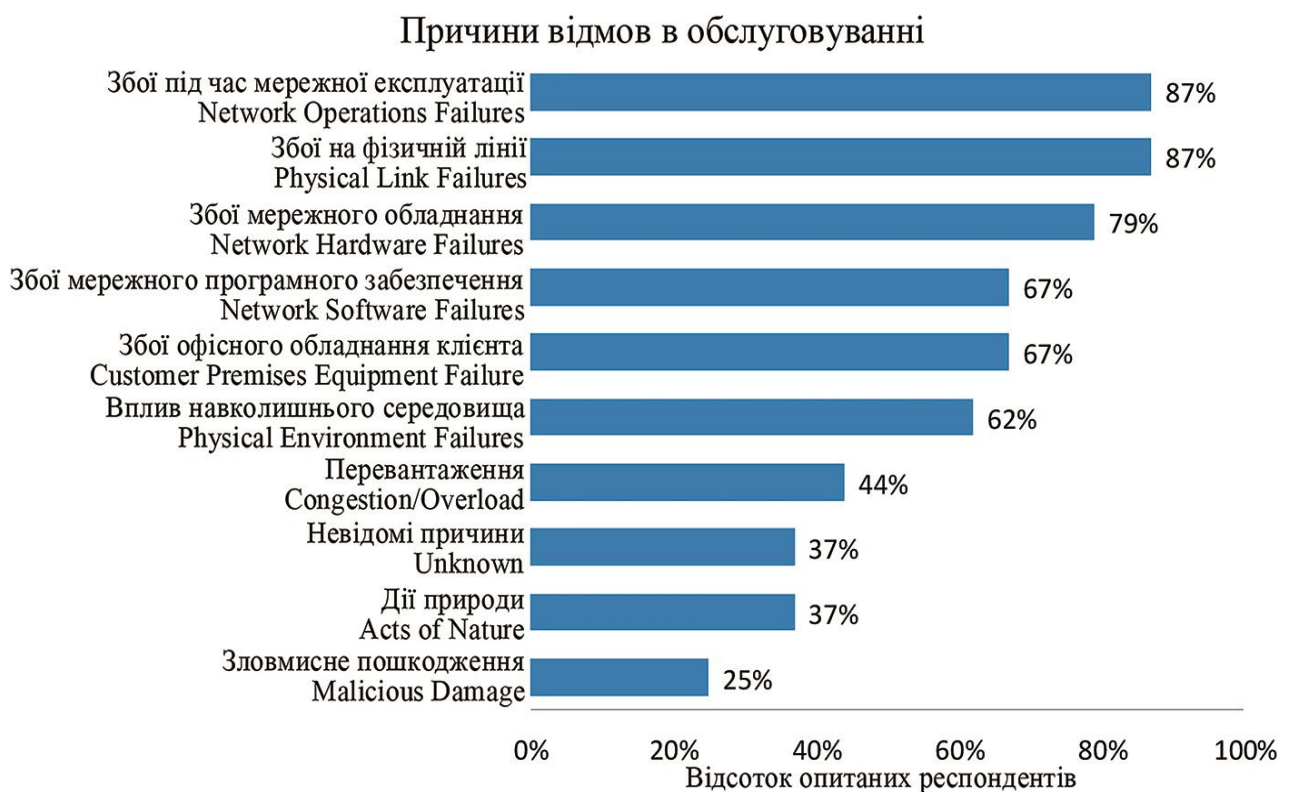


Рис. 2.1. Основні причини, що викликають відмови в обслуговуванні

Варто зазначити, що відмовостійкість мереж була визначена як окремий аспект забезпечення якості обслуговування, що зосереджує увагу на параметрах, пов'язаних із надійністю ІКМ. Надзвичайна важливість QoR обумовлена її значенням для функціонування мереж, а також впливає з широкого спектра технологій, що забезпечують диференційовану QoS кінцевим користувачам (рис. 2.2) [3, 5]. Вимірювані показники для кількісного визначення відмовостійкості вказані у відповідних стандартах ІТУ-Т та ІЕТФ [13–16].

## Типи відмов і відсоток їх появи

Типи виходу з ладу		Відсоток, %
Конфігурація оновлення	програмного забезпечення	22
	апаратного забезпечення	9
Збої програмного забезпечення	площина управління	15
	площина даних	5
	інші	5
Збій обладнання	управління	7
	карта введення/виведення	7
Відмови каналів зв'язку		20
Вимкнення електроенергії		1
Інші/невідомі		9

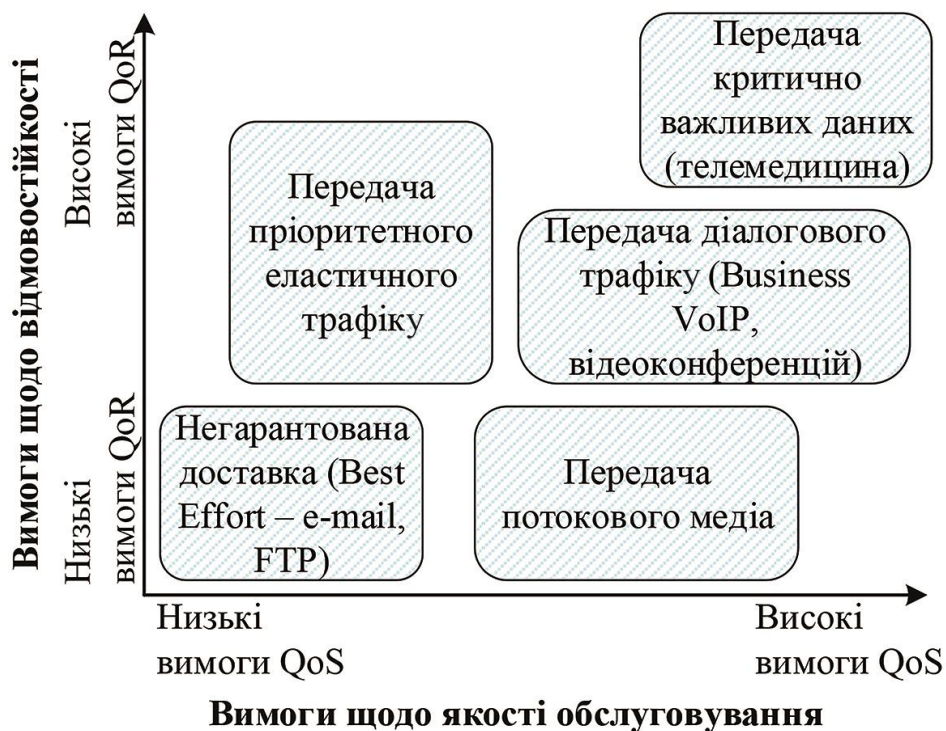


Рис. 2.2. Співвідношення вимог щодо якості обслуговування та відмовостійкості [5]

Основними засобами забезпечення відмовостійкості ІКМ є:

- інженерні методики організації експлуатації, технічного обслуговування та ремонту комунікаційного обладнання;
- засоби діагностики (самодіагностики) та перевірки (оцінки) працездатності елементів мережі;
- протоколи моніторингу та збирання інформації про стан мережі;

- засоби превентивного виявлення відмов елементів мережі та аналізу ймовірних несправностей;
- протоколи резервування (дуплікації) елементів мережі та її сегментів;
- протоколи маршрутизації та балансування навантаження;
- методи планування мережі з введенням структурної та функціональної надлишковості;
- методи реконфігурації мережі.

Отже, маршрутизація є одним з дієвих технологічних засобів забезпечення відмовостійкості ІКМ, що може реалізовуватися як у процесі визначення та використання найбільш надійних маршрутів (проактивне рішення), так і під час швидкої перемаршрутизації потоків у разі відмови та резервування елементів мережі (реактивне рішення).

## **2.2. Класифікація засобів відмовостійкої маршрутизації в ІКМ**

На сьогоднішній день класифікацію засобів відмовостійкої маршрутизації в ІКМ можна провести за такими критеріями (рис. 2.3) [1, 17–32]:

- за рівнем забезпечення резервування (захисту) елементів мережі;
- за типом підтримуваної схеми захисту;
- за підтримкою захисту рівня QoS;
- за місцем реалізації відмовостійкої маршрутизації в мережі;
- за типом використовуваної схеми резервування.

У разі відсутності резервування (захисту) елементів мережі та реалізації стратегії багатошляхової маршрутизації можуть використовуватися шляхи наступних класів. У шляхів, які не перетинаються, спільними є лише вузли відправника та отримувача. Якщо шляхи містять хоча б один спільний вузол та (або) канал, то вони називаються такими, що перетинаються. Якщо шляхи мають спільні вузли, тоді вони називаються шляхами, що перетинаються за вузлами, а якщо спільні канали – шляхами, що перетинаються за каналами (рис. 2.4).

Для забезпечення резервування (захисту) елементів мережі в процесі відмовостійкої маршрутизації передбачається розрахунок одночасно з основним ще й резервного шляху. Тоді в разі відмови елемента мережі з метою зменшення часу переривання обслуговування важливо не тільки скоротити час для того, щоб переорієнтувати трафік на резервний шлях (тобто дії перемикання щодо відновлення інколи містять розрахунок резервних шляхів після збою), але також зосередити увагу на інших етапах процедури



відновлення, зображених на рис. 2.5, які зазвичай складаються з виявлення та локалізації відмов, повідомлення про них та перемикання на резервний шлях щодо відновлення обслуговування [5].

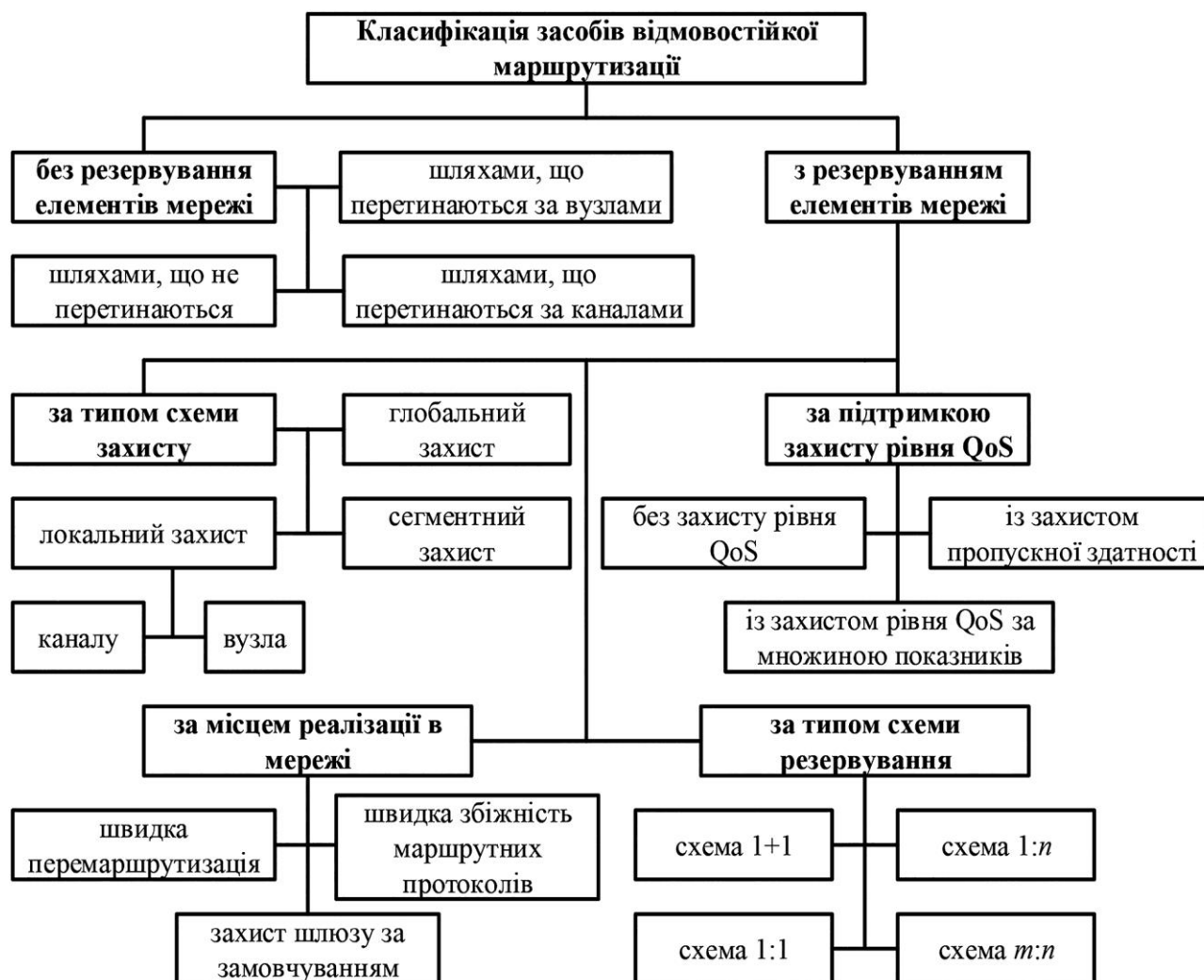


Рис. 2.3. Класифікація засобів відмовостійкої маршрутизації в ІКМ



Рис. 2.4. Класифікація шляхів за умови багатошляхової маршрутизації

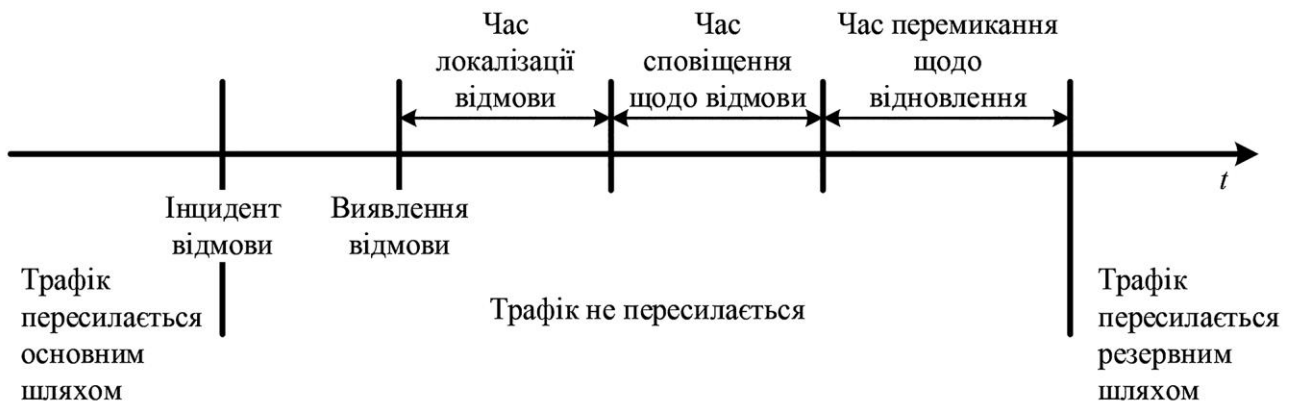


Рис. 2.5. Елементи процедури відновлення обслуговування

За типом підтримуваної схеми захисту в реалізації відмовостійкої маршрутизації в загальному випадку виокремлюють локальний захист (каналу, вузла), глобальний захист (шляху) та сегментний захист (множина елементів мережі) [5, 19, 20]. Схема захисту каналу (link protection) є найбільш простим рішенням і передбачає створення резервного маршруту в обхід аварійного каналу (рис. 2.6). За умови виявлення аварії маршрутизатор направляє потік пакетів на заздалегідь створений резервний маршрут. Пакети передаються резервним маршрутом до моменту розрахунку нового основного маршруту від відправника до отримувача.

Схема захисту вузла (node protection) використовується в разі відмови маршрутизатора (node failure). У цьому випадку резервний маршрут не повинен містити в собі вузол, який захищається. Фактично реалізація цієї схеми зводиться до захисту всіх каналів, безпосередньо підключених до вузла, який захищається (рис. 2.7). Схема захисту маршруту (path protection), наприклад, у мережах MPLS належить до глобальних механізмів захисту. У процесі реалізації захисту шляху основний і резервний маршрути можуть мати спільними лише вузли відправника та отримувача (рис. 2.8).

За підтримкою захисту рівня якості обслуговування виокремлюють засоби відмовостійкої маршрутизації без захисту рівня QoS, із захистом одного QoS-показника, як правило, пропускну здатності, та із захистом рівня QoS за множиною показників. У разі забезпечення захисту пропускну здатності відбувається резервування необхідного каналного ресурсу, потрібного для успішної передачі пакетів як основним, так і резервним маршрутом [5]. Схема захисту рівня QoS реалізується в тому випадку, коли доступності резервного шляху недостатньо, а необхідно гарантувати, що уздовж цього шляху буде необхідний обсяг пропускну здатності. Це особливо важливо для потоків пакетів, чутливих до пропускну здатності, затримки та джитеру.

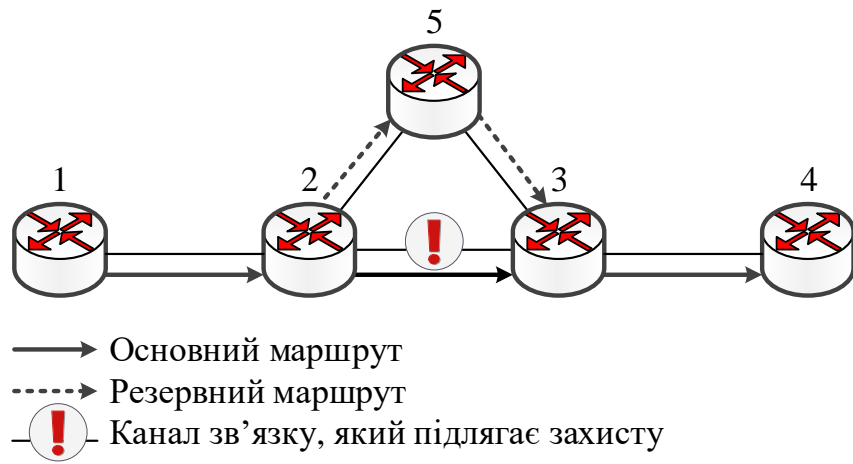


Рис. 2.6. Приклад реалізації схеми захисту каналу

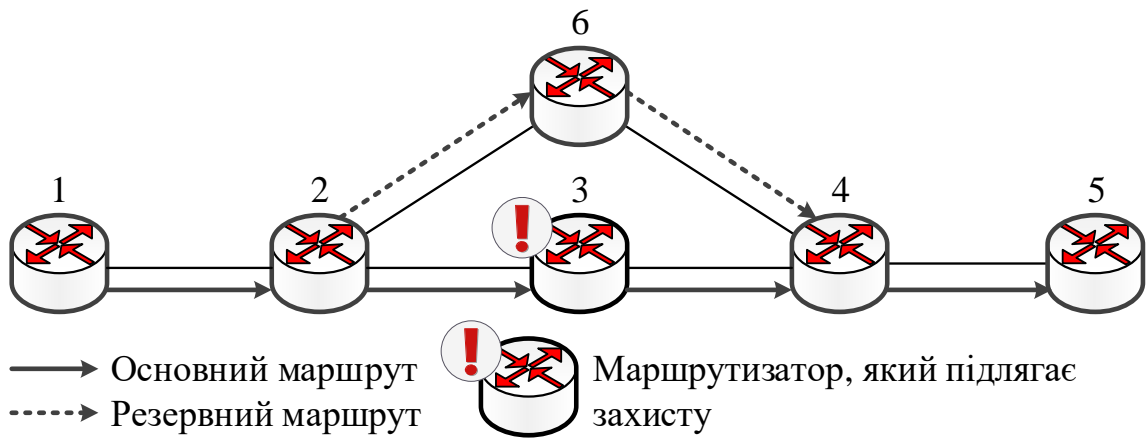


Рис. 2.7. Приклад реалізації схеми захисту вузла

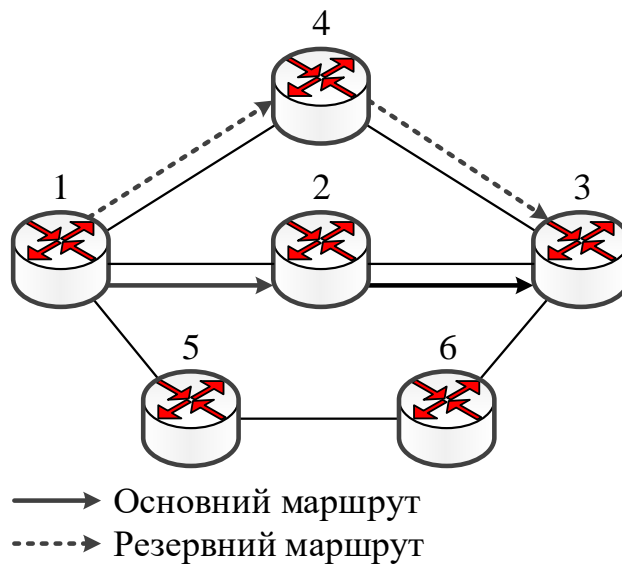


Рис. 2.8. Приклад реалізації схеми захисту маршруту

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. 2.9) [33].

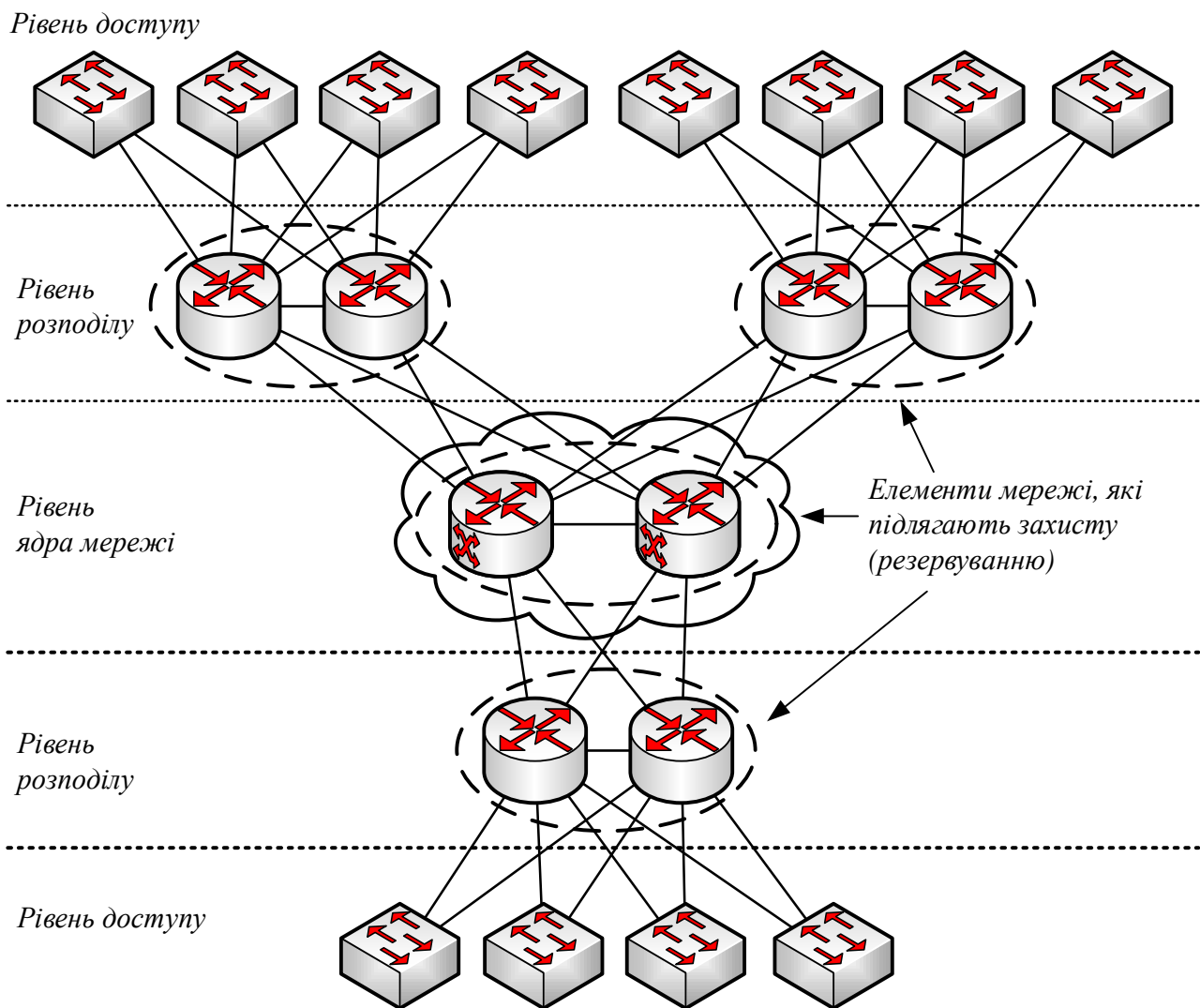


Рис. 2.9. Багаторівнева архітектура забезпечення відмовостійкості ІКМ

На рівні доступу задача відмовостійкої маршрутизації зводиться до захисту шлюзу за замовчуванням, тобто маршрутизатора, до якого комутується та чи інша мережа доступу. Це можливо організувати, коли мережі доступу комутуються одночасно до декількох приграничних маршрутизаторів, інтерфейси яких конфігуруються відповідним протоколом як віртуальний шлюз за замовчуванням. В IP-мережах до таких протоколів належать Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Gateway Load Balancing Protocol (GLBP), Common Address Redundancy Protocol (CARP) [24–27].

Для підвищення доступності приграничних маршрутизаторів у разі відмови основного шлюзу протокол в автоматичному режимі здійснює перемикання потоків на резервний шлюз. Так, наприклад, за умови застосування протоколу VRRP аналізується стан мережі та визначається інтерфейс віртуального маршрутизатора, який у подальшому використовується мережею доступу для підключення до транспортної мережі. Крім того, балансування навантаження за декількома інтерфейсами віртуального маршрутизатора здатне підвищити доступність і надійність з'єднання, однак така функціональність не властива всім протоколам (табл. 2.2) [24, 27].

Таблиця 2.2

### Порівняння протоколів резервування шлюзу за замовчуванням

Характеристика	HSRP	VRRP	GLBP	CARP
Застосування	Cisco Proprietary	IEEE Standard	Cisco Proprietary	Not a standard (BSD based OS)
Стандарт	RFC 2281	RFC 5798	Ні	Ні
Рівень моделі OSI	Мережний	Мережний	Канальний	Мережний
Балансування навантаження	Не підтримується	Підтримується	Підтримується	Підтримується
IPv6	Підтримується	Підтримується	Підтримується	Підтримується
Переваги	– легка конфігурація; – низьке навантаження мережі службовим трафіком.	– спрощене управління мережею; – висока адаптованість; – низьке навантаження мережі службовим трафіком; – балансування навантаження; – мінімізація обчислювальних витрат.	– ефективне використання мережних ресурсів; – висока доступність; – автоматичне балансування навантаження; – низькі витрати на адміністрування; – ефективне проектування рівня доступу.	– відкрита альтернатива HSRP і VRRP; – резервування для брандмауерів та маршрутизаторів; – балансування навантаження.
Недоліки	– неефективний для передачі трафіку реального часу; – слабкий рівень безпеки; – пропрієтарний протокол Cisco.	– слабкий рівень безпеки (не містить жодного типу автентифікації).	– пропрієтарний протокол Cisco; – висока складність управління мережею.	– несумісність з чинними стандартами; – слабкий рівень безпеки.

Найбільш суттєвими недоліками наявних рішень щодо відмовостійкої IP-маршрутизації вважаються такі:

- не враховується потоковий характер мережного трафіку;
- обмежені можливості для балансування навантаження з необхідністю адміністративної конфігурації;
- відсутність узгодженого рішення взаємопов'язаних завдань вибору шлюзу за замовчуванням і маршрутизації у транспортній мережі.

Наприклад, як показано в [24], для забезпечення балансування навантаження за інтерфейсами шлюзів за замовчуванням можуть використовуватися такі механізми: Round Robin та Weighted (зважене) в GLBP, Host-dependent у GLBP та VRRP.

Метод Round Robin передбачає рівномірне балансування навантаження за всіма інтерфейсами віртуального шлюзу, що є прийнятним рішенням лише у разі приблизно однакової доступності приграничних маршрутизаторів транспортної мережі. В іншому випадку доцільно використовувати зважене балансування навантаження, у якому трафік, що надходить від мереж доступу, розподіляється між інтерфейсами віртуального маршрутизатора пропорційно їх адміністративній вазі. Третій механізм (host-dependent) реалізує псевдобалансування, коли певний віртуальний інтерфейс шлюзу для однієї мережі доступу є основним інтерфейсом, а для іншої мережі доступу – резервним. Таким чином, для забезпечення нерівномірного балансування навантаження між приграничними маршрутизаторами транспортної мережі з різною доступністю необхідно адміністративно проводити додаткову конфігурацію обладнання.

Ці механізми балансування значно знижують швидкість реакції мережі на можливі збої та обмежують функціональність мережних рішень для захисту шлюзів (резервування). Крім того, навіть у разі оптимізації балансування навантаження для захисту шлюзу відсутня гарантія, що після вибору шлюзу за замовчуванням у транспортній мережі є маршрут, який має необхідну пропускну здатність 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.

На рівні ядра мережі функціонал відмовостійкої маршрутизації, як правило, здійснюється в межах технологій швидкої IGP/BGP конвергенції (Fast IGP/BGP convergence) та швидкої перемаршрутизації (Fast ReRoute), які реалізуються в мережах IP та MPLS [1]. У межах технології Fast IGP/BGP convergence забезпечується мінімізація часу реакції ІКМ на можливі відмови

її елементів [1, 17–23, 28–30]. Цей процес ще називається збіжністю мережі (network convergence) або процесом синхронізації таблиць маршрутизації після зміни топології. У загальному випадку під час збіжності необхідно використати час на такі процеси:

- виявлення аварії в мережі;
- передача інформації про аварію, тобто поширення LSA (Link-state advertisement) у мережі;
- обчислення найкоротших шляхів на всіх маршрутизаторах у разі отримання нової інформації про стан ІКМ;
- оновлення маршрутних таблиць на всіх маршрутизаторах у мережі.

Скоротити час збіжності в межах технології IP Fast ReRoute (IP FRR) можна за рахунок зменшення часу виявлення аварії, таймера протоколу Hello; затримок у разі поширення інформації LSA (LSA/LSP flooding) на підставі використання алгоритму експоненційного відтермінування, який дозволяє динамічно розрахувати затримку для генерації LSA; затримок оброблення тощо. Адміністративне зменшення кожного з цих часових параметрів може негативно позначитися на обсягах службового трафіку, що циркулює в мережі, тобто спричинити його неконтрольоване зростання. Тому поряд з вибором у розумних межах значень перелічених параметрів необхідно реалізовувати і доступні схеми резервування ресурсів мережі.

Технологія Fast ReRoute застосовується в IP/MPLS-мережах для захисту елементів транспортної мережі – каналу, вузла, шляху та пропускної здатності мережі загалом. В IP-мережах для підвищення відмовостійкості використовується технологія IP FRR [18, 28], яка багато в чому аналогічна технології Fast ReRoute, що функціонує в мережах MPLS-TE. Метою технології IP FRR є знаходження альтернативного шляху передачі пакетів у разі можливої несправності каналу або вузла мережі без виникнення мікропетель (microloops). За умови швидкої перемаршрутизації застосовуються протоколи IP-мереж, такі як OSPF та I-IS-IS. Якщо маршрутизатор знає про декілька маршрутів з рівною метрикою (вартістю) (Equal Cost MultiPaths, ECMP) від відправника до отримувача, а деякі з них не мають аварійних каналів або вузлів, то такі шляхи можна використовувати як резервні. За відсутності таких шляхів маршрутизатор шукає безпосередньо підключеного сусіда, який має маршрут, що не містить аварійного каналу/вузла до отримувача. Такий шлях через безпосередньо підключеного сусіда називають альтернативним маршрутом без петель (Loop Free Alternate, LFA) [21].

У разі способу альтернативного U-обходу (U-turn Alternates), якщо шляхи ESMR/LFA недоступні, маршрутизатор може сформувати обхідний шлях за рахунок відправлення пакетів у напрямку відправника (джерела), але через інший маршрутизатор, у якого в таблиці маршрутизації може зберігатися альтернативний шлях до вузла призначення. Шляхи відновлення через такі маршрутизатори називають шляхами відновлення мультитранзитної ділянки, і стандартний спосіб такого відновлення представлений у RFC 5714 [28]. На цей час запропоновано декілька варіантів реалізації способів альтернативного U-обходу [1]:

- пряма вказівка в заголовку IP-пакета на заборону пересилання пакета маршрутизатора, у якого відмовив канал [34];
- відправлення пакета іншому маршрутизатору, який має альтернативні відношення зв'язності з ділянкою, у якій розміщений вузол-отримувач;
- використання маршрутизаторами декількох топологічних конфігурацій дерев найкоротших маршрутів (мультитопологій) з можливістю переходу між ними в разі відмови каналу [29];
- тунелювання трафіку в напрямку U-обходу елемента, що відмовив, до місця, де може бути продовжена його безаварійна передача.

Також слід зазначити, що технології IP/MPLS-мереж, як і більшість рішень, пов'язаних з підвищенням мережної надійності, ґрунтуються на реалізації різноманітних схем резервування [1, 5, 35]:

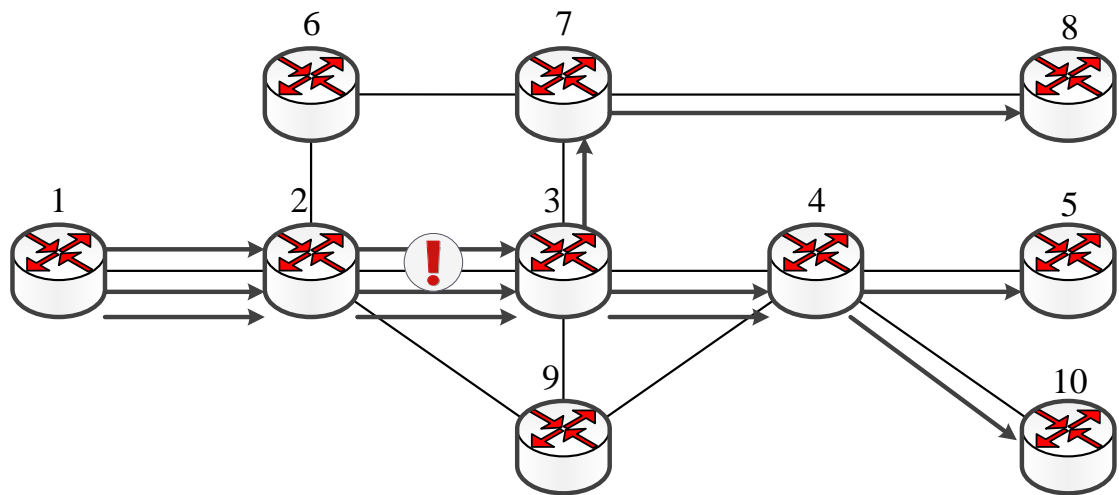
- схема 1+1, за якої потік пакетів передається одночасно і основним, і резервним маршрутами;
- схема 1:1, коли для кожного робочого маршруту створюється резервний шлях, який не повинен містити проблемний елемент мережі (канал або вузол);
- схема 1:n, за якої створюється *один* резервний шлях для *n* основних шляхів (*facility backup*);
- схема *m:n*, коли створюється *m* резервних шляхів для *n* основних шляхів.

Приклад застосування схеми 1:1 у випадку необхідності захисту каналу зв'язку та вузла показано на рис. 2.10 і 2.11 відповідно.

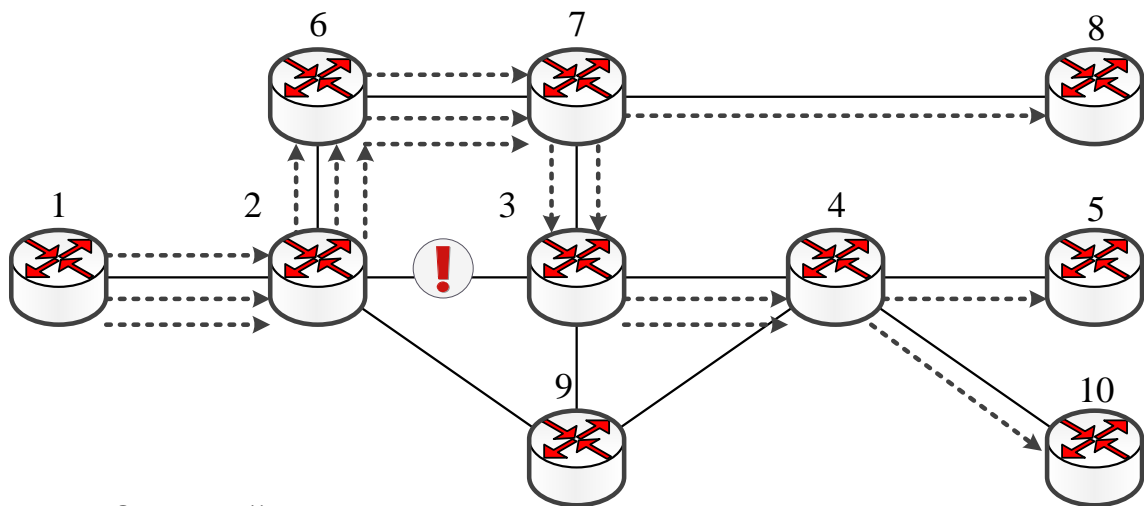
З точки зору використання пропускної здатності політики щодо відмовостійкості класифікуються на виділені (*dedicated*) та спільні (*shared*) механізми. У виділеній схемі захисту певний обсяг пропускної здатності зарезервовано для перемаршрутизації кожного потоку. Навпаки, у разі застосування механізму спільного захисту резервна пропускна здатність може спільно використовуватися (ділитися) між потоками, на які не впливають одні й ті самі відмови. Це дозволяє зменшити обсяг необхідного для резерву мережного ресурсу, але призводить до ускладнення обчислювальних завдань. На вибір



схеми відновлення/захисту також впливає протокол маршрутизації, що застосовується. Наприклад, у технології MPLS дозволяється явно обирати шлях для кожного потоку пакетів, гарантуючи тим самим більш гнучку політику маршрутизації та дозволяючи використання схеми захисту шляху. Тоді відповідно до протоколу OSPF маршрутизація відбувається за допомогою дерев найкоротших шляхів, і зазвичай застосовується саме схема відновлення.



а) застосування основного шляху



- > Основний маршрут
- - -> Резервний маршрут
- ! Канал зв'язку, який підлягає захисту

б) використання резервного шляху

Рис. 2.10. Приклад реалізації схеми захисту каналу зв'язку в разі використання схеми резервування 1:1

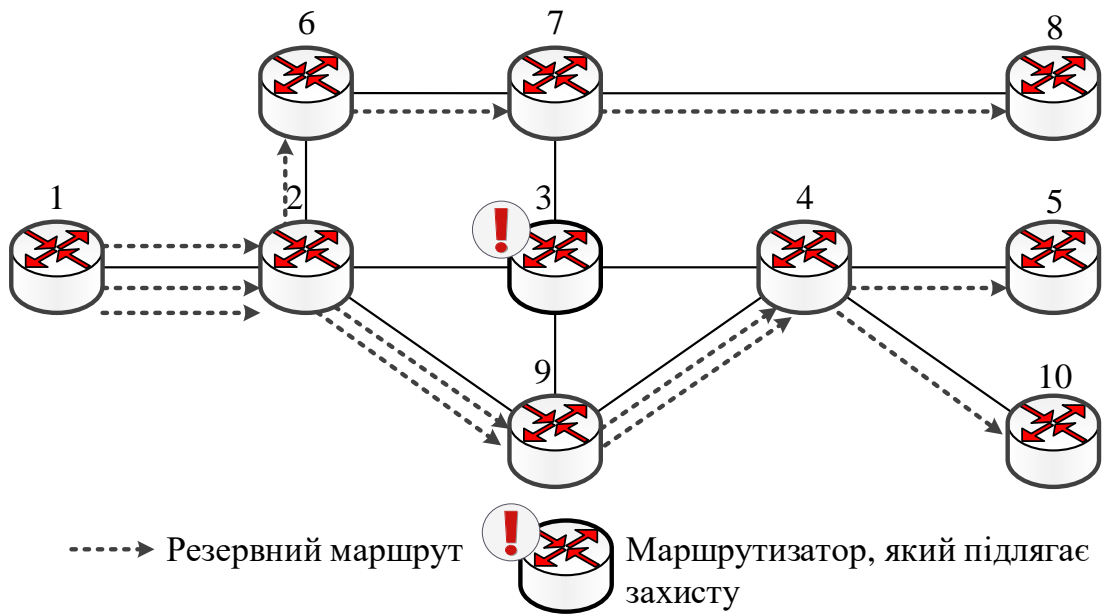


Рис. 2.11. Приклад визначення резервного шляху під час захисту вузла з використанням схеми резервування 1:1

Застосування механізму спільного захисту продемонстровано для реалізації схеми резервування 1: $n$  на рис. 2.12. У цьому випадку розраховується один резервний шлях для  $n$  основних шляхів і реалізується так звана схема *facility backup*, за рахунок чого підвищується масштабованість отримуваних рішень щодо відмовостійкої маршрутизації.

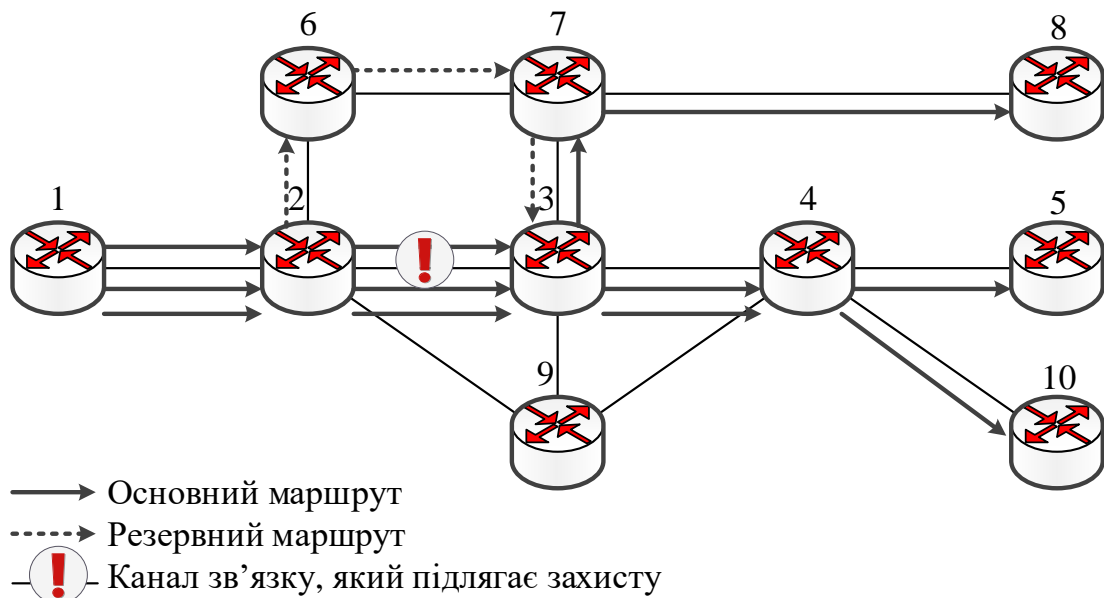


Рис. 2.12. Приклад захисту каналу зв'язку за умови використання схеми 1: $n$

У випадку відмови вузла схема 1:n його захисту залежно від топології мережі може бути більш складною, що показано на рис. 2.13. Тут резервними (обхідними) є кілька каналів зв'язку, які є спільними елементами єдиного резервного маршруту для декількох основних.

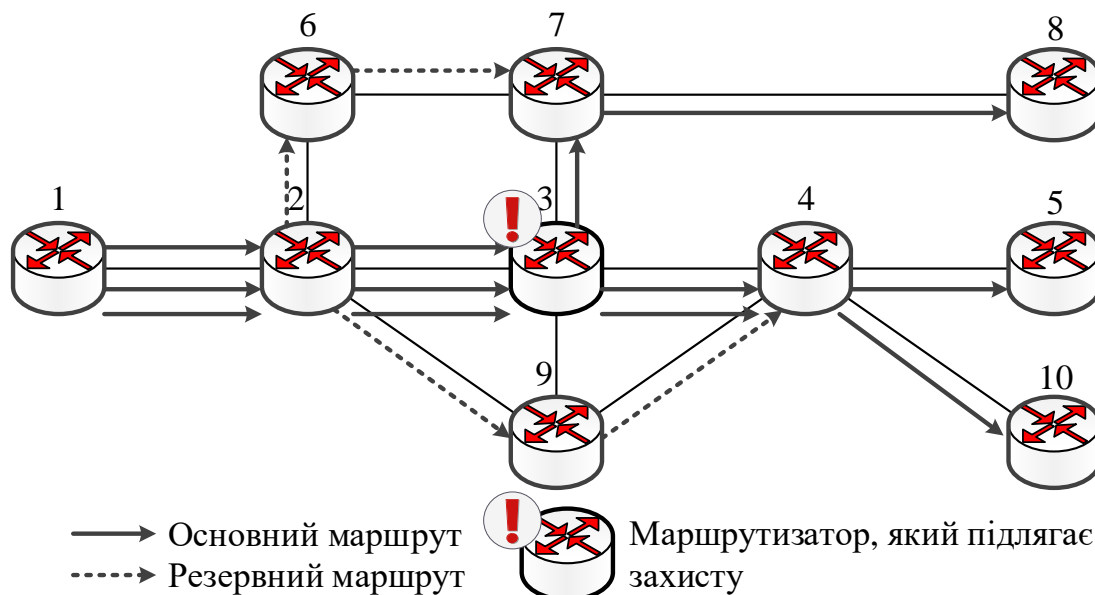


Рис. 2.13. Приклад захисту вузла в разі застосування схеми резервування 1:n

Отже, можна зробити висновок, що розглянуті протокольні рішення орієнтують на підвищення відмовостійкості мережі на підставі введення ресурсної надлишковості, пов'язаної з реалізацією тієї чи іншої схеми захисту елементів ІКМ. Тобто підвищення надійності ІКМ супроводжується необхідністю залучення додаткових обсягів каналного та буферного ресурсу, що негативно впливає на продуктивність мережі загалом. Тому за умови відмовостійкої маршрутизації дуже важливо забезпечити збалансоване використання доступного мережного, насамперед каналного, ресурсу, основане на ефективному балансуванні навантаження в ІКМ, щоб захист елементів мережі не призвів до її перевантаження та істотного зниження рівня QoS. Науково-практичному напрямку реалізації швидкої перемаршрутизації з балансуванням навантаження в мережах MPLS (MPLS Traffic Engineering Fast ReRoute, MPLS TE FRR) також присвячено досить багато технологічних рішень [31, 32].

Як показав проведений аналіз [1, 3–6, 14–32], у процесі реалізації відмовостійкої маршрутизації в SDN виникають певні особливості. Зокрема залежно від місця розташування мережного елемента, який відмовив, ця проблема охоплює три основні площини: площину передачі даних; площину управління; площину комунікацій між елементами площин даних та

управління. Особливо гостро проблема забезпечення відмовостійкості постає на рівні інфраструктури через наявність на ньому великої кількості різнотипних мережних елементів (комутаторів, маршрутизаторів, шлюзів, каналів зв'язку тощо) і впливу широкого спектра чинників, що спричиняють відмови (рис. 2.1). Водночас важливо врахувати, що централізація функцій щодо управління трафіком у SDN негативно позначається на масштабованості протокольних рішень щодо відмовостійкої маршрутизації. Тому ці задачі в SDN зазнають певної модифікації як на рівні їх постановки, так і отримання кінцевого рішення, що й буде розглянуто в подальших підрозділах цієї роботи.

### 2.3. Аналіз моделей і методів відмовостійкої маршрутизації в ІКМ

Аналіз відомих рішень щодо відмовостійкої маршрутизації взагалі та швидкої перемаршрутизації зокрема [36–62] дозволив сформулювати перелік ключових вимог, яким повинні відповідати перспективні рішення в цій сфері і, насамперед, математичні моделі та методи, на яких вони ґрунтуються:

- урахування потокового характеру трафіку, що є відмінною рисою більшості мультимедійних послуг і обов'язковим моментом у реалізації схем захисту пропускної здатності та інших показників якості обслуговування в мережі;
- оптимізаційна постановка задачі: орієнтація на оптимізацію використання наявного мережного ресурсу;
- висока масштабованість рішень щодо відмовостійкої маршрутизації;
- підтримка базових схем захисту мережних елементів (вузла/каналу зв'язку/шляху/пропускної здатності);
- узгоджене вирішення окремих завдань відмовостійкої маршрутизації, наприклад, захист шлюзу за замовчуванням, швидка перемаршрутизація тощо;
- розширення можливостей наявних рішень щодо підтримки балансування навантаження, пов'язаних з реалізацією багатошляхової стратегії маршрутизації з відповідною підтримкою схем захисту не одного шляху, а мультишляху, тобто декількох шляхів, якими передаються пакети одного і того ж потоку;
- прийнятна обчислювальна складність рішень маршрутизації.

Серед евристичних алгоритмів відмовостійкої маршрутизації розглянемо найбільш вагомі, які були виокремлені під час проведеного аналізу робіт [36–46]. Так, у роботі [36] запропоновано адаптивний евристичний алгоритм відмовостійкої маршрутизації на основі використання графа  $(n, k)$ -зірки, який має широкі властивості щодо масштабованості. Автори реалізують ідею

зібрання інформації, яка використовується в процесі маршрутизації на графі  $n$ -зірки, для застосування на графі  $(n, k)$ -зірки  $(S_{n,k})$  (рис. 2.14).

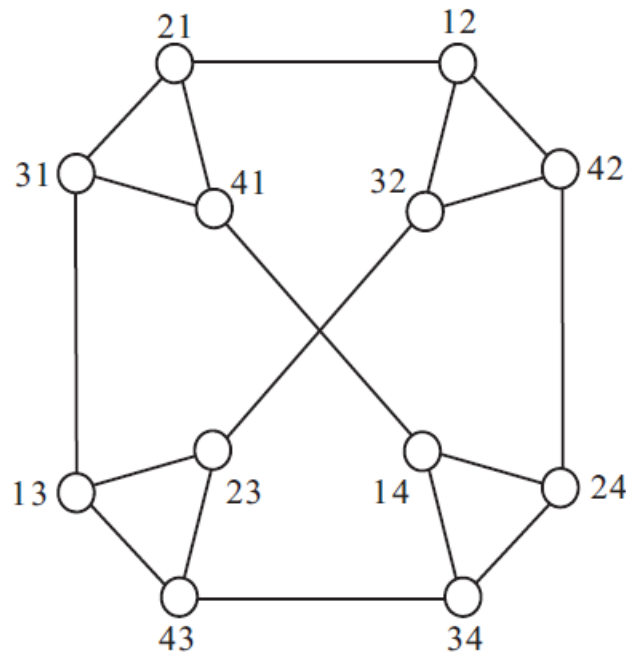


Рис. 2.14. Приклад графа  $(4, 2)$ -зірки  $(S_{4,2})$

У цьому випадку кожен вузол  $S_{n,k}$  ідентифікується за допомогою перестановки  $k$ , вибраної з  $\{1, 2, \dots, n\}$ , де  $n$  та  $k$  (якщо  $1 \leq k \leq n-1$ ) є кількістю доступних для вибору та вибраних символів відповідно. Також авторами [36] запропоновано використання ймовірнісного вектора безпеки (Probabilistic Safety Vector, PSV) та розроблено алгоритм маршрутизації з метою визначення безвідмовного маршруту за допомогою PSV. Зазначимо, що ефективність маршрутизації PSV погіршується зі збільшенням відсотка вузлів, які відмовили, особливо за умови перевищення порогу відмов вузлів у 25%. Для підвищення ефективності маршрутизації з більшим відсотком відмов вузлів також запропоновано адаптивний метод визначення порогу для PSV. Одночасно ефективність маршрутизації оцінювалася за середньою довжиною шляхів. Перевагами цього методу можна вважати його прийнятну обчислювальну складність.

У роботі [37] авторами запропоновано евристичний алгоритм відмовостійкої маршрутизації в mesh-мережах на основі мурашиного алгоритму пошуку оптимального шляху, коли враховуються вузли, що відмовили. У цьому випадку для розв'язання задачі відмовостійкої маршрутизації в запропонованому алгоритмі використовувався алгоритм оптимізації мурашиної колонії (Ant Colony Optimization, ACO) за умови застосування кольорових

феромонних мурах для подолання проблеми відновлення функціонування мережних елементів. Запропоноване рішення порівнювалося з алгоритмом відмовостійкої маршрутизації в mesh-мережах з використанням збалансованого кільця [37]. Результати моделювання показали, що запропонований алгоритм швидко реагував на відмови в мережі, щоб у кожний момент часу можна було вибрати оптимальний шлях від відправника до отримувача. Продуктивність алгоритму було підвищено за допомогою оновлень мурах з метою інформування інших вузлів про виявлений найкоротший шлях.

У праці [38] було запропоновано алгоритми відмовостійкої маршрутизації для ієрархічних дуальних мереж (Hierarchical Dual-Net, HDN) з обмеженою чи довільною кількістю вузлів, що відмовили. Зокрема HDN побудовано на основі симетричного графа, що називається базовою мережею, як тривимірний тора та  $n$ -вимірний гіперкуба. Наведені алгоритми дозволяють знайти маршрут без відмов між відправником та отримувачем за умови відомої множини вузлів, що відмовили.

У статті [39] авторами розроблено механізм швидкої перемаршрутизації в IP-мережах із використанням кістякових дерев із коренем, які не перетинаються за дугами, що гарантує відновлення від збоїв  $(k - 1)$  каналів зв'язку в мережі, яка описується  $k$ -реберно зв'язним графом. Оскільки кістякові дерева, які не перетинаються за дугами (рис. 2.15), можуть бути побудовані за час, пропорційний квадрату розміру мережі, запропонований підхід забезпечує високу масштабованість. Крім того, проведені експериментальні результати показали, що використання кістякових дерев, які не перетинаються за дугами, для відновлення після декількох відмов зменшує довжину шляху порівняно з раніше відомими методами.

Відомо, що інколи під час відмовостійкої маршрутизації виникає задача визначення шляху між двома вузлами в мережі, які повинні проходити через певні транзитні вузли. Наприклад, це може знадобитися у випадку, коли трафік, що передається, має бути проаналізований за допомогою глибокої перевірки пакетів з міркувань мережної безпеки на деякому специфічному вузлі мережі. Так, у статті [41] пропонується нова рекурсивна евристика для пошуку найкоротшого маршруту без циклів від вузла відправника до вузла отримувача, який відвідує певний набір транзитних вузлів у мережі. Для забезпечення стійкості до відмов уздовж шляху було запропоновано евристичний підхід, який модифікувався для того, щоб захистити розрахований шлях за допомогою відповідного резервного шляху, який не перетинається з основним за вузлами. Працездатність запропонованої евристики

в обчисленні шляху із захистом і без нього оцінювалася порівняно із розв'язанням цієї задачі методами цілочисельного лінійного програмування (Integer Linear Programming, ILP). У цьому випадку методи ILP можуть не отримати шукане рішення протягом заданого часу. Особливо це стосується мереж великої розмірності, що виправдовує необхідність розроблення саме евристичних алгоритмів.

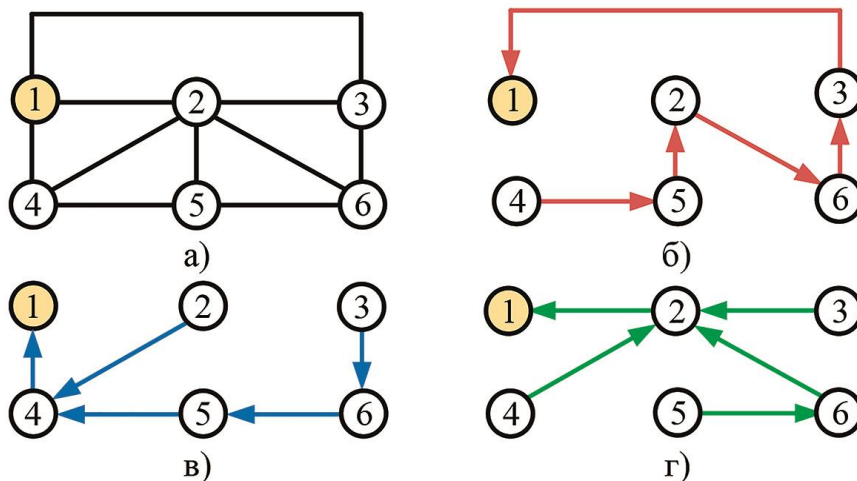


Рис. 2.15. Приклад дерев, які моделюють розв'язання задачі перемаршрутизації шляхами, що не перетинаються за каналами зв'язку:

а – мережа; б – червоне дерево; в – синє дерево; г – зелене дерево

Розглянемо ефективні графові та комбінаторні рішення щодо відмовостійкої маршрутизації, представлені в працях [47–52]. У роботі [47] запропоновано нові алгоритми відмовостійкої 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 один із сусідніх вузлів, щоб відправити повідомлення, беручи до уваги приблизні маршрутні ймовірності. Проведене авторами комп'ютерне моделювання підтвердило ефективність запропонованих алгоритмів [47].

Відомо, що вузли безпроводових сенсорних мереж (Wireless Sensor Networks, WSN) можуть швидко виходити з ладу, що призводить до відмов під час маршрутизації та блокування зв'язку. У свою чергу в роботі [48] запропоновано алгоритм відмовостійкої маршрутизації на основі використання структурованих орієнтованих графів де Брюїна (Fault-Tolerant Routing Based on the Structured Directional de Bruijn Graph, FTRSDDDB) для підвищення ефективності маршрутизації для WSN. Алгоритм випадково розгортає деякі супервузли (super nodes) з великим запасом енергії та потужною

продуктивністю у WSN. Ці вузли відповідальні за збирання топологічної інформації з WSN для створення таблиці маршрутизації з резервуванням, а також для надання послуг передачі даних та маршрутизації для інших вузлів (popular nodes). Алгоритм FTRSDDDB оптимізує топологічну структуру мережі, використовуючи граф де Брюїна, і може швидко знайти сусідні вузли, які відмовили, та недійсний маршрут, а потім обчислити новий маршрут з низькою умовною вартістю, що значно підвищує продуктивність відмовостійкої маршрутизації у WSN. Проведені експериментальні дослідження показали високу ефективність алгоритму FTRSDDDB порівняно з іншими алгоритмами відмовостійкої маршрутизації (Gossiping, DD, Low Energy Adaptive Clustering Hierarchy (LEACH)), навіть в умовах атак шкідливих вузлів у WSN.

У дослідженні [49] було запропоновано модель відмовостійкої маршрутизації на основі графа зірки з векторами безпеки (безвідмовності). У цьому випадку використання вектора безпеки здатне забезпечувати ефективну відмовостійку маршрутизацію в ІКМ на основі шаблонів маршрутів. Виходячи з концепції шаблону маршрутів, спочатку визначається неорієнтований вектор безпеки. Крім того, авторами запропоновано кілька методів розв'язання задач щодо визначення довжини векторів безпеки та класифікації шаблонів маршрутів [49].

У працях [50, 51] було запропоновано моделі відмовостійкої маршрутизації на основі рівнів безпеки із застосуванням млинцевих графів та графів «гіперзірка». Крім того, було проведено порівняння таких типів графів, як «гіперзірка», «зірка», «гіперкуб» та «млинцевий граф» щодо ефективності їх використання за умови відмовостійкої маршрутизації.

У роботі [52] досліджено можливості застосування для підвищення відмовостійкості ІКМ циркулянтних графів, які забезпечують високу гнучкість щодо кількості вузлів та зв'язності мережі (рис. 2.16). Запропоновано архітектуру оптичної мережі на основі циркулянтного графа спільно з відмовостійкою маршрутизацією. Показано, що підвищення зв'язності мережі допомагає зменшити необхідну кількість використаних довжин хвиль для одночасної взаємодії між усіма вузлами. Також у [52] розроблено модель оцінки надійності з'єднання в разі відмови як вузлів, так і каналів зв'язку мережі. Зокрема із застосуванням запропонованого алгоритму надійність зростала майже лінійно із зростанням зв'язності мережі в логарифмічному масштабі.

Проте найбільш перспективними та ефективними є саме потокові моделі та методи відмовостійкої маршрутизації [4–6, 53–59], оскільки вони враховують поточковий характер трафіку, що передається в сучасних ІКМ.



У цьому випадку технологічна задача відмовостійкої маршрутизації формулюється в оптимізаційній формі, орієнтуючи на оптимізацію використання мережних ресурсів та допускаючи реалізацію схем захисту пропускної здатності мережі.

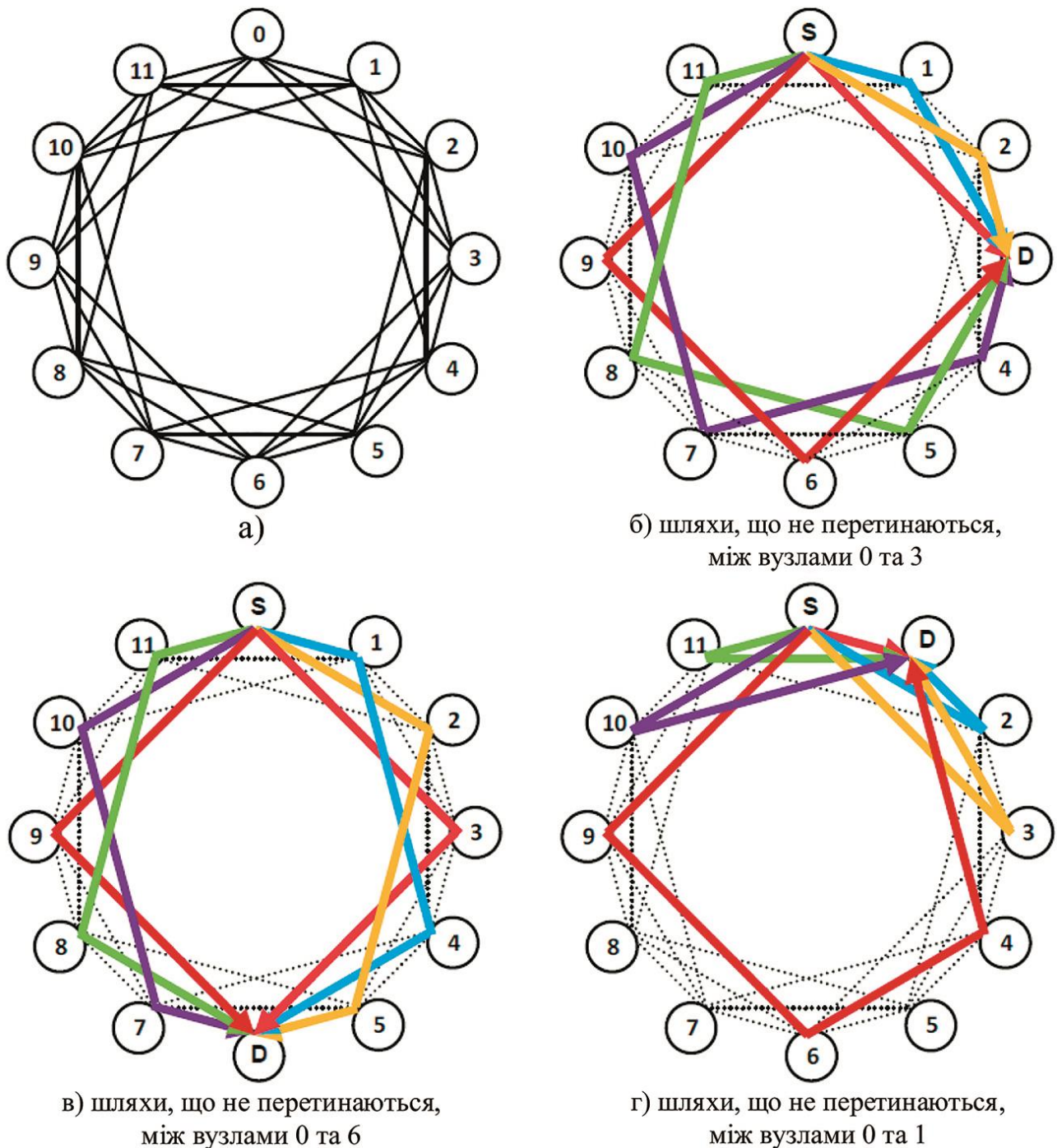


Рис. 2.16. Архітектура мережі на основі циркулянтного графа та приклади відмовостійкої маршрутизації шляхами, що не перетинаються за вузлами

Відомо, що основні та резервні шляхи у разі швидкої перемаршрутизації MPLS можуть бути визначені як найкоротші шляхи відповідно до умовної вартості каналів зв'язку або як явно розраховані довільні шляхи. В обох

випадках вибір маршруту можна оптимізувати таким чином, щоб максимальну завантаженість каналів зв'язку для множини розглянутих сценаріїв відмов було мінімізовано. У статті [53] авторами запропоновано лінійну оптимізаційну модель для розрахунку шляхів як у випадку реалізації одношляхової стратегії маршрутизації, так і за умови багатошляхової маршрутизації з метою забезпечення балансування навантаження. Отримані авторами результати щодо завантаженості каналів зв'язку у використанні запропонованої лінійної моделі під час одношляхової та багатошляхової маршрутизації було порівняно з відповідними значеннями для шляхів, розрахованих згідно зі стандартними процедурами для IP-мереж, що дозволило визначити вигоду у використанні мережних ресурсів.

У свою чергу робота [54] присвячена вирішенню завдання мінімізації споживання енергії у відмовостійких ІКМ. У використанні підходу, запропонованого авторами, для кожного запиту має бути надана пара шляхів (основний та резервний), що не перетинаються за каналами зв'язку, і використовується спільна схема захисту (резервування). Споживання енергії здійснюється лише тими каналами зв'язку, що використовуються за відсутності відмов, але мережний ресурс задіюється як основним, так і резервним шляхами. Отже, автори [54] пропонують механізм спільного захисту (*shared protection*), який не залежить від відмов, у разі MPLS-маршрутизації, а сформульована задача носить назву *спільного захисту за умови вдосконаленого трафік-інжинірингу (Shared protection Smart Traffic Engineering, SSTE)*. Зокрема задача SSTE є NP-складною, оскільки містить задачу визначення дерев Штейнера. Проте в роботі [54] наведено формулювання цієї задачі за Бендерсом, яке є набагато ефективнішим з обчислювальної точки зору.

У праці [55] запропоновано алгоритми розрахунку шляхів для відмовостійкої маршрутизації, які не перетинаються за вузлами та проходять через задані вузли. Задача розрахунку найкоротшого шляху, що проходить через задану множину вузлів, має принаймні таку ж складність, як і задача комівояжера, тому в літературі їй не було приділено значної уваги. Незважаючи на це, нещодавно було запропоновано ефективне формулювання цієї задачі як задачі ILP. Це формулювання, по-перше, адаптоване під включення обмеження, яке гарантує, що отриманий шлях може бути захищений за допомогою резервного шляху, який не перетинається з основним за вузлами, а по-друге, має бути отримана така пара основного та резервного шляхів, які не перетинаються за вузлами та мають мінімальну вартість за умови, що кожен з них повинен проходити через певний набір заданих вузлів.

Проте обчислювальні експерименти показали, що зазначені підходи у масштабних мережах можуть не дозволити розв'язати задачу відмовостійкої маршрутизації протягом заданого часу. Тому для її розв'язання автори запропонували евристику, яка здатна знайти рішення в більшості випадків. Крім того, отримані рішення мають прийнятну відносну похибку стосовно вартості отриманого шляху або пари шляхів, а процесорний час, який потребує евристика, значно менший за час, який вимагає вирішувач ILP.

У дослідженні [56] представлено рішення щодо розподілу резервної пропускної здатності (*Spare Capacity Allocation, SCA*) у використанні спільного резервного захисту шляху за умови подвійних відмов каналів зв'язку (*dual link failures*). Ця робота розширює застосування задачі SCA в IP mesh-мережах та WDM. Отже, у розв'язанні задачі SCA потоки пакетів попередньо розподіляються за одним робочим і двома резервними шляхами, що взаємно не перетинаються, використовуючи схему спільного резервного захисту шляху (*Shared Backup Path Protection, SBPP*). Метод матричного резервного забезпечення (*Spare Provision Matrix, SPM*) агрегує інформацію щодо кожного потоку та обчислює загальну вільну пропускну здатність для подвійних відмов каналів зв'язку. Цей метод має достатню масштабованість і гнучкість. Задача SCA сформульована як задача нелінійного цілочисельного програмування і розділена на дві послідовні лінійні підзадачі: одна дозволяє знайти всі первинні резервні шляхи, а інша знаходить всі вторинні резервні шляхи. Авторами розширено термінологію у захисті каналів 1+1 та 1:1 для захисту резервного шляху. Крім того, у роботі показано, що вдосконалений евристичний алгоритм успішної безвідмовної маршрутизації (*Successive Survivable Routing, SSR*) для випадку подвійних відмов добре масштабується в мережах великого розміру.

Використання резервних шляхів є загальною методикою забезпечення захисту в разі відмови елементів ІКМ (вузлів/каналів зв'язку/шляхів тощо). Однак обчислення відповідних множин основних і резервних шляхів, що не перетинаються, потребує значного часу, використовуючи доступні алгоритми (наприклад, підхід Бхандарі [57]). Це, у свою чергу, може значно вплинути на здатність мережі обслуговувати динамічні потоки (тобто ті, що характеризуються відносно короткою тривалістю надання послуги). Щоб забезпечити вирішення цієї проблеми, у роботі [57] запропоновано підхід щодо попереднього обчислення множини шляхів, які не перетинаються, з метою отримання можливості обслуговування потоків одразу після їх надходження в мережу. Цей підхід оснований на спостереженні, що задача обчислення множини шляхів, які не перетинаються за вузлами, еквівалентна

задачі визначення «найдешевшого» циклу топології мережі, що проходить через вузли відправника та отримувача відповідного потоку. Зокрема авторами [57] запропоновано узагальнення цієї схеми, якщо припустити, що будь-яка пара шляхів, які не перетинаються за вузлами, може бути отримана шляхом об'єднання базових циклів, визначених для топології мережі (рис. 2.17).

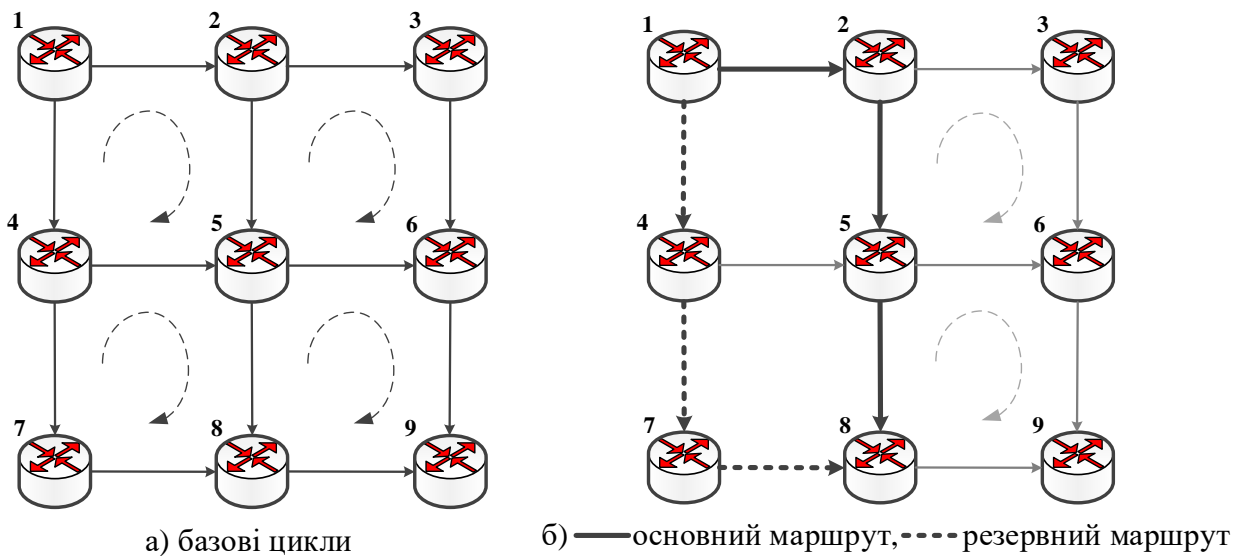


Рис. 2.17. Ілюстрація основної ідеї схеми попереднього розрахунку основного та резервного шляхів, що не перетинаються

У [57] вводиться новий метод для розрахунку «найдешевших» циклів на основі так званих базових циклів, що, як підтверджено для реальних мережних топологій, зменшує до 70 % часу, необхідного для встановлення шляхів, що не перетинаються за вузлами (порівняно з результатами, отриманими за схемою Бхандарі).

На сьогоднішній день ІКМ мають гарантувати, що всі вузлові пари, які беруть участь у комунікаціях критичних інфраструктур, мають високу доступність. Як правило, лише невелика частка трафіку та користувачів потребує високого рівня доступності, але саме такий тип трафіку вимагає перегляду мережних рішень у проектуванні відмовостійких ІКМ. У статтях [58, 59] запропоновано новий підхід до вирішення завдання ефективного забезпечення високого рівня міжкінцевої доступності, а саме використання концепції спайна. Основна ідея полягає в тому, щоб ввести високодоступну множину каналів зв'язку та вузлів, так званий *спайн (spine)*, у топології мережі та відповідний захист і маршрутизацію з метою надання диференційованих класів відмовостійкості з різним рівнем доступності. У роботі [58] досліджено саму концепцію спайна на прикладі, що ілюструє потенційні переваги цього підходу. Також було показано, як структурні властивості топології мережі можуть бути

використані для визначення евристики у виборі відповідного спайна та порівняні з випадком, коли всі мережні компоненти мають однакову доступність.

Концепція застосування спайнів показана на наступному прикладі. Нехай повнозв'язна мережа, представлена графом (рис. 2.18), містить чотири вузли та шість каналів зв'язку. Зокрема для кожного  $l$ -го каналу зв'язку відома його метрика доступності  $a_l$ , яка змінюється в межах від 0 до 1 [58]. У цьому прикладі обрано спайн, що містить канали зв'язку  $1 \rightarrow 2$ ,  $1 \rightarrow 3$  та  $1 \rightarrow 4$ , які мають вищі значення метрики доступності  $a_1$ ,  $a_5$  та  $a_4$  відповідно.

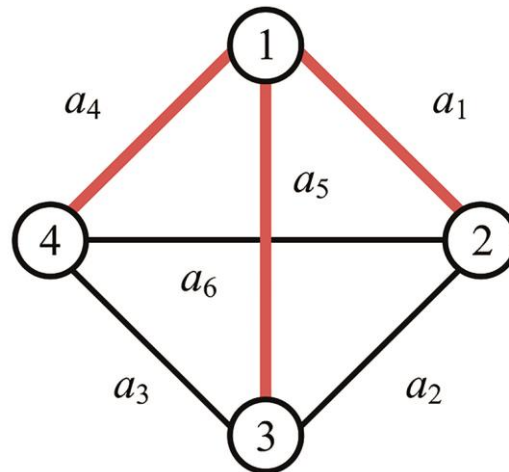


Рис. 2.18. Приклад мережі з повнозв'язною топологією та обраного спайна на ній

Таким чином, доступність основного маршруту (*working path*,  $WP$ ) для потоку, що передається, визначається за виразом [58]

$$A^{WP} = \prod_{l \in WP} a_l.$$

Аналогічно цій формулі визначається доступність резервного маршруту  $A^{BP}$  (*backup path*,  $BP$ ). Тоді як доступність мережі для потоку, що передається, можна отримати таким чином [58]:

$$A = 1 - (1 - A^{WP})(1 - A^{BP}).$$

Подібні результати є важливим кроком на шляху оптимального проектування фізичної мережі для підтримки методів захисту (резервування) для досягнення високого рівня доступності елементів ІКМ.

Далі задача ефективного забезпечення високого рівня міжкінцевої доступності під час передачі потоків між вузлами ІКМ формулювалася у вигляді оптимізаційної за умови використання різних критеріїв оптимальності:

- максимізація суми доступностей основних шляхів для всіх потоків;

– максимізація мінімального рівня доступності основних шляхів для всіх потоків.

У дослідженнях останніх років велика увага приділяється концепції надання диференційованих класів відмовостійких послуг через ІКМ. У деяких випадках учені намагалися вирішити ці завдання шляхом створення множини категорій послуг із різними схемами захисту. Проте більшість з них орієнтовані на застосування в однорангових мережах та не мають узгодженої міжрівневої координації в багаторівневих (ієрархічних) сценаріях. Крім того, зростає потреба в наданні послуг з високими вимогами до відмовостійкості в мережах майбутнього. Це, однак, має бути зроблено економічно ефективним способом і без надмірної складності. У статті [59] запропоновано вдосконалення попереднього підходу на основі спайнів, який дозволяє спростити синтез необхідного механізму та забезпечує як високу відмовостійкість, так і її диференціацію. Отже, цей підхід використовує ідею концепції спайна щодо введення підмереж на фізичному рівні з відносно високою доступністю каналів зв'язку та вузлів [58]. Це створює основу для диференціації відмовостійкості між різними класами потоків. Потім міжрівневе відображення та маршрутизація з урахуванням спайна виконуються таким чином, щоб інформація щодо здатності диференціювання передавалася на верхній рівень. Крім того, у [58] запропоновано два оптимізаційних формулювання задачі маршрутизації та відображення, а також оцінено їх ефективність у багаторівневому сценарії.

Серед досліджень щодо відмовостійкості в SDN можна виокремити роботи [5, 12, 60–62]. Так, наприклад, у [60] наведено алгоритм локальної швидкої перемаршрутизації (*Local Fast Reroute, LFR*) з агрегацією потоків у програмно-конфігурованих мережах. В алгоритмі LFR у разі виявлення відмови каналу зв'язку всі потоки трафіку, вражені відмовою, агрегуються у так званий «великий» потік. Далі локальний резервний шлях для перемаршрутизації динамічно розгортається контролером SDN для агрегованого потоку. Таким чином, алгоритм LFR зменшує кількість поточних операцій між контролером SDN та комутаційним обладнанням. Отримані результати довели, що LFR забезпечує швидке відновлення, мінімізуючи загальну кількість потоків у SDN.

Зростання складності сучасних мережних застосунків та величезний попит на інтернет-ресурси вимагають від інфраструктур ІКМ здатності адаптуватися до вимог високого ступеня робастності та надійності. Як було сказано вище, у SDN надзвичайно актуальним є саме завдання підвищення відмовостійкості та вчасного оновлення інформації про стан мережі, яким присвячено дослідження [61]. У ньому визначені нові алгоритми,

спрямовані на покращення пошуку резервних шляхів у мережах великої розмірності в разі одиночних відмов каналів зв'язку з мінімальними часовими витратами на оновлення інформації про стан мережі. Нове рішення спрямоване на підвищення ефективності та зменшення операцій з оброблення службової інформації під час відмов каналів зв'язку.

Також слід відзначити, що забезпечення узгодженого вирішення завдань балансування навантаження та відмовостійкої маршрутизації (наприклад, MPLS TE FRR) найчастіше призводить до підвищення обчислювальної складності та зниження масштабованості протокольних рішень. Відомо, що ефективність протокольного рішення багато в чому визначається адекватністю та якістю покладеної в його основу математичної моделі розрахунку. Як показав проведений аналіз [63], порядок FRR і TE визначається під час розв'язання оптимізаційних задач різного рівня складності. У цьому випадку реалізація схеми захисту пропускну здатності мережі, як правило, призводить до нелінійного формулювання оптимізаційної задачі та відповідного зростання обчислювальної складності отримуваних рішень.

#### **2.4. Система потокових моделей відмовостійкої маршрутизації без резервування елементів ІКМ**

Важливе місце з точки зору підвищення відмовостійкості ІКМ відводиться засобам багатошляхової маршрутизації, коли для доставки пакетів того чи іншого потоку одночасно використовується не один шлях, а множина маршрутів. Зокрема в роботах [64–67] запропоновані маршрутні рішення, орієнтовані на використання шляхів, що не перетинаються, тобто в яких спільними є тільки вузли відправника та отримувача пакетів. Використання маршрутів, які не перетинаються, гарантує, що відмова (вихід з ладу, перевантаження або компрометація) одного елемента (вузла або каналу) мережі спричинить відмову лише одного, а не декількох маршрутів [64, 66], що має місце в разі маршрутизації шляхами, які перетинаються. Як показав проведений аналіз [64–67, 68, 69], перспективні теоретичні рішення в цьому напрямі мають забезпечувати:

- урахування особливостей як структури мережі, параметрів каналів зв'язку, так і характеристик трафіку, що передається;
- підтримку мультипотокості, тобто модель має описувати порядок маршрутизації не одного, а одночасно декількох потоків з урахуванням їх взаємного впливу;

– контроль за можливим перевантаженням елементів мережі за рахунок виконання умов збереження потоку у вузлах мережі та запобігання перевантаження каналів зв'язку.

#### 2.4.1. Синтез та дослідження потокової моделі багатошляхової маршрутизації в ІКМ шляхами, що не перетинаються

Введемо наступні позначення, які є актуальними для всього другого розділу роботи. Припустимо, що структуру ІКМ описує граф  $\Gamma = (R, E)$ , в якому  $R = \{R_i; i = \overline{1, m}\}$  – це множина вершин, що моделюють маршрутизатори, а  $E = \{E_{i,j}; i, j = \overline{1, m}; i \neq j\}$  – множина дуг, які представляють канали зв'язку в ІКМ. Тоді  $|E| = n$  визначає кількість каналів зв'язку в ІКМ. Кожну дугу  $E_{i,j} \in E$  зважимо пропускну здатністю  $\varphi_{i,j}$  відповідного каналу зв'язку. Також нехай  $s_k$  і  $d_k$  – вузол-відправник і вузол-отримувач пакетів  $k$ -го потоку відповідно, а  $\lambda^k$  – середня інтенсивність пакетів  $k$ -го потоку з множини  $K$ . Керуючою змінною є величина  $x_{i,j}^k$ , яка характеризує частку  $k$ -го потоку, що передається каналом зв'язку  $E_{i,j} \in E$ .

У синтезі потокової моделі багатошляхової маршрутизації шляхами, що не перетинаються, за основу були прийняті введені в підрозділі 1.7 умови збереження потоку (1.3), реалізації багатошляхової стратегії маршрутизації (1.2) та відсутності перевантаження каналів зв'язку ІКМ (1.4). Як приклад у розв'язанні маршрутної задачі буде мінімізуватися лінійна цільова функція такого вигляду:

$$J = \sum_{k \in K} \sum_{E_{i,j} \in E} c_{i,j}^k x_{i,j}^k, \quad (2.1)$$

де  $c_{i,j}^k$  – метрика каналу зв'язку між  $i$ -м та  $j$ -м вузлами ІКМ.

Розглянемо випадок, коли в мережі необхідно реалізувати багатошляхову маршрутизацію шляхами, що не перетинаються, з можливістю регулювання кількості використовуваних маршрутів, як це зроблено, наприклад, у роботах [64, 66]. Під час проведеного дослідження встановлено, що в разі багатошляхової маршрутизації шляхами, які не перетинаються, необхідно, щоб виконувалося таке припущення (гіпотеза): у кожен транзитний вузол потік повинен входити не більше ніж за одним каналом зв'язку  $i$ , відповідно, виходити також не більше ніж за одним вихідним КЗ. За наведеною гіпотезою



в позначеннях базової моделі (1.2)–(1.4) для всіх вхідних інтерфейсів  $i$ -го транзитного вузла повинні виконуватися такі умови [70]:

$$\sum_{j:E_{j,i} \in E} \sum_{\substack{l:E_{l,i} \in E, \\ l \neq j}} x_{j,i}^k x_{l,i}^k = 0, \quad (2.2)$$

а для всіх вихідних інтерфейсів  $i$ -го транзитного вузла мережі мають бути справедливими такі рівності:

$$\sum_{n:E_{i,n} \in E} \sum_{\substack{m:E_{i,m} \in E, \\ m \neq n}} x_{i,n}^k x_{i,m}^k = 0. \quad (2.3)$$

Виконання умов (2.2) та (2.3) гарантує, що потік, який проходить через  $i$ -й транзитний вузол, надходить не більше ніж від одного суміжного вузла і передається не більше ніж одному суміжному вузлу. Тобто відбувається формування множини шляхів, що не перетинаються, у яких спільними є тільки вузли відправника та отримувача. З огляду на нелінійність умов (2.2) та (2.3) оптимізаційна задача, пов'язана з мінімізацією виразу (2.1) в разі лінійних обмежень (1.2)–(1.4), належить до класу задач нелінійного програмування.

Для забезпечення регулювання числа використовуваних шляхів, які не перетинаються, у реалізації багатошляхової маршрутизації кожного  $k$ -го потоку позначимо через  $M_{UB}^k$  верхнє граничне значення (Upper Bound) кількості шляхів, що не перетинаються, яке визначається через степінь вершин, що моделюють вузли відправника й отримувача, тобто кількістю інцидентних цим вершинам дуг (каналів зв'язку) [70]:

$$M_{UB}^k = \min(\xi(s_k), \xi(d_k)), \quad (2.4)$$

де  $\xi(s_k)$  – степінь вершини (вузла) відправника  $k$ -го потоку;

$\xi(d_k)$  – степінь вершини (вузла) отримувача  $k$ -го потоку.

Фактично використовуване число  $M^k$  шляхів, що не перетинаються, у процесі маршрутизації  $k$ -го потоку, застосовуючи модель (1.2)–(1.4), (2.1)–(2.4), за аналогією з виразом (2.4) можна розрахувати таким чином [70]:

$$M^k = \sum_{j:E_{i,j} \in E} \left[ x_{i,j}^k \right] \text{ або } M^k = \sum_{n:E_{i,n} \in E} \left[ x_{i,n}^k \right] \text{ при } R_i = s_k, R_m = d_k, \quad (2.5)$$

де  $\sum_{j:E_{i,j} \in E} \left[ x_{i,j}^k \right]$  – кількість вихідних інтерфейсів, за якими  $k$ -й потік виходить

з вузла-відправника;

$\sum_{n: E_{n,m} \in E} \left[ x_{n,m}^k \right]$  – кількість вхідних інтерфейсів, за якими  $k$ -й потік надходить до вузла-отримувача.

Величина  $M^k$  може бути як оцінюваним параметром, так і керованою величиною, тобто за її допомогою можна задавати мінімальне, максимальне або визначати задане (оптимальне) число використовуваних шляхів, що не перетинаються, у реалізації багатошляхової маршрутизації. Межі зміни цієї величини визначаються за допомогою нерівності

$$1 \leq M^k \leq M_{UB}^k. \quad (2.6)$$

Проведено перевірку працездатності (адекватності) запропонованої потокової моделі багатошляхової маршрутизації в ІКМ шляхами, що не перетинаються, з регулюванням числа використовуваних маршрутів на множині мережних структур. Як приклад розглянемо структуру мережі, що складалася з 12 вузлів і 25 каналів зв'язку (рис. 2.19). У цьому випадку вузлами «відправник–отримувач» були перший і дванадцятий вузли відповідно. Пропускна здатність кожного з каналів зв'язку, для прикладу, дорівнювала 100 пакетам за секунду (1/с).

Спочатку проаналізуємо результат рішення, отримуваний у разі використання базової потокової моделі (1.2)–(1.4), (2.1), коли метрика каналів зв'язку дорівнювала одиниці ( $c_{i,j}^k = 1$ ). Нехай між парою вузлів «відправник–отримувач» передавався потік пакетів інтенсивністю 300 1/с. Кінцевий порядок багатошляхової маршрутизації, отриманий на основі моделі (1.2)–(1.4), (2.1), наведено на рис. 2.19, де в розриві того чи іншого каналу зв'язку зображено інтенсивність потоку, що протікає по ньому. Аналіз рис. 2.19 показав, що базова модель (1.2)–(1.4), (2.1) забезпечує розрахунок множини маршрутів, які перетинаються як за вузлами, так і за каналами зв'язку. Для зручності незадіяні в маршрутизації канали зв'язку зображені на рис. 2.19 штриховою лінією.

Далі проведемо розв'язання задачі багатошляхової маршрутизації, але вже шляхами, що не перетинаються, тобто з урахуванням сформульованих умов (2.2) і (2.3). Результат розрахунку за умови тих самих вихідних даних показано на рис. 2.20, який представлено такими трьома ( $M^k = 3$ ) шляхами, що не перетинаються:  $R_1 \rightarrow R_2 \rightarrow R_5 \rightarrow R_9 \rightarrow R_{12}$ ,  $R_1 \rightarrow R_3 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{12}$  і  $R_1 \rightarrow R_4 \rightarrow R_8 \rightarrow R_{11} \rightarrow R_{12}$ . За кожним з цих шляхів передається потік інтенсивністю 100 1/с.

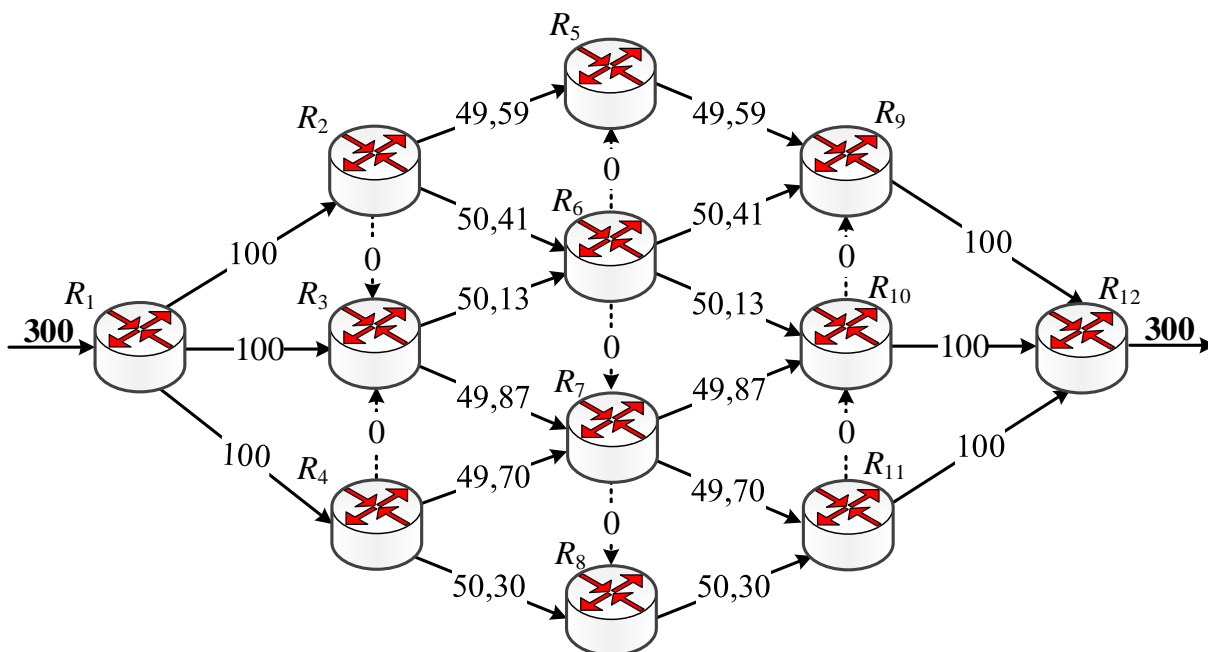


Рис. 2.19. Результат розрахунку множини шляхів з використанням базової моделі (1.2)–(1.4), (2.1) для обслуговування потоку інтенсивністю 300 1/с

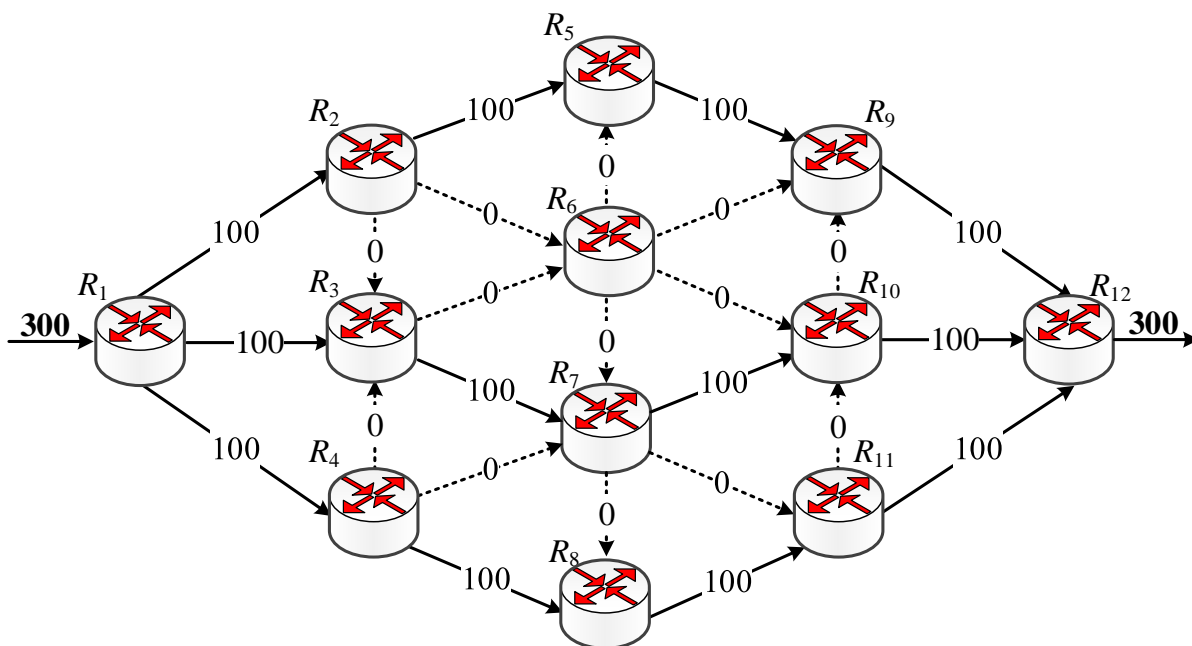


Рис. 2.20. Результат розрахунку множини шляхів з використанням умов маршрутизації (2.2) і (2.3) шляхами, що не перетинаються, для обслуговування потоку інтенсивністю 300 1/с

Змінимо дещо вихідні дані: нехай на вхід мережі надходить потік інтенсивністю 100 1/с, а  $M^k = 2$ , якщо  $M_{UB}^k = 3$ , тобто умова (2.6) виконується. Тоді використання моделі (1.2)–(1.4), (2.1)–(2.6) визначило порядок маршрутизації

потоків в ІКМ, представлений на рис. 2.21. Шляхи  $R_1 \rightarrow R_2 \rightarrow R_5 \rightarrow R_9 \rightarrow R_{12}$  і  $R_1 \rightarrow R_4 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{12}$  також не перетинаються.

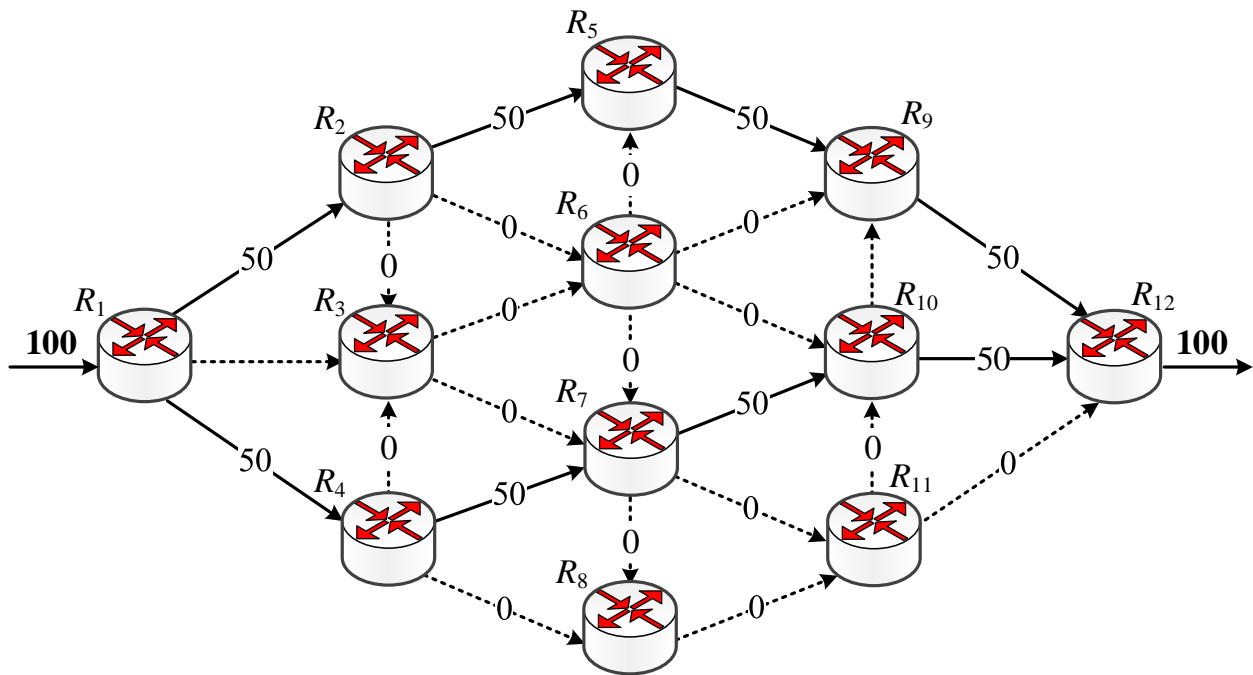


Рис. 2.21. Результат розрахунку множини шляхів з використанням умов (2.2), (2.3) і (2.6) для обслуговування потоку інтенсивністю 100 1/с ( $M^k = 2$ )

Отже, результати дослідження підтвердили працездатність та адекватність запропонованої потокової моделі багатошляхової маршрутизації шляхами, що не перетинаються, з регулюванням кількості використовуваних маршрутів у різних умовах зміни характеристик потоків.

Модель може забезпечувати отримання необхідних рішень також з іншими маршрутними метриками, які входять до критерію оптимальності (2.1), або з іншими критеріями оптимальності, наприклад (1.15), за умов (1.13), що позначиться як на характері визначених маршрутів, так і на порядку балансування навантаження цими шляхами.

#### 2.4.2. Синтез та дослідження потокової моделі багатошляхової маршрутизації в ІКМ шляхами, що перетинаються за вузлами

Варто окремо зазначити, що реалізація багатошляхової маршрутизації шляхами, що не перетинаються, як правило, не сприяє збалансованому використанню доступного мережного (канального) ресурсу, що негативно позначається на продуктивності ІКМ та рівні якості обслуговування загалом.

Пошук компромісу в питанні забезпечення відмовостійкості ІКМ, з одного боку, та якості обслуговування, з іншого, призвів до того, що в деяких важливих випадках вимоги щодо перетинання використовуваних шляхів можна дещо знизити і застосовувати шляхи, які допускають перетин, наприклад, лише за вузлами ІКМ. У таких маршрутах спільними є не тільки вузли «відправник» та «отримувач», але й деякі транзитні вузли, проте вони не містять спільних каналів зв'язку. Це є особливо актуальним для безпроводових мереж, в яких радіоканали більш схильні до перевантаження та/або компретації переданих даних на фізичному рівні ЕМВВС [64, 65]. Тобто в таких випадках, коли до відмов схильні саме канали зв'язку, а не вузли ІКМ, доцільно використовувати маршрути, що перетинаються лише за вузлами, бо це може призвести до підвищення продуктивності мережі із забезпеченням того ж рівня відмовостійкості, що й за умови задіяння маршрутів, які не перетинаються взагалі.

Розглянемо випадок, коли в ІКМ необхідно реалізувати багатошляхову маршрутизацію за шляхами, що перетинаються за вузлами. У межах цієї моделі необхідно, щоб виконувалося таке припущення (гіпотеза) для всіх вхідних і вихідних інтерфейсів  $i$ -го транзитного вузла, які використовуються: кожен вхідний потік заданої інтенсивності також повинен відповідати вихідному потоку такої ж інтенсивності [71, 72]:

$$\sum_{m=1}^{N_{in}} \prod_{n=1}^{N_{out}} x_{m,i}^k (x_{m,i}^k - x_{i,n}^k) = 0, \quad (2.7)$$

де  $N_{in}$  – кількість вхідних інтерфейсів  $i$ -го транзитного вузла;

$N_{out}$  – кількість вихідних інтерфейсів  $i$ -го транзитного вузла.

Крім того, має бути виконана протилежна умова: кожен вихідний потік заданої інтенсивності повинен відповідати вхідному потоку з тією ж інтенсивністю [71, 72]:

$$\sum_{n=1}^{N_{out}} \prod_{m=1}^{N_{in}} x_{i,n}^k (x_{i,n}^k - x_{m,i}^k) = 0. \quad (2.8)$$

Виконання нелінійних умов (2.7) та (2.8) гарантує, що потоки, які передаються через  $i$ -й транзитний вузол, надходять з однієї і тієї ж кількості сусідніх вузлів, які передаються іншим суміжним вузлам з однаковою інтенсивністю. Таким чином, формується множина шляхів, що мають не тільки спільну пару вузлів «відправник» та «отримувач», а також використовують спільні транзитні вузли. Можливість регулювання кількості використовуваних

маршрутів, як це зроблено в пункті 2.4.1, може бути застосована і для випадку шляхів, що перетинаються за вузлами.

Нехай необхідно розв'язати задачу багатошляхової маршрутизації шляхами, що перетинаються за вузлами. Для розв'язання задачі з використанням запропонованої потокової моделі як ІКМ застосовувалася мережа з восьми вузлів і 15 каналів зв'язку, що показано на рис. 2.22. Вузлами «відправник–отримувач» були перший і восьмий вузли відповідно. У розривах каналів зв'язку вказана їх пропускна здатність, яка вимірюється в пакетах за секунду (1/с) (рис. 2.22).

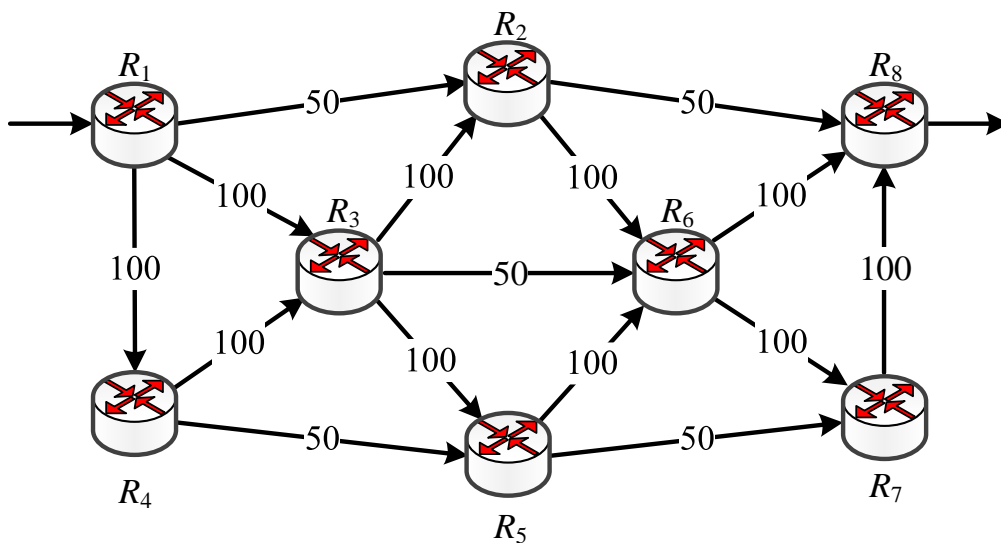


Рис. 2.22. Структура досліджуваної ІКМ

Для наочності розглянемо приклад, коли під час багатошляхової маршрутизації мінімізується кількість переприйомів пакетів на вузлах, тобто  $c_{i,j} = 1$ . Тоді максимальна продуктивність напрямку зв'язку між першим та восьмим вузлами ІКМ у разі реалізації багатошляхової маршрутизації шляхами, що перетинаються за вузлами, буде становити 250 1/с (рис. 2.23). На рис. 2.23 в розриві того чи іншого каналу зв'язку зображена інтенсивність потоку, який протікає за ним. Незадіяні під час маршрутизації канали показані штриховою лінією.

Таким чином, за умови передачі потоку інтенсивністю 250 1/с отримана множина маршрутів містить такі три  $(M^k = 3)$  шляхи:

$$R_1 \rightarrow R_2 \rightarrow R_8,$$

$$R_1 \rightarrow R_3 \rightarrow R_2 \rightarrow R_6 \rightarrow R_8,$$

$$R_1 \rightarrow R_4 \rightarrow R_3 \rightarrow R_5 \rightarrow R_6 \rightarrow R_7 \rightarrow R_8, \text{ що перетинаються за вузлами.}$$

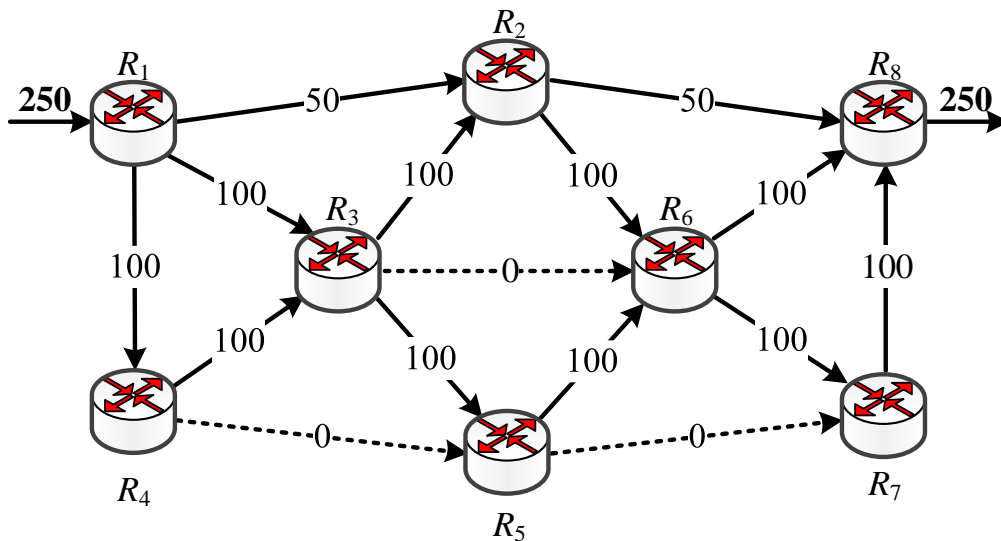


Рис. 2.23. Результат розрахунку множини шляхів з використанням умов (2.7), (2.8) обслуговування потоку інтенсивністю 250 1/с

Зокрема у шляхів  $R_1 \rightarrow R_2 \rightarrow R_8$  і  $R_1 \rightarrow R_3 \rightarrow R_2 \rightarrow R_6 \rightarrow R_8$  вузол  $R_2$  є спільним, а шляхи  $R_1 \rightarrow R_3 \rightarrow R_2 \rightarrow R_6 \rightarrow R_8$  і  $R_1 \rightarrow R_4 \rightarrow R_3 \rightarrow R_5 \rightarrow R_6 \rightarrow R_7 \rightarrow R_8$  у цьому випадку мають два спільних вузли, а саме транзитні вузли  $R_3$  і  $R_6$ . Шляхом  $R_1 \rightarrow R_2 \rightarrow R_8$  передається потік інтенсивністю 50 1/с, а шляхами  $R_1 \rightarrow R_3 \rightarrow R_2 \rightarrow R_6 \rightarrow R_8$  і  $R_1 \rightarrow R_4 \rightarrow R_3 \rightarrow R_5 \rightarrow R_6 \rightarrow R_7 \rightarrow R_8$  – потоки інтенсивністю по 100 1/с.

Для прикладу у використанні множини маршрутів, що не перетинаються ( $R_1 \rightarrow R_2 \rightarrow R_8$ ,  $R_1 \rightarrow R_3 \rightarrow R_6 \rightarrow R_8$  та  $R_1 \rightarrow R_4 \rightarrow R_5 \rightarrow R_7 \rightarrow R_8$ ), продуктивність напрямку зв'язку між першим та восьмим вузлами за умови пропускних здатностей каналів зв'язку, зазначених на рис. 2.22, становитиме лише 150 1/с. Таким чином, перехід до задіяння шляхів, що перетинаються за вузлами, у розглянутому прикладі сприяє зростанню продуктивності обраного напрямку зв'язку приблизно в 1,7 раза. Одночасно із зростанням розміру мережі та зв'язності маршрутизаторів, коли кількість шляхів, що перетинаються, зростає, вигравш за продуктивністю збільшувався до 2,5–4 разів.

## 2.5. Потокова модель швидкої перемаршрутизації в ІКМ

Як зазначалось у підрозділі 2.2, швидка перемаршрутизація належить до засобів відмовостійкої маршрутизації, що реалізується на рівні ядра ІКМ та основана на введенні ресурсної надлишковості [19, 20]. Тобто одночасно з основним шляхом (мультишляхом) для кожного потоку має розраховуватись і резервний шлях (мультишлях), що не проходить через проблемні елементи

мережі (вузли, канали, сегменти), які захищаються. Це накладає певні особливості на саму структуру моделі швидкої перемаршрутизації в ІКМ.

В описі потокової моделі швидкої перемаршрутизації в ІКМ варто зазначити, що надалі через  $x_{i,j}^k$  будуть позначатися маршрутні змінні, кожна з яких характеризує частку інтенсивності  $k$ -го потоку в каналі зв'язку, що представляється дугою  $E_{i,j} \in E$  і міститься в *основному* маршруті. Кількість маршрутних змінних  $x_{i,j}^k$  відповідає добутку  $|K| \cdot |E|$ . Крім того, мають місце умови збереження потоку (1.3), реалізації багатопляхової стратегії маршрутизації (1.2) та відсутності перевантаження каналів зв'язку ІКМ (1.4).

У разі використання в ІКМ однопляхової маршрутизації потоків мають місце умови (1.1). Для визначення резервних маршрутів, як зазначено в роботах [5, 12, 41, 55, 57], вводяться додаткові маршрутні змінні  $\bar{x}_{i,j}^k$ , кожна з яких характеризує частку  $k$ -го потоку в каналі зв'язку, представленого дугою  $E_{i,j}$ , але вже *резервного* шляху/мультишляху. Наприклад, для забезпечення зв'язності резервного одноадресного шляху/мультишляху на змінні  $\bar{x}_{i,j}^k$  накладаються обмеження, аналогічні (1.3) [73, 74]:

$$\left\{ \begin{array}{l} \sum_{j: E_{i,j} \in E} \bar{x}_{i,j}^k - \sum_{j: E_{j,i} \in E} \bar{x}_{j,i}^k = 0; \quad k \in K^0, \quad R_i \neq s_k, d_k; \\ \sum_{j: E_{i,j} \in E} \bar{x}_{i,j}^k - \sum_{j: E_{j,i} \in E} \bar{x}_{j,i}^k = 1; \quad k \in K^0, \quad R_i = s_k; \\ \sum_{j: E_{i,j} \in E} \bar{x}_{i,j}^k - \sum_{j: E_{j,i} \in E} \bar{x}_{j,i}^k = -1; \quad k \in K^0, \quad R_i = d_k. \end{array} \right. \quad (2.9)$$

Для реалізації багатоадресної маршрутизації на змінні  $\bar{x}_{i,j}^k$  накладаються обмеження, аналогічні (1.7)–(1.10).

## 2.6. Формалізація умов забезпечення захисту вузла, каналу, маршруту та пропускної здатності під час швидкої перемаршрутизації в ІКМ

Як показав проведений у підрозділі 2.2 аналіз, у процесі швидкої перемаршрутизації можуть підтримуватися кілька основних схем захисту елементів мережі: вузла, каналу, шляху та його пропускної здатності. У працях [75, 76] формалізовано в аналітичному вигляді умови для підтримки зазначених схем захисту як елементи відповідних математичних моделей.



Так, у роботі [75] пропонується для реалізації схеми захисту каналу  $E_{i,j} \in E$  на маршрутні змінні  $\bar{x}_{i,j}^k$ , що відповідають за визначення резервного шляху, накласти додаткові обмеження, аналогічні (1.1). Зокрема в разі реалізації одношляхової стратегії маршрутизації має місце таке обмеження:

$$\bar{x}_{i,j}^k \in \{0; \delta_{i,j}^k\}, \quad (2.10)$$

тоді як у випадку багатошляховій маршрутизації

$$0 \leq \bar{x}_{i,j}^k \leq \delta_{i,j}^k, \quad (2.11)$$

де

$$\delta_{i,j}^k = \begin{cases} 0, & \text{за умови захисту каналу зв'язку } E_{i,j}; \\ 1, & \text{в іншому випадку.} \end{cases} \quad (2.12)$$

Виконання умов (2.10)–(2.12) гарантує, що канал  $E_{i,j} \in E$ , який захищається, не буде застосовуватися резервним маршрутом. Умови (2.10) та (2.11) мають лінійний характер, на відміну від нелінійних виразів, запропонованих у роботі [74], що сприяє зниженню обчислювальної складності отримання кінцевих протокольних рішень.

Для забезпечення захисту вузла в праці [74] пропонується використовувати нелінійні вирази для реалізації цієї схеми. Тоді як в роботі [55] запропоновано підхід, оснований на введенні лінійних умов у вигляді

$$\sum_{R_j \in R_i^*} (x_{j,i}^k + \bar{x}_{j,i}^k) \leq 1, \text{ якщо } R_j \in R_i^*, j = \overline{1, m}, \quad (2.13)$$

які, однак, справедливі лише у разі використання одношляхової стратегії маршрутизації, де через  $R_i^* = \{R_j : E_{j,i} \neq 0; j = \overline{1, m}; i \neq j\}$  позначено підмножину маршрутизаторів, які є суміжними для вершини  $R_i$ .

У цій роботі пропонується узагальнення умов (2.10) та (2.11) на випадок захисту множини каналів зв'язку, інцидентних вузлу  $R_i \in R$ , що захищається [75, 76]. Тоді в разі одношляхової маршрутизації мають місце такі обмеження:

$$\bar{x}_{i,j}^k \in \{0; \delta_{i,j}^k\}, \text{ якщо } R_j \in R_i^*, j = \overline{1, m}, \quad (2.14)$$

а у випадку використання багатошляхової стратегії вводиться система умов

$$0 \leq \bar{x}_{i,j}^k \leq \delta_{i,j}^k, \text{ якщо } R_j \in R_i^*, j = \overline{1, m}, \quad (2.15)$$

де вибір значень  $\delta_{i,j}^k$  підпорядковується умові (2.12).

Отже, виконання вимог умов (2.14), (2.15) гарантує захист вузла  $R_i \in R$ , забороняючи використання резервним маршрутом усіх каналів, які виходять з цього вузла. Оскільки захисту підлягають лише транзитні маршрутизатори, то заборона на застосування вихідних каналів запобігає включенню до резервного шляху і вхідних каналів для цього вузла  $R_i$ , що в результаті сприяє захисту вузла загалом. Варто зазначити, що умови захисту заздалегідь визначених вузлів і каналів мережі, як правило, є лінійними, а їх урахування критично не позначається на складності обчислення маршрутних змінних  $x_{i,j}^k$  та  $\bar{x}_{i,j}^k$ , що відповідають за формування множини основних і резервних маршрутів відповідно.

У разі реалізації схеми захисту шляху необхідно забезпечити відсутність спільних вузлів і каналів як в основному, так і резервному маршрутах. Тоді за аналогією з результатами, отриманими в роботі [55], для реалізації одношляхової маршрутизації необхідно виконати такі лінійні умови:

$$\sum_{R_j \in R_i^*} \sum_{R_p \in R_i^*} (x_{j,i}^k + \bar{x}_{p,i}^k) \leq 1, \quad \forall R_i \in R \setminus \{s_k, d_k\}. \quad (2.16)$$

Універсальні умови захисту шляху, які справедливі й для одношляхової, і для багатошляхової маршрутизації, мають нелінійний вигляд:

$$\sum_{R_j \in R_i^*} \sum_{R_p \in R_i^*} x_{j,i}^k \bar{x}_{p,i}^k = 0, \quad \forall R_i \in R \setminus \{s_k, d_k\}. \quad (2.17)$$

Вигляд виразів (2.17) дещо відрізняється від умов, запропонованих у [74]:

$$\sum_{R_i \in R} \sum_{\substack{R_j \in R, \\ i \neq j}} x_{i,j}^k \bar{x}_{i,j}^k = 0,$$

оскільки в раніше відомому рішенні резервний мультишлях допускав вузловий перетин з основним. Отже, введені умови (2.17) є більш чіткими.

Через необхідність здійснення резервування пропускнуої здатності мережі, а також з метою запобігання можливого перевантаження каналів зв'язку ІКМ у реалізації стратегій як одношляхової, так і багатошляхової маршрутизації основними і резервними маршрутами в модель за аналогією з результатами, отриманими в роботі [77], вводяться в загальному вигляді такі умови:

$$\sum_{k \in K} \lambda^k \cdot \max [x_{i,j}^k, \bar{x}_{i,j}^k] \leq \varphi_{i,j}, \quad E_{i,j} \in E. \quad (2.18)$$

Тобто довільний канал зв'язку  $E_{i,j} \in E$  під час швидкої перемаршрутизації не повинен перевантажуватися потоками, які протікають основними або

резервними шляхами. У моделюванні процесів швидкої перемаршрутизації виникають певні складнощі в разі формалізації умов захисту пропускної здатності мережі, коли лише деякі з потоків, що передаються, перемикаються з основних на резервні маршрути. У роботах [73, 74] умови для реалізації одношляхової швидкої перемаршрутизації мають такий вигляд:

$$\sum_{k \in K} \lambda^k \left( \frac{x_{i,j}^k + \bar{x}_{i,j}^k}{x_{i,j}^k \bar{x}_{i,j}^k + 1} \right) \leq \varphi_{i,j}, E_{i,j} \in E. \quad (2.19)$$

У найбільш загальному випадку, включаючи і варіант (2.19), тобто в разі реалізації одночасно одношляхової та багатошляхової швидкої маршрутизації, умови захисту пропускної здатності ІКМ записують таким чином [74]:

$$\frac{1}{2} \sum_{k \in K} \lambda^k \left[ x_{i,j}^k + \bar{x}_{i,j}^k + \left| x_{i,j}^k - \bar{x}_{i,j}^k \right| \right] \leq \varphi_{i,j}, E_{i,j} \in E. \quad (2.20)$$

Отже, умови захисту пропускної здатності (ПЗ) мережі (2.19) та (2.20) фактично зводяться до виконання умов запобігання перевантаження каналів зв'язку для реалізації швидкої перемаршрутизації, які справедливі навіть тоді, коли не всі, а лише деякі потоки будуть перенаправлені з основного на резервний маршрут. У цьому випадку для цих потоків завжди залишатиметься незадіяною деяка частина ПЗ каналів зв'язку резервних маршрутів, реалізуючи тим самим схему захисту пропускної здатності під час організації швидкої перемаршрутизації в ІКМ.

Окремо варто зазначити, що умови (2.19) та (2.20) є адекватними і для випадку організації багатоадресної або ширококомовної маршрутизації, коли маршрутні змінні  $x_{i,j}^k$  та  $\bar{x}_{i,j}^k$  визначають порядок балансування навантаження відповідно до обмежень (1.7)–(1.10).

## **2.7. Дослідження оптимальності рішень щодо швидкої перемаршрутизації в ІКМ**

### **2.7.1. Формування критерію оптимальності рішень щодо швидкої перемаршрутизації на основі метрик**

З огляду на те, що в загальному випадку вибір маршрутів (як основних, так і резервних) в ІКМ можна зробити множиною способів, доцільно задачу відмовостійкої маршрутизації сформулювати як оптимізаційну, щоб отримане рішення сприяло, наприклад, мінімізації використання доступного мережного ресурсу та/або покращенню рівня балансування навантаження, якості обслуговування загалом. Важливим моментом у формулюванні будь-якої

оптимізаційної задачі є вибір критерію оптимальності отримуваних рішень, вигляд якого, з одного боку, повинен адекватно відображати фізичний зміст процесу, що моделюється, а з іншого, – надавати можливість отримання шуканих результатів із заданими вимогами (прийнятною точністю, обчислювальною складністю в реальному часі тощо).

Класичний підхід у розв’язанні маршрутних задач в ІКМ полягає в мінімізації сумарної метрики розрахованого маршруту. Так, у роботах [73, 74] у процесі розрахунку маршрутних змінних для розв’язання задач відмовостійкої маршрутизації пропонується використовувати критерій оптимальності, пов’язаний з мінімізацією такої лінійної цільової функції:

$$F = \sum_{k \in K} \sum_{E_{i,j} \in E} c_{i,j}^k x_{i,j}^k + \sum_{k \in K} \sum_{E_{i,j} \in E} \bar{c}_{i,j}^k \bar{x}_{i,j}^k, \quad (2.21)$$

де  $c_{i,j}^k$  і  $\bar{c}_{i,j}^k$  – маршрутні метрики каналів зв’язку, які застосовуються в обчисленні основного та резервного шляхів відповідно.

Функція (2.21) кількісно характеризує сумарні витрати на формування та використання основного та резервного маршрутів між парою вузлів «відправник» та «отримувач». Крім того, у дослідженнях [73, 74] встановлено необхідність її доповнення умовою

$$\sum_{k \in K} \sum_{E_{i,j} \in E} c_{i,j}^k x_{i,j}^k \leq \sum_{k \in K} \sum_{E_{i,j} \in E} \bar{c}_{i,j}^k \bar{x}_{i,j}^k, \quad (2.22)$$

виконання якої гарантує те, що основний шлях (мультишлях) завжди буде не гіршим за резервний у межах обраних метрик  $c_{i,j}^k$  і  $\bar{c}_{i,j}^k$ , тобто кожен  $k$ -й потік спочатку має використовувати, наприклад, найкоротший з точки зору кількості переприйомів (якщо  $c_{i,j}^k = \bar{c}_{i,j}^k = 1$ ) або більш продуктивний (за умови  $c_{i,j}^k = \bar{c}_{i,j}^k = 10^7 / \varphi_{i,j}$ ) шлях/шляхи.

Як показав проведений аналіз, використання критерію (2.21) дійсно забезпечує адекватне рішення поставленого завдання щодо відмовостійкої маршрутизації, проте спостерігається і низка проблемних моментів, які в подальшому можуть негативно позначитися на результативності практичної реалізації моделі (1.1)–(1.4), (2.9)–(2.20) загалом. Насамперед це стосується зниження загальної продуктивності ІКМ з огляду на те, що застосування резервних шляхів так чи інакше пов’язано із залученням додаткового мережного ресурсу (канального та буферного), який з цієї причини не зможе бути використаний іншими потоками.

З іншого боку, необхідність розрахунку поряд з основними маршрутами ще й множини резервних шляхів пов'язана з підвищенням обчислювального навантаження на маршрутизатори ІКМ, а також необхідністю підтримки маршрутних таблиць підвищеної розмірності, в яких би зберігалися дані як про основні, так і резервні шляхи. Зокрема шляхи цих двох типів необхідно не тільки розрахувати, але ще й підтримувати в активному стані. Загалом перелічені чинники, разом зі зниженням продуктивності ІКМ, негативно позначаються на масштабованості рішень, пов'язаних з відмовостійкою маршрутизацією. Особливо це критично для ІКМ великої розмірності і з розгалуженою мережною структурою (високою зв'язністю вузлів).

Перелічені недоліки є спільними практично для всіх технологій, пов'язаних з підвищенням надійності мережі загалом, і є своєрідною «платою» за забезпечення заданого рівня відмовостійкості кінцевих рішень. Для мінімізації цих недоліків бажано, щоб унаслідок проведених розрахунків резервний шлях якомога менше відрізнявся за складом каналів і вузлів від основного – в ідеалі лише на проблемний елемент мережі, що підлягає подальшому захисту. Це має сприяти введенню мінімальної ресурсної надлишковості, коли резервуванню підлягатимуть мінімальні обсяги пропускну здатності каналів мережі, що позитивно позначиться на її продуктивності та показниках якості обслуговування загалом. Крім того, тоді на вузлах мережі для кожного потоку можуть зберігатися вже не дві маршрутні таблиці (для основного та резервного шляху), а одна, але з мінімально необхідними коригуваннями, що стосуються відмінностей основного та резервного шляхів.

Тоді за аналогією з підходом, описаним у роботі [75], критерій (2.21) пропонується замінити на мінімум такої цільової функції:

$$F = \sum_{k \in K} \sum_{E_{i,j} \in E} c_{i,j}^k x_{i,j}^k + \sum_{k \in K} \sum_{E_{i,j} \in E} \bar{c}_{i,j}^k \bar{x}_{i,j}^k - \sum_{k \in K} \sum_{E_{i,j} \in E} b_{i,j}^k x_{i,j}^k \bar{x}_{i,j}^k, \quad (2.23)$$

в якій введення третього доданка якраз пов'язано із забезпеченням максимального збігу резервного шляху з основним за складом каналів і вузлів, що містяться в них;  $b_{i,j}^k$  – досить великий за своєю величиною штрафний коефіцієнт ( $b_{i,j}^k \gg c_{i,j}^k$  і  $b_{i,j}^k \gg \bar{c}_{i,j}^k$ ). Знак мінус перед третім доданком вводиться з тієї причини, що ступінь збігу резервного й основного шляхів необхідно максимізувати, а метрики основного та резервного шляхів (перший і другий доданок у (2.23)) повинні бути мінімальними.

## 2.7.2. Характеристика оптимізаційних задач швидкої перемаршрутизації на основі метрик та методів їх розв'язання

Вирішення завдання щодо швидкої перемаршрутизації в межах запропонованого вдосконалення потокової моделі (1.1)–(1.4), (2.9)–(2.21), (2.23) зводиться до розв'язання оптимізаційної задачі, пов'язаної з мінімізацією цільової функції (2.23) за наявності системи обмежень:

- (1.1) або (1.2), що відповідають за реалізацію одношляхової або багатошляхової маршрутизації відповідно;
- (1.3) та (2.9), що описують умови збереження потоку у вузлах основного та резервного шляху (мультишляху);
- (2.10), (2.11), (2.14), (2.15) та (2.16), (2.17), що вводяться для реалізації можливих схем захисту елементів мережі (каналу, вузла та шляху відповідно);
- (2.19), (2.20), що формалізують умови запобігання перевантаження каналів зв'язку мережі та захисту пропускної здатності мережі, включаючи випадок, коли лише деякі з потоків перемикаються на резервні шляхи;
- (2.22), яка відповідає за те, що основний шлях (мультишлях) завжди буде не гірший, ніж резервний у межах обраних метрик.

Залежно від виду цільової функції та обмежень, які визначаються обраною стратегією маршрутизації (одношляховою або багатошляховою), сформульована оптимізаційна задача може належати до того чи іншого класу задач математичного програмування, що потребує використання відповідного методу розв'язання (табл. 2.3). З огляду на те, що обмеження (2.17), які вводяться для реалізації схеми захисту шляху, та умови (2.19) і (2.20), пов'язані із запобіганням перевантаження каналів зв'язку мережі, мають нелінійний характер, то і сформульована оптимізаційна задача в будь-якому випадку належатиме до класу задач нелінійного програмування.

Таблиця 2.3

### Характеристика оптимізаційних задач відмовостійкої маршрутизації та методів їх розв'язання

Клас оптимізаційної задачі	Методи розв'язання
<b>Стратегія маршрутизації: одношляхова</b>	
змішаного цілочисельного нелінійного програмування	метод округлення, метод гілок і меж, методи послідовної лінеаризації, метод імітації відпалу, генетичний алгоритм, різні змішані (гібридні) методи
<b>Стратегія маршрутизації: багатошляхова</b>	
нелінійного програмування	метод невизначених множників Лагранжа, метод штрафних функцій, градієнтні методи

Крім того, у реалізації одношляхової маршрутизації маршрутні змінні матимуть булевий характер, у зв'язку з чим розв'язувана оптимізаційна задача вже належатиме до підкласу задач змішаного цілочисельного нелінійного програмування (Mixed Integer Nonlinear Programming, MINLP).

За відсутності необхідності в захисті шляху та/або його пропускної здатності сформульована задача належатиме до класу задач булевого програмування (у разі одношляхової маршрутизації) або лінійного програмування (за умови багатошляхової маршрутизації).

### 2.7.3. Обґрунтування вибору вагових коефіцієнтів у критерії оптимальності рішень щодо швидкої перемаршрутизації в ІКМ

Особливості розв'язання задачі швидкої перемаршрутизації з використанням моделі (1.1)–(1.4), (2.9)–(2.21), (2.23) продемонструємо на прикладі мережної структури, зображеної на рис. 2.24. Представлена мережа складається з 13 маршрутизаторів та 22 каналів зв'язку. У розривах каналів зв'язку вказані їх пропускні здатності. Нехай маршрутні метрики каналів приймали значення  $10^7/\varphi_{i,j}$  за аналогією з протоколом IGRP.

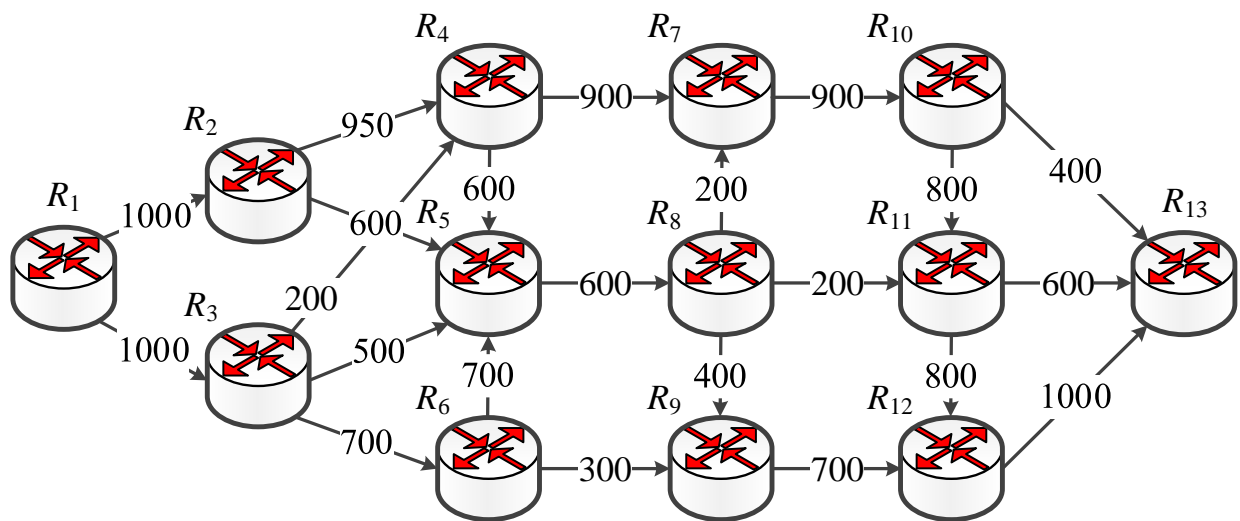


Рис. 2.24. Приклад структури ІКМ, що досліджуються

Під час дослідження встановлено низку закономірностей. По-перше, якщо для реалізації схем захисту вузла та каналу в ІКМ обирати співвідношення числових значень коефіцієнтів у (2.23) так, як пропонується в [74–76], тобто  $b_{i,j}^k \gg c_{i,j}^k$  і  $b_{i,j}^k \gg \bar{c}_{i,j}^k$ , то визначальним у цільовій функції буде третій доданок. Це призводить до того, що в розрахунках як основний, так і резервний шлях завжди, поки це можливо, тобто за відсутності

перевантаження ІКМ, повністю збігатимуться, обходячи елемент мережі, який захищається. Наприклад, якщо необхідно передавати пакети з інтенсивністю 100 1/с від першого маршрутизатора до тринадцятого із забезпеченням захисту четвертого маршрутизатора, то основний і резервний шляхи пройдуть послідовно через маршрутизатори  $R_1 \rightarrow R_3 \rightarrow R_6 \rightarrow R_9 \rightarrow R_{12} \rightarrow R_{13}$ . Однак оптимальним маршрутом, з точки зору пропускної здатності та кількості переприйомів, є шлях  $R_1 \rightarrow R_2 \rightarrow R_4 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{13}$ . Таким чином, подібний вибір співвідношення коефіцієнтів у цільовій функції (2.23) може призвести до значної втрати продуктивності ІКМ, особливо якщо елемент (вузол або канал), який захищається і не включається в основний маршрут, є частиною високопродуктивної ділянки мережі.

Під час дослідження встановлено, що більш ефективною є така ієрархія співвідношень між ваговими коефіцієнтами в цільовій функції (2.23):  $c_{i,j}^k \gg b_{i,j}^k$  і  $b_{i,j}^k \gg \bar{c}_{i,j}^k$ . Тоді основний маршрут завжди буде мати найкращу метрику незалежно від того, містить він елемент мережі, що захищається, чи ні. Ключовим критерієм для вибору резервного шляху тоді стане його мінімальне розходження з основним маршрутом за складом каналів, що його утворюють. Продемонструємо ці можливості на мультипотоківому прикладі.

Нехай в ІКМ, структура якої зображена на рис. 2.24, необхідно захистити високошвидкісний канал між маршрутизаторами  $R_4$  і  $R_7$  під час передачі пакетів двох потоків, що мають такі характеристики:

- $\lambda^1 = 100$  1/с від вузла-відправника  $s_1 = R_1$  до вузла-отримувача  $d_1 = R_{13}$ ;
- $\lambda^2 = 100$  1/с від вузла-відправника  $s_2 = R_2$  до вузла-отримувача  $d_2 = R_{10}$ .

Ілюстрація отриманого рішення за умови використання запропонованої моделі наведена на рис. 2.25, де основний шлях зображений суцільною лінією, резервний – пунктирною, тоді як канали зв'язку, що не використовуються, показані напівпрозорими лініями. У розривах каналів зв'язку вказані їх пропускні здатності (1/с).

У цьому випадку основні маршрути проходять через такі маршрутизатори:

- $R_1 \rightarrow R_2 \rightarrow R_4 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{13}$  – для першого потоку;
- $R_2 \rightarrow R_4 \rightarrow R_7 \rightarrow R_{10}$  – для другого потоку;

а резервні шляхи можна записати в такому вигляді:

- $R_1 \rightarrow R_2 \rightarrow R_4 \rightarrow R_5 \rightarrow R_8 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{13}$  – для першого потоку;
- $R_2 \rightarrow R_4 \rightarrow R_5 \rightarrow R_8 \rightarrow R_7 \rightarrow R_{10}$  – для другого потоку.



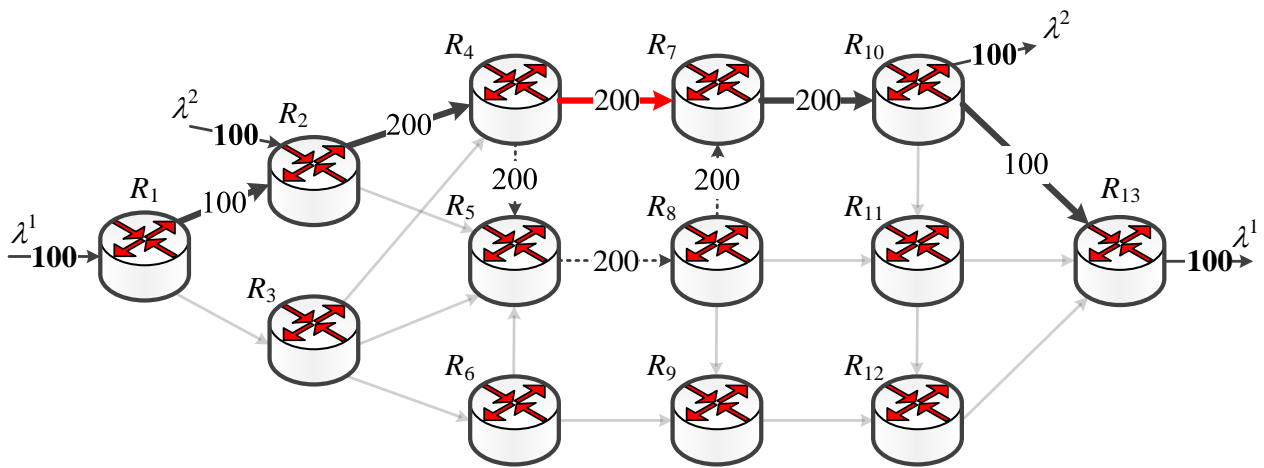


Рис. 2.25. Результати розв'язання задачі швидкої перемаршрутизації в ІКМ на основі використання критерію (2.23) та підтримки схеми «facility backup»

Як видно з отриманих результатів розрахунків (рис. 2.25), канал  $E_{4,7}$ , який захищається, має досить високу пропускну здатність (900 л/с) і використовується в основних маршрутах обох потоків, що позитивно позначається на продуктивності кінцевих рішень. З точки зору масштабованості ІКМ важливо зазначити, що отримане рішення щодо захисту зазначеного каналу максимально відповідає вимогам схеми «facility backup» [5, 34]. Це проявляється в тому, що спільний елемент  $E_{4,7}$  основних маршрутів для розглянутих двох потоків захищено однією (спільною для цих потоків) резервною ділянкою  $R_4 \rightarrow R_5 \rightarrow R_8 \rightarrow R_7$ . Тоді резервний шлях відрізняється від основного за чотирма каналами зв'язку.

Варто зазначити, що вимогам схеми «facility backup» також відповідає і рішення  $R_4 \rightarrow R_5 \rightarrow R_8 \rightarrow R_{11} \rightarrow R_{10}$  як частина резервних маршрутів. Однак воно не є оптимальним з точки зору критерію (2.23), тому що в цьому випадку резервний шлях відрізняється від основного за шістьма КЗ.

Окремо слід виокремити випадок, коли під час розрахунку резервних шляхів виникає неоднозначність у їх виборі. Приклад подібної ситуації наведений на рис. 2.26, на якому в розривах каналів зв'язку вказані їх пропускі здатності. Нехай основний шлях містить канал  $E_{1,4}$ , що захищається, тоді резервний шлях може пройти як через  $R_2$ , так і через  $R_3$  – у кожному із зазначених випадків третій доданок у цільовій функції (2.23) прийме одне й те саме значення.

Тому у виборі резервного шляху важливо враховувати метрики каналів резервних маршрутів, представлених ваговими коефіцієнтами, для чого і було

введено в критерій оптимальності (2.23) другий доданок. У матриці числа переприйомів (як у протоколі RIP) ці два резервних шляхи є ідентичними.

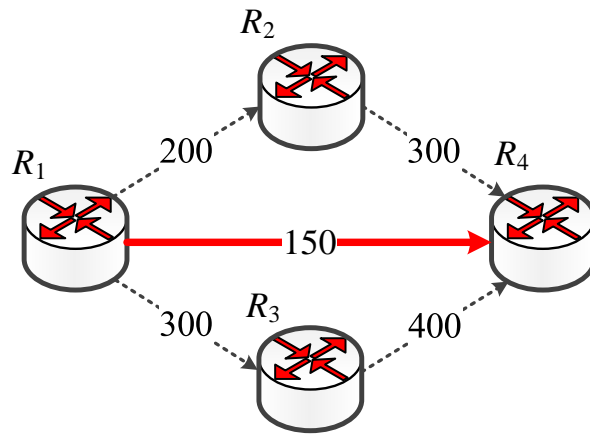


Рис. 2.26. Приклад виникнення неоднозначності у виборі резервного шляху

Однак у разі використання метрики протоколу IGRP  $(10^7/\phi_{i,j})$  буде оптимальним резервний шлях  $R_1 \rightarrow R_3 \rightarrow R_4$ , тому що він має пропускну здатність 300 1/с. Неоптимальний резервний маршрут  $R_1 \rightarrow R_2 \rightarrow R_4$  має дещо меншу пропускну здатність (200 1/с).

Удосконалена модель швидкої перемаршрутизації може використовуватися і в тому випадку, коли як основний, так і резервний шляхи є мультишляхами, тобто містять кілька маршрутів від відправника до отримувача. Припустимо, що на структурі ІКМ, наведеної на рис. 2.24, пакети передаються від першого маршрутизатора до 13-го з інтенсивністю 700 1/с. Нехай необхідно реалізувати схему захисту шляху, зокрема основний і резервний мультишляхи не повинні мати спільних вузлів і каналів, тобто третій доданок у цільовій функції (2.23) дорівнюватиме нулю. Тоді на рис. 2.27 показано результат вирішення поставленого завдання за допомогою запропонованої потокової моделі швидкої перемаршрутизації в ІКМ, де, як і раніше, основний мультишлях представлено суцільною лінією, резервний – пунктирною, а невикористовувані канали зв'язку зображені напівпрозорими лініями. У розривах каналів зв'язку вказано інтенсивність потоку пакетів (1/с).

Таким чином, основний мультишлях містить два шляхи (рис. 2.27). Першим шляхом  $R_1 \rightarrow R_2 \rightarrow R_4 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{13}$  передається потік пакетів з інтенсивністю 400 1/с, а другим  $R_1 \rightarrow R_2 \rightarrow R_4 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{11} \rightarrow R_{13}$  – потік з інтенсивністю 300 1/с.

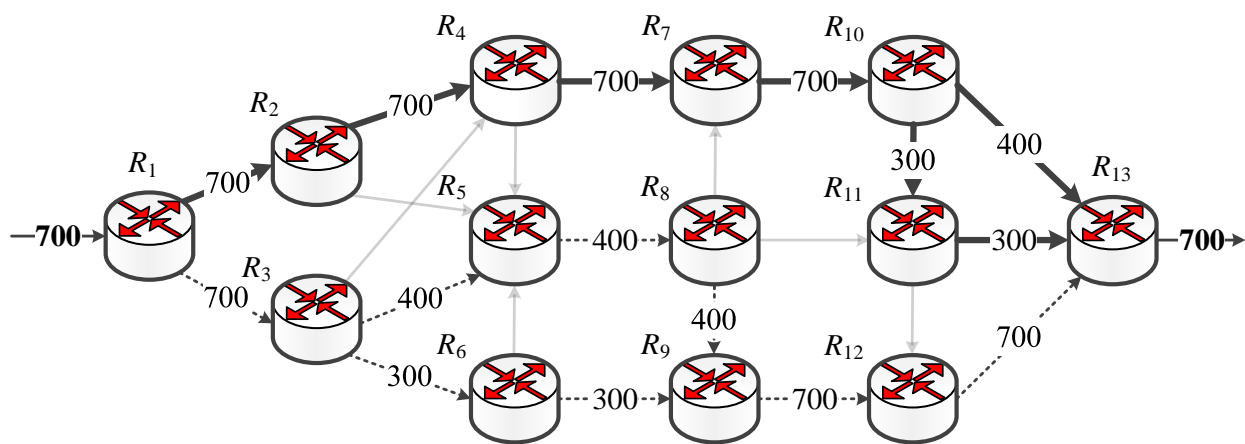


Рис. 2.27. Результат розв'язання задачі багатошляхової швидкої перемаршрутизації в ІКМ з використанням критерію оптимальності (2.23)

Резервний мультишлях також складається з двох маршрутів. Першим шляхом, який формується послідовністю маршрутизаторів  $R_1 \rightarrow R_3 \rightarrow R_5 \rightarrow R_8 \rightarrow R_9 \rightarrow R_{12} \rightarrow R_{13}$ , пакети передаються з інтенсивністю 400 1/с, а другим  $R_1 \rightarrow R_3 \rightarrow R_6 \rightarrow R_9 \rightarrow R_{12} \rightarrow R_{13}$  – потік з інтенсивністю 300 1/с. Відповідно до отриманих результатів розрахунку основний і резервний мультишляхи не мають спільних мережних елементів (вузлів або каналів), що позитивно впливає на рівень відмовостійкості ІКМ, а реалізація багатошляхової стратегії маршрутизації сприяє підвищенню якості обслуговування.

#### 2.7.4. Білінійний критерій оптимальності рішень щодо швидкої перемаршрутизації в процесі реалізації схеми захисту шляху

Нелінійність умов захисту мультишляху (2.17) негативно позначається на рівні обчислювальної складності рішень щодо швидкої перемаршрутизації. Тому в роботі пропонується використовувати критерій оптимальності, який оснований на мінімізації такої білінійної цільової функції [77, 78]:

$$\begin{aligned}
 F = & \sum_{k \in K} \sum_{E_{i,j} \in E} c_{i,j}^k x_{i,j}^k x_{i,j}^k + \sum_{k \in K} \sum_{E_{i,j} \in E} c_{i,j}^k x_{i,j}^k + \sum_{k \in K} \sum_{E_{i,j} \in E} \bar{c}_{i,j}^k \bar{x}_{i,j}^k \bar{x}_{i,j}^k + \\
 & + \sum_{k \in K} \sum_{E_{i,j} \in E} \bar{c}_{i,j}^k \bar{x}_{i,j}^k + \sum_{R_i \in R \setminus \{s_k, d_k\}} \sum_{R_j \in R_i^*} \sum_{R_p \in R_i^*} h x_{j,i}^k \bar{x}_{p,i}^k, \quad (2.24)
 \end{aligned}$$

де  $h$  – ваговий коефіцієнт, який характеризує важливість білінійного доданка в критерії оптимальності (2.24).

Перший і другий доданки у виразі (2.24) визначають умовні вартості формування та використання основного шляху/мультишляху, а третій і четвертий – резервного. П'ятий доданок є найбільш важливим і відповідає за

реалізацію схеми захисту шляху, тобто за відсутність спільних вузлів і каналів в основному і резервному маршрутах. Таким чином, установлюється така система ієрархії співвідношень вагових коефіцієнтів у цільовій функції (2.24):

$$h \gg c_{i,j}^k \text{ і } h \gg \bar{c}_{i,j}^k, \quad (2.25)$$

а також доданків:

$$\begin{aligned} & \sum_{k \in K} \sum_{E_{i,j} \in E} c_{i,j}^k x_{i,j}^k x_{i,j}^k + \sum_{k \in K} \sum_{E_{i,j} \in E} \bar{c}_{i,j}^k x_{i,j}^k \leq \\ & \leq \sum_{k \in K} \sum_{E_{i,j} \in E} \bar{c}_{i,j}^k \bar{x}_{i,j}^k \bar{x}_{i,j}^k + \sum_{k \in K} \sum_{E_{i,j} \in E} \bar{c}_{i,j}^k \bar{x}_{i,j}^k. \end{aligned} \quad (2.26)$$

Виконання умови (2.26) гарантує, що розрахований основний шлях/мультишлях не поступатиметься за ефективністю резервному.

Отже, у межах проведеного вдосконалення математичної моделі завдання швидкої перемаршрутизації було сформульовано в оптимізаційній формі. Зокрема критерієм оптимальності є мінімум цільової функції (2.24), а обмеженнями – умови (1.2), (1.3), (2.9), (2.11), (2.12), (2.15). Для реалізації швидкої перемаршрутизації в ІКМ розрахунок шуканих маршрутних змінних забезпечується внаслідок розв'язання задачі нелінійного програмування. Крім того, пропоноване вдосконалення моделі швидкої перемаршрутизації з білінійним критерієм оптимальності для захисту мультишляху є більш строгим, ніж у [74], тому що основний і резервний маршрути, які розраховуються, не перетинаються ні за вузлами, ні за каналами.

Проведемо аналіз впливу квадратичних доданків критерію (2.24) та завантаженості мережі на характер результативних маршрутних рішень для ІКМ на прикладі мережної структури, наведеної на рис. 2.28, за умови захисту мультишляху між вузлом-відправником  $s_1 = R_1$  і вузлом-отримувачем  $d_1 = R_9$ . У розривах каналів зв'язку вказані їх пропускні здатності. Для забезпечення розрахунку шляхів з максимальною продуктивністю маршрутні метрики каналів зв'язку приймали значення  $10^7 / \varphi_{i,j}$  за аналогією з протоколом IGRP.

Нехай інтенсивність потоку пакетів становить  $\lambda^1 = 200$  1/с. Тоді на рис. 2.29, а наведено результат розрахунків на випадок відсутності в критерії (2.24) квадратичних доданків, який визначив реалізацію одношляхової маршрутизації (без балансування навантаження). Основний шлях, що проходить через маршрутизатори  $R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_6 \rightarrow R_9$ , представлено суцільною лінією, резервний  $R_1 \rightarrow R_4 \rightarrow R_7 \rightarrow R_8 \rightarrow R_9$  – пунктирною, тоді як канали зв'язку, які не використовуються, зображені

напівпрозорими лініями. На рис. 2.29 у розривах каналів зв'язку вказано інтенсивність потоку пакетів (1/с).

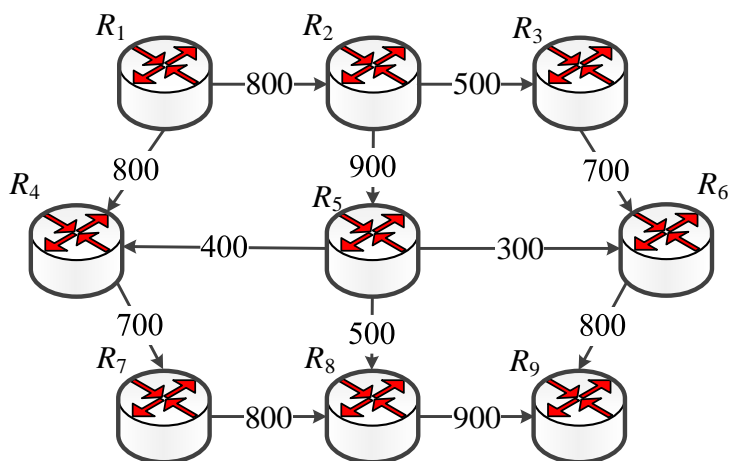
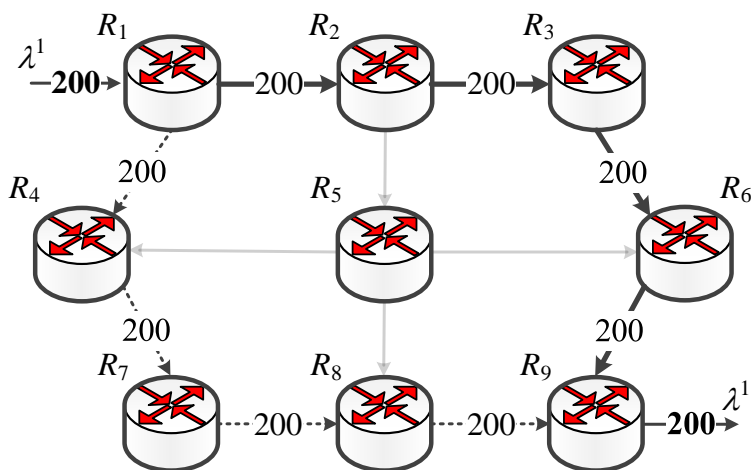
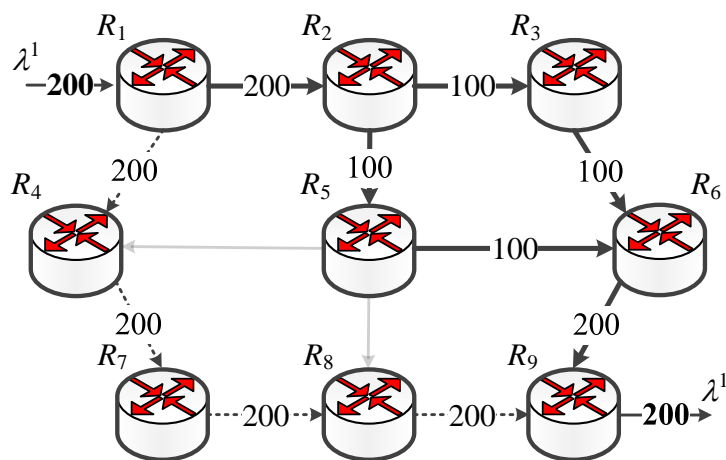


Рис. 2.28. Вихідна структура ІКМ, що досліджувалась



а) без квадратичних доданків у (2.24)



б) з квадратичними доданками в (2.24)

Рис. 2.29. Послідовність швидкої перемаршрутизації потоку з інтенсивністю 200 1/с на основі використання критерію оптимальності (2.24)

Введення квадратичних доданків у критерій (2.24) сприяло реалізації багатошляхової швидкої перемаршрутизації (рис. 2.29, б), коли основний мультишлях був представлений двома маршрутами:

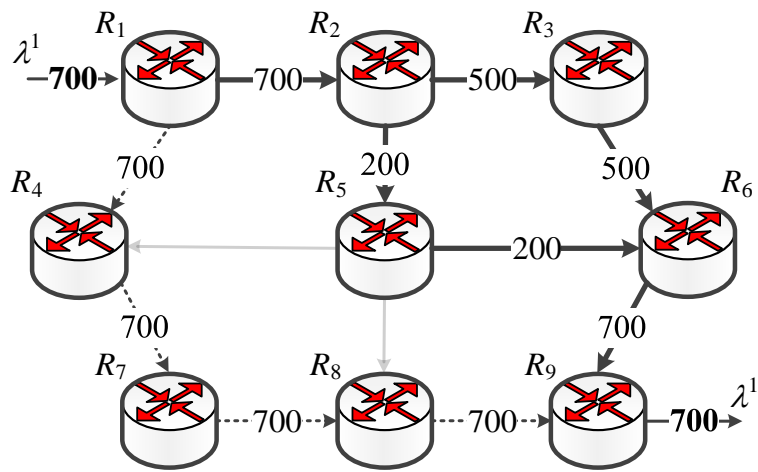
–  $R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_6 \rightarrow R_9$  за умови передачі потоку з інтенсивністю 100 1/с;

–  $R_1 \rightarrow R_2 \rightarrow R_5 \rightarrow R_6 \rightarrow R_9$  у разі передачі потоку з інтенсивністю 100 1/с; тоді як резервний шлях проходить через маршрутизатори:

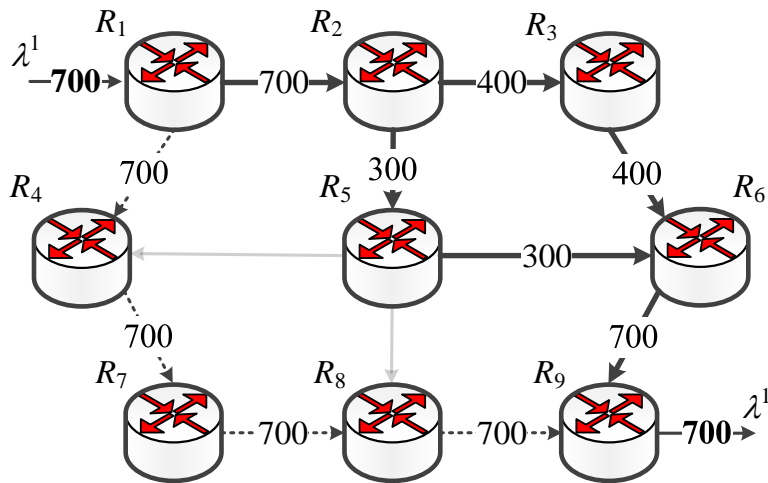
–  $R_1 \rightarrow R_4 \rightarrow R_7 \rightarrow R_8 \rightarrow R_9$ .

У випадку збільшення завантаженості мережі, коли інтенсивність потоку становила  $\lambda^1 = 700$  1/с, використання критерію (2.24) сприяло реалізації багатошляхової швидкої перемаршрутизації. У цьому випадку основний мультишлях складався з двох шляхів:  $R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_6 \rightarrow R_9$  та  $R_1 \rightarrow R_2 \rightarrow R_5 \rightarrow R_6 \rightarrow R_9$ . Зокрема, якщо квадратичні члени в функції (2.24) були відсутні, то потік балансувався між ними частинами за 500 та 200 1/с відповідно (рис. 2.30, а). У разі введення квадратичних доданків у цільову функцію (2.24) потік балансувався між основними маршрутами частинами за 400 та 300 1/с відповідно (рис. 2.30, б). Резервний шлях в обох випадках забезпечував передачу всього потоку через маршрутизатори  $R_1 \rightarrow R_4 \rightarrow R_7 \rightarrow R_8 \rightarrow R_9$ .

Отже, введення квадратичних членів у критерій (2.24) дозволяє, по-перше, забезпечити реалізацію багатошляхової швидкої перемаршрутизації навіть за умови невисокої завантаженості мережі, тоді як без їх введення здійснювалося послідовне вмикання шляхів відповідно до збільшення їх метрик; по-друге, у разі високої завантаженості ІКМ вдалося забезпечити краще балансування навантаження в мережі (рис. 2.30). Введення в критерій (2.24) відповідної білінійної форми дозволило забезпечити розрахунок основного та резервного шляху/мультишляху, які не перетинаються ні за вузлами, ні за каналами.



а) без квадратичних доданків у (2.24)



б) з квадратичними доданками в (2.24)

Рис. 2.30. Порядок швидкої перемаршрутизації потоку з інтенсивністю 700 1/с на основі використання критерію оптимальності (2.24)

### 2.7.5. Приклади розв'язання задачі швидкої перемаршрутизації багатоадресних потоків в ІКМ

Розглянемо особливості організації швидкої перемаршрутизації багатоадресних потоків за умови реалізації різних схем захисту елементів мережі [73]. Нехай структура аналізованої мережі представлена на рис. 2.31, тобто вона складається з п'яти маршрутизаторів і семи каналів зв'язку, у розривах яких вказані їх пропускі здатності (1/с). Вузол-відправник – перший маршрутизатор ( $s_1 = R_1$ ), вузли-отримувачі – третій, четвертий і п'ятий маршрутизатори. Інтенсивність багатоадресного потоку становить  $\lambda^1 = 70$  1/с.

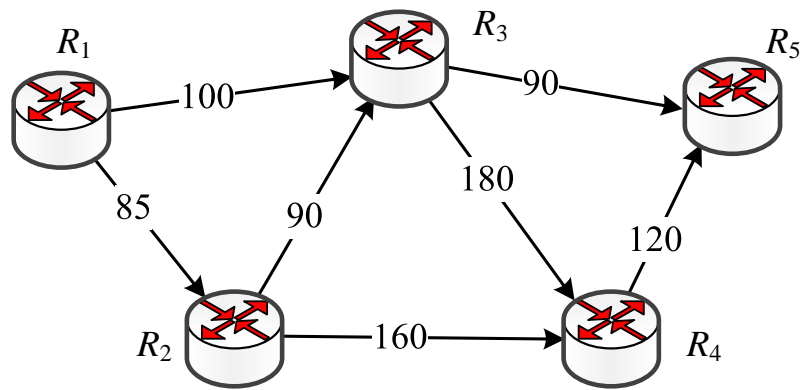


Рис. 2.31. Структура аналізованої мережі під час маршрутизації одного багатоадресного потоку

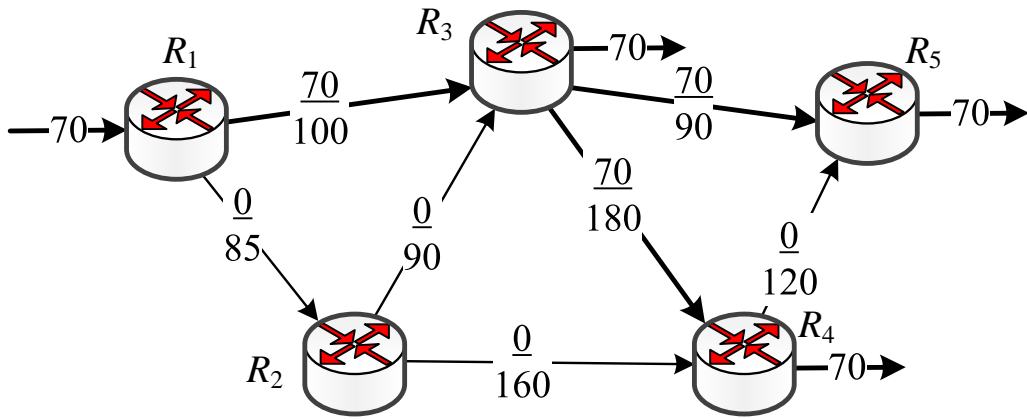
На рис. 2.32 наведено приклади розв'язання задачі швидкої перемаршрутизації багатоадресного потоку в мережі, наприклад, із захистом каналу зв'язку  $E_{1,3}$  у разі мінімізації кількості переприйомів пакетів ( $c_{i,j}^k = \bar{c}_{i,j}^k = 1$ ). Тоді як основне дерево маршрутів є рішенням, представленим на рис. 2.32, а, зокрема «довжина» цього дерева мінімальна та становить три канали. Резервне дерево маршрутів (рис. 2.32, б), яке складається з чотирьох КЗ, відповідно до реалізованої схеми захисту не містить каналу  $E_{1,3}$ . На рис. 2.32 в розривах каналів зв'язку вказано дріб, в якому в чисельнику наведено інтенсивність потоку пакетів, а в знаменнику – пропускну здатність цього ж каналу. Як зображено на рис. 2.32, і основне, і резервне дерево маршрутів можуть обслужити багатоадресний потік інтенсивністю 70 1/с.

У процесі реалізації схеми захисту шляху дерево основного маршруту представлено на рис. 2.32, а, а резервне дерево маршрутів тоді буде також містити чотири канали й мати структуру, наведену на рис. 2.33.

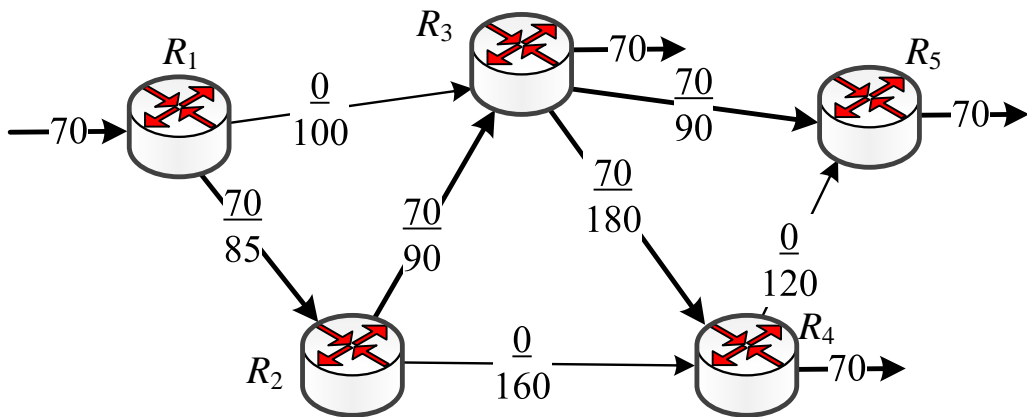
Порядок швидкої перемаршрутизації багатоадресного потоку також сильно залежить від типу використовуваної маршрутної метрики. Якщо вибрати метрику, орієнтовану на врахування пропускну здатності КЗ, тобто якщо  $c_{i,j}^k = \bar{c}_{i,j}^k = 10^7 / \varphi_{i,j}$ , то й основне дерево маршрутів, і резервне дещо зміняться (рис. 2.34). Так, наприклад, для захисту каналу  $E_{1,3}$  застосування цієї метрики дозволяє підвищити пропускну здатність основного маршруту до 120 1/с (рис. 2.34, а). Резервний маршрут (рис. 2.34, б) також міститиме більш продуктивні канали, ніж у рішенні, наведеному на рис. 2.32, б, що призведе до зниження середньої затримки та ймовірності втрат пакетів.

Рішення, запропоноване на рис. 2.34, також повністю відповідає вимогам схеми «facility backup».





а) основне дерево маршрутів для багатоадресного потоку



б) резервне дерево маршрутів для багатоадресного потоку

Рис. 2.32. Приклад розв'язання задачі швидкої перемаршрутизації багатоадресного потоку в мережі із захистом каналу зв'язку  $E_{1,3}$  за умови мінімізації кількості переприйомів пакетів

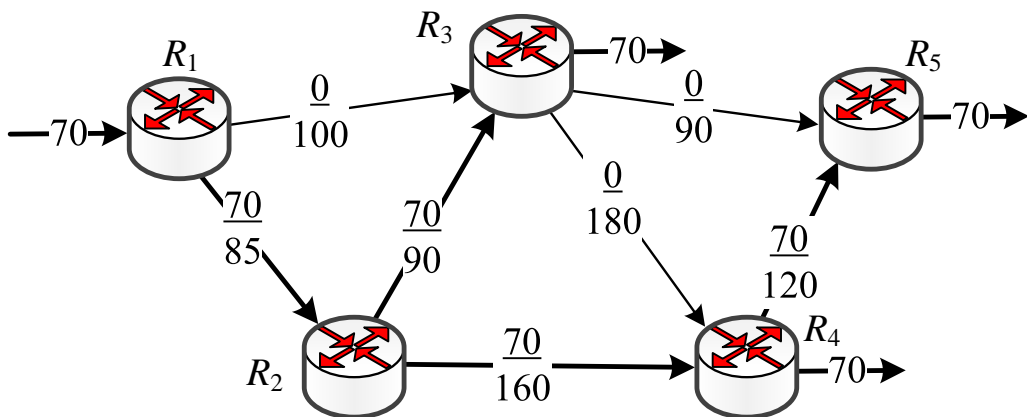
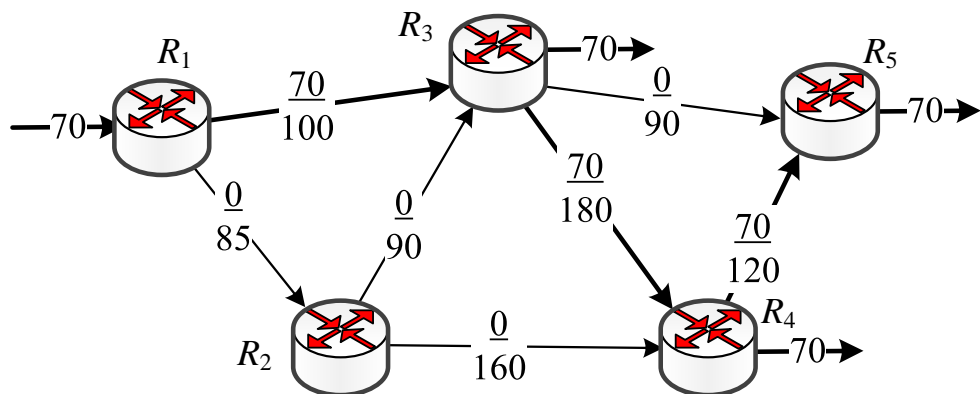
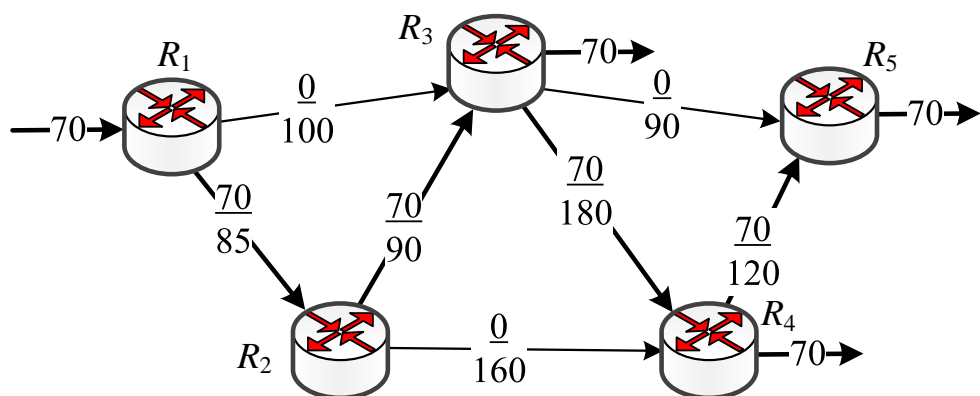


Рис. 2.33. Приклад розв'язання задачі швидкої перемаршрутизації багатоадресного потоку в мережі із захистом шляху за умови мінімізації кількості переприйомів пакетів



а) основне дерево маршрутів для багатоадресного потоку



б) резервне дерево маршрутів для багатоадресного потоку

Рис. 2.34. Приклад розв'язання задачі швидкої перемаршрутизації багатоадресного потоку в мережі із захистом каналу зв'язку  $E_{1,3}$

за умови використання метрики  $c_{i,j}^k = \bar{c}_{i,j}^k = 10^7 / \varphi_{i,j}$

## 2.8. Рішення щодо швидкої перемаршрутизації з балансуванням навантаження в ІКМ

Реалізація відмовостійкої маршрутизації з резервуванням мережних елементів основане на введенні ресурсної надлишковості, коли одночасно з визначенням основного маршруту (ОМ) розраховується і резервний маршрут (РМ) відповідно до реалізованої схеми захисту. У зв'язку з цим у вирішенні завдань швидкої перемаршрутизації важливо забезпечити збалансоване використання доступного мережного, насамперед каналного ресурсу, щоб захист елемента мережі не спричинив перевантаження ІКМ та істотне зниження рівня QoS. Тому для науки та практики є актуальним дослідження, спрямоване на розвиток концепції швидкої перемаршрутизації з балансуванням навантаження (Traffic Engineering Fast ReRoute, TE FRR) [31, 32, 63]. Тому в цьому підрозділі будуть запропоновані теоретичні рішення

щодо узгодженого вирішення завдань швидкої перемаршрутизації та балансування навантаження, орієнтованих на зниження обчислювальної складності та підвищення масштабованості протокольних рішень у процесі реалізації як одношляхової, так і багатошляхової стратегії маршрутизації.

### 2.8.1. Синтез та дослідження дворівневого методу одношляхової швидкої перемаршрутизації з балансуванням навантаження в ІКМ

Для забезпечення балансування навантаження в ІКМ на принципах концепції Traffic Engineering під час реалізації одношляхової швидкої перемаршрутизації (1.1) в ІКМ пропонується модифікувати модель (1.3), (2.9), (2.10), (2.14), (2.17), по-перше, змінивши форму умов захисту ПЗ (2.19) зі збереженням їх фізичного змісту, по-друге, сформулювавши задачу розрахунку маршрутних змінних  $x_{i,j}^k$  і  $\bar{x}_{i,j}^k$  як оптимізаційну, пов'язану з балансуванням навантаження в ІКМ, а по-третє, увівши дворівневу функціональну ієрархію розрахунків маршрутних змінних різних типів.

Тоді умови (2.19) пропонується представити в формі [81, 82]

$$\sum_{k \in K} \lambda^k \left( x_{i,j}^k + \bar{x}_{i,j}^k - x_{i,j}^k \bar{x}_{i,j}^k \right) \leq \alpha \varphi_{i,j}, \quad E_{i,j} \in E, \quad (2.27)$$

де  $\alpha$  – додатково введена змінна, яка визначає верхній поріг завантаженості каналів зв'язку ІКМ і підпорядковується умовам [79, 80]:

$$0 \leq \alpha \leq 1. \quad (2.28)$$

Відзначимо, що ліві частини нерівностей (2.19) і (2.27) завжди дають однаковий числовий результат. Критерієм оптимальності розв'язань задачі швидкої перемаршрутизації в ІКМ за аналогією з результатами, отриманими в [79, 80], буде мінімум уведеного в (2.27) порога  $\alpha$ , тобто

$$\min_{x, \bar{x}, \alpha} \alpha. \quad (2.29)$$

Виконання умов (2.27)–(2.29) дозволяє забезпечити оптимальне балансування навантаження у процесі реалізації схеми захисту пропускної здатності розрахованих шляхів. У межах пропонованого методу вводиться дворівнева ієрархія розрахунків, яка підпорядковується принципу прогнозування взаємодій теорії ієрархічних багаторівневих систем [83, 84]. Тоді на нижньому рівні (рис. 2.35) пропонується здійснювати розрахунок маршрутних змінних  $x_{i,j}^k$ , які відповідають за визначення основних шляхів у мережі, під час мінімізації порогу  $\alpha$  (2.29), але за умови фіксованих значень  $\bar{x}_{i,j}^k$ , що задаються на верхньому ієрархічному рівні. У цьому випадку

важливо забезпечити задоволення умов-обмежень (1.1), (1.3), (2.17), (2.28), а для захисту шляху – додатково й умови (2.27). У разі такого формулювання задачі умови (2.17) і (2.27) уже будуть лінійними, тому що значення  $\bar{x}_{i,j}^k$  для нижнього рівня є відомими.

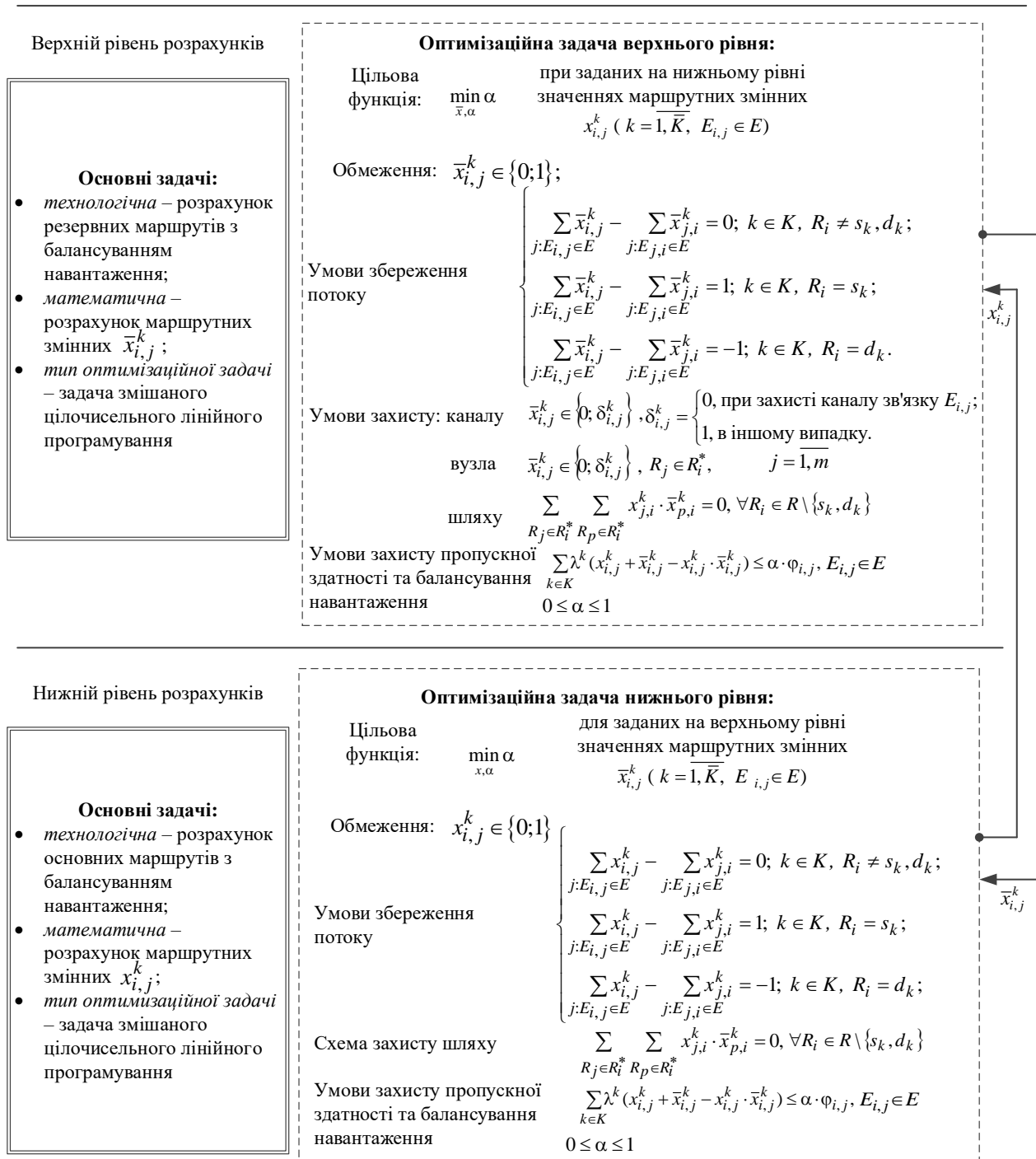


Рис. 2.35. Структура дворівневого методу швидкої перемаршрутизації з балансуванням навантаження в ІКМ [81]

На верхньому рівні ієрархії (рис. 2.35) розраховуються маршрутні змінні  $\bar{x}_{i,j}^k$ , які відповідають за формування (а фактично прогнозування) резервних маршрутів, також шляхом мінімізації змінної  $\alpha$  (2.29) за умови фіксованих і розрахованих на нижньому рівні значень маршрутних змінних  $x_{i,j}^k$ . У процесі оптимізації на цьому рівні необхідно виконати умови:

- у разі реалізації схеми захисту шляху – (2.9), (2.17), (2.27) і (2.28);
- у випадку реалізації схем захисту каналу або вузла – (2.9), (2.27), (2.28) і (2.10) або (2.14).

З огляду на те що для верхнього рівня розрахунку значення  $x_{i,j}^k$  відомі, то умови (2.17) і (2.27) також стають лінійними. Таким чином, процес розв'язання сформульованої задачі швидкої перемаршрутизації в ІКМ набуває ітераційного характеру. Зокрема критерієм завершення розрахунків є досягнення оптимуму (2.29), що проявляється в близькості значень цільової функції (2.29), розрахованої на сусідніх ітераціях, але на різних ієрархічних рівнях.

Важливо зазначити, що для забезпечення захисту каналу, вузла, шляху та пропускної здатності в мережі застосування описаного методу дозволяє відмовитися від розв'язання вихідної нелінійної та досить розмірної оптимізаційної задачі шляхом переходу до ітераційного розв'язання лінійних оптимізаційних задач удвічі меншої розмірності (рис. 2.35).

Це неодмінно позначається на кінцевій масштабності протокольних рішень щодо швидкої перемаршрутизації з балансуванням навантаження в мережі загалом. Таким чином, ефективність запропонованого методу безпосередньо залежить від кількості ітерацій, за які він забезпечує пошук оптимальних з точки зору критерію (2.29) значень маршрутних змінних, що відповідають за формування основних і резервних маршрутів. Ця функціональна особливість запропонованого методу підлягає додатковому дослідженню.

Особливості роботи методу продемонструємо на числовому прикладі. За основу буде взята структура мережі, показана на рис. 2.36. У табл. 2.4 вказані пропускні здатності каналів зв'язку мережі.

Нехай у мережі (рис. 2.36) необхідно забезпечити вирішення завдань швидкої перемаршрутизації з реалізацією схеми захисту шляху для двох потоків, характеристики яких наведені в табл. 2.5.

Як показали результати проведеного аналізу, запропонований метод швидкої перемаршрутизації в ІКМ для вихідних даних, представлених у табл. 2.4 та 2.5, забезпечував знаходження оптимальних значень маршрутних

змінних (1.1), (2.10) і порога завантаженості (2.28) (рис. 2.37) у середньому за 2–3 ітерації (рис. 2.38). Зокрема, як видно з рис. 2.37 та 2.38, кількість ітерацій збільшується до трьох у разі рівності або близькості значень інтенсивностей потоків пакетів, що передаються. У табл. 2.6–2.8 для прикладу показані результати розрахунків для трьох ітерацій роботи методу за умови  $\lambda^1 = 240$  1/с та  $\lambda^2 = 220$  1/с.

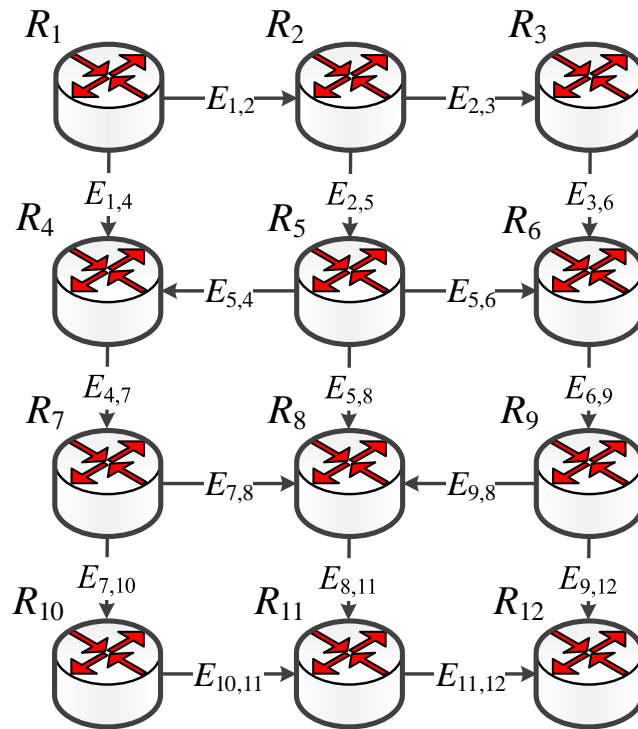


Рис. 2.36. Структура аналізованої ІКМ

Таблиця 2.4

**Пропускні здатності каналів зв'язку мережі**

Канал зв'язку	Пропускна здатність, 1/с	Канал зв'язку	Пропускна здатність, 1/с	Канал зв'язку	Пропускна здатність, 1/с
$E_{1,2}$	800	$E_{5,6}$	300	$E_{7,10}$	500
$E_{2,3}$	500	$E_{4,7}$	700	$E_{8,11}$	900
$E_{1,4}$	800	$E_{5,8}$	500	$E_{9,12}$	800
$E_{2,5}$	900	$E_{6,9}$	800	$E_{10,11}$	700
$E_{3,6}$	700	$E_{7,8}$	400	$E_{11,12}$	600
$E_{5,4}$	400	$E_{9,8}$	500		

## Характеристики потоків

Номер потоку	Інтенсивність потоку	Відправник	Отримувач
1	$\lambda^1 = 10 \div 250$ 1/с	$R_1$	$R_{12}$
2	$\lambda^2 = 10 \div 250$ 1/с	$R_5$	$R_{11}$

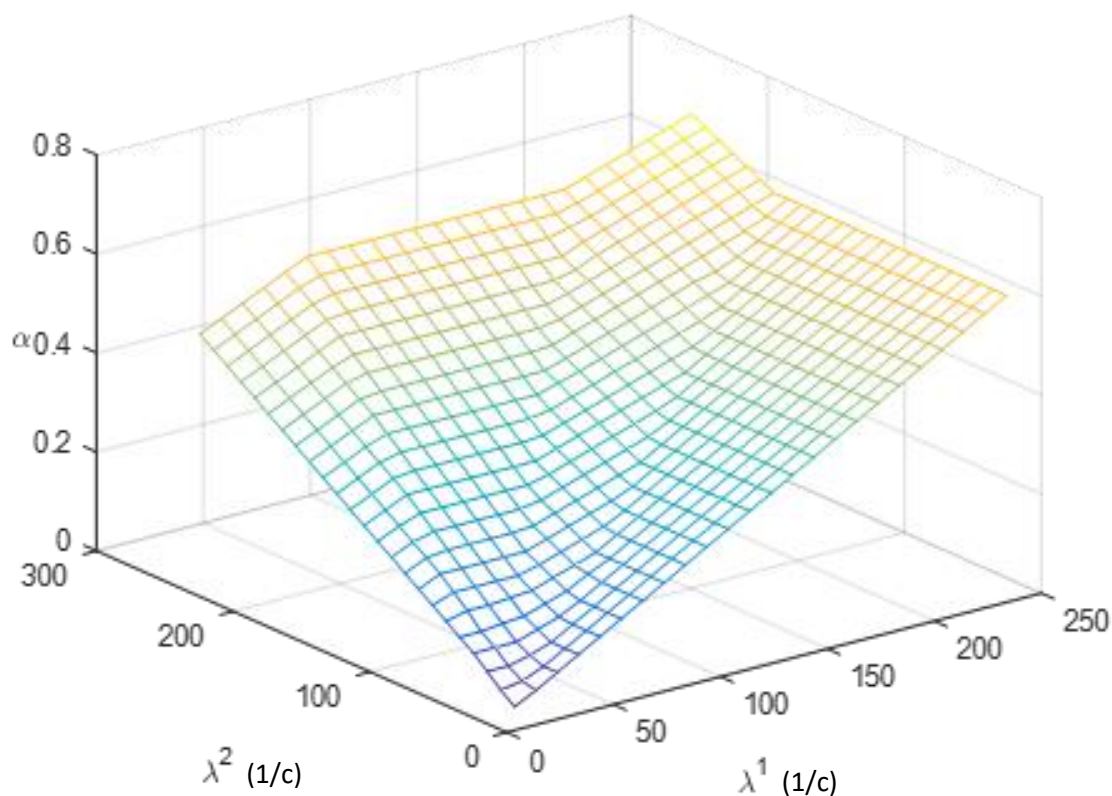


Рис. 2.37. Залежність порога завантаженості каналів зв'язку мережі (2.28) від інтенсивностей потоків пакетів, що передаються (у разі захисту шляхів для двох потоків)

У цих таблицях для кожного каналу вказано коефіцієнт його використання

$$\alpha_{i,j} = \frac{\sum_{k \in K} \max[x_{i,j}^k, \bar{x}_{i,j}^k] \cdot \lambda^k}{\varphi_{i,j}}. \quad (2.30)$$

Фактично  $\alpha$  (2.28) є граничним, тобто максимальним значенням серед множини коефіцієнтів  $\alpha_{i,j}$  (2.30).

Після першої ітерації роботи методу саме завантаженість каналу  $E_{7,10}$  визначає значення порога завантаженості каналів зв'язку мережі в 0,92 (табл. 2.6). У цьому випадку для першого потоку основний шлях проходить через маршрутизатори  $R_1 \rightarrow R_4 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{11} \rightarrow R_{12}$ , а резервний –  $R_1 \rightarrow R_2 \rightarrow R_5$

$\rightarrow R_6 \rightarrow R_9 \rightarrow R_{12}$ . Тоді як для другого потоку основний шлях визначається маршрутизаторами  $R_5 \rightarrow R_8 \rightarrow R_{11}$ , а резервний –  $R_5 \rightarrow R_4 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{11}$ .

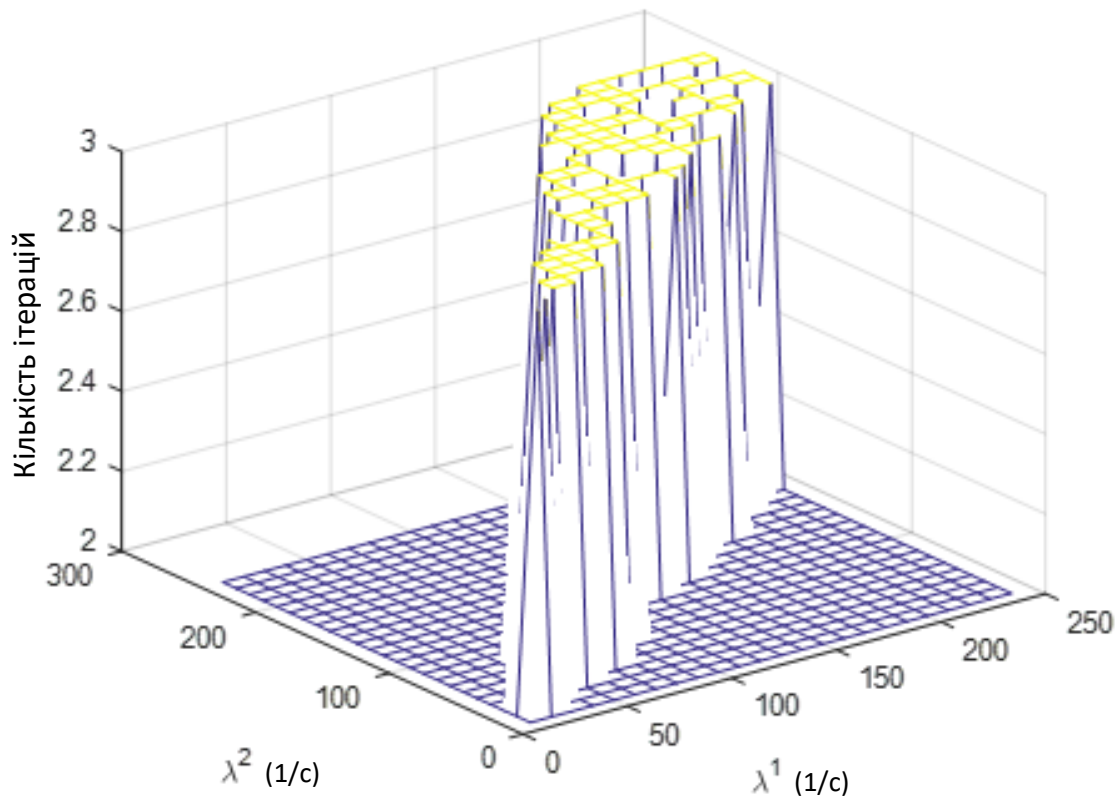


Рис. 2.38. Залежність кількості ітерацій роботи запропонованого методу від інтенсивностей потоків пакетів, що передаються (у разі захисту шляхів для двох потоків)

Після другої ітерації метод забезпечує подальше зниження порога завантаженості каналів зв'язку до 0,8, який (табл. 2.7) визначається за коефіцієнтом використання каналу  $E_{5,6}$ . У цьому випадку основний шлях для першого потоку є  $R_1 \rightarrow R_4 \rightarrow R_7 \rightarrow R_8 \rightarrow R_{11} \rightarrow R_{12}$ , а резервний –  $R_1 \rightarrow R_2 \rightarrow R_5 \rightarrow R_6 \rightarrow R_9 \rightarrow R_{12}$ . Зокрема для другого потоку основний і резервний шляхи залишаються незмінними.

І тільки після третьої ітерації метод визначив кінцеве розв'язання задачі швидкої перемаршрутизації з  $\alpha = 0,657$  (табл. 2.8). Тут для першого потоку основний шлях представлений маршрутизаторами  $R_1 \rightarrow R_4 \rightarrow R_7 \rightarrow R_8 \rightarrow R_{11} \rightarrow R_{12}$ , а резервний –  $R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_6 \rightarrow R_9 \rightarrow R_{12}$ . Як і раніше, для другого потоку основний і резервний шляхи не змінилися.



Таблиця 2.6

Результати розрахунку після першої ітерації роботи методу ( $\alpha = 0,92$ )

Канал зв'язку	Перший потік		Другий потік		$\alpha_{i,j}$
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях	
$E_{1,2}$	0	240	0	0	0,3
$E_{2,3}$	0	0	0	0	0
$E_{1,4}$	240	0	0	0	0,3
$E_{2,5}$	0	240	0	0	0,267
$E_{3,6}$	0	0	0	0	0
$E_{5,4}$	0	0	0	220	0,55
$E_{5,6}$	0	240	0	0	0,8
$E_{4,7}$	240	0	0	220	0,657
$E_{5,8}$	0	0	220	0	0,44
$E_{6,9}$	0	240	0	0	0,3
$E_{7,8}$	0	0	0	0	0
$E_{9,8}$	0	0	0	0	0
$E_{7,10}$	240	0	0	220	0,92
$E_{8,11}$	0	0	220	0	0,244
$E_{9,12}$	0	240	0	0	0,3
$E_{10,11}$	240	0	0	220	0,657
$E_{11,12}$	240	0	0	0	0,4

Продемонструємо особливості роботи запропонованого методу під час реалізації схеми захисту каналу  $E_{8,11}$  для тих самих двох потоків (табл. 2.5). У цьому випадку відповідно до умов (2.14) захист каналу  $E_{8,11}$  фактично забезпечує захист маршрутизатора  $R_8$ . Як показали результати проведеного аналізу, запропонований дворівневий метод одношляхової швидкої перемаршрутизації в ІКМ (табл. 2.4) забезпечував знаходження оптимальних значень маршрутних змінних (1.1), (2.10) і порога завантаженості (2.28) (рис. 2.39) у середньому також за 2–3 ітерації (рис. 2.40).

Таблиця 2.7

Результати розрахунку після другої ітерації роботи методу ( $\alpha = 0,8$ )

Канал зв'язку	Перший потік		Другий потік		$\alpha_{i,j}$
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях	
$E_{1,2}$	0	240	0	0	0,3
$E_{2,3}$	0	0	0	0	0
$E_{1,4}$	240	0	0	0	0,3
$E_{2,5}$	0	240	0	0	0,267
$E_{3,6}$	0	0	0	0	0
$E_{5,4}$	0	0	0	220	0,55
$E_{5,6}$	0	240	0	0	0,8
$E_{4,7}$	240	0	0	220	0,657
$E_{5,8}$	0	0	220	0	0,44
$E_{6,9}$	0	240	0	0	0,3
$E_{7,8}$	240	0	0	0	0,6
$E_{9,8}$	0	0	0	0	0
$E_{7,10}$	0	0	0	220	0,44
$E_{8,11}$	240	0	220	0	0,511
$E_{9,12}$	0	240	0	0	0,3
$E_{10,11}$	0	0	0	220	0,314
$E_{11,12}$	240	0	0	0	0,4

Запропонований дворівневий метод одношляхової швидкої перемаршрутизації, як і для реалізації схеми захисту шляху (рис. 2.37), забезпечував досить поступову зміну порогового значення завантаженості каналів зв'язку мережі (2.29). Це є перевагою отриманого рішення, тому що воно сприяє відповідній сталій зміні й ключових показників якості обслуговування (середньої затримки та ймовірності втрат пакетів), які багато в чому залежать від завантаженості каналів зв'язку мережі.

Таблиця 2.8

Результати розрахунку після третьої ітерації роботи методу ( $\alpha = 0,657$ )

Канал зв'язку	Перший потік		Другий потік		$\alpha_{i,j}$
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях	
$E_{1,2}$	0	240	0	0	0,3
$E_{2,3}$	0	240	0	0	0,48
$E_{1,4}$	240	0	0	0	0,3
$E_{2,5}$	0	0	0	0	0
$E_{3,6}$	0	240	0	0	0,343
$E_{5,4}$	0	0	0	220	0,55
$E_{5,6}$	0	0	0	0	0
$E_{4,7}$	240	0	0	220	0,657
$E_{5,8}$	0	0	220	0	0,44
$E_{6,9}$	0	240	0	0	0,3
$E_{7,8}$	240	0	0	0	0,6
$E_{9,8}$	0	0	0	0	0
$E_{7,10}$	0	0	0	220	0,44
$E_{8,11}$	240	0	220	0	0,511
$E_{9,12}$	0	240	0	0	0,3
$E_{10,11}$	0	0	0	220	0,314
$E_{11,12}$	240	0	0	0	0,4

У табл. 2.9–2.11 для прикладу показані результати розрахунків для трьох ітерацій роботи методу за умови  $\lambda^1 = 240$  1/с і  $\lambda^2 = 240$  1/с. Після першої ітерації роботи методу завантаженість каналу  $E_{7,10}$  визначає значення порога завантаженості каналів зв'язку мережі в 0,96 (табл. 2.9). Зокрема для першого потоку основний шлях проходить через маршрутизатори  $R_1 \rightarrow R_4 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{11} \rightarrow R_{12}$ , а резервний –  $R_1 \rightarrow R_2 \rightarrow R_5 \rightarrow R_6 \rightarrow R_9 \rightarrow R_{12}$ . Тоді для другого потоку основний шлях проходить через маршрутизатори  $R_5 \rightarrow R_8 \rightarrow R_{11}$ , а резервний –  $R_5 \rightarrow R_4 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{11}$ .

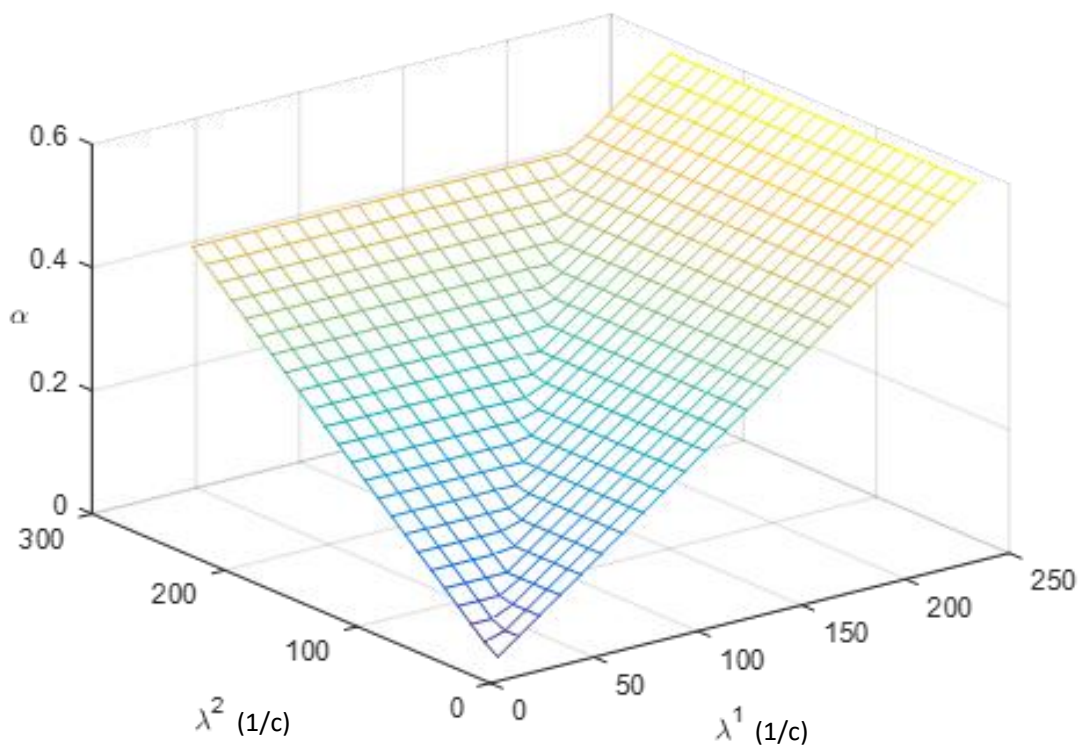


Рис. 2.39. Залежність порога завантаженості каналів зв'язку мережі (2.28) від інтенсивностей потоків пакетів, що передаються (у разі захисту каналу  $E_{8,11}$ )

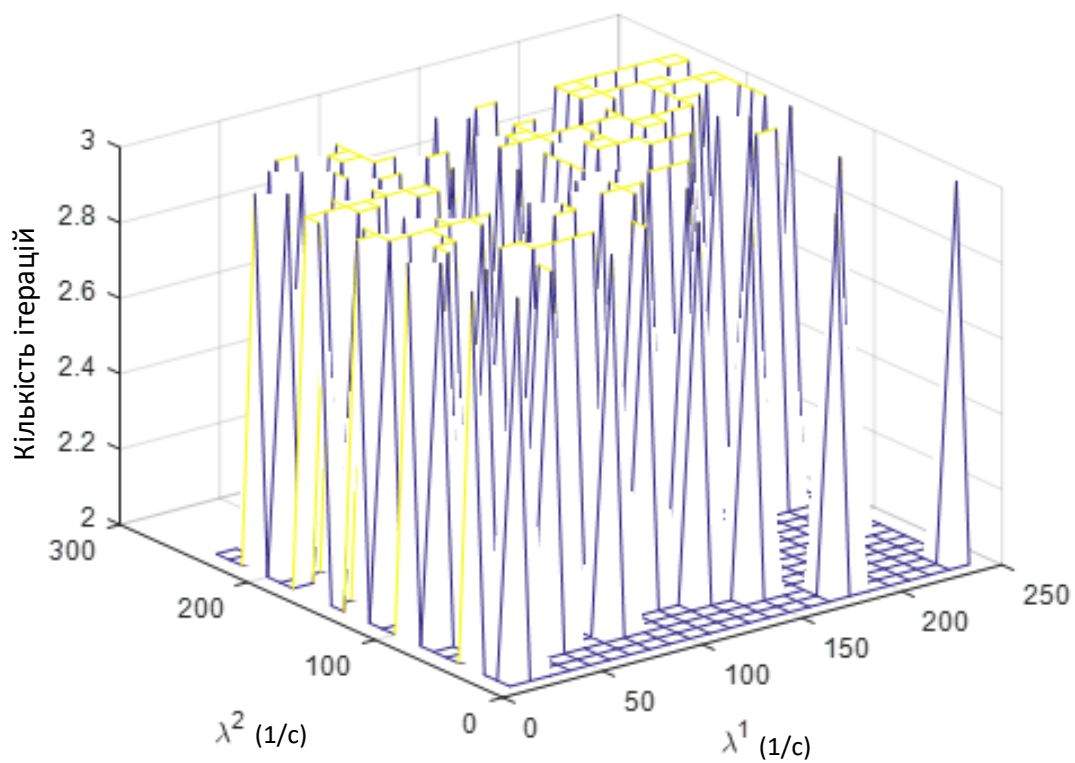


Рис. 2.40. Залежність кількості ітерацій роботи запропонованого методу від інтенсивностей потоків пакетів, що передаються (у разі захисту каналу  $E_{8,11}$ )

Таблиця 2.9

Результати розрахунку після першої ітерації роботи методу ( $\alpha = 0,96$ )

Канал зв'язку	Перший потік		Другий потік		$\alpha_{i,j}$
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях	
$E_{1,2}$	0	240	0	0	0,3
$E_{2,3}$	0	0	0	0	0
$E_{1,4}$	240	0	0	0	0,3
$E_{2,5}$	0	240	0	0	0,267
$E_{3,6}$	0	0	0	0	0
$E_{5,4}$	0	0	0	240	0,6
$E_{5,6}$	0	240	0	0	0,8
$E_{4,7}$	240	0	0	240	0,6857
$E_{5,8}$	0	0	240	0	0,48
$E_{6,9}$	0	240	0	0	0,3
$E_{7,8}$	0	0	0	0	0
$E_{9,8}$	0	0	0	0	0
$E_{7,10}$	240	0	0	240	0,96
$E_{8,11}$	0	0	240	0	0,2667
$E_{9,12}$	0	240	0	0	0,3
$E_{10,11}$	240	0	0	240	0,6857
$E_{11,12}$	240	0	0	0	0,4

Після другої ітерації метод забезпечує подальше зниження порога завантаженості каналів зв'язку до 0,8, який у цьому випадку (табл. 2.10) визначається за коефіцієнтом використання каналу  $E_{5,6}$ . Тут для першого потоку основний шлях містить маршрутизатори  $R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_6 \rightarrow R_9 \rightarrow R_{12}$ , а резервний –  $R_1 \rightarrow R_2 \rightarrow R_5 \rightarrow R_6 \rightarrow R_9 \rightarrow R_{12}$ . У той час як для другого потоку основний і резервний шляхи збігаються та приймають вигляд  $R_5 \rightarrow R_4 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{11}$ , але вже не містять у собі канал  $E_{8,11}$ , що захищається.

Таблиця 2.10

Результати розрахунку після другої ітерації роботи методу ( $\alpha = 0,8$ )

Канал зв'язку	Перший потік		Другий потік		$\alpha_{i,j}$
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях	
$E_{1,2}$	240	240	0	0	0,3
$E_{2,3}$	240	0	0	0	0,48
$E_{1,4}$	0	0	0	0	0
$E_{2,5}$	0	240	0	0	0,2667
$E_{3,6}$	240	0	0	0	0,3429
$E_{5,4}$	0	0	240	240	0,6
$E_{5,6}$	0	240	0	0	0,8
$E_{4,7}$	0	0	240	240	0,3429
$E_{5,8}$	0	0	0	0	0
$E_{6,9}$	240	240	0	0	0,3
$E_{7,8}$	0	0	0	0	0
$E_{9,8}$	0	0	0	0	0
$E_{7,10}$	0	0	240	240	0,48
$E_{8,11}$	0	0	0	0	0
$E_{9,12}$	240	240	0	0	0,3
$E_{10,11}$	0	0	240	240	0,3429
$E_{11,12}$	0	0	0	0	0

Запропонований метод розрахував оптимальний порядок швидкої перемаршрутизації двох потоків пакетів після третьої ітерації з  $\alpha = 0,6$  (табл. 2.11). Таку завантаженість можна спостерігати для каналу  $E_{5,4}$ . У цьому випадку для першого потоку основний і резервний шляхи збігаються та проходять через маршрутизатори  $R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_6 \rightarrow R_9 \rightarrow R_{12}$  так само, як і для другого потоку маршрутизатори  $R_5 \rightarrow R_4 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{11}$  визначають і основний, і резервний шляхи. Однак жоден з розрахованих маршрутів не містить елемент мережі, який захищається, а саме канал  $E_{8,11}$ .

Таблиця 2.11

Результати розрахунку після третьої ітерації роботи методу ( $\alpha = 0,6$ )

Канал зв'язку	Перший потік		Другий потік		$\alpha_{i,j}$
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях	
$E_{1,2}$	240	240	0	0	0,3
$E_{2,3}$	240	240	0	0	0,48
$E_{1,4}$	0	0	0	0	0
$E_{2,5}$	0	0	0	0	0
$E_{3,6}$	240	240	0	0	0,3429
$E_{5,4}$	0	0	240	240	0,6
$E_{5,6}$	0	0	0	0	0
$E_{4,7}$	0	0	240	240	0,3429
$E_{5,8}$	0	0	0	0	0
$E_{6,9}$	240	240	0	0	0,3
$E_{7,8}$	0	0	0	0	0
$E_{9,8}$	0	0	0	0	0
$E_{7,10}$	0	0	240	240	0,48
$E_{8,11}$	0	0	0	0	0
$E_{9,12}$	240	240	0	0	0,3
$E_{10,11}$	0	0	240	240	0,3429
$E_{11,12}$	0	0	0	0	0

Як показано в табл. 2.9–2.11, основні шляхи, розраховані для кожного з переданих потоків, можуть проходити через елементи мережі, що захищаються, а саме канал  $E_{8,11}$  і маршрутизатор  $R_8$ . Резервні шляхи не містили канали та маршрутизатори мережі, що захищалися.

Наведений приклад продемонстрував працездатність запропонованого дворівневого методу швидкої перемаршрутизації. У цьому випадку кінцеве значення порога завантаженості каналів зв'язку мережі (2.29), отримане за допомогою цього методу, повністю відповідало результатам централізованого

розрахунку маршрутних змінних  $x_{i,j}^k$  і  $\bar{x}_{i,j}^k$  за умови використання критерію (2.29) і наявності обмежень (1.1), (1.3), (2.9), (2.10), (2.14), (2.17), (2.27), (2.28). Розрахунок змінних (1.1), (2.10) у розв'язанні оптимізаційної задачі змішаного цілочисельного лінійного програмування (Mixed Integer Linear Programming, MILP), представленої цільовою функцією (2.29), виконувалося за допомогою інструментарію Optimization Toolbox середовища MatLab, зокрема функції `intlinprog`. У цьому випадку згідно з (2.29) було отримано рішення двох завдань: швидкої перемаршрутизації та балансування навантаження.

Результати дослідження для інших мережних структур і вихідних даних також дозволили сформулювати умови, за яких запропонований дворівневий метод демонстрував максимальну ефективність з точки зору отримання оптимальних рішень щодо забезпечення одношляхової швидкої перемаршрутизації з балансуванням навантаження каналів зв'язку ІКМ за критерієм (2.29) і реалізацією необхідних схем захисту елементів мережі. Насамперед, варто зазначити, що з ростом розмірності мережних структур і зв'язності маршрутизаторів ІКМ через наявність більшої кількості маршрутів між парами «відправник–отримувач» і додаткового доступного мережного (канального) ресурсу запропонований метод дозволяє забезпечити краще балансування навантаження за критерієм (2.29) для вирішення завдань швидкої перемаршрутизації. Особливо це помітно в реалізації схем захисту шляху та його пропускної здатності, які вимагають наявності надлишкового мережного ресурсу. Крім того, запропонований метод демонстрував максимальну ефективність у разі одношляхової швидкої перемаршрутизації більшої кількості потоків з різними відправниками та отримувачами, а також високими пакетними інтенсивностями.

### **2.8.2. Синтез та дослідження лінійної оптимізаційної моделі багатошляхової швидкої перемаршрутизації з балансуванням навантаження в ІКМ**

Масштабована реалізація багатошляхової стратегії швидкої перемаршрутизації стикається з проблемою подолання нелінійності умов захисту пропускної здатності ІКМ (2.20). Тому в цьому пункті роботи пропонується доповнити модель (1.2), (1.3), (2.9), (2.11), (2.15), (2.17) для забезпечення лінійного вигляду умов захисту пропускної здатності мережі в процесі реалізації як одношляхової, так і багатошляхової швидкої



перемаршрутизації такими модифікованими умовами запобігання перевантаження з метою забезпечення балансування навантаження в мережі [85, 86]:

$$\sum_{k \in K} \lambda^k u_{i,j}^k \leq \alpha \varphi_{i,j}, E_{i,j} \in E \quad (2.31)$$

за умови

$$x_{i,j}^k \leq u_{i,j}^k \text{ і } \bar{x}_{i,j}^k \leq u_{i,j}^k, \quad (2.32)$$

де  $u_{i,j}^k$  також є змінними, які підлягають розрахунку

$$0 \leq u_{i,j}^k \leq 1 \quad (2.33)$$

і є верхнім порогом (ВП) значень маршрутних змінних основних і резервних шляхів. Критерієм оптимальності розв'язань задач ТЕ FRR залишається вираз (2.29), модифікований під розширену множину керуючих змінних:

$$\min_{x, \bar{x}, u, \alpha} \alpha. \quad (2.34)$$

Таким чином, рішення вихідного технологічного завдання багатошляхової швидкої перемаршрутизації з балансуванням навантаження в ІКМ із захистом каналу, вузла та пропускної здатності мережі було зведено до розв'язання оптимізаційної задачі лінійного програмування з критерієм (2.34) за наявності множини обмежень (1.2), (1.3), (2.9), (2.11), (2.15), (2.17), (2.31)–(2.33), які обираються залежно від реалізованої схеми захисту.

Особливості роботи моделі ТЕ FRR продемонструємо на розрахунковому прикладі. Зокрема структура досліджуваної мережі зображена на рис. 2.41, а в розривах каналів зв'язку мережі вказані їх пропускні здатності.

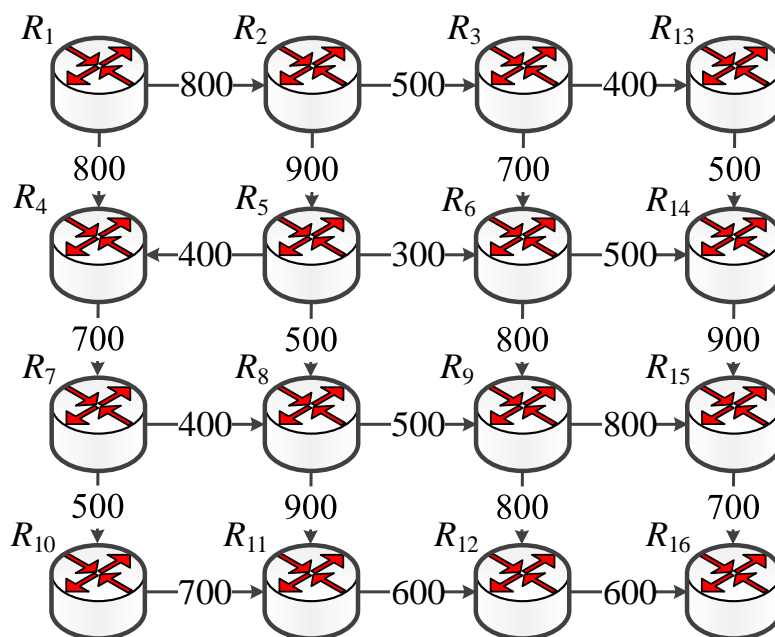


Рис. 2.41. Структура досліджуваної мережі

Нехай у мережі необхідно забезпечити розв'язання задачі багатошляхової швидкої перемаршрутизації двох потоків. У цьому випадку пакети першого потоку передавалися від  $R_1$  до  $R_{16}$ . Пакети другого потоку – від  $R_5$  до  $R_{12}$ . Припустимо, що інтенсивності цих потоків змінювались у таких межах:  $\lambda^1 = 10 \div 400$  1/с і  $\lambda^2 = 10 \div 400$  1/с. У табл. 2.12 показані мінімальні та максимальні значення виграшу щодо значень критерію (2.34) у реалізації багатошляхової маршрутизації порівняно з використанням одношляхової маршрутизації за умови захисту кожного з каналів зв'язку окремо. Таким чином, у захисті каналів зв'язку використання моделі (1.2), (1.3), (2.9), (2.11), (2.15), (2.17), (2.31)–(2.33) дозволяє покращити критерій (2.34) у середньому від 37,12 % до 59,41 %.

Для наочності на рис. 2.42 показано залежність верхнього порога завантаженості каналів зв'язку від значень інтенсивностей потоків, якщо реалізується, наприклад, схема захисту каналу  $E_{8,11}$  у випадку багатошляхової (рис. 2.42, а) або одношляхової маршрутизації (рис. 2.42, б).

Отже, реалізація багатошляхової маршрутизації у разі ТЕ FRR і захисту каналу  $E_{8,11}$  дозволяє покращити значення критерію (2.34) від 44,44 % до 61,54 % порівняно з використанням одношляхової ТЕ-маршрутизації (рис. 2.43).

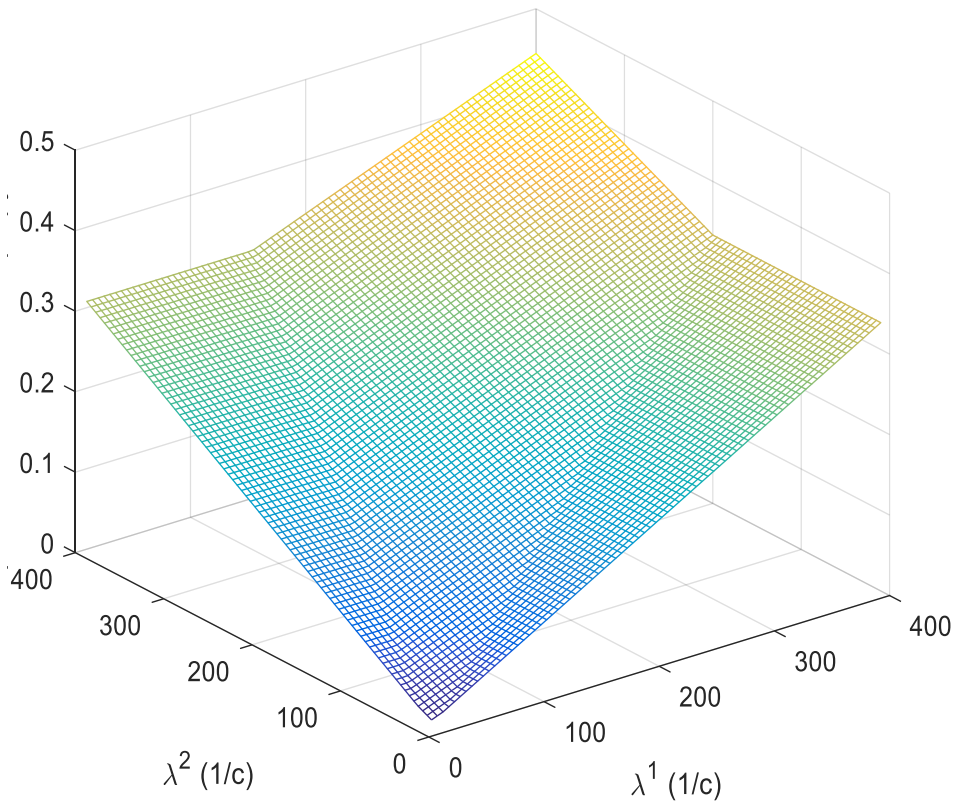
Більш докладно розглянемо випадок використання запропонованої моделі ТЕ FRR у процесі передачі пакетів двох потоків з інтенсивностями  $\lambda^1 = 400$  1/с та  $\lambda^2 = 300$  1/с (табл. 2.13). У цьому випадку завантаженість для кожного каналу зв'язку  $E_{i,j} \in E$  визначалася як

$$\alpha_{i,j} = \frac{\sum_{k \in K} u_{i,j}^k \lambda^k}{\varphi_{i,j}}. \quad (2.35)$$

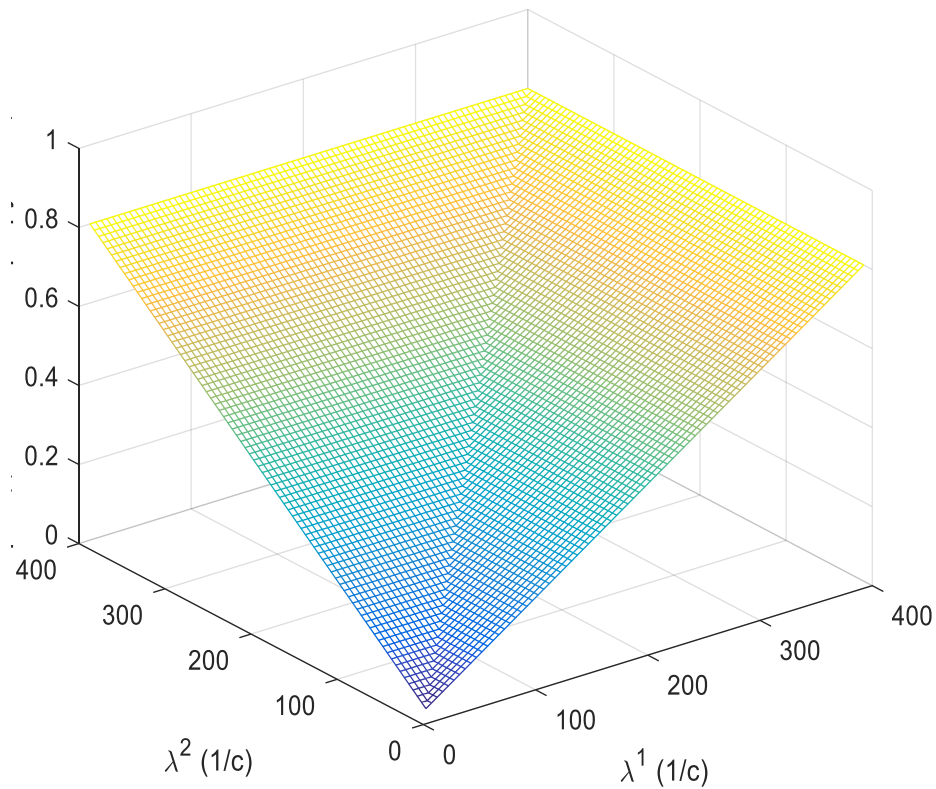
У табл. 2.13 також показано порядок одно- та багатошляхової маршрутизації та балансування двох потоків за каналами зв'язку мережі з використанням запропонованої моделі ТЕ FRR (1.2), (1.3), (2.9), (2.11), (2.15), (2.17), (2.31)–(2.34). Зокрема  $\alpha$  (2.34) є максимальним значенням серед множини коефіцієнтів  $\alpha_{i,j}$  (2.35). Відповідно до отриманих результатів розрахунку (табл. 2.13) реалізація одношляхової маршрутизації в захисті каналу  $E_{8,11}$  забезпечила значення  $\alpha = 0,8$ , тоді як застосування багатошляхової маршрутизації –  $\alpha = 0,39$ , що на 51,25 % краще, ніж у разі одношляхової стратегії.

**Виграш за критерієм (2.34) у разі реалізації  
багатошляхової маршрутизації порівняно з використанням  
одношляхової маршрутизації за умови захисту  
кожного з каналів зв'язку мережі окремо**

Канал зв'язку, що захищається	Виграш, %	
	min	max
$E_{1,2}$	28,57	58,33
$E_{2,3}$	28,57	61,54
$E_{1,4}$	37,5	58,33
$E_{2,5}$	47,37	58,33
$E_{3,6}$	44,44	61,54
$E_{5,4}$	37,5	61,54
$E_{5,6}$	37,5	61,54
$E_{4,7}$	23,08	37,05
$E_{5,8}$	40,17	61,54
$E_{6,9}$	44,44	61,54
$E_{7,8}$	44,44	61,54
$E_{8,9}$	28,57	61,54
$E_{7,10}$	41,18	58,33
$E_{8,11}$	44,44	61,54
$E_{9,12}$	16,67	60,55
$E_{10,11}$	41,18	58,33
$E_{11,12}$	23,08	58,33
$E_{3,13}$	47,37	61,54
$E_{13,14}$	47,37	61,54
$E_{6,14}$	47,37	61,54
$E_{14,15}$	47,37	61,54
$E_{9,15}$	47,37	61,54
$E_{15,16}$	16,67	58,33
$E_{12,16}$	28,57	58,33



а) за умови багатошляхової маршрутизації



б) за умови одношляхової маршрутизації

Рис. 2.42. Залежність верхнього порога завантаженості каналів зв'язку мережі від значень інтенсивностей потоків, якщо реалізується схема захисту каналу  $E_{8,11}$

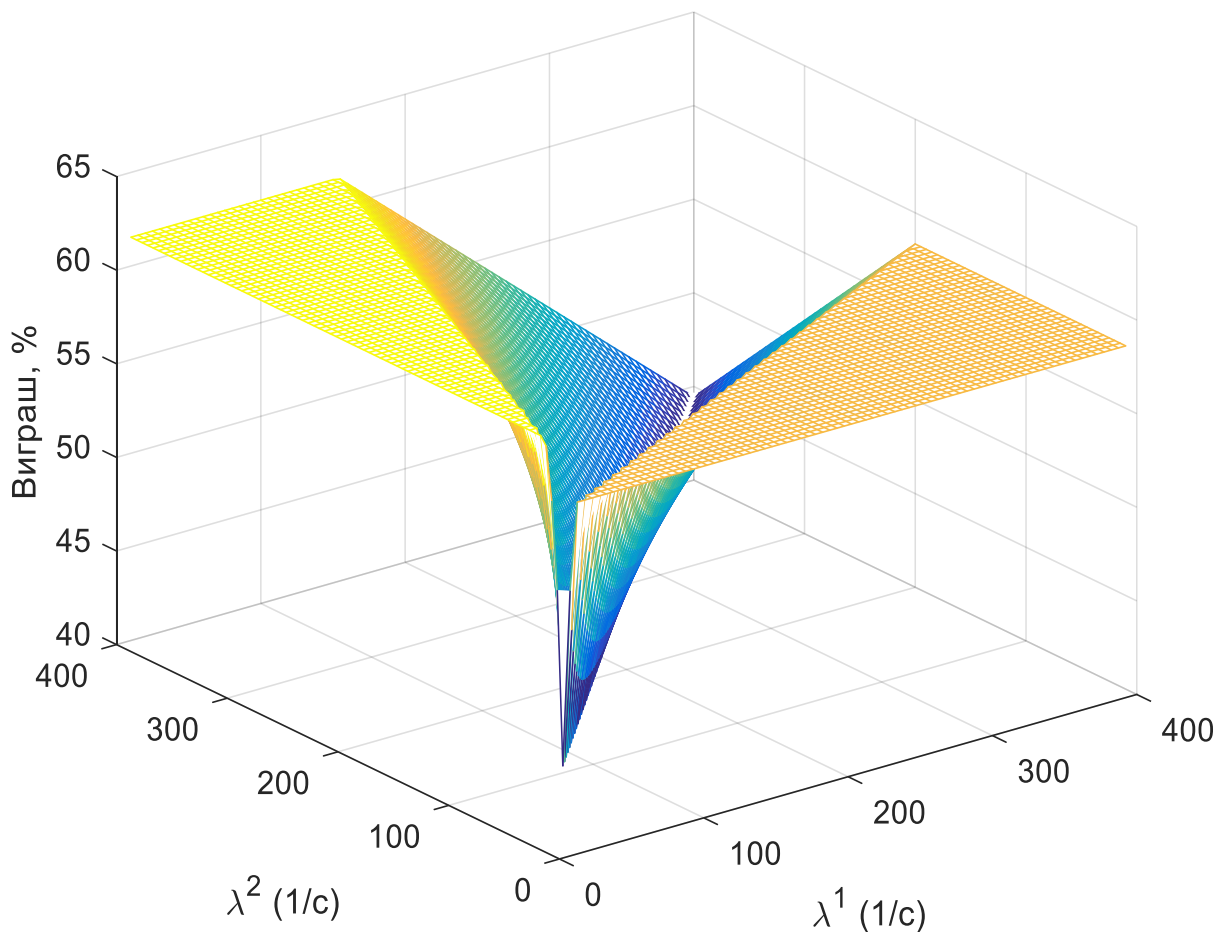


Рис. 2.43. Виграш за критерієм (2.34) від реалізації багатошляхової маршрутизації порівняно з використанням одношляхової маршрутизації (захист каналу  $E_{8,11}$ )

У табл. 2.14 показані мінімальні та максимальні значення виграшу щодо значень критерію (2.34) під час реалізації багатошляхової маршрутизації порівняно з використанням одношляхової маршрутизації за умови захисту кожного з вузлів мережі окремо. Таким чином, у разі захисту вузлів мережі застосування запропонованої моделі дозволяє покращити критерій (2.34) в середньому від 31,5 % до 56,3 %.

На рис. 2.44, наприклад, показано, що реалізація багатошляхової маршрутизації за умови захисту вузла  $R_9$  дозволяє від 16,67 % до 60,55 % покращити значення критерію (2.34) порівняно з одношляховою маршрутизацією.

Таблиця 2.13

**Результати порівняння за критерієм (2.34) одно- та багатопляхової швидкої перемаршрутизації в разі захисту каналу  $E_{8,11}$**

КЗ	Багатопляхова маршрутизація						$\alpha_{i,j}$	Однопляхова маршрутизація						$\alpha_{i,j}$
	Перший потік			Другий потік				Перший потік			Другий потік			
	ОМ	РМ	ВП	ОМ	РМ	ВП		ОМ	РМ	ВП	ОМ	РМ	ВП	
$E_{1,2}$	257,50	256,93	267,91	0	0	0	0,37	400	400	400	0	0	0	0,50
$E_{2,3}$	188,42	194,44	194,44	0	0	0	0,39	0	0	0	0	0	0	0
$E_{1,4}$	142,50	143,07	192,67	0	0	0	0,35	0	0	0	0	0	0	0
$E_{2,5}$	69,08	62,49	142,64	0	0	0	0,32	400	400	400	0	0	0	0,44
$E_{3,6}$	133,28	138,09	171,75	0	0	0	0,36	0	0	0	0	0	0	0
$E_{5,4}$	8,62	9,08	32,03	83,38	92,69	106,81	0,35	0	0	0	300	300	300	0,75
$E_{5,6}$	19,99	23,58	23,57	89,15	93,09	93,09	0,39	0	0	0	0	0	0	0
$E_{4,7}$	151,12	152,15	163,14	83,38	92,69	99,06	0,37	0	0	0	300	300	300	0,43
$E_{5,8}$	40,47	29,83	50,14	127,47	114,22	134,53	0,37	400	400	400	0	0	0	0,80
$E_{6,9}$	95,78	102,81	153,04	89,15	93,09	146,44	0,37	0	0	0	0	0	0	0
$E_{7,8}$	68,42	43,88	82,50	32,66	6,52	52,99	0,34	0	0	0	0	0	0	0
$E_{8,9}$	69,45	73,71	73,71	114,23	120,74	120,74	0,39	400	400	400	0	0	0	0,80
$E_{7,10}$	82,70	108,27	108,27	50,72	86,17	86,17	0,39	0	0	0	300	300	300	0,60
$E_{8,11}$	39,44	0	137,71	45,90	0	137,98	0,31	0	0	0	0	0	0	0
$E_{9,12}$	49,00	60,85	76,63	203,38	213,83	222,45	0,37	400	400	400	0	0	0	0,50
$E_{10,11}$	82,70	108,27	140,51	50,72	86,17	111,48	0,36	0	0	0	300	300	300	0,43
$E_{11,12}$	122,14	108,27	126,88	96,62	86,17	100,64	0,382	0	0	0	300	300	300	0,50
$E_{3,13}$	55,14	56,35	78,87	0	0	0	0,34	0	0	0	0	0	0	0
$E_{13,14}$	55,14	56,35	89,92	0	0	0	0,33	0	0	0	0	0	0	0
$E_{6,14}$	57,49	58,86	90,32	0	0	0	0,33	0	0	0	0	0	0	0
$E_{14,15}$	112,63	115,21	168,42	0	0	0	0,33	0	0	0	0	0	0	0
$E_{9,15}$	116,23	115,67	175,17	0	0	0	0,34	0	0	0	0	0	0	0
$E_{15,16}$	228,86	230,88	240,10	0	0	0	0,37	0	0	0	0	0	0	0
$E_{12,16}$	171,14	169,12	183,21	0	0	0	0,37	400	400	400	0	0	0	0,67

**Виграш за критерієм (2.34) під час реалізації  
багатошляхової маршрутизації порівняно з використанням  
одношляхової маршрутизації за умови захисту  
кожного з вузлів мережі окремо**

Вузол, що захищається	Виграш, %	
	min	max
$R_2$	28,57	58,33
$R_3$	28,57	61,54
$R_4$	23,08	37,5
$R_6$	33,33	61,54
$R_7$	23,08	37,5
$R_8$	30,97	60,55
$R_9$	16,67	60,55
$R_{10}$	41,18	58,33
$R_{11}$	41,18	58,33
$R_{13}$	47,37	61,54
$R_{14}$	47,37	61,54
$R_{15}$	16,67	58,33

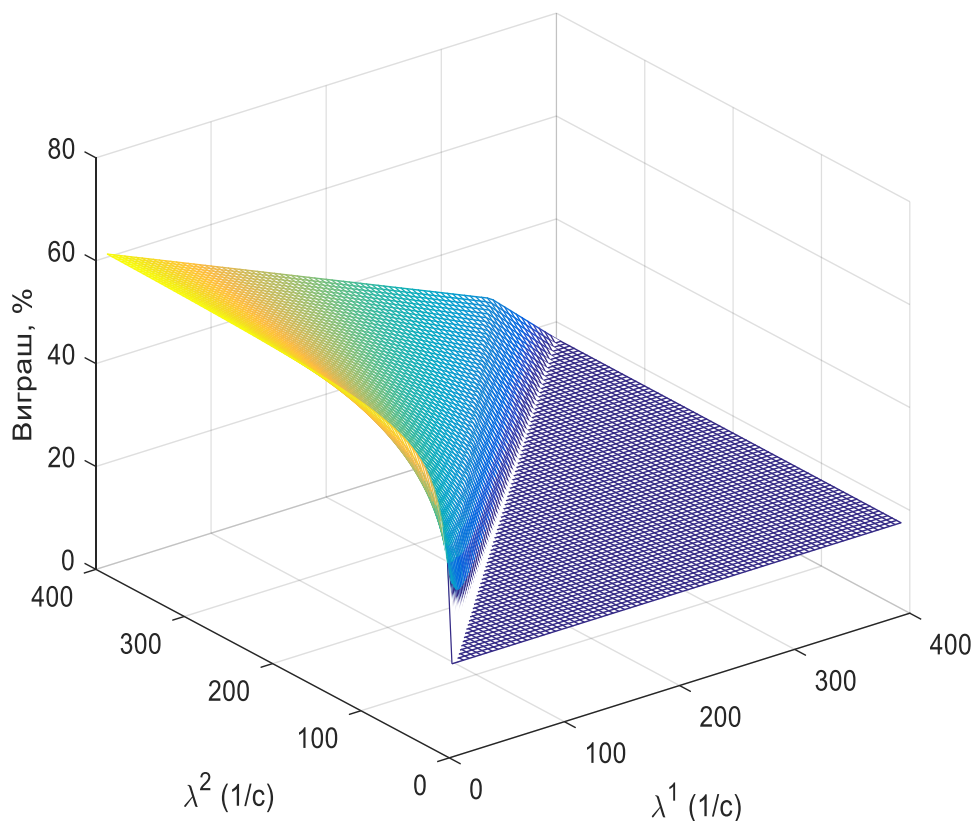


Рис. 2.44. Виграш за критерієм (2.34) від реалізації багатошляхової маршрутизації порівняно з використанням одношляхової маршрутизації (захист вузла  $R_9$ )

## 2.9. Потокова модель відмовостійкої маршрутизації із захистом шлюзу за замовчуванням

Як було показано в підрозділі 2.2, сфера застосування відмовостійкої маршрутизації не обмежується лише захистом елементів транспортної мережі. Дуже важливим моментом у підвищенні відмовостійкості ІКМ є реалізація захисту шлюзу за замовчуванням, за допомогою якого мережі доступу комутуються до транспортної мережі. Результати аналізу наявних теоретичних та протокольних рішень у цьому напрямі дозволили сформулювати такі вимоги до перспективних моделей і методів відмовостійкої маршрутизації із захистом шлюзу за замовчуванням: орієнтація на потокові рішення; підтримка балансування навантаження між інтерфейсами віртуального шлюзу за замовчуванням; забезпечення погодженого розв'язання задач захисту шлюзу за замовчуванням на границі мереж і швидкої перемаршрутизації на рівні транспортної мережі.

### 2.9.1. Графова модель відмовостійкої маршрутизації в ІКМ

Нехай структура ІКМ описується за допомогою графа  $\Gamma = (M, L)$  (рис. 2.45). Зокрема  $M = R \cup V$  – множина вершин графа, що містить дві підмножини:  $R = \{R_i, i = \overline{1, m}\}$  – множина вершин, що моделюють маршрутизатори транспортної мережі (ТМ),  $V = \{V_j, j = \overline{1, v}\}$  – множина вершин, що моделюють мережі доступу (МД) ІКМ [87–90].

У свою чергу множина  $R$  також містить дві підмножини:  $R^+$  – множина вершин, що моделюють приграничні маршрутизатори транспортної мережі, тобто маршрутизатори, до яких можуть бути підключені мережі доступу, де  $m^+ = |R^+|$  – загальне число приграничних маршрутизаторів у ТМ;  $R^-$  – множина вершин, що моделюють транзитні маршрутизатори транспортної мережі, де  $m^- = |R^-|$  – загальна кількість транзитних маршрутизаторів у ТМ.

Підмножиною множини  $R^+$  є множина  $R_j^+$ , що моделює ті приграничні маршрутизатори, а точніше їх інтерфейси, які утворюють віртуальний маршрутизатор для  $j$ -ї мережі доступу, що описується вершиною  $V_j$ . Тоді  $m_j^+ = |R_j^+|$  – загальне число приграничних маршрутизаторів, що утворюють



віртуальний маршрутизатор для  $j$ -ї мережі доступу. Наприклад, як показано на рис. 2.46, для першої мережі доступу віртуальним маршрутизатором є множина маршрутизаторів, представлених вершинами  $R_1$ ,  $R_2$  та  $R_3$ , тобто  $m_1^+ = 3$ ; для другої мережі віртуальний маршрутизатор утворюють інтерфейси маршрутизаторів, що моделюються вершинами  $R_2$  та  $R_3$ , тобто  $m_2^+ = 2$ .

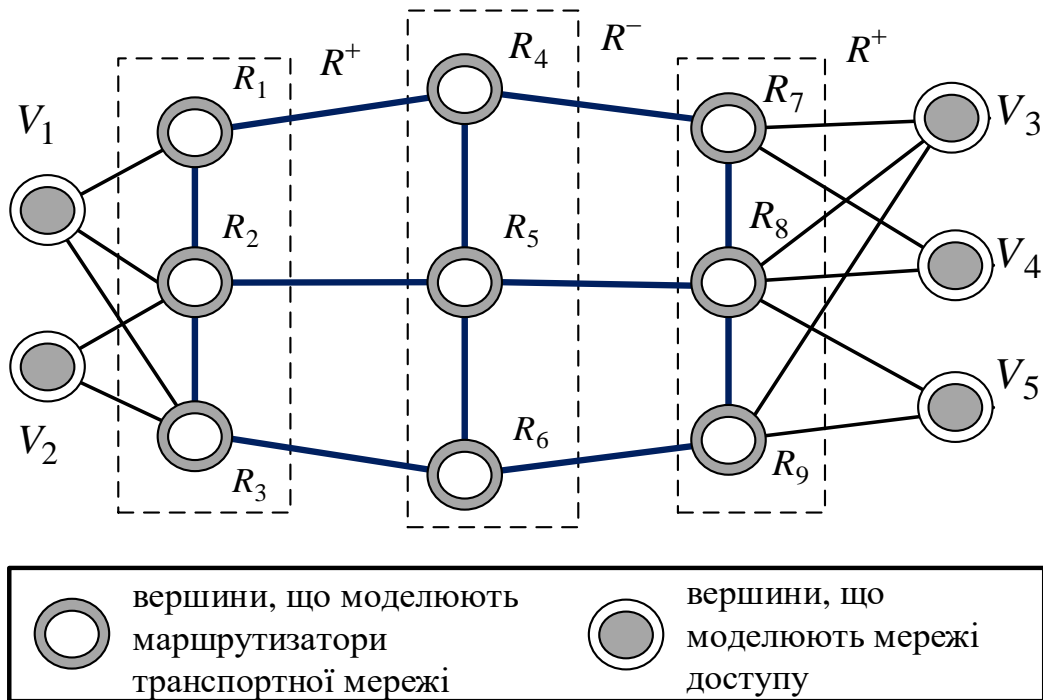


Рис. 2.45. Приклад опису структури ІКМ у вигляді графа

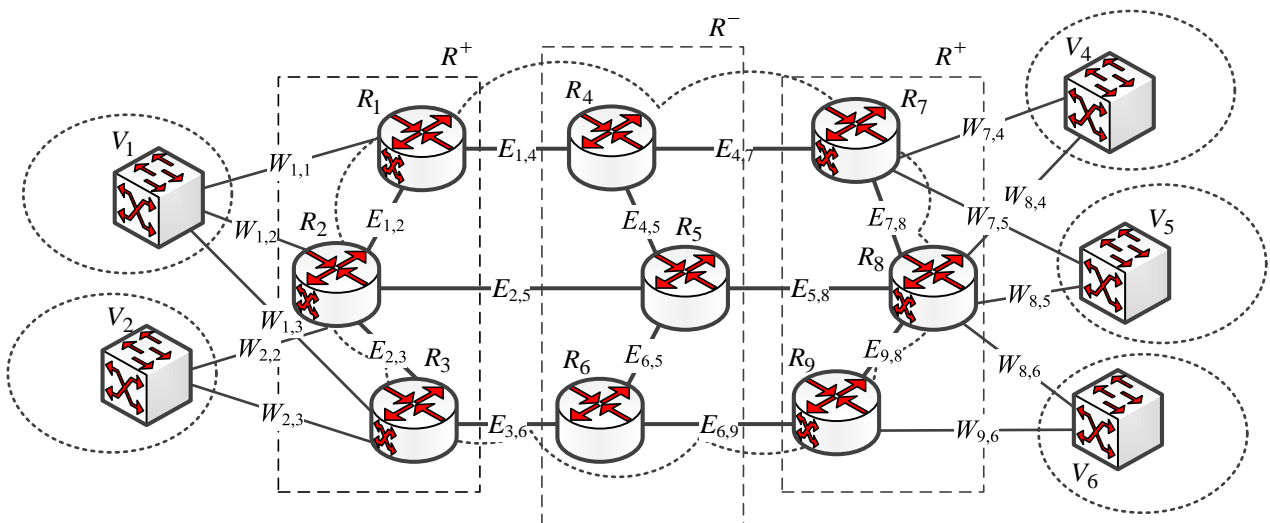


Рис. 2.46. Приклад структури ІКМ, яка містить транспортну мережу та п'ять мереж доступу

Отже, множини  $R_j^+$  ( $j = \overline{1, v}$ ) можуть перетинатися, тому що інтерфейси одного й того ж приграничного маршрутизатора можуть бути у складі різних віртуальних маршрутизаторів. У свою чергу множина дуг  $L = E \cup W$  вихідного графа  $\Gamma$  містить також дві підмножини:  $E = \{E_{i,j}, i, j = \overline{1, m}, i \neq j\}$  – множина каналів зв'язку транспортної мережі,  $W = \{W_{i,j}, i = \overline{1, v}, j = \overline{1, m^+}\}$  – множина ліній доступу, що з'єднують мережі доступу та приграничні маршрутизатори транспортної мережі. Кожній дузі  $E_{i,j} \in E$  графа, що моделює відповідний КЗ транспортної мережі, як і раніше, ставиться у відповідність пропускна здатність цього каналу.

### 2.9.2. Потокова модель відмовостійкої маршрутизації в ІКМ

Нехай кожному  $k$ -му потоку з множини  $K$ , що надходять на приграничні маршрутизатори від мереж доступу, зіставляється низка параметрів:  $V_s^k$  – мережа доступу, яка є джерелом  $k$ -го потоку;  $V_d^k$  – мережа доступу, що є отримувачем  $k$ -го потоку пакетів;  $\lambda^k$  – це, як і раніше, середня інтенсивність пакетів  $k$ -го потоку (1/с). Тоді внаслідок розв'язання задачі відмовостійкої маршрутизації в ІКМ за допомогою запропонованої моделі необхідно розрахувати три типи керуючих змінних, які належать до основного маршруту:

- $x_{i,j}^k$  – маршрутна змінна, що характеризує частку  $k$ -го потоку в каналі зв'язку транспортної мережі, представленого дугою  $E_{i,j}$ ;
- $y_{i,j}^k$  – змінна доступу, що характеризує частку  $k$ -го потоку, який протікає в лінії доступу, представленій дугою  $W_{i,j}$ , тобто від мережі доступу  $V_i$  до приграничного маршрутизатора  $R_j$  транспортної мережі;
- $z_{j,i}^k$  – змінна доступу, що характеризує частку  $k$ -го потоку, який протікає в лінії доступу, представленій дугою  $W_{j,i}$ , тобто від приграничного маршрутизатора  $R_j$  ТМ до мережі доступу  $V_i$ .

Кількість маршрутних змінних  $x_{i,j}^k$  відповідає добутку  $|K| \cdot |E|$ , тоді як загальна кількість змінних доступу  $y_{i,j}^k$  і  $z_{j,i}^k$  визначається як  $v \cdot m^+ \cdot |K|$ .

На керуючі змінні згідно з їх фізичним змістом накладається низка обмежень. На маршрутні змінні  $x_{i,j}^k$  у разі використання одношляхової маршрутизації потоків у ТМ мають місце умови (1.1), а у випадку багатшляхової – (1.2). Під час підключення в певний момент часу мережі доступу лише до одного інтерфейсу віртуального маршрутизатора, як це реалізовано, наприклад, у протоколі HSRP [26], на змінні доступу накладаються обмеження у вигляді

$$\left\{ \begin{array}{l} y_{i,j}^k \in \{0;1\}; \\ \sum_{j:R_j \in R_i^+} \prod_{k \in K} y_{i,j}^k = 1; \end{array} \right. \quad i \quad \left\{ \begin{array}{l} z_{j,i}^k \in \{0;1\}; \\ \sum_{j:R_j \in R_i^+} \prod_{k \in K} z_{j,i}^k = 1. \end{array} \right. \quad (2.36)$$

За можливості балансування трафіку за всіма доступними інтерфейсами віртуального маршрутизатора так, як це реалізовано в протоколах VRRP, GLBP і CARP [24, 25, 27], умови (2.36) замінюються на нерівності:

$$0 \leq y_{i,j}^k \leq 1 \quad \text{та} \quad 0 \leq z_{j,i}^k \leq 1. \quad (2.37)$$

Крім того, на доповнення до (2.37) мають місце такі умови:

$$\sum_{R_j \in R_p^+} y_{p,j}^k = 1, \quad V_p = V_s^k; \quad (2.38)$$

$$\sum_{R_j \in R_h^+} z_{j,h}^k = 1, \quad V_h = V_d^k. \quad (2.39)$$

Ці умови вводяться для того, щоб не допустити втрат пакетів на ділянках «мережа доступу – віртуальний маршрутизатор ТМ» (2.38) і «віртуальний маршрутизатор ТМ – мережа доступу» (2.39).

Для забезпечення узгодженості в процесі розрахунку керуючих змінних, що відповідають за реалізацію відмовостійкої маршрутизації, важливо виконати дещо видозмінені порівняно з (1.3) умови збереження потоку:

$$\left\{ \begin{array}{l} \sum_{j:E_{i,j} \in E} x_{i,j}^k - \sum_{j:E_{j,i} \in E} x_{j,i}^k = 0; \quad k \in K, R_i \in R^-; \\ \sum_{j:E_{i,j} \in E} x_{i,j}^k - \sum_{j:E_{j,i} \in E} x_{j,i}^k = y_{p,i}^k; \quad k \in K, R_i \in R^+, V_p = V_s^k; \\ \sum_{j:E_{i,j} \in E} x_{i,j}^k - \sum_{j:E_{j,i} \in E} x_{j,i}^k = -z_{i,h}^k; \quad k \in K, R_i \in R^+, V_h = V_d^k. \end{array} \right. \quad (2.40)$$

У (2.40) індекс  $j$  вказує на номер вхідного або вихідного інтерфейсу  $i$ -го маршрутизатора, через який  $k$ -й потік відповідно надходить або відправляється

через маршрутизатор. Умови (2.40) гарантують відсутність втрат пакетів на маршрутизаторах ТМ і в ІКМ загалом, а також те, що потік будь-якого користувача з МД приймається та обслуговується транспортною мережею.

Для забезпечення відмовостійкості ІКМ загалом, у якій МД з ТМ з'єднані через певний віртуальний інтерфейс/інтерфейси маршрутизатора, вводяться додаткові керуючі змінні, які визначають резервний шлях для тих самих відправника та отримувача [5, 55–59]. З математичної точки зору необхідно розрахувати такі додаткові керуючі змінні:

–  $\bar{x}_{i,j}^k$  – маршрутна змінна, що характеризує частку  $k$ -го потоку в каналі зв'язку  $E_{i,j}$  резервного шляху відповідно до умов (2.10) або (2.11) для ТМ;

–  $\bar{y}_{i,j}^k$  – змінна доступу, що характеризує частку  $k$ -го потоку, який протікає в резервній лінії доступу  $W_{i,j}$ ;

–  $\bar{z}_{j,i}^k$  – змінна доступу, що характеризує частку  $k$ -го потоку, який протікає в резервній лінії доступу  $W_{j,i}$ .

Як і у випадку формування основного маршруту, змінні доступу для резервного шляху обмежені умовами, аналогічними до (2.36) та (2.39). Крім того, ті самі умови (2.38)–(2.40) відповідно повинні запобігати втратам пакетів і забезпечити збереження потоку в транспортній мережі для резервного шляху. Для уникнення можливого перевантаження каналів зв'язку ТМ і забезпечення захисту пропускної здатності ІКМ загалом вводяться умови (2.20).

Для реалізації схеми захисту шлюзу за замовчуванням з можливістю балансування навантаження за всіма доступними інтерфейсами віртуального маршрутизатора в модель вводяться такі нелінійні умови [89, 90]:

$$\sum_{i:V_i \in V} y_{i,j}^k \bar{y}_{i,j}^k + \sum_{n:E_{j,n} \in E} x_{j,n}^k \bar{x}_{j,n}^k = 0, R_j \in R^+. \quad (2.41)$$

Якщо ці умови виконуються, це гарантує, що приграничний маршрутизатор  $R_j$  (тобто всі інцидентні до цього вузла канали зв'язку та лінії доступу) використовується або основним, або резервним шляхом.

У запропонованій моделі отримані також такі лінійні умови у здійсненні підключення мережі доступу лише до одного інтерфейсу віртуального маршрутизатора (тобто без балансування навантаження) [89, 90]:

$$\begin{cases} x_{j,n}^k + \bar{x}_{j,n}^k \leq 1; \\ y_{i,j}^k + \bar{y}_{i,j}^k \leq 1. \end{cases} \quad (2.42)$$

Виконання умов (2.42) гарантує, що приграничний маршрутизатор  $R_j$  буде використано  $k$ -м потоком лише в одному шляху – основному або резервному.

За аналогією з (2.23), (2.24) за критерій оптимальності отримуваних рішень щодо відмовостійкої маршрутизації пропонується вибрати мінімум такої цільової функції [89]:

$$\begin{aligned}
 J = & \sum_{k \in K} \sum_{E_{i,j} \in E} c_{i,j}^k x_{i,j}^k + \sum_{k \in K} \sum_{E_{i,j} \in E} \bar{c}_{i,j}^k \bar{x}_{i,j}^k + \sum_{k \in K} \sum_{W_{i,j} \in W} b_{i,j}^k y_{i,j}^k + \\
 & + \sum_{k \in K} \sum_{W_{i,j} \in W} \bar{b}_{i,j}^k \bar{y}_{i,j}^k + \sum_{k \in K} \sum_{W_{j,i} \in W} a_{j,i}^k z_{j,i}^k + \\
 & + \sum_{k \in K} \sum_{W_{j,i} \in W} \bar{a}_{j,i}^k \bar{z}_{j,i}^k - \sum_{k \in K} \sum_{E_{i,j} \in E} d_{i,j}^k x_{i,j}^k \bar{x}_{i,j}^k, \quad (2.43)
 \end{aligned}$$

де  $c_{i,j}^k$  і  $\bar{c}_{i,j}^k$  – метрики каналів зв'язку, які використовуються в обчисленні основного та резервного шляхів відповідно в ТМ, а сьомий доданок вноситься в цільову функцію для покращення масштабованості [74] шляхом максимізації збігу між основним і резервним шляхами за незахищеними каналами зв'язку, тоді як  $d_{i,j}^k \gg c_{i,j}^k$  і  $d_{i,j}^k \gg \bar{c}_{i,j}^k$ .

Вагові коефіцієнти  $b_{i,j}^k$  і  $a_{j,i}^k$  у свою чергу є набором метрик доступу для  $k$ -го потоку, який визначає умовну вартість підключення МД до приграничного маршрутизатора під час вибору шлюзу за замовчуванням;  $\bar{b}_{i,j}^k$  і  $\bar{a}_{j,i}^k$  мають той самий фізичний зміст, але для резервних ліній доступу. Вибір цих показників у запропонованому рішенні визначається за допомогою зворотних функцій коефіцієнтів готовності ліній доступу. Отже, перший та другий доданки у виразі (2.43) описують умовну вартість використання каналів зв'язку ТМ основним і резервним шляхами, а доданки з третього до шостого відображають умовну вартість на використання основних і резервних ліній доступу для вхідного трафіку до ТМ або вихідного трафіку з ТМ відповідно.

Таким чином, у вирішенні технологічного завдання щодо відмовостійкої маршрутизації за умови реалізації одношляхової стратегії в ТМ без балансування навантаження на рівні приграничних маршрутизаторів необхідно розв'язати задачу змішаного цілочисельного нелінійного програмування (MINLP) у ході мінімізації (2.43) з урахуванням умов (1.1), (2.20), (2.36), (2.40), (2.42). У разі реалізації багатошляхової стратегії в ТМ та балансування навантаження на рівні приграничних маршрутизаторів оптимізаційна задача

прийме вигляд задачі нелінійного програмування (NLP) з обмеженнями (1.2), (2.20), (2.37)–(2.41).

### 2.9.3. Дослідження схеми захисту шлюзу за замовчуванням у разі використання різних стратегій маршрутизації в ІКМ

Нехай мережа доступу  $V_1$  є джерелом потоку інтенсивністю 300 1/с, а отримувачем пакетів цього потоку є мережа доступу  $V_6$  (рис. 2.46). Необхідно забезпечити захист шлюзу за замовчуванням – маршрутизатор  $R_2$ . Продемонструємо функціонування схеми захисту шлюзу за замовчуванням для випадків одношляхової та багатошляхової маршрутизації. Пропускні здатності каналів зв'язку ТМ наведені в табл. 2.15. Під час дослідження встановлено, що саме ці значення визначали маршрутні метрики  $c_{i,j}^k$  та  $\bar{c}_{i,j}^k$  (2.43) для всіх відповідних каналів зв'язку транспортної мережі, які розраховувалися за аналогією з метрикою протоколу IGRP, а саме  $10^7/\phi_{i,j}$ . Це дозволило забезпечити розрахунок маршрутів з максимальною пропускнуою здатністю.

Таблиця 2.15

#### Пропускні здатності каналів зв'язку транспортної мережі

Канал зв'язку ТМ	$E_{1,2}$	$E_{2,3}$	$E_{1,4}$	$E_{2,5}$	$E_{3,6}$	$E_{4,5}$
Пропускна здатність, 1/с	150	110	350	400	400	300
Канал зв'язку ТМ	$E_{6,5}$	$E_{4,7}$	$E_{5,8}$	$E_{6,9}$	$E_{7,8}$	$E_{9,8}$
Пропускна здатність, 1/с	200	200	800	350	100	120

Для забезпечення вибору найбільш надійного приграничного маршрутизатора (інтерфейсу віртуального маршрутизатора) у процесі реалізації відмовостійкої маршрутизації пропонується вагові коефіцієнти (метрики доступу)  $b_{i,j}^k$ ,  $\bar{b}_{i,j}^k$  і  $a_{j,i}^k$ ,  $\bar{a}_{j,i}^k$  у (2.43) обирати як функцію, що є оберненою до коефіцієнтів готовності  $(A_{i,j})$  тієї чи іншої лінії доступу  $(W_{i,j})$  та/або інтерфейсу приграничного маршрутизатора. Нехай коефіцієнти готовності ліній доступу представлені в табл. 2.16.

## Коефіцієнти готовності ліній доступу

Лінія доступу	$W_{1,1}$	$W_{1,2}$	$W_{1,3}$	$W_{8,6}$	$W_{9,6}$
$A_{i,j}$	0,999	0,9999	0,998	0,9995	0,999

Тоді варіант розв'язання задачі одношляхової відмовостійкої маршрутизації з реалізацією схеми захисту шлюзу за замовчуванням, отриманий з використанням запропонованої моделі, наведено на рис. 2.47. Інтенсивності потоків пакетів для основного і резервного шляхів показано в розривах каналів зв'язку мережі. Основний шлях формується маршрутизаторами транспортної мережі таким чином:  $R_2 \rightarrow R_5 \rightarrow R_8$ . Вибір цього рішення визначається, з одного боку, більш надійним шлюзом за замовчуванням для мереж доступу  $V_1$  та  $V_6$  (відповідно до коефіцієнтів готовності, наведених у табл. 2.16), а з іншого – вибором шляху в ТМ з максимальною пропускнуою здатністю. У разі відмови шлюзу за замовчуванням, тобто маршрутизатора  $R_2$ , потік пакетів автоматично переключиться на резервний маршрут:  $R_1 \rightarrow R_4 \rightarrow R_5 \rightarrow R_8$ .

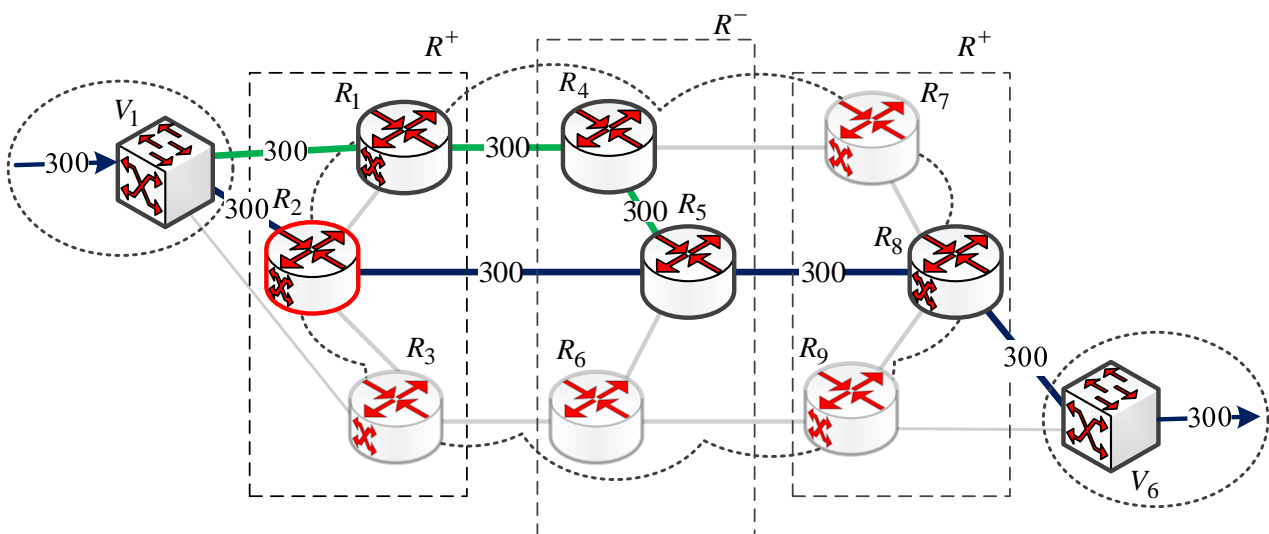
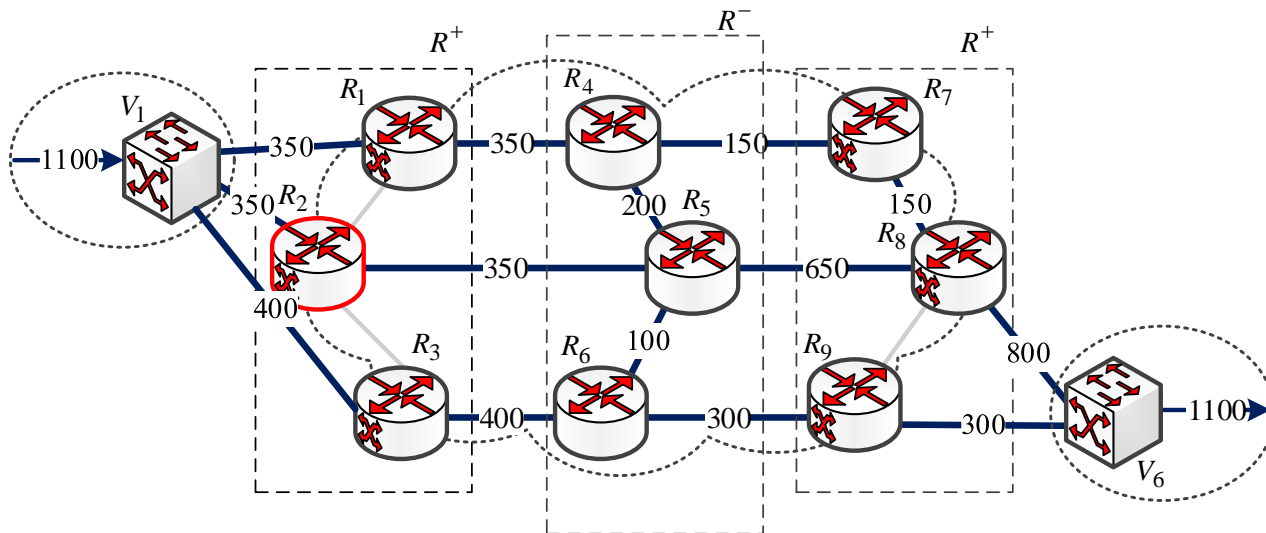


Рис. 2.47. Приклад розв'язання задачі одношляхової відмовостійкої маршрутизації

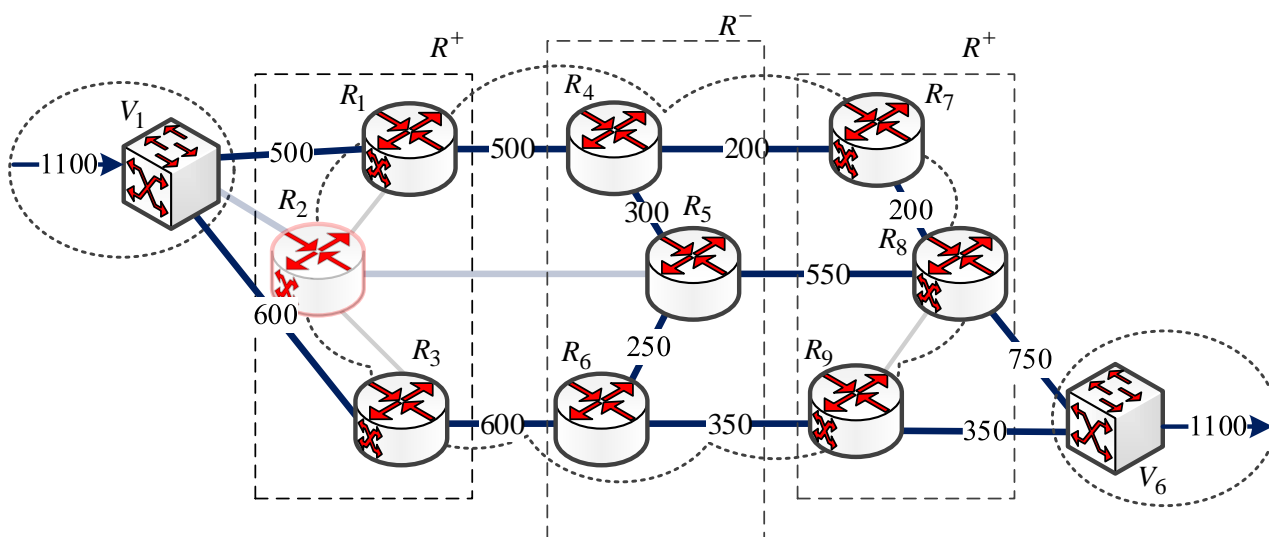
У дослідженні багатошляхової відмовостійкої маршрутизації вихідні дані не змінювались, але інтенсивність потоку становила 1100 1/с. Результат розв'язання поставленої задачі показано на рис. 2.48. Тоді основний мультишлях (рис. 2.48, а) складається з таких маршрутів:

- $R_1 \rightarrow R_4 \rightarrow R_7 \rightarrow R_8$  за умови передачі потоку з інтенсивністю 150 1/с;

- $R_1 \rightarrow R_4 \rightarrow R_5 \rightarrow R_8$  у випадку передачі потоку з інтенсивністю 200 1/с;
- $R_2 \rightarrow R_5 \rightarrow R_8$  у разі передачі потоку з інтенсивністю 350 1/с;
- $R_3 \rightarrow R_6 \rightarrow R_5 \rightarrow R_8$  за умови передачі потоку з інтенсивністю 100 1/с;
- $R_3 \rightarrow R_6 \rightarrow R_9$  у разі передачі потоку з інтенсивністю 300 1/с.



а) основний мультишлях



б) резервний мультишлях

Рис. 2.48. Приклад розв'язання задачі багатошляхової відмовостійкої маршрутизації

Це рішення ґрунтується на можливості забезпечення балансування навантаження за всіма доступними інтерфейсами віртуальних маршрутизаторів:  $R_1$ ,  $R_2$  та  $R_3$  для мережі доступу  $V_1$ , і  $R_8$ ,  $R_9$  – для  $V_6$  відповідно. Це також супроводжується використанням багатошляхової маршрутизації безпосередньо в транспортній мережі. У цьому випадку в разі відмови шлюзу за



замовчуванням  $R_2$  відповідно до розрахунків, отриманих у межах запропонованої моделі, потік буде автоматично перенаправлено на резервний мультитракт (рис. 2.48, б), за винятком маршруту з  $R_2$ :

- $R_1 \rightarrow R_4 \rightarrow R_7 \rightarrow R_8$  у випадку передачі потоку з інтенсивністю 200 1/с;
- $R_1 \rightarrow R_4 \rightarrow R_5 \rightarrow R_8$  у разі передачі потоку з інтенсивністю 300 1/с;
- $R_3 \rightarrow R_6 \rightarrow R_5 \rightarrow R_8$  за умови передачі потоку з інтенсивністю 250 1/с;
- $R_3 \rightarrow R_6 \rightarrow R_9$  у випадку передачі потоку з інтенсивністю 350 1/с.

Загалом результати дослідження підтвердили адекватність запропонованої моделі та ефективність отриманих на її основі маршрутних рішень з точки зору рівня відмовостійкості та продуктивності ІКМ.

### **Висновки до другого розділу**

1. Подальший розвиток отримала система поточкових моделей відмовостійкої маршрутизації без резервування елементів ІКМ шляхами, що не перетинаються або перетинаються лише за вузлами (2.1)–(2.8), з регулюванням числа використовуваних маршрутів (2.5), (2.6). Новизною рішень є введення в структуру моделей нелінійних умов застосування шляхів заданого типу (2.2), (2.3) та (2.7), (2.8) за умови балансування навантаження, які використовувалися як обмеження в розв'язанні оптимізаційної задачі (2.1) відмовостійкої маршрутизації. Представлене рішення, основане на використанні шляхів, які перетинаються за вузлами, є компромісом у разі забезпечення відмовостійкості та безпеки, з одного боку, та якості обслуговування, з іншого. Це є актуальним в умовах, коли місцем відмов та/або компрометації є саме канали зв'язку, а не вузли ІКМ. Як показали проведені дослідження, загалом запропоновані рішення дозволили забезпечити підвищення продуктивності мережі приблизно в 1,7 рази. У цьому випадку зі зростанням розміру мережі та зв'язності маршрутизаторів вииграш за продуктивністю збільшувався до 2,5–4 разів.

2. Удосконалення отримала поточкова модель швидкої перемаршрутизації (1.1), (1.2), (2.9)–(2.20), у межах якої технологічне завдання вдалося представити в формі оптимізаційної задачі. Під час проведеного вдосконалення вдалося сформулювати в лінійній формі умови захисту вузла та каналу (2.10)–(2.16) у разі реалізації як одношляхової, так і багатошляхової стратегій маршрутизації. Обґрунтовано до використання лінійно-квадратичний критерій оптимальності, оснований на мінімізації цільової функції (2.23). Установлено систему ієрархії співвідношень вагових коефіцієнтів у цільовій функції (2.23),

за якої забезпечувалися б максимальні значення продуктивності ІКМ і масштабованості рішень щодо швидкої перемаршрутизації, зокрема на основі оптимізації роботи схеми захисту схильних до відмов елементів мережі одною (спільною для множини потоків) резервною ділянкою – «facility backup».

Крім того, запропоновано білінійний критерій оптимальності (2.24), що містить умови захисту шляху за можливості реалізації як одношляхової, так і багатошляхової стратегій маршрутизації. Установлено систему ієрархії співвідношень вагових коефіцієнтів (метрик) цільовій функції (2.24), коли забезпечувалися коректні рішення щодо швидкої перемаршрутизації. Працездатність та адекватність запропонованої потокової моделі швидкої перемаршрутизації підтверджена на певних розрахункових прикладах у процесі вирішення завдань одношляхової та багатошляхової маршрутизації у разі реалізації різних схем захисту елементів мережі.

3. У розділі представлено дворівневий метод одношляхової швидкої перемаршрутизації з балансуванням навантаження в ІКМ, який забезпечує реалізацію схем захисту каналу, вузла, шляху та їх пропускної здатності. Показано, що ефективна реалізація принципів швидкої перемаршрутизації з балансуванням навантаження в ІКМ, наприклад із застосуванням програмно-конфігурованих архітектур, може бути основана на використанні математичної моделі (1.1), (2.9)–(2.23), яка передбачає централізацію рішення досить складних маршрутних завдань на відповідних SDN-контролерах. У цьому випадку чинниками складності є їх висока розмірність  $(2 \cdot |K| \cdot |E|)$  та нелінійність (2.17)–(2.19) у процесі реалізації схем захисту шляху та пропускної здатності ІКМ, що передбачає підвищені вимоги до продуктивності даних контролерів.

У межах запропонованого обчислювального методу відповідно до принципу прогнозування взаємодій пропонується поділ за двома ієрархічними рівнями функцій розрахунку основних (нижній рівень) і резервних (верхній рівень) маршрутів у разі особливого запису раніше відомих умов захисту пропускної здатності мережі (2.27). Це дозволило відмовитися від вихідної досить розмірної та нелінійної оптимізаційної задачі шляхом переходу до ітераційного розв'язання лінійних оптимізаційних задач удвічі меншого розміру. Реалізація на практиці подібного підходу дозволить істотно знизити вимоги до обчислювальної потужності сервера (контролера) маршрутів, на який покладено централізовані вирішення завдань маршрутизації в мережі. Проведений аналіз запропонованого дворівневого методу (рис. 2.32–2.36) підтвердив його працездатність та ефективність з точки зору отримання

оптимальних рішень щодо забезпечення збалансованої завантаженості каналів зв'язку (2.28), (2.29) та реалізації необхідних схем захисту елементів мережі у разі швидкої перемаршрутизації в ІКМ. Зокрема ефективність отриманих за допомогою запропонованого дворівневого методу рішень повністю відповідає результатам централізованих розрахунків.

4. Запропоновано математичну модель багатошляхової швидкої перемаршрутизації з балансуванням навантаження в ІКМ, представлену виразами (1.2)–(1.4), (2.9), (2.11), (2.15), (2.17) і (2.31)–(2.34). Новизною запропонованої моделі є те, що узгоджене вирішення завдань з ТЕ та FRR із захистом каналу, вузла та пропускної здатності забезпечується під час розв'язання задачі лінійної оптимізації. Критерієм оптимальності був мінімум верхнього порога завантаженості каналів зв'язку мережі (2.34) потоками, що протікають як за основними, так і за резервними маршрутами. Перехід від нелінійних умов захисту пропускної здатності (2.18) (2.20) до лінійного аналога (2.31) було досягнуто шляхом певного розширення числа змінних, що розраховуються, (2.32) і (2.33), які визначають верхній поріг для маршрутних змінних основного та резервного шляхів. Подібний підхід орієнтує на зниження обчислювальної складності в розрахунку маршрутних змінних, відповідальних за формування основного та резервного шляхів, і забезпечує збалансовану завантаженість каналів зв'язку мережі відповідно до вимог концепції Traffic Engineering.

Результати проведеного аналізу запропонованої моделі на низці числових прикладів підтвердили її адекватність і можливість отримання оптимальних розв'язань задачі швидкої перемаршрутизації з балансуванням навантаження в ІКМ у процесі реалізації різних схем захисту елементів мережі (каналу, вузла) та пропускної здатності. Показано, що вииграш від реалізації багатошляхової стратегії маршрутизації у випадку ТЕ FRR дозволив знизити верхній поріг завантаженості каналів зв'язку в середньому від 37,12 % до 59,41 % за умови захисту каналу та від 31,5 % до 56,3 % у разі захисту вузла, що позитивно позначається і на рівні якості обслуговування в мережі загалом.

5. У розділі представлено узгоджене рішення щодо захисту шлюзу за замовчуванням та швидкої перемаршрутизації в ІКМ на основі синтезу відповідної потокової математичної моделі (1.1), (1.2), (2.36)–(2.43). У межах запропонованої моделі задача відмовостійкої маршрутизації була зведена до розв'язання оптимізаційної задачі нелінійного програмування з цільовою функцією (2.43) та обмеженнями (2.36)–(2.42). Частина керуючих змінних (2.36), (2.37) відповідає за вибір шлюзу за замовчуванням у мережі доступу,

а частина (1.2), (2.10) – за вибір шляху або мультишляху в транспортній мережі. Сформульовано умови захисту шлюзу за замовчуванням як у разі балансування навантаження (2.41), так і без балансування (2.42). Задача відмовостійкої маршрутизації із захистом шлюзу за замовчуванням сформульована як оптимізаційна (2.43), де вибір маршрутних метрик забезпечувався таким чином, щоб вибір шлюзу за замовчуванням виконувався за критерієм максимального коефіцієнта готовності (табл. 2.16), а вибір маршруту в транспортній мережі – відповідно до критерію максимальної пропускної здатності (за аналогією з протоколом IGRP). Наведені розрахункові приклади продемонстрували особливості застосування запропонованої моделі для вирішення завдання захисту шлюзу за замовчуванням за умови відмовостійкості маршрутизації в ІКМ для випадку реалізації одношляхової (рис. 2.47) та багатошляхової маршрутизації (рис. 2.48). Результати підтвердили ефективність запропонованої моделі та адекватність отриманих розрахункових результатів.

Як правило, збільшення кількості маршрутизаторів і каналів зв'язку в мережі призводить до підвищення обчислювальної складності отримуваних рішень. Водночас ефективність використання запропонованої моделі також багато в чому визначається розміром транспортної мережі та кількістю мереж доступу. Чим більше існує варіантів вибору шлюзу за замовчуванням і можливих шляхів у транспортній мережі, тим ефективнішою є саме оптимізаційне формулювання задачі для узгодженого вирішення цих завдань. У цих визначених умовах скоординовані рішення забезпечують більш високу ефективність відмовостійкої маршрутизації в мережі порівняно з наявними, в яких завдання вибору шлюзу та маршрутизації вирішуються окремо.

### **Перелік джерел посилання до другого розділу**

1. Макаренко С.И. Время сходимости протоколов маршрутизации при отказах в сети. Системы управления, связи и безопасности. 2015. № 2. С. 45–98. URL: <http://journals.intelgr.com/scs/archive/2015-02/03-Makarenko.pdf>.

2. Matsubara D., Egawa T., Nishinaga N., Kafle V.P., Shin M.K., Galis A. Toward future networks: A viewpoint from ITU-T. IEEE Communications Magazine. 2013. Vol. 51, No. 3. P. 112–118.

3. Cholda P., Tapolcai J., Cinkler T., Wajda K., Jajszczyk A. Quality of resilience as a network reliability characterization tool. IEEE network. 2009. Vol. 23, No. 2. P. 11–19. DOI: 10.1109/MNET.2009.4804331.

4. Tipper D. Resilient network design: challenges and future directions. *Telecommunication Systems*. 2014. Vol. 56, No. 1. P. 5–16. DOI: 10.1007/s11235-013-9815-x.
5. Rak J. *Resilient Routing in Communication Networks (Computer Communications and Networks)*, 1st edition. Springer, 2015. 181 p.
6. Mauthe A., Hutchison D., Cetinkaya E.K., Ganchev I., Rak J., Sterbenz J.P., Gunkelk M., Smith P., Gomes T. Disaster-resilient communication networks: Principles and best practices. *Resilient Networks Design and Modeling (RNDM) 2016: Proceedings of the 8th International Workshop*. Halmstad, Sweden, 13–15 September, 2016. IEEE, 2016. P. 1–10. DOI: 10.1109/RNDM.2016.7608262.
7. Björck F., Henkel M., Stirna J., Zdravkovic J. Cyber resilience-fundamentals for a definition. *New Contributions in Information Systems and Technologies*. 2015. Vol. 353. Springer, Cham. P. 311–316. DOI: [https://doi.org/10.1007/978-3-319-16486-1\\_31](https://doi.org/10.1007/978-3-319-16486-1_31).
8. Fink G.A., Griswold R.L., Beech Z.W. Quantifying cyber-resilience against resource-exhaustion attacks. *Resilient Control Systems (ISRCS) 2014: Proceedings of the 7th International Symposium*, Denver, CO, USA, 19–21 August, 2014. IEEE, 2014. P. 1–8. DOI: 10.1109/ISRCS.2014.6900093.
9. Choras M., Kozik R., Bruna M.P.T., Yautsiukhin A., Churchill A., Maciejewska I., Eguinoa I., Jomni A. Comprehensive approach to increase cyber security and resilience. *Availability, Reliability and Security (ARES) 2015: Proceedings of the 10th International Conference*. Toulouse, France, 24–27 August, 2015. IEEE, 2015. P. 686–692. DOI: 10.1109/ARES.2015.30.
10. Musman S. Assessing prescriptive improvements to a system's cyber security and resilience. *Systems Conference (SysCon) 2016: Proceedings of the Annual IEEE Conference*. Orlando, FL, USA, 18–21 April, 2016. IEEE, 2016. P. 1–6. DOI: 10.1109/SYSCON.2016.7490660.
11. Galinec D., Steingartner W. Combining cybersecurity and cyber defense to achieve cyber resilience. *Informatics 2017: Proceedings of the IEEE 14th International Scientific Conference*. Poprad, Slovakia, 14–16 November, 2017. IEEE, 2017. P. 87–93. DOI: 10.1109/INFORMATICS.2017.8327227.
12. Rak J., Papadimitriou D., Niedermayer H., Romero P. Information-driven network resilience: Research challenges and perspectives. *Optical Switching and Networking*, 2017. Vol. 23, Part 2. P. 156–178. DOI: <https://doi.org/10.1016/j.osn.2016.06.002>.
13. Chaparadza R., Wodczak M., Meriem T.B., De Lutiis P., Tcholtchev N., Ciavaglia L. Standardization of resilience & survivability, and autonomic fault-

management, in evolving and future networks: an ongoing initiative recently launched in ETSI. Design of Reliable Communication Networks (DRCN) 2013: Proceedings of the 9th International Conference. Budapest, Hungary, 4–7 March, 2013. IEEE, 2013. P. 331–341.

14. ETSI TS 103 195-2 V1.1.1. Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 2: An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management. May 2018. 149 p. URL: [https://www.etsi.org/deliver/etsi\\_ts/103100\\_103199/10319502/01.01.01\\_60/ts\\_10319502v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/103100_103199/10319502/01.01.01_60/ts_10319502v010101p.pdf).

15. ETSI TS 103 194 V1.1.1. Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Scenarios, Use Cases and Requirements for Autonomic/Self-Managing Future Internet. October 2014. 67 p. URL: [https://www.etsi.org/deliver/etsi\\_ts/103100\\_103199/103194/01.01.01\\_60/ts\\_103194v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/103100_103199/103194/01.01.01_60/ts_103194v010101p.pdf).

16. ITU-T Rec. Y. 2614. Network reliability in public telecommunication data networks. August 2008. 20 p. URL: <https://www.itu.int/rec/T-REC-Y.2614-201108-I/en>.

17. Hariyawan M.Y. Comparison Analysis of Recovery Mechanism at MPLS Network. International Journal of Electrical and Computer Engineering (IJECE). 2011. Vol. 1, No. 2. P. 151–160. DOI: <http://dx.doi.org/10.11591/ijece.v1i2.84>.

18. Papán J., Segeč P., Palúch P. Analysis of existing IP Fast Reroute mechanisms. Information and Digital Technologies (IDT): Proceedings of the 2015 International Conference, Zilina, Slovakia, 7–9 July 2015. IEEE, 2015. P. 291–297. DOI: 10.1109/DT.2015.7222986.

19. Hussain I. Fault-Tolerant IP and MPLS Networks (Networking Technology). Indianapolis: Cisco Press, 2005. 336 p.

20. Koren I., Krishna C. Fault-Tolerant Systems. Morgan Kaufmann, 2007. 400 p.

21. RFC 7490. Remote Loop-Free Alternate (LFA) Fast Reroute (FRR). April 2015. 29 p. URL: <https://tools.ietf.org/pdf/rfc7490.pdf>.

22. RFC 7811. An Algorithm for Computing IP/LDP Fast Reroute Using Maximally Redundant Trees (MRT-FRR). June 2016. 118 p. URL: <https://tools.ietf.org/pdf/rfc7811.pdf>.

23. RFC 7812. An Architecture for IP/LDP Fast Reroute Using Maximally Redundant Trees (MRT-FRR). June 2016. 44 p. URL: <https://tools.ietf.org/pdf/rfc7812.pdf>.

24. Pavlik J., Komarek A., Sobeslav V., Horalek J. Gateway redundancy protocols. Computational Intelligence and Informatics (CINTI) 2014: Proceedings of

the IEEE 15th International Symposium. Budapest, Hungary, 19–21 November, 2014. IEEE, 2014. P. 459–464. DOI: 10.1109/CINTI.2014.7028719.

25. RFC 5798. Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6. March 2010. 40 p. URL: <https://tools.ietf.org/pdf/rfc5798.pdf>.

26. RFC 2281. Cisco Hot Standby Router Protocol (HSRP). March 1998. 17 p. <https://tools.ietf.org/pdf/rfc2281.pdf>.

27. First Hop Redundancy Protocol comparison (HSRP, VRRP, GLBP) with the diagram (2013). Cisco Networking Center. URL: <http://cisco.netcommunity.com/2013/01/first-hop-redundancy-protocol.html>.

28. RFC 5714. IP Fast Reroute Framework. January 2010. 15 p. URL: <https://tools.ietf.org/pdf/rfc5714.pdf>.

29. RFC 4915. Multi-Topology (MT) Routing in OSPF. June 2007. 20 p. URL: <https://tools.ietf.org/pdf/rfc4915.pdf>.

30. RFC 1853. IP in IP Tunneling. October 1995. 8 p. URL: <https://tools.ietf.org/pdf/rfc1853.pdf>.

31. RFC 6445. Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base for Fast Reroute. November 2011. 53 p. URL: <https://tools.ietf.org/pdf/rfc6445.pdf>.

32. RFC 4090. Fast Reroute Extensions to RSVP-TE for LSP Tunnels. May 2005. 38 p. URL: <https://tools.ietf.org/pdf/rfc4090.pdf>.

33. Tiso J., Teare D. Designing Cisco Network Service Architectures (ARCH): Foundation Learning Guide. Cisco press. 2011. 733 p.

34. Medhi D., Ramasamy K. Network Routing, Second Edition: Algorithms, Protocols, and Architectures (The Morgan Kaufmann Series in Networking) 2nd Edition. Cambridge, MA, USA: Elsevier Inc., 2018. 1018 p.

35. Janevski T. NGN Architectures, Protocols and Services. 1st Edition. Wiley, 2014. 366 p.

36. Chiu C.W., Huang K.S., Yang C.B., Tseng, C.T. An adaptive heuristic algorithm with the probabilistic safety vector for fault-tolerant routing on the (n, k)-star graph. International Journal of Foundations of Computer Science. 2014. Vol. 25, No. 06. P. 723–743.

37. Soleimany A., Azmoodeh S. More Improvement by Helping Ant to Fault-Tolerant Heuristic Routing Algorithm in Mesh Networks. Research Journal of Applied Sciences, Engineering and Technology. 2013. Vol. 6, No. 4. P. 622–630. DOI: 10.19026/rjaset.6.4172.

38. Arai J., Li Y. Fault-Tolerant Routing Algorithms for Hierarchical Dual-Nets with Limited and Arbitrary Number of Faulty Nodes. *International Journal of Networking and Computing*. 2015. Vol. 5, No. 2. P. 329–346.
39. Elhourani T., Gopalan A., Ramasubramanian S. IP fast rerouting for multi-link failures. *IEEE/ACM Transactions on Networking*. 2016. Vol. 24, No. 5. P. 3014–3025. DOI: 10.1109/TNET.2016.2516442.
40. Gopalan A., Ramasubramanian S. IP fast rerouting and disjoint multipath routing with three edge-independent spanning trees. *IEEE/ACM Transactions on Networking*. 2016. Vol. 24, No. 3. P. 1336–1349. DOI: 10.1109/TNET.2015.2440179.
41. Martins L., Gomes T., Tipper D. An efficient heuristic for calculating a protected path with specified nodes. *Resilient Networks Design and Modeling (RNDM): Proceedings of the 8th International Workshop, Halmstad, Sweden, 13–15 September, 2016*. IEEE, 2016. P. 150–157. DOI: 10.1109/RNDM.2016.7608281.
42. Antonakopoulos S., Bejerano Y., Koppol P. Full protection made easy: The DisPath IP fast reroute scheme. *IEEE/ACM Transactions on Networking*. 2015. Vol. 23, No. 4. P. 1229–1242. DOI: 10.1109/TNET.2014.2369855.
43. Kuang K., Wang S., Wang X. Discussion on the combination of loop-free alternates and maximally redundant trees for IP networks fast reroute. *Communications (ICC): Proceedings of the International Conference, Sydney, NSW, Australia, 10–14 June, 2014*. IEEE, 2014. P. 1131–1136. DOI: 10.1109/ICC.2014.6883473.
44. Menth M., Braun W. Performance comparison of not-via addresses and maximally redundant trees (MRTs). *Integrated Network Management (IM 2013): Proceedings of the IFIP/IEEE International Symposium, Ghent, Belgium, 27–31 May, 2013*. IEEE, 2013. P. 218–225.
45. Braun W., Menth M. Loop-free alternates with loop detection for fast reroute in software-defined carrier and data center networks. *Journal of Network and Systems Management*. 2016. Vol. 24, No. 3. P. 470–490. DOI: 10.1007/s10922-016-9369-9.
46. Braun W., Albert M., Eckert T., Menth M. Performance comparison of resilience mechanisms for stateless multicast using bier. *Integrated Network and Service Management (IM): Proceedings of the IFIP/IEEE Symposium, Lisbon, Portugal, 8-12 ay, 2017*. IEEE, 2017. P. 230–238. DOI: 10.23919/INM.2017.7987284.
47. Duong T.D., Kaneko K. Fault-Tolerant Routing Based on Approximate Directed Routable Probabilities for Hypercubes. In: Xiang Y., Cuzzocrea A.,



Hobbs M., Zhou W. (eds) Algorithms and Architectures for Parallel Processing. ICA3PP 2011. Lecture Notes in Computer Science, Vol. 7016. Springer, Berlin, Heidelberg. P 106–116. DOI: [https://doi.org/10.1007/978-3-642-24650-0\\_10](https://doi.org/10.1007/978-3-642-24650-0_10).

48. Lu C., Hu D. A Fault-Tolerant Routing Algorithm for Wireless Sensor Networks Based on the Structured Directional de Bruijn Graph. *Cybernetics and Information Technologies*. 2016. Vol. 16, No. 2. P. 46–59. DOI: 10.1515/cait-2016-0019.

49. Yeh S.I., Yang C.B., Chen H.C. Fault-tolerant routing on the star graph with safety vectors. *Parallel Architectures, Algorithms and Networks 2002 (I-SPAN'02): Proceedings of the International Symposium*. Makati City, Metro Manila, Philippines, 22–24 May, 2002. IEEE, 2002. P. 301–306. DOI: 10.1109/ISPAN.2002.1004298.

50. Nishiyama Y., Hirai Y., Kaneko K. Fault-Tolerant Routing Based on Improved Safety Levels in Pancake Graphs. *Parallel and Distributed Computing, Applications and Technologies (PDCAT) 2014: Proceedings of the 15th International Conference*. Hong Kong, China, 9–11 December, 2014. IEEE, 2014. P. 76–81. DOI: 10.1109/PDCAT.2014.20.

51. Nishiyama Y., Sasaki Y., Hirai Y., Nakajo H., Kaneko K. Fault-tolerant Routing based on Routing Capabilities in a Hyper-Star Graph. *Journal of Information Science and Engineering*. 2017. P. 1–13.

52. Wang D., McNair J. Circulant-graph-based fault-tolerant routing for all-optical WDM LANs. *GLOBECOM 2010: Proceedings of the Global Telecommunications Conference*. Miami, FL, USA, 6–10 December, 2010. IEEE, 2010. P. 1–5. DOI: 10.1109/GLOCOM.2010.5683293.

53. Pióro M., Tomaszewski A., Żukowski C., Hock D., Hartmann M., Menth M. Optimized IP-based vs. explicit paths for one-to-one backup in MPLS fast reroute. *NETWORKS 2010: Proceedings of the 14th International Telecommunications Network Strategy and Planning Symposium*. Warsaw, Poland. 27–30 September, 2010. IEEE, 2010. P. 1–6. DOI: 10.1109/NETWKS.2010.5624923.

54. Addis B., Carello G., Mattia S. Survivable green traffic engineering with shared protection. *Networks*. 2017. Vol. 69, No. 1. P. 6–22. DOI: <https://doi.org/10.1002/net.21717>.

55. Gomes T., Martins L., Ferreira S., Pascoal M., Tipper D. Algorithms for determining a node-disjoint path pair visiting specified nodes. *Optical Switching and Networking*. 2017. Vol. 23. P. 189–204. DOI: <https://doi.org/10.1016/j.osn.2016.05.002>.

56. Liu V.Y., Tipper D. Spare capacity allocation using shared backup path protection for dual link failures. *Computer Communications*. 2013. Vol. 36, No. 6. P. 666–677. DOI: 10.1016/j.comcom.2012.09.007.
57. Myslitski K., Rak J., Kuszner Ł. Toward fast calculation of communication paths for resilient routing. *Networks*. 2017. Vol. 70, No. 4. P. 308–326. DOI: <https://doi.org/10.1002/net.21789>.
58. Gomes T., Tipper D., Alashaikh A. A novel approach for ensuring high end-to-end availability: The spine concept. *Design of Reliable Communication Networks (DRCN) 2014: Proceedings of the 10th International Conference*. Ghent, Belgium, 1–3 April, 2014. IEEE, 2014. P. 1–8. DOI: 10.1109/DRCN.2014.6816142.
59. Alashaikh A., Tipper D., Gomes T. March, 2016. Supporting differentiated resilience classes in multilayer networks. *Design of Reliable Communication Networks (DRCN) 2016: Proceedings of the 12th International Conference*. Paris, France. 15–17 March, 2017. IEEE, 2016. P. 31–38. DOI: 10.1109/DRCN.2016.7470832.
60. Zhang X., Cheng Z., Lin R., He L., Yu S., Luo H. Local Fast Reroute With Flow Aggregation in Software Defined Networks. *IEEE Communications Letters*. 2017. Vol. 21, No. 4. P. 785–788. DOI: 10.1109/LCOMM.2016.2638430.
61. Malik A., Aziz B., Adda M., Ke C.H. Optimisation methods for fast restoration of software-defined networks. *IEEE Access*. 2017. Vol. 5. P. 16111–16123. DOI: 10.1109/ACCESS.2017.2736949.
62. Rzym G., Wajda K., Chołda P. SDN-based WAN optimization: PCE implementation in multi-domain MPLS networks supported by BGP-LS. *Image Processing & Communications*. 2017. Vol. 22, No. 1. P. 35–48. DOI: <https://doi.org/10.1515/ipc-2017-0004>.
63. Wang N., Ho K., Pavlou G., Howarth M. An overview of routing optimization for internet traffic engineering. *IEEE Communications Surveys & Tutorials*. 2008. Vol. 10, No. 1. P. 36–56. DOI: 10.1109/COMST.2008.4483669.
64. Lou W., Kwon Y. H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks. *IEEE Transactions on Vehicular Technology*. 2006. Vol. 55, No. 4. P. 1320–1330. DOI: 10.1109/TVT.2006.877707.
65. Lou W., Liu W., Fang Y. SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks. *INFOCOM 2004: Proceedings of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*. Hong Kong, China, 7–11 March, 2004. IEEE, 2004. P. 2404–2413. DOI: 10.1109/INFCOM.2004.1354662.

66. Alouneh S., En-Nouaary A., Agarwal A. A Multiple LSPs Approach to Secure Data in MPLS Networks. *Journal of Networks*. 2007. Vol. 2, No. 4. P. 51–58. DOI: 10.4304/jnw.2.4.51–58.
67. Alouneh S., Agarwal A., En-Nouaary A. A Novel Path Protection Scheme for MPLS Networks using Multi-path Routing. *Computer Networks: The International Journal of Computer and Telecommunications Networking*. 2009. Vol. 53, No. 9. P. 1530–1545. DOI: 10.1016/j.comnet.2009.02.001.
68. Natarajan M. Graph Theory Algorithms for Mobile Ad Hoc Networks. *Informatica – An International Journal of Computing and Informatics*. 2012. Vol. 36. P. 185–200.
69. Suurballe J.W. Disjoint paths in a network. *Networks*. 1974. Vol. 4, No. 2. P. 125–145.
70. Єременко А.С. Поточкова модель многопутевої маршрутизації по непересекаючимся путям в телекомунікаційній мережі. *Проблеми телекомунікацій*. 2015. № 1 (16). С. 85–93. URL: [http://pt.journal.kh.ua/2015/1/1/151\\_yeremenko\\_disjoint.pdf](http://pt.journal.kh.ua/2015/1/1/151_yeremenko_disjoint.pdf).
71. Yeremenko O.S. Enhanced Flow-based Model of Multipath Routing with Overlapping by Nodes Paths. *Problems of Infocommunications Science and Technology (PIC S&T): Proceedings of the IEEE Second International Scientific-Practical Conference, Kharkiv, Ukraine, 13–15 October, 2015*. Kharkiv: Kharkiv National University of Radio Electronics, 2015. P. 42–45.
72. Єременко О.С., Андрушко Д.В. Модель маршрутизації в телекомунікаційній мережі з використанням шляхів, що перетинаються за вузлами. *Вісник Національного університету «Львівська політехніка»*. Серія: «Радіоелектроніка та телекомунікації». 2015. № 818. С. 181–188.
73. Lemeshko O.V., Arous K.M., Yeremenko O.S. Fault-Tolerant Unicast, Multicast and Broadcast Routing Flow-based Models. *Scholars Journal of Engineering and Technology (SJET)*. 2015. Vol. 3, Issue 4A. P. 343–350.
74. Лемешко А.В., Єременко А.С., Тарики Н., Арус К.М. Повышение масштабируемости и производительности решений по отказоустойчивой маршрутизации в телекоммуникационных сетях. *Системи обробки інформації*. 2016. № 1(138). С. 152–156.
75. Lemeshko A.V., Yeremenko O.S., Tariki N. Improvement of flow-oriented fast reroute model based on scalable protection solutions for telecommunication network elements. *Telecommunications and Radio Engineering*. 2017. Vol. 76, Issue 6. P. 477–490. DOI: 10.1615/TelecomRadEng.v76.i6.30.

76. Yeremenko O.S., Lemeshko O.V., Tariki N. Fast ReRoute Scalable Solution with Protection Schemes of Network Elements. Electrical and Computer Engineering (UKRCON): Proceedings of the First Ukraine Conference, Kiev, Ukraine, 29 May – 2 June 2017. IEEE, 2017. P. 783–788. DOI: 10.1109/UKRCON.2017.8100353.

77. Еременко А.С., Тарики Н., Евдокименко М.А. Оптимизационная модель отказоустойчивой маршрутизации с билинейными условиями защиты пути. Радиоэлектроника и информатика. 2017. № 2 (77). С. 9–14.

78. Yeremenko O., Lemeshko O., Tariki N., Hailan A.M. Research of Optimization model of Fault-Tolerant Routing with Bilinear Path Protection Criterion. Advanced Information and Communication Technologies (AICT): Proceedings of the 2nd International Conference, Lviv, Ukraine, 4–7 July, 2017. IEEE, 2017. P. 219–222. DOI: 10.1109/AIACT.2017.8020105.

79. Seok Yo., Lee Yo., Choi Ya., Kim C. A constrained multipath traffic engineering scheme for MPLS networks. International Conference on Communications ICC 2002 (Cat. No.02CH37333): Proceedings of the IEEE International Conference. New York, NY, USA, 28 April – 2 May, 2002. IEEE, 2002. P. 2431–2436. DOI: 10.1109/ICC.2002.997280.

80. Wang Y., Wang Z. Explicit routing algorithms for Internet Traffic Engineering Computer Communications and Networks: Proceedings of the Eight International Conference. Boston, USA, 11–13 October, 1999. IEEE, 1999. P. 582–588.

81. Lemeshko O., Yeremenko O. Enhanced method of fast re-routing with load balancing in software-defined networks. Journal of ELECTRICAL ENGINEERING. 2017. Vol. 68, Issue 6. P. 444–454. DOI: 10.1515/jee-2017-0079.

82. Lemeshko O., Yeremenko O., Hailan A.M. Two-level Method of Fast ReRouting in Software-Defined Networks. Problems of Infocommunications Science and Technology (PIC S&T): Proceedings of the Fourth International Scientific-Practical Conference, Kharkov, Ukraine, 10–13 October, 2017. IEEE, 2017 P. 376–379. DOI: 10.1109/INFOCOMMST.2017.8246420.

83. Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем. Москва: Мир, 1973. 344 с.

84. Сингх М., Титли А. Системы: декомпозиция, оптимизация и управление. Москва: Машиностроение, 1986. 494 с.

85. Лемешко О.В., Єременко О.С. Розробка та дослідження лінійної оптимізаційної моделі швидкої перемаршрутизації з балансуванням навантаження в телекомунікаційних мережах. Радиоэлектроника и информатика. 2017. № 4 (79). С. 18–25.

86. Lemeshko O., Yeremenko O. Linear Optimization Model of MPLS Traffic Engineering Fast ReRoute for Link, Node, and Bandwidth Protection. *Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET): Proceedings of the 14th International Conference, Lviv–Slavske, Ukraine, 20–24 February, 2018.* IEEE, 2018. P. 1–5. DOI: 10.1109/TCSET.2018.8336365.

87. Yeremenko O., Tariki N., Hailan A.M. Fault-tolerant IP routing flow-based model. *Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET): Proceedings of the 13th International Conference, Lviv, Ukraine, 23–26 February, 2016.* IEEE, 2016. P. 655–657. DOI: 10.1109/TCSET.2016.7452143.

88. Lemeshko O.V., Yeremenko O.S., Tariki N., Hailan A.M. Fault-Tolerance Improvement for Core and Edge of IP Network. *Computer Sciences and Information Technologies (CSIT): Proceedings of the XIth International Scientific and Technical Conference, Lviv, Ukraine, 6–10 Sept. 2016.* IEEE, 2016. P. 161–164. DOI: 10.1109/STC-CSIT.2016.7589895.

89. Lemeshko O., Yeremenko O., Tariki N. Solution for the Default Gateway Protection within Fault-Tolerant Routing in an IP Network. *International Journal of Electrical and Computer Engineering Systems.* 2017. Vol. 8, No. 1. P. 19–26.

90. Yeremenko O., Tariki N., Vavenko T. Default Gateway Protection Scheme in Fault-Tolerant IP Routing. *Problems of Infocommunications Science and Technology (PIC S&T): Proceedings of the Third International Scientific-Practical Conference, Kharkiv, Ukraine, 4–6 Oct. 2016.* IEEE, 2016. P. 223–226. DOI: 10.1109/INFOCOMMST.2016.7905389.

## РОЗДІЛ 3

### МОДЕЛІ ТА МЕТОДИ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

#### 3.1. Характеристика засобів мережної безпеки в інфокомунікаціях

Як показав проведений аналіз [1–19], одним з найважливіших завдань, що регламентується стандартами побудови ІКМ, є реалізація функцій інформаційної безпеки. За стандартом ІТУ-Т Х-805 [20] в архітектурі безпеки (рис. 3.1) ІКМ умовно виокремлюють такі площини та рівні:

- функціональні площини безпеки:
  - контролю (для передачі службової інформації для моніторингу стану ресурсів ІКМ);
  - управління (для передачі службової інформації з метою поточного управління ресурсами ІКМ);
  - користувача (для передачі інформації);
- рівні безпеки:
  - інфраструктури, яка складається з елементів ІКМ (каналів зв'язку, маршрутизаторів, серверів тощо);
  - сервісів (послуг), що надаються кінцевим користувачам ІКМ та провайдерам;
  - застосунків, які беруть участь у комунікаційному процесі та генерують трафік користувачів, який циркулює в мережі.

Відповідно до цих площин і рівнів формуються модулі захисту ІКМ, які характеризуються такими параметрами: управління доступом; автентифікація; збереження інформації; конфіденційність даних; безпека зв'язку; цілісність даних; доступність; секретність.

За вимогами стандартів ІТУ, забезпечення інформаційної безпеки здійснюється в межах трьох рівнів: безпеки інфраструктури, безпеки сервісів і безпеки застосунків (рис. 3.1) [20]. У цьому випадку ефективність роботи верхніх двох рівнів цілком і повністю визначається ефективністю функціонування засобів рівня безпеки інфраструктури, основними завданнями якого є: забезпечення безпеки на рівні мережних елементів (комутаторів, маршрутизаторів, серверів), каналів зв'язку та маршрутів загалом, які з них складаються.

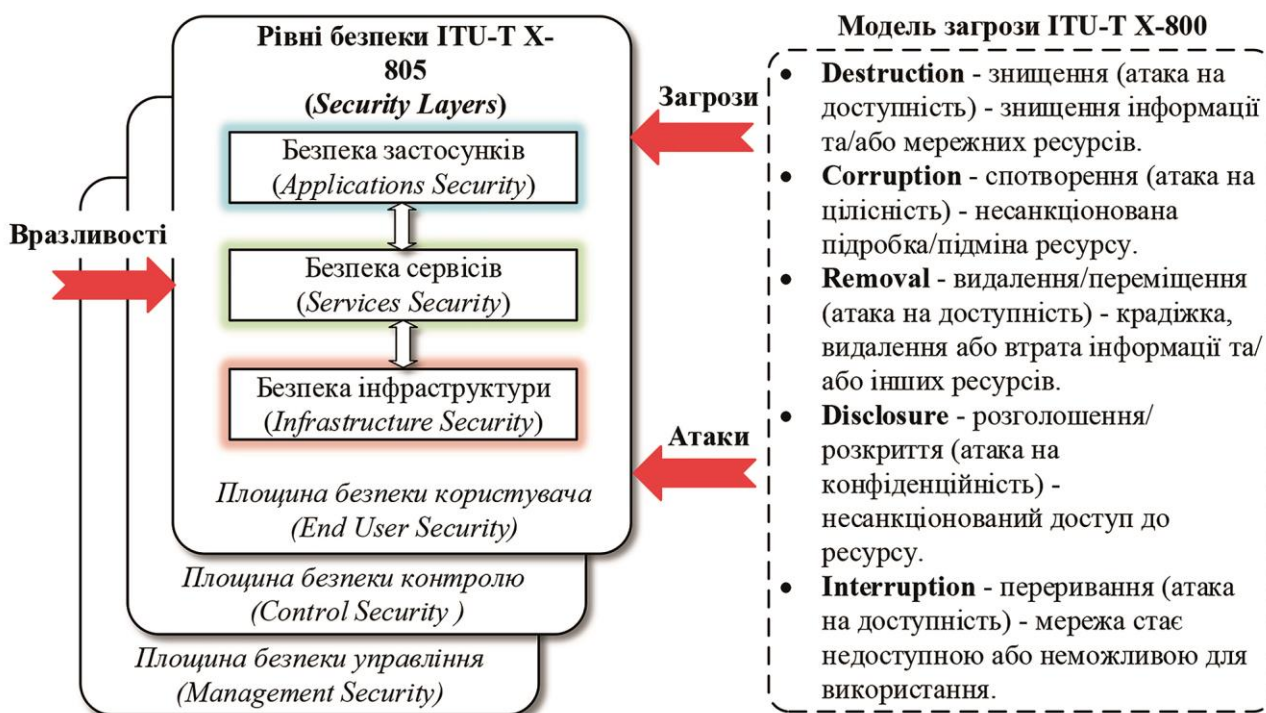


Рис. 3.1. Архітектура безпеки відповідно до стандарту ІТУ-Т Х-805

Якщо розглядати забезпечення мережної безпеки з точки зору рівнів моделі ЕМВВС (Open Systems Interconnection, OSI) і стандарту ISO 7498-1, а також архітектури безпеки згідно з ISO 7498-2 [21–23], то відповідність їх рівнів може бути представлена у вигляді схеми (рис. 3.2). Зокрема сервіси безпеки мають забезпечуватися протоколами відповідних рівнів моделі взаємодії відкритих систем. У свою чергу безпека на мережному рівні повинна підтримуватися і забезпечуватися також протоколами маршрутизації.

До засобів забезпечення мережної безпеки, як правило, належать автентифікація; криптографічний захист; системи аналізу та аудиту; виконання політик безпеки; використання міжмережних екранів; застосування систем виявлення та протидії атакам; управління трафіком і контроль доступу [24, 25]. Важливе значення в управлінні трафіком під час конфігурування мережного обладнання відводиться завданням формування списків доступу (Access Control List, ACL) [12, 13, 24]. Списки доступу можна використовувати для контролю над потоками пакетів, їх ідентифікації, для обмеження поширення оновлень маршрутизації, але однією з найбільш важливих причин застосування списків доступу є забезпечення мережної безпеки. Списки доступу є складниками функціональних можливостей «брандмауера» (міжмережного екрана, Firewall) маршрутизаторів, які часто розташовані між LAN і WAN мережами. Можна також використовувати списки доступу для управління трафіком на маршрутизаторах, розміщених між двома мережами.



Рис. 3.2. Відповідність рівнів OSI та моделі безпеки

ACL дозволяють фільтрувати мережний трафік шляхом заборони або дозволу передачі пакетів, що надходять на вхідні та/або вихідні інтерфейси маршрутизатора. У процесі фільтрації трафіку маршрутизатор перевіряє кожен пакет і приймає рішення про те, передати його або відкинути, ґрунтуючись на ACL. Крім того, у розподілі каналного ресурсу ІКМ під час конфігурування механізмів PQ, CQ, CBWFQ і LLQ за допомогою посилань на ACL можна конкретизувати, яким саме пакетам (потокам) виділяється та чи інша черга та пропускна здатність інтерфейсу. Стандартні ACL використовуються для фільтрації пакетів винятково на основі IP-адреси відправника пакетів на мережному рівні моделі OSI, тоді як розширені ACL можуть оперувати інформацією про ймовірного відправника та/або отримувача пакетів, що належить мережному та транспортному рівням моделі OSI: IP-адреси, номери портів транспортних протоколів TCP та UDP, значення полів пріоритету пакетів тощо.

Основним недоліком технологій фільтрації трафіку, оснований на використанні ACL, є те, що їх налаштування на маршрутизаторі здійснюється вручну адміністратором мережі, як правило, у режимі командного рядка. Це, з одного боку, негативно позначається на оперативності реакції на



можливі загрози безпеці мережі та комутаційного обладнання, а з іншого, – установлює пряму залежність між рівнем підготовки, досвіду та кваліфікації адміністраторів мережі загалом та рівнем її безпеки. Крім того, у разі виходу з ладу мережного обладнання на відновлення раніше налаштованих списків доступу можуть знадобитися тижні, тому в SDN-мережах ACL, як правило, зберігаються на серверах мережної операційної системи, а в перспективі завдання формування та коригування ACL мають бути автоматизовані.

Ключове значення в забезпеченні мережної безпеки також мають криптографічні засоби захисту інформації, які широко реалізуються в сучасних ІКМ. Наприклад, за умови порогової криптографії на стороні відправника конфіденційне повідомлення (секрет) розбивається на декілька частин, які загалом мають доставлятися отримувачу незалежно одна від одної. Зокрема повідомлення може бути дешифровано лише за наявності в отримувача більш ніж заданої порогової кількості його частин. Таким чином, у використанні порогової криптографії зломисник має скомпрометувати не менше за порогову кількість частин повідомлення. Слід зазначити, що порогова криптографія вважається однією з найбезпечніших криптосистем та використовується в сучасних рішеннях, наприклад, таких як RSA (алгоритм Рівеста–Шаміра–Алдемана), криптосистема Пейє, криптосистема Дамгорда–Юрика, схема Ель-Гамалія, алгоритм електронного цифрового підпису із застосуванням еліптичних кривих [26–28].

Концепція порогової криптографії широко використовується та має різне застосування для побудови сучасних ІКМ і реалізується в технологіях хмарних обчислень, механізмах автентифікації, управлінні ключами, технології Інтернету речей (Internet of Things, IoT), мобільних самоорганізованих мережах (Mobile Ad hoc Network, MANET), сенсорних мережах, електронних цифрових підписах, застосунках електронного голосування, візуальній криптографії тощо (табл. 3.1) [27].

Схеми розділення секрету (secret sharing schemes) можна класифікувати таким чином [28]:

- проактивне розділення секрету;
- динамічне розділення секрету;
- розділення секрету з можливостями вето;
- робастне розділення секрету;
- поліноміальне розділення секрету;
- схеми, основані на китайській теоремі про остачі (Chinese Remainder Theorem, CRT);

- анонімне розділення секрету;
- розділення секрету на основі систематичних блокових кодів;
- розділення секрету у вигляді «чорної скрині» (black box secret sharing);
- візуальне розділення секрету.

Таблиця 3.1

### Напрями застосування різних порогових схем в ІКМ

Напрямок застосування	Схема порогового розділення секрету	Переваги використання
Хмарні обчислення	Схема Шаміра	Зменшення кількості ключів; забезпечення конфіденційності приватних даних; безпечно та надійне зберігання даних; безпечна передача даних.
Автентифікація	Схема Шаміра, криптосистема Пейє	Швидка групова автентифікація користувачів; стійкість до масиву атак, масштабованість, гнучкість; легковагова, масштабована групова автентифікація в IoT; анонімна автентифікація в IoT.
Ad-Hoc мережі	Схема Шаміра, порогова криптографія на основі еліптичних кривих (ECC)	Стійкість до сертифікатів фальшивих відкритих ключів, захист від уразливостей, спричинених шкідливими вузлами; високий рівень безпеки, доступний сервіс керування ключами.
Електронний цифровий підпис	Схема Шаміра, схема Шаміра з криптосистемою Ель-Гамалія	Відстежуваність підписів, множина політик підпису; відсутність потреби в довіреній третій стороні.
Електронне голосування	Схема Шаміра, схема Асмута–Блума, криптосистема Пейє	Зменшення порушення цілісності даних, відсутність потреби в довіреній третій стороні; надійність, конфіденційність; підтримка множинного та нульового вибору, ієрархічність; використання властивості гомоморфності.
Цифрове оброблення зображень	Схема Шаміра	Безпечна передача зображення через незахищені мережі.

Так, наприклад, схема Шаміра належить до схем поліноміального розділення секрету, тоді як схема Асмута–Блума основана на використанні теореми CRT. У схемі візуального розділення секрету візуальне зображення було як конфіденційне повідомлення. До прикладів забезпечення мережної безпеки також може належати концепція безпечної маршрутизації, яка реалізована в ІКМ, наприклад, за допомогою механізму SPREAD [29–33]. Це рішення основане на багатопляховій передачі частин конфіденційного повідомлення, які сформовані відповідно до схеми Шаміра. Зокрема чим більше шляхів буде використано та чим менше вони будуть перетинатися, тим з меншою ймовірністю компрометації повідомлення буде доставлено отримувачу. Подібні особливості у свою чергу накладають додаткові вимоги на використовувані математичні моделі та методи маршрутизації в ІКМ.

### 3.2. Аналіз методів безпечної маршрутизації в ІКМ

У роботі [34] було запропоновано новий евристичний підхід щодо безпечної міждоменної маршрутизації *Secure Multi-Party Computation (SMPC)*. У цьому випадку міждоменна маршрутизація передбачає координацію між взаємно «недовірливими» сторонами, що призводить до виникнення вимог, відповідно до яких протокол BGP забезпечує автономність, гнучкість і конфіденційність шляхом розподіленого виконання рішень на основі політик під час процесу ітеративного обчислення маршруту. Цей підхід має слабку збіжність і робить планування та забезпечення відмовостійкості складним завданням. У зв'язку з цим у [34] запропоновано принципово інший підхід до обчислення міждоменного маршруту на основі SMPC, який забезпечує кращу гарантію конфіденційності, ніж BGP, і дозволяє розгортати нові парадигми політик.

У праці [35] отримав подальшого розвитку алгоритм безпечної оверлейної маршрутизації на основі схеми ймовірнісного передрозподілу ключів, яка набула широкого застосування в безпроводових мережах. Запропоновано масштабоване рішення для мереж високої розмірності з кількістю вузлів більшою ніж тисяча, що базується на детерміністському алгоритмі на основі алгоритму Дейкстри (*Deterministic Dijkstra-based Algorithm, DDA*), який дозволяє розраховувати оптимальні безпечні шляхи в оверлейних безпроводових мережах за умови часової складності, значно нижчій, ніж в оригінальному алгоритмі. Також у [35] запропоновано відповідну апроксимацію для знаходження шляху, близького до оптимального, з точністю до 1 % порівняно з DDA.

У роботах [29, 30] представлено та досліджено механізми SPREAD (Secure Protocol for Reliable dAta Delivery) та H-SPREAD (Hybrid Secure Protocol for Reliable dAta Delivery) посилення безпечної передачі повідомлень у MANET (рис. 3.3). Основна ідея полягає в тому, щоб розділити конфіденційне повідомлення на кілька фрагментів – частин, а потім передавати ці частини від відправника до отримувача множиною шляхів, які не перетинаються, так, щоб навіть якщо певну кількість частин повідомлення буде скомпрометовано, секретне повідомлення загалом залишиться нескомпрометованим. Запропоновано загальну архітектуру системи: математичну модель для створення та реконструкції частин повідомлення, оптимальний розподіл його частин за декількома шляхами з точки зору безпеки, а також підходи щодо розрахунку мультишляху в мережах MANET.

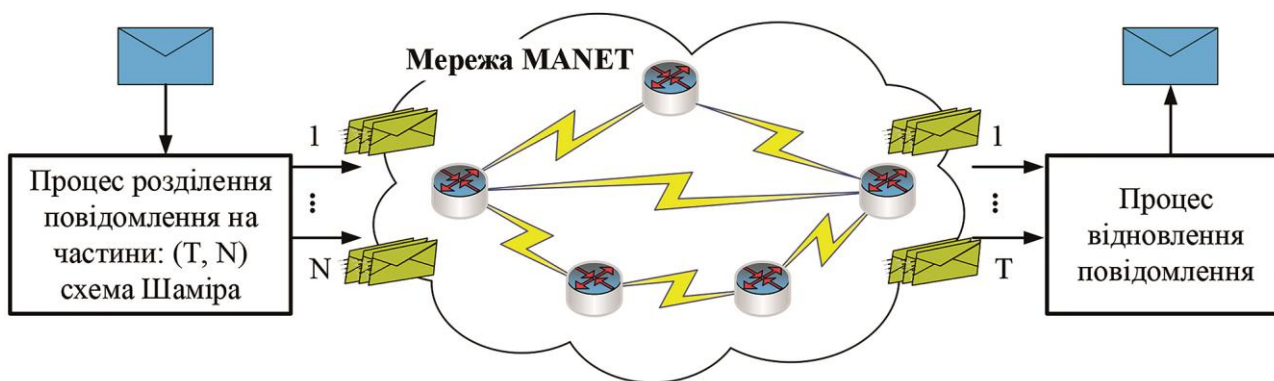


Рис. 3.3. Загальна архітектура роботи механізму SPREAD

Порівняно з проводовими мережами забезпечення безпеки в MANET пов'язано з виявленням і запобіганням множини наявних уразливостей та атак [36]. По-перше, радіоканали більш сприйнятливі до атак як пасивного прослуховування, так і активного втручання в сигнали та здійснення завад. По-друге, більшість протоколів маршрутизації в MANET припускають довірчі взаємодії між вузлами для здійснення передачі пакетів. Залежність від такої взаємодії робить передачу даних більш уразливою щодо несанкційного доступу, підміни даних та атак типу «відмова в обслуговуванні». По-третє, відсутність фіксованої інфраструктури та централізованого управління ускладнює застосування більшості традиційних рішень щодо забезпечення мережної безпеки.

Унаслідок використання механізму SPREAD вдається знизити ймовірність компрометації переданого повідомлення, тому що помітно ускладнюється завдання зловмисника: йому необхідно скомпрометувати не один маршрут, яким передається нерозділене повідомлення, а всі шляхи, якими передаються його частини. Зокрема під компрометацією повідомлення розуміється подія, пов'язана з несанкційним доступом до його вмісту.

Для забезпечення безпечної маршрутизації повідомлення в мережі відповідно до механізму SPREAD необхідно вирішити такі завдання [29, 30]:

1. Розрахунок множини маршрутів, що не перетинаються, між заданими вузлами «відправник» і «отримувач».

2. Розділення конфіденційного повідомлення, що передається, на множину частин відповідно до обраної схеми Шаміра.

3. Розподіл множини частин повідомлення між множиною маршрутів, визначених у процесі вирішення першого завдання.

Варто окремо зазначити, що ймовірність компрометації шляху багато в чому залежить як від кількості складників його вузлів і каналів зв'язку, так і від параметрів їх безпеки, тобто кожен елемент (вузол, канал) шляху може бути скомпрометований з певною ймовірністю. У загальному випадку шляхи, які використовуються для передачі частин розділеного відповідно до схеми Шаміра [29, 30, 33] повідомлення, можуть мати різні значення ймовірності компрометації. На жаль, у межах відомих рішень, присвячених реалізації механізму SPREAD, не враховуються параметри безпеки (зокрема ймовірність компрометації) цих шляхів. Крім того, подібні рішення орієнтовані на використання лише шляхів, які не перетинаються, що негативно впливає на ефективність використання доступного мережного ресурсу.

У роботах [37, 38] пропонується під час вибору маршруту в ІКМ враховувати ризики інформаційної безпеки. Це забезпечується шляхом відповідного формування маршрутних метрик, коли в них сумісно з QoS-показниками враховується і показник ризику інформаційної безпеки елементів системи маршрутизації. Цей підхід дозволяє динамічно вибрати найбільш безпечний маршрут потоків, що передаються, як в умовах активних атак, так і в разі пасивного аналізу ризиків у системі маршрутизації.

### **3.3. Удосконалення методу безпечної маршрутизації повідомлень шляхами, що не перетинаються: проактивний підхід**

#### **3.3.1. Метод безпечної маршрутизації повідомлень шляхами, що не перетинаються в ІКМ**

Як показав проведений аналіз [29–33, 37, 38], можливість аналітичного розрахунку ймовірності компрометації повідомлення, що передається в мережі, багато в чому визначається особливостями структурної побудови ІКМ і типами використовуваних маршрутів. Відомо, що множину шляхів у мережі можна

умовно поділити на дві підмножини: підмножина шляхів, що не перетинаються, та підмножина шляхів, які допускають вузловий або канальний перетин [39–42].

Одним з напрямів забезпечення заданого рівня мережної безпеки в ІКМ є реалізація механізму SPREAD, оснований на багатошляховій маршрутизації повідомлення, що передається, попередньо розділеного на частини відповідно до схеми Шаміра [26–32]. Унаслідок застосування такої схеми вдається знизити ймовірність компрометації переданого повідомлення, тому що зловмисник для його компрометації повинен скомпрометувати, як правило, усі шляхи, якими передаються частини розділеного повідомлення.

У межах відомого методу безпечної маршрутизації використовуються такі позначення:

### Константи

$S_{msg}$ і $D_{msg}$	вузли «відправник» та «отримувач» для повідомлення, що передається;
$M$	кількість використовуваних шляхів, що не перетинаються, у разі маршрутизації частин повідомлення;
$M_i$	кількість каналів зв'язку в $i$ -му шляху, які можуть бути скомпрометовані ( $i = \overline{1, M}$ );
$p_i^j$	імовірність компрометації $j$ -го каналу зв'язку $i$ -го шляху ( $i = \overline{1, M}$ , $j = \overline{1, M_i}$ );
$(T, N)$	параметри схеми Шаміра, де $N$ – загальна кількість частин, на які розділяється повідомлення, що передається, унаслідок застосування схеми Шаміра; $T$ – мінімальна кількість частин, за якими можливо відновити повідомлення, що передається ( $T \leq N$ );
$\gamma_P$	допустима ймовірність компрометації повідомлення в мережі.

### Кількісні показники

$P_i$	імовірність компрометації $i$ -го шляху ( $i = \overline{1, M}$ );
$P_{msg}$	імовірність компрометації повідомлення загалом за умови його передачі частинами мережею.

### Змінні

$n_i$	цілочисельна змінна, яка характеризує кількість частин повідомлення, що передаються за $i$ -м шляхом ( $i = \overline{1, M}$ ).
-------	---

У механізмі SPREAD у процесі багатошляхової маршрутизації та балансування кількості частин конфіденційного повідомлення шляхами необхідно забезпечити заданий рівень мережної безпеки, представленої, наприклад, імовірністю компрометації переданого повідомлення:

$$P_{msg} \leq \gamma_P. \quad (3.1)$$

Під час подальших міркувань передбачається, що відправник та отримувач безпечні, тобто ймовірності компрометації вузла-відправника та вузла-отримувача дорівнюють нулю. Крім того, вважається [29, 30], якщо елемент (вузол, канал) шляху скомпрометовано, то всі фрагменти, що передаються через цей елемент, також будуть скомпрометовані. Тоді ймовірність компрометації  $i$ -го шляху, що складається з  $M_i$  елементів, можна розрахувати за допомогою формули

$$p_i = 1 - \left(1 - p_i^1\right)\left(1 - p_i^2\right) \dots \left(1 - p_i^{M_i}\right) = 1 - \prod_{j=1}^{M_i} \left(1 - p_i^j\right). \quad (3.2)$$

Крім того, для розрахунку керуючих змінних  $n_i$  ( $i = \overline{1, M}$ ), що регламентують процес розподілу фрагментів повідомлення, яке передається, шляхами, що не перетинаються, має виконуватися така умова [29]:

$$\sum_{i=1}^M n_i = N. \quad (3.3)$$

У разі використання схеми Шаміра з параметрами  $T < N$  мають виконуватися умови

$$N - n_i < T, \quad (i = \overline{1, M}), \quad (3.4)$$

тоді як у разі використання схеми без надмірності, якщо  $T = N$ , мають місце такі умови:

$$1 \leq n_i \leq T - 1, \quad (i = \overline{1, M}). \quad (3.5)$$

Виконання умови (3.5) гарантує, що у випадку компрометації всіх маршрутів, крім  $i$ -го, зломисникові не вдасться відновити повідомлення загалом.

Однією з основних умов, яка в обов'язковому порядку має виконуватися в процесі безпечної маршрутизації, є те, що ймовірність компрометації повідомлення в разі його передачі мережею не повинна перевищувати заданого допустимого значення (3.1). Тоді ймовірність компрометації повідомлення, розділеного на  $N$  частин відповідно до схеми Шаміра  $(N, N)$  і переданого за  $M$  шляхами, визначається виразом [29]

$$P_{msg} = \prod_{i=1}^M p_i. \quad (3.6)$$

Перевагами описаного методу є те, що використання множини шляхів, що не перетинаються, у процесі передачі частин конфіденційного повідомлення дуже спрощує розрахунок імовірності його компрометації в мережі за допомогою виразів (3.2)–(3.6).

### 3.3.2. Дослідження методу безпечної маршрутизації повідомлень шляхами, що не перетинаються

Розглянемо окремо задачу розподілу кількості частин повідомлення, що передається, між множиною маршрутів, які не перетинаються. Вона буде представлена як оптимізаційна у застосуванні виразів (3.1)–(3.6). Проведемо порівняльний аналіз її розв’язань з використанням чотирьох моделей з різними критеріями оптимальності отримуваних рішень [43, 44].

Першою моделлю (*Модель 1*) була раніше запропонована в роботах [29, 30] модель, що використовується в механізмі SPREAD і представлена виразами (3.1)–(3.6). Друга модель (*Модель 2*) (3.1)–(3.3), (3.5), (3.6), яка підлягає порівнянню, відрізнялася від першої тим, що критерієм оптимальності був мінімум цільової функції, представленої таким виразом:

$$J = \sum_{i=1}^M p_i n_i . \quad (3.7)$$

Використання критерію (3.7) дозволяє забезпечити такий порядок безпечної маршрутизації повідомлення в мережі, коли максимальна кількість його частин буде передаватися шляхом з мінімальною ймовірністю компрометації. І навпаки, шляхом з максимальною ймовірністю компрометації буде передаватися мінімальна кількість частин того самого повідомлення.

*Модель 3* для забезпечення оптимального балансування кількості частин повідомлення множиною маршрутів передбачає введення додаткових умов:

$$n_i \leq \beta \quad (i = \overline{1, M}), \quad (3.8)$$

де  $\beta$  – верхній динамічно керований поріг кількості частин повідомлення, які передаються в мережі шляхами, що не перетинаються.

У цій же моделі критерієм оптимальності маршрутних рішень обрано мінімум такої цільової функції:

$$J = \beta + \sum_{i=1}^M p_i n_i . \quad (3.9)$$

Мінімізація виразу (3.9) має здійснюватися у виконанні умов (3.3) та (3.8), що дозволить забезпечити балансування кількості частин повідомлення, які передаються в кожному з обраних шляхів. Уведення в цільову функцію (3.9)



доданку  $\sum_{i=1}^M p_i n_i$  спрямовано на досягнення такої мети: у випадку, якщо загальна кількість частин  $N$  не кратна кількості обраних шляхів  $M$ , то більша кількість фрагментів буде передаватися кращим з точки зору ймовірності компрометації маршрутом. Це є важливою перевагою запропонованого рішення від попередньо відомих [29, 30].

У свою чергу *Модель 4* представлена умовами-обмеженнями (3.1)–(3.3), (3.6) у разі використання критерію оптимальності

$$J = \sum_{i=1}^M (p_i n_i)^2. \quad (3.10)$$

Особливості описаних моделей 1÷4 будуть продемонстровані на такому прикладі. Припустимо, що задано пару вузлів відправника й отримувача, між якими існують три доступні шляхи, що не перетинаються, з різною кількістю елементів: вузлів і каналів зв'язку між ними (рис. 3.4).

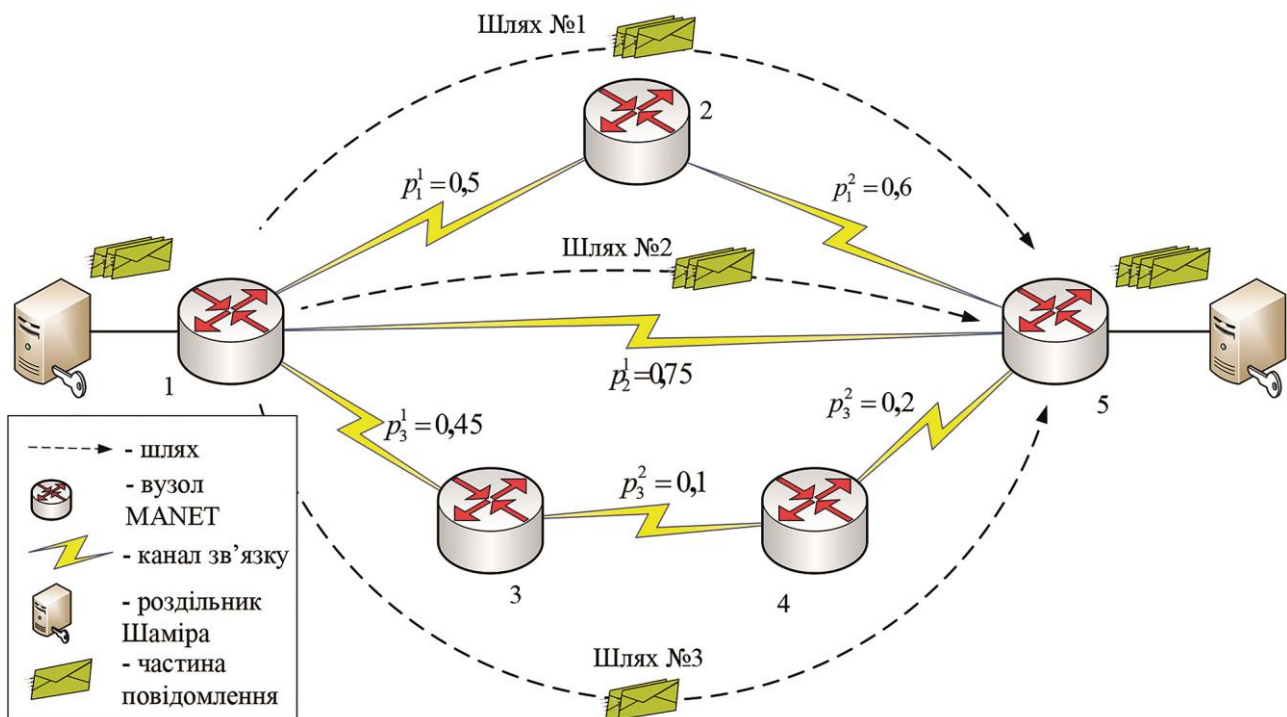


Рис. 3.4. Вихідна структура MANET

Нехай у цьому прикладі до компрометації схильні лише канали зв'язку, що є досить справедливим для MANET. У процесі розрахунків вихідними будуть такі дані:

– для розділення повідомлення на частини реалізується два випадки схеми Шаміра, а саме (10, 10) без надмірності та (8, 10) з надмірністю;

– ймовірності компрометації каналів зв'язку відповідно до їх нумерації і належності до шляхів, що не перетинаються (рис. 3.4), приймають такі значення:  $p_1^1 = 0,5$ ;  $p_1^2 = 0,6$ ;  $p_2^1 = 0,75$ ;  $p_3^1 = 0,45$ ;  $p_3^2 = 0,1$ ;  $p_3^3 = 0,2$ .

Тоді ймовірності компрометації шляхів, отримані в процесі використання виразу (3.2), такі:  $p_1 = 0,8$ ,  $p_2 = 0,75$ ,  $p_3 = 0,604$ . Крім того, у табл. 3.2 показано допустимі рішення задачі розподілу кількості частин шляхами, що не перетинаються, які були отримані під час використання раніше описаних чотирьох моделей.

Таблиця 3.2

**Порівняння моделей розподілу кількості частин повідомлення між множиною маршрутів, що не перетинаються, з їх оптимальним балансуванням**

Номер моделі	Кількість частин повідомлення в окремому шляху залежно від методу балансування			
	Модель 1	Модель 2	Модель 3	Модель 4
Номер шляху	Схема Шаміра без надмірності (10, 10)			
1	8	1	2	3
2	1	1	4	3
3	1	8	4	4
Номер шляху	Схема Шаміра з надмірністю (8, 10)			
1	4	1	2	3
2	3	1	4	3
3	3	8	4	4

Розглянемо випадок з використанням схеми Шаміра без надмірності, наприклад (10, 10). Аналіз результатів розрахунків та порівняння отриманих значень кількості частин повідомлення, які передавалися різними шляхами, показали, що всі чотири моделі можуть дати задовільні рішення. Це можна пояснюється тим, що для компрометації всього повідомлення всі три шляхи повинні бути скомпрометовані. Однак найкращі моделі – це *Моделі 3 та 4*, оскільки вони передбачають адаптацію до параметрів безпеки елементів мережі, коли максимальна кількість частин повідомлення передається найкращим шляхом за рівнем ймовірності компрометації (табл. 3.2).

У використанні *Моделі 1* (табл. 3.2) одним з можливих рішень розподілу частин повідомлення за шляхами є рішення, коли максимальна кількість фрагментів ( $n_1 = 8$ ) буде передаватися найгіршим шляхом з точки зору ймовірності компрометації ( $p_1 = 0,8$ ), що є недоліком цієї моделі (рис. 3.5).

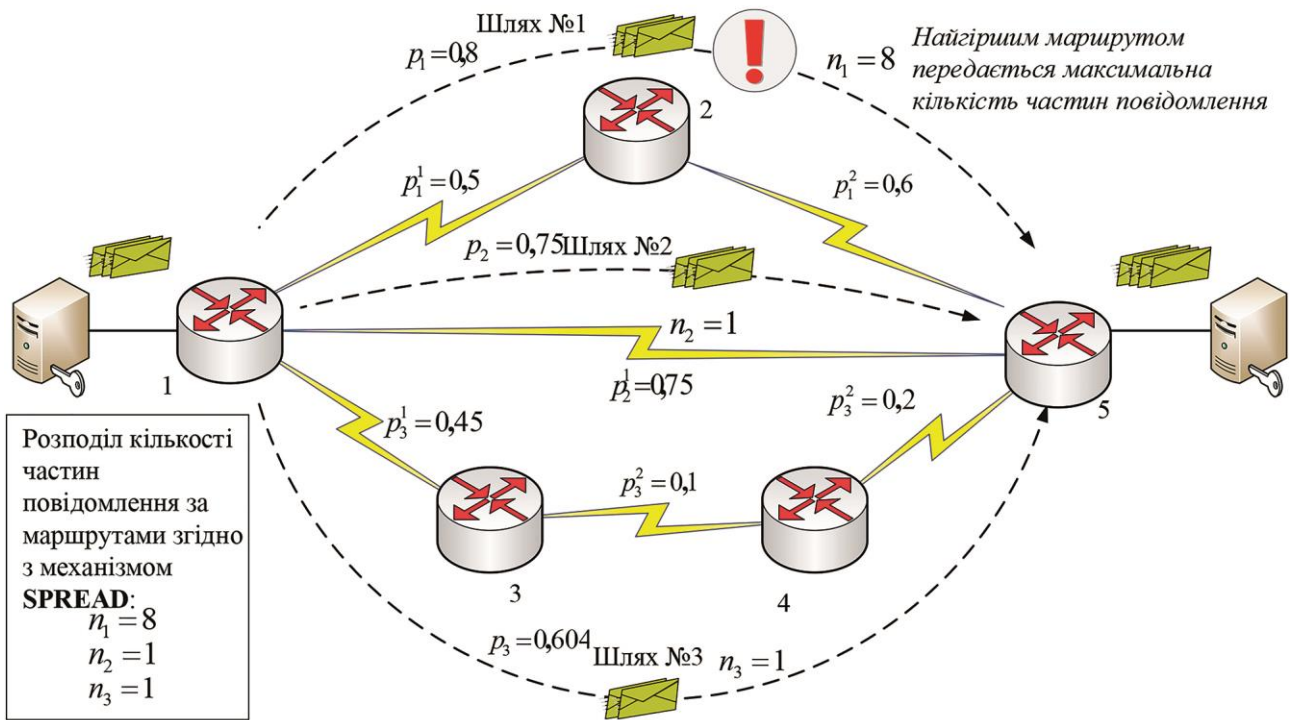


Рис. 3.5. Розподіл кількості частин повідомлення за маршрутами згідно з механізмом SPREAD (Модель 1)

Відповідно до *Моделі 2* за допомогою схеми Шаміра (10, 10) розподіл частин повідомлення за шляхами мережі показав, що максимальна кількість фрагментів ( $n_3 = 8$ ) передавалася найкращим з точки зору ймовірності компрометації шляхом ( $p_3 = 0,604$ ), а їх мінімальна кількість ( $n_1 = 1$ ) передавалася найгіршим шляхом ( $p_1 = 0,8$ ).

Розглянемо приклад використання схеми Шаміра з надмірністю, наприклад, (8, 10). Найкращі рішення були надані *Моделями 1 і 4*, оскільки для компрометації всього повідомлення всі три шляхи мали бути скомпрометовані. Хоча у *Моделі 2* зловмисник повинен скомпрометувати лише один шлях для реконструкції повідомлення, що передається ( $n_3 = 8, T = 8$ ), тоді як у *Моделі 3* треба скомпрометувати два шляхи ( $n_2 = 4, n_3 = 4, T = 8$ ).

*Модель 1* у цьому випадку забезпечує досить ефективне рішення з точки зору оптимального розподілу частин повідомлення (табл. 3.2). *Модель 4* на основі умов обмежень (3.1)–(3.3), (3.6) та критерію оптимальності (3.10) дає найкраще рішення (рис. 3.6) порівняно з усіма іншими моделями. Використовуючи цю модель, можна забезпечити, з одного боку, оптимальне балансування частин повідомлення, переданих через окремі шляхи в мережі, що не перетинаються, а з іншого, – адаптацію до параметрів безпеки

(імовірності компрометації) окремих елементів мережі: каналів зв'язку та маршрутів загалом. У цьому випадку мінімальна кількість фрагментів ( $n_1 = 3$ ) передається найгіршим шляхом з точки зору ймовірності компромісу, а їх максимальна кількість ( $n_3 = 4$ ) передається найкращим шляхом (табл. 3.2).

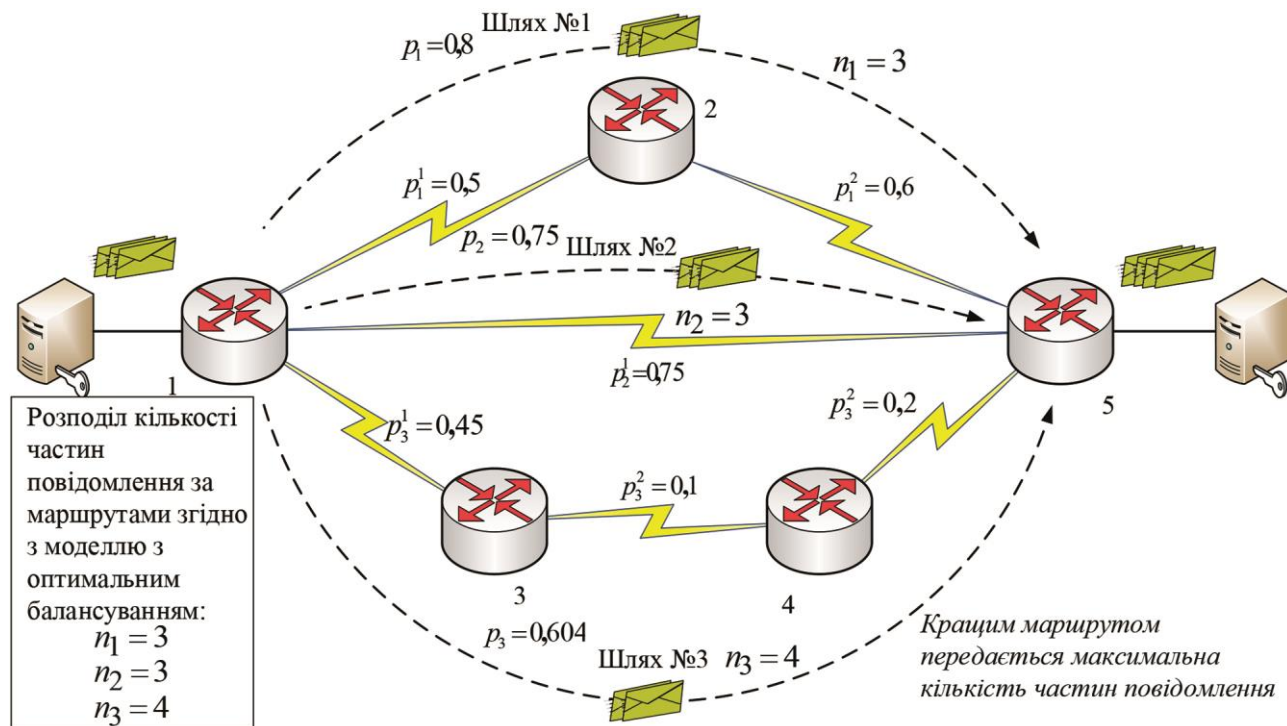


Рис. 3.6. Розподіл кількості частин повідомлення за маршрутами згідно з *Моделлю 4*

Таким чином, реалізація *Моделі 4* передбачає метод безпечної багатошляхової маршрутизації з оптимальним балансуванням частин повідомлення в MANET, який містить такі етапи:

1. Аналіз архітектури MANET (кількість елементів мережі, вимоги щодо якості обслуговування та безпеки, сигнально-завадова обстановка тощо).
2. Розрахунок множини шляхів, що не перетинаються, між заданими вузлами відправника та отримувача відповідно до умови (3.1).
3. Фрагментація повідомлення, що передається, за обраною схемою Шаміра з надлишковістю або без надлишковості.
4. Оптимальний розподіл частин повідомлення за множиною шляхів, що не перетинаються, на основі моделі, яка містить вирази (3.1)–(3.3), (3.6) та критерій оптимальності (3.10).

### **3.4. Метод безпечної маршрутизації повідомлень шляхами, що перетинаються: проактивний підхід**

У розглянутих у підрозділі 3.3 рішеннях щодо безпечної маршрутизації, зокрема в механізмі SPREAD, виконання умови (3.1) цілком і повністю визначається параметрами використовуваних шляхів, що не перетинаються, а завдання балансування частин повідомлення цими шляхами полягає у виконанні умов (3.3)–(3.5). Тому якщо використання множини шляхів, які не перетинаються, не дозволяє задовольнити вимогу (3.1), то поставлене завдання щодо забезпечення заданого рівня мережної безпеки залишається невирішеним.

У цьому випадку інтуїтивно можна припустити, що використання на тій же мережній топології шляхів, які перетинаються, могло б сприяти поліпшенню шуканої ймовірності компрометації переданого повідомлення і, як наслідок, до успішного вирішення поставленого завдання. Як показав проведений аналіз, у разі використання шляхів, що перетинаються, процедура числової оцінки ймовірності компрометації повідомлення, яке передається, помітно ускладнюється, а в низці випадків стає неможливою (в аналітичному вигляді) [30]. У зв'язку з цим актуальним є завдання пошуку компромісного рішення, пов'язаного з визначенням такого класу маршрутів, що перетинаються, для яких можливо в аналітичному вигляді розрахувати, а отже, і контролювати ймовірність компрометації конфіденційного повідомлення, яке передається.

У цьому підрозділі зроблено спробу розширення класу шляхів, що перетинаються, у використанні яких усе ще можливо здійснити аналітичну оцінку ймовірності компрометації повідомлення, яке передається. Це дозволить створити умови для контролю за виконанням вимог щодо рівня мережної безпеки (3.1) в умовах використання шляхів, які перетинаються [45–48].

У цьому контексті необхідно додатково ввести ще два типи шляхів: простий і композитний. Простий шлях завжди утворений послідовним з'єднанням каналів зв'язку мережі, а ймовірність його компрометації розраховується за допомогою формули (3.2). У свою чергу композитні шляхи є більш складними структурними формами, що містять перетин простих шляхів. У зв'язку з цим уточнимо раніше введені та введемо додаткові позначення [47]:

## Константи

- $\tilde{M}$  кількість використовуваних композитних шляхів, що не перетинаються, які можуть використовуватися в процесі маршрутизації частин повідомлення;
- $\tilde{M}_i$  кількість фрагментів в  $i$ -му композитному шляху, які можуть бути скомпрометовані ( $i = \overline{1, \tilde{M}}$ );
- $M_i$  кількість каналів зв'язку в  $i$ -му композитному шляху, які можуть бути скомпрометовані ( $i = \overline{1, \tilde{M}}$ );
- $p_i^j$  імовірність компрометації  $j$ -го каналу зв'язку  $i$ -го композитного шляху ( $i = \overline{1, \tilde{M}}$ ,  $j = \overline{1, M_i}$ ).

## Кількісні показники

- $\tilde{p}_i^j$  імовірність компрометації  $j$ -го фрагмента  $i$ -го композитного шляху ( $i = \overline{1, \tilde{M}}$ ,  $j = \overline{1, \tilde{M}_i}$ );
- $\tilde{P}_i$  імовірність компрометації  $i$ -го композитного шляху ( $i = \overline{1, \tilde{M}}$ );
- $\tilde{P}_{msg}$  імовірність компрометації повідомлення загалом за умови його передачі частинами за композитними шляхами.

## Змінні

- $n_i$  цілочисельна змінна, яка характеризує кількість частин повідомлення, що передаються за  $i$ -м композитним шляхом ( $i = \overline{1, \tilde{M}}$ ).

Для того щоб забезпечувалася можливість формулювання в аналітичному вигляді виразу для розрахунку ймовірності компрометації композитного шляху в процесі безпечної маршрутизації, він повинен містити два типи фрагментів, що складаються з послідовного (рис. 3.7, а) або з паралельного з'єднання каналів зв'язку (рис. 3.7, б). На рис. 3.7, в наведено приклад композитного шляху з послідовним з'єднанням двох фрагментів мережі. Перший фрагмент представлений паралельним з'єднанням каналів зв'язку, а другий – послідовним.

На рис. 3.7, в показано структуру мережі, яка містить один композитний шлях, що складається з каналів двох простих шляхів, які перетинаються між собою. Перший простий шлях представлений вузлами  $1 \rightarrow 2 \rightarrow 3 \rightarrow 4$ , а другий –  $1 \rightarrow 3 \rightarrow 4$ . З іншого боку, цей композитний шлях містить два послідовно з'єднаних фрагменти. Перший фрагмент складається з паралельно з'єднаних каналів зв'язку  $1 \rightarrow 3$  та послідовності каналів  $1 \rightarrow 2$  та  $2 \rightarrow 3$ . Тоді як другий фрагмент представлений каналом зв'язку  $3 \rightarrow 4$ .

Тоді ймовірність компрометації композитного шляху (рис. 3.7, в) розраховується відповідно до виразу

$$\tilde{p}_1 = 1 - (1 - \tilde{p}_1^1)(1 - \tilde{p}_1^2). \quad (3.11)$$

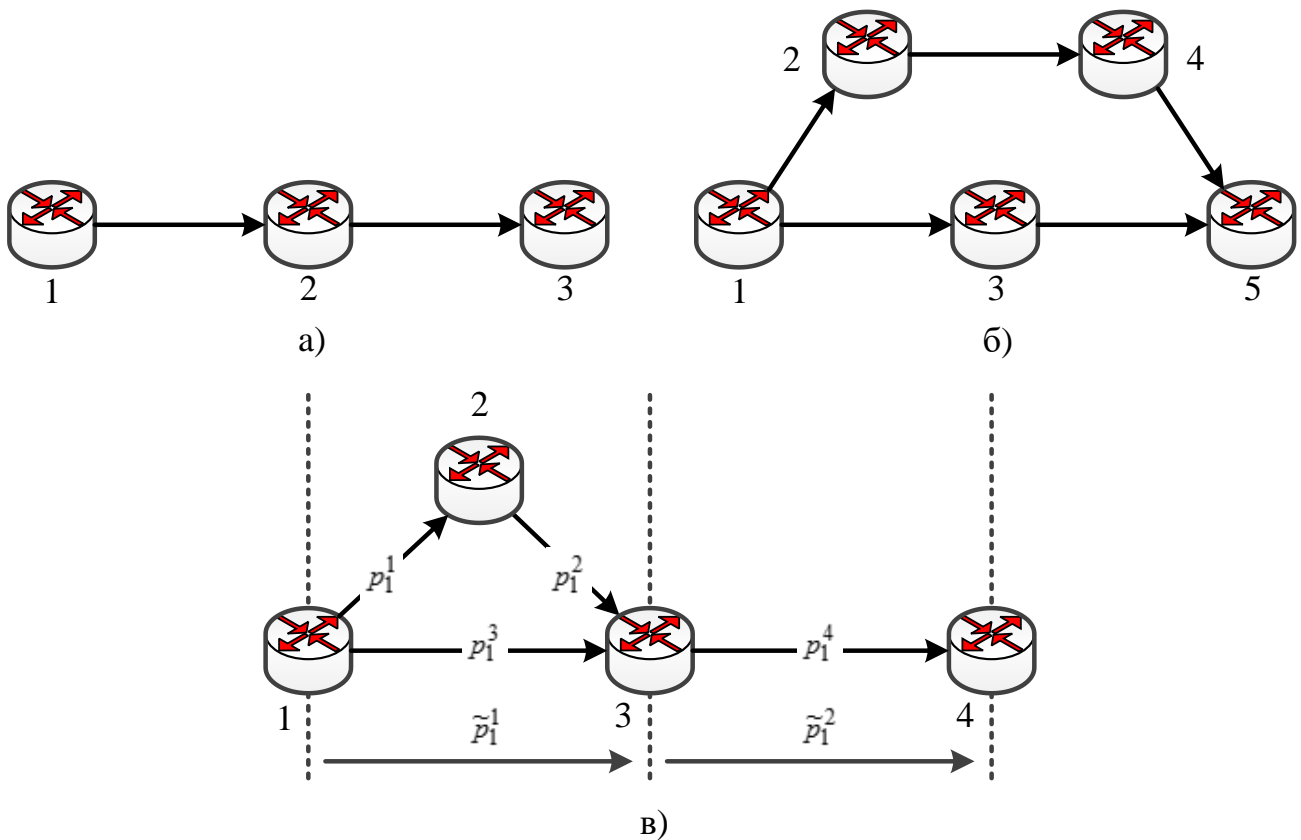


Рис. 3.7. Приклади типів фрагментів і композитного шляху:  
 а – послідовне з'єднання каналів зв'язку;  
 б – паралельне з'єднання каналів зв'язку; в – композитний шлях

У виразі (3.11) імовірності компрометації першого та другого фрагментів визначаються через імовірності компрометації каналів зв'язку, які вони містять:

$$\tilde{p}_1^1 = \left[ 1 - (1 - p_1^1)(1 - p_1^2) \right] p_1^3, \quad \tilde{p}_1^2 = p_1^4.$$

Отже, у загальному випадку ймовірність компрометації  $i$ -го композитного шляху, що складається з  $\tilde{M}_i$  фрагментів, може бути розрахована відповідно до такого виразу [47]:

$$\tilde{p}_i = 1 - \prod_{j=1}^{\tilde{M}_i} (1 - \tilde{p}_i^j). \quad (3.12)$$

Якщо для доставки повідомлення використовується єдиний композитний шлях, то ймовірність компрометації цього повідомлення визначається

ймовірністю компрометації цього композитного шляху. У більш загальному випадку, коли частини повідомлення передаються за множиною композитних шляхів, що не перетинаються, для розрахунку ймовірності компрометації повідомлення необхідно використовувати такий вираз [47]:

$$\tilde{P}_{msg} = \prod_{i=1}^{\tilde{M}} \tilde{p}_i, \quad (3.13)$$

який є модифікацією формули (3.6).

Приклад подібного випадку показано на рис. 3.8, коли для передачі частин повідомлення використовуються два шляхи, що не перетинаються:

- перший шлях є композитним і складається з таких каналів зв'язку 1→2, 2→3, 2→4, 3→5, 4→5, 5→7;
- другий шлях є простим і містить канали зв'язку 1→6 і 6→7.

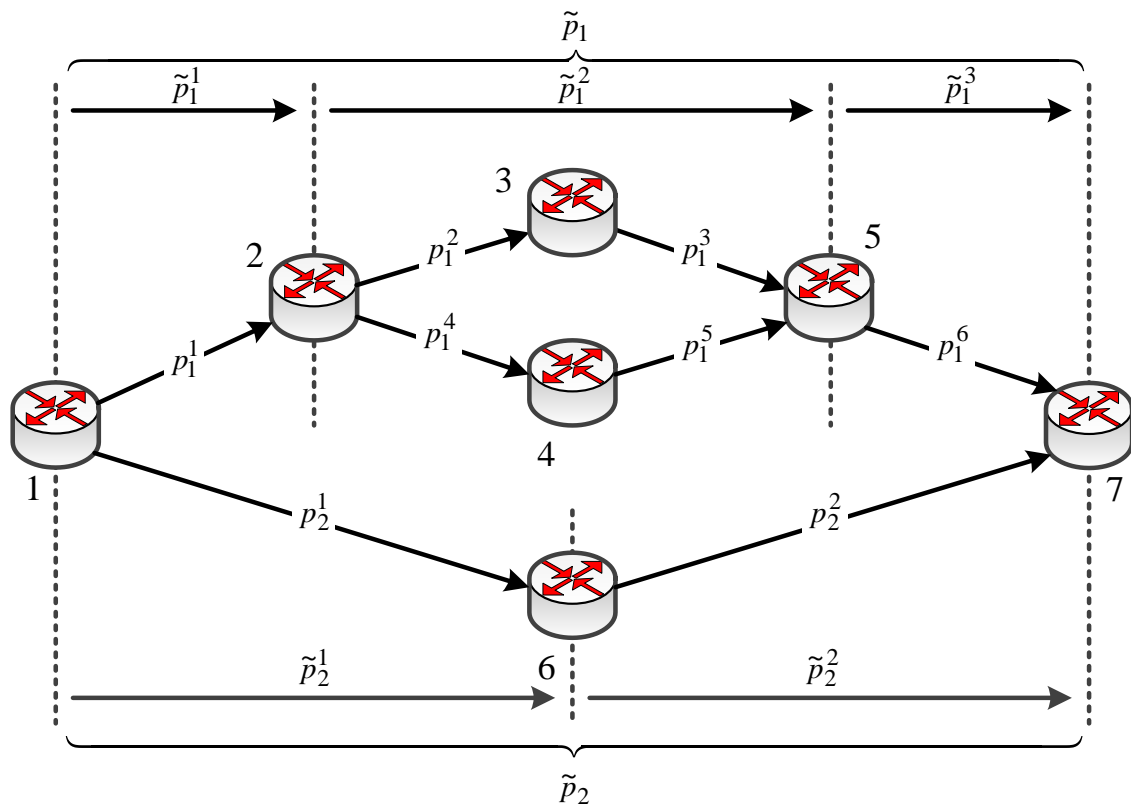


Рис. 3.8. Приклад використання двох шляхів: композитного та простого

У свою чергу перший (композитний) шлях складається з трьох послідовно з'єднаних мережних фрагментів:

- перший фрагмент представлений каналом зв'язку 1→2;
- другий фрагмент оснований на паралельному з'єднанні таких каналів зв'язку: 2→3, 3→5 і 2→4, 4→5;
- третій фрагмент представлений каналом зв'язку 5→7.



Тоді для цієї мережної структури (рис. 3.8) імовірність компрометації повідомлення у використанні двох різнотипних описаних вище шляхів буде визначатися таким чином:

$$P_{msg} = \tilde{p}_1 \cdot \tilde{p}_2. \quad (3.14)$$

У виразі (3.14) імовірності компрометації композитного та простого шляхів (першого та другого відповідно) виражаються через імовірності компрометації їх фрагментів і каналів зв'язку як

$$\begin{aligned} \tilde{p}_1 &= 1 - (1 - \tilde{p}_1^1)(1 - \tilde{p}_1^2)(1 - \tilde{p}_1^3) = \\ &= 1 - (1 - p_1^1) \left( 1 - \left[ 1 - (1 - p_1^2)(1 - p_1^3) \right] \times \left[ 1 - (1 - p_1^4)(1 - p_1^5) \right] \right) (1 - p_1^6); \end{aligned} \quad (3.15)$$

$$\tilde{p}_2 = 1 - (1 - \tilde{p}_2^1)(1 - \tilde{p}_2^2) = 1 - (1 - p_2^1)(1 - p_2^2). \quad (3.16)$$

У загальному випадку один композитний шлях може містити кілька послідовно з'єднаних фрагментів з паралельним з'єднанням каналів зв'язку. Позначимо через  $h_i$  максимальну кількість паралельно з'єднаних каналів зв'язку за всіма фрагментами  $i$ -го композитного шляху. Тоді умова (3.5) набуде вигляду [47]

$$h_i \leq n_i \leq T - 1, \quad (i = \overline{1, \tilde{M}}), \quad (3.17)$$

а її виконання дозволить таким чином розподілити частини повідомлення за паралельно з'єднаними каналами мережних фрагментів композитних шляхів, щоб у кожному з них передавалося ненульове число таких частин повідомлення та були справедливі вирази (3.12) і (3.13).

Крім того, умова (3.4) з урахуванням композитного характеру використовуваних шляхів набуде вигляду

$$N - n_i < T, \quad (i = \overline{1, \tilde{M}}). \quad (3.18)$$

У зв'язку з цим в основу запропонованого методу безпечної маршрутизації частин повідомлення, яке передається за множиною шляхів, що перетинаються, може бути покладено розв'язання оптимізаційної задачі, пов'язаної з використанням критерію оптимальності

$$\min_{n_i} \prod_{i=1}^{\tilde{M}} \tilde{p}_i(n_i), \quad (3.19)$$

що гарантує мінімізацію ймовірності компрометації переданого повідомлення [47]. Крім того, на керуючі змінні залежно від використовуваної схеми Шаміра накладаються обмеження (3.12), (3.17) або (3.18), а також аналог умови (3.3), представлений рівністю

$$\sum_{i=1}^{\tilde{M}} n_i = N. \quad (3.20)$$

Сформульована оптимізаційна задача належить до класу задач нелінійного цілочисельного програмування (Nonlinear Integer Programming), тому що змінні, які підлягають розрахунку, є цілочисельними, а критерій оптимальності (3.19) є нелінійним.

Запропонований метод безпечної маршрутизації повідомлень за множиною шляхів, які перетинаються, є засобом проактивного підходу щодо поліпшення рівня мережної безпеки. Це визначається тим, що на основі постійного аналізу стану мережі, її структури та параметрів безпеки каналів зв'язку, а також у процесі оптимального балансування частин конфіденційних повідомлень шляхами, які перетинаються, реалізуються всі доступні можливості для того, щоб максимально знизити ймовірність компрометації даних, які передаються.

### **3.5. Аналіз запропонованого методу безпечної маршрутизації повідомлень шляхами, що перетинаються**

#### **3.5.1. Дослідження методу безпечної маршрутизації повідомлень шляхами, що перетинаються, у разі використання єдиного композитного шляху**

Під час дослідження запропонованого методу буде проведено аналіз впливу на ймовірність компрометації повідомлення параметрів безпеки окремих каналів зв'язку та фрагментів мережі. Крім того, оцінимо виграш за ймовірністю компрометації, отримуваний за умови використання запропонованого в підрозділі 3.4 методу, порівняно з раніше відомим, описаним у пункті 3.3.1. Особливості розрахунку ймовірності компрометації повідомлення будуть продемонстровані на мережній структурі, показаній на рис. 3.7, в. Вихідними даними були значення, представлені в табл. 3.3. В останньому рядку табл. 3.3 наведено результат розв'язання поставленої оптимізаційної задачі, пов'язаної з мінімізацією виразу (3.19) у разі обмежень (3.12), (3.17), (3.20) у процесі реалізації схеми Шаміра (10, 10) та  $h_1 = 2$ .

Таблиця 3.3

#### **Вихідні дані для дослідження в разі використання єдиного композитного шляху**

Канал зв'язку	1→2	2→3	1→3	3→4
№ каналу зв'язку в шляху	1	2	3	4
Ймовірність компрометації каналу зв'язку	0,1	0,2	0÷1	0÷1
Кількість частин повідомлення	5	5	5	10

У процесі передачі повідомлення від першого до четвертого вузла його частини прямували за двома маршрутами, що перетинаються: 1→2→3→4 і

1→3→4, тобто канал 3→4 в них був спільним. У дослідженні передбачалося, що ймовірності компрометації першого та другого каналів були фіксованими та становили 0,1 і 0,2 відповідно, а ймовірності компрометації третього та четвертого каналів змінювалися в межах від 0 до 1.

Розрахунок імовірності компрометації проводився для двох випадків:

– у першому випадку для розрахунку ймовірності компрометації повідомлень ( $\tilde{P}_{msg}$ ) використовувався підхід, описаний у підрозділі 3.4 і оснований на виразах (3.11)–(3.13), (3.18);

– у другому випадку в розрахунках застосовувався підхід (3.2)–(3.6), викладений у пункті 3.3.1, який передбачає використання лише шляхів, що не перетинаються. Щодо рис. 3.7, в це передбачає використання або шляху 1→3→4, якому відповідала ймовірність компрометації  $P_{msg}^1$ , або шляху 1→2→3→4, компрометація якого оцінювалася ймовірністю  $P_{msg}^2$ .

Тоді на рис. 3.9 показано характер залежності ймовірності компрометації повідомлення, переданого шляхами різних типів для мережної структури, наведеної на рис. 3.7, в, від значень імовірності компрометації четвертого каналу  $p_1^4$  (відкладені по осі абсцис).

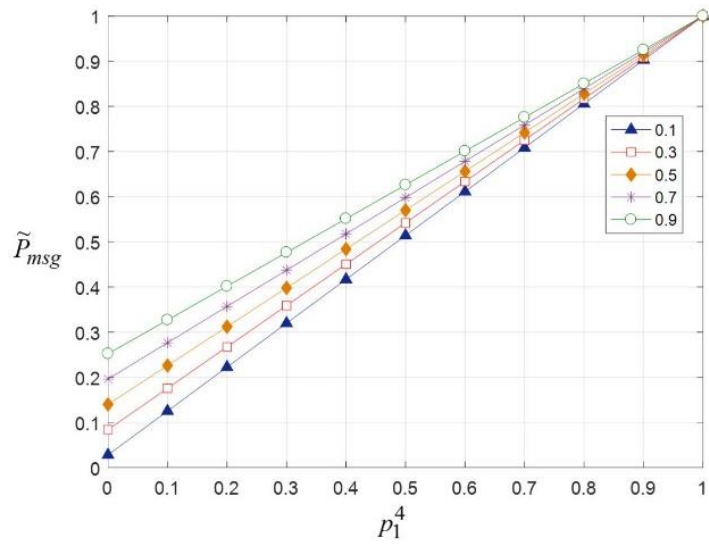
Кожній з множини прямих відповідало своє значення ймовірності компрометації третього каналу ( $p_1^3$ ). Як показано на рис. 3.9, зі зростанням  $p_1^3$  та  $p_1^4$  ймовірність компрометації повідомлення, що передається за умови використання композитного шляху та простого шляху 1→3→4, завжди зростала, але характер залежності в разі використання шляхів різних типів (що перетинаються та не перетинаються) істотно відрізнявся. З огляду на те, що простий шлях 1→2→3→4 не містив третій канал (рис. 3.7, в), то ймовірність його компрометації залежала лише від  $p_1^4$  і не залежала від  $p_1^3$  (рис. 3.9, в).

Для кількісної оцінки виграшу за ймовірністю компрометації повідомлень від застосування запропонованого методу, оснований на використанні шляхів, що перетинаються, порівняно з раніше відомими рішеннями використовувалися вирази:

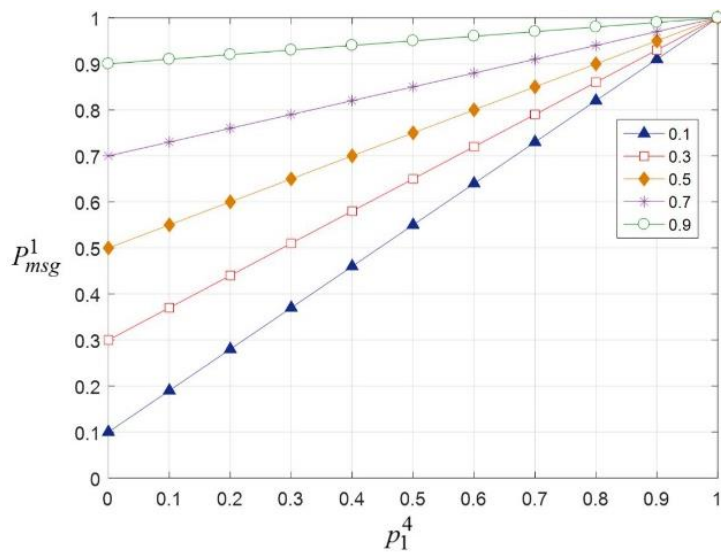
$$\Delta_1 = \frac{P_{msg}^1 - \tilde{P}_{msg}}{P_{msg}^1} \cdot 100\% , \quad (3.21)$$

а також

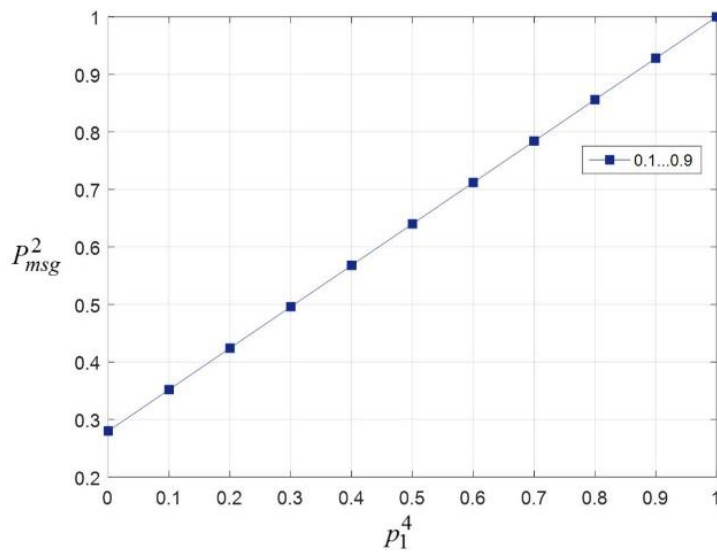
$$\Delta_2 = \frac{P_{msg}^2 - \tilde{P}_{msg}}{P_{msg}^2} \cdot 100\% . \quad (3.22)$$



а)



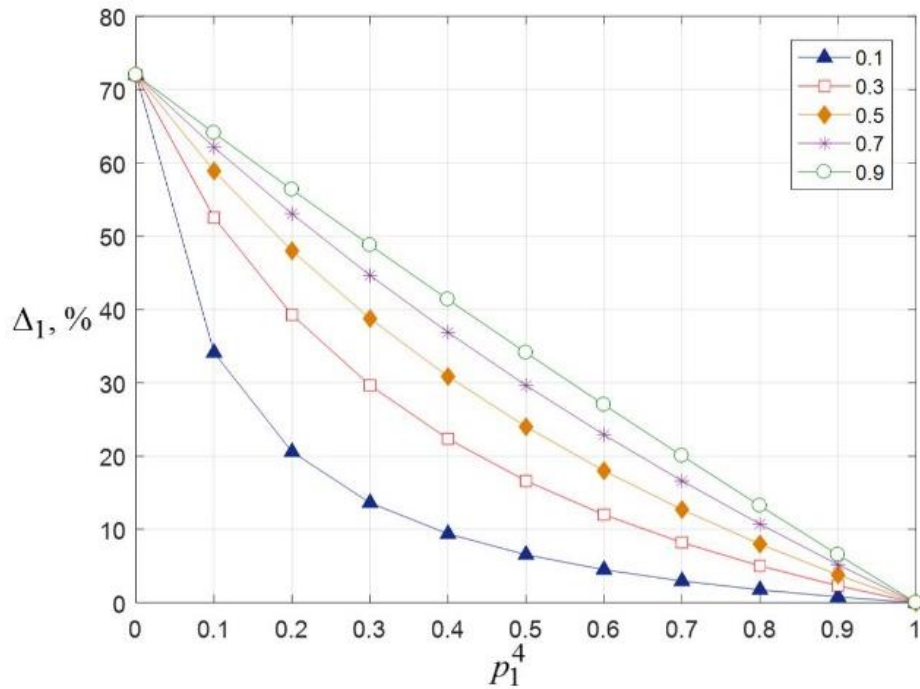
б)



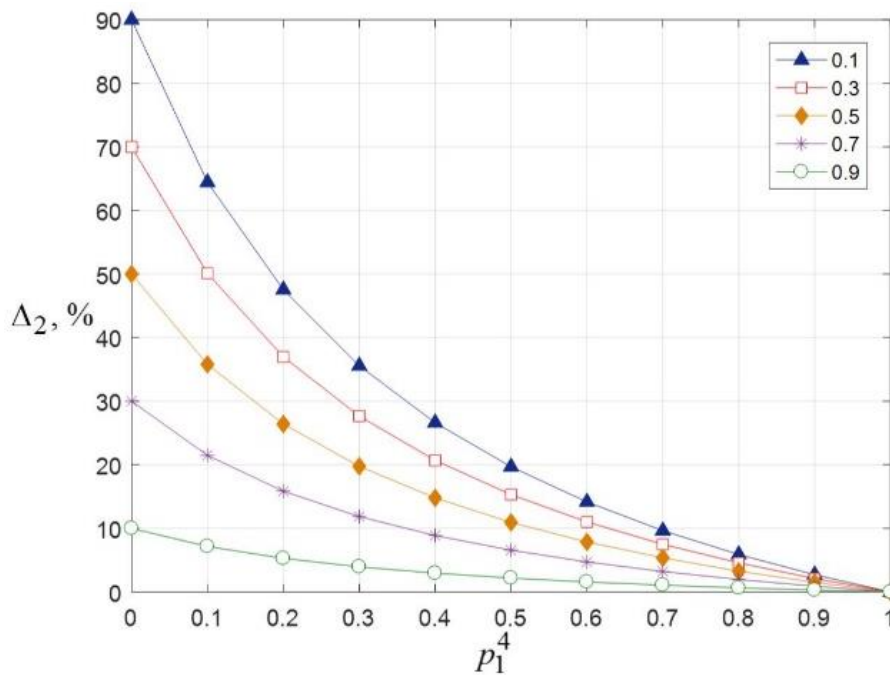
в)

Рис. 3.9. Залежність імовірності компрометації повідомлення, яке передається шляхами різних типів для мережної структури, наведеної на рис. 3.7, в

Відповідно до цих виразів отримані графіки, зображені на рис. 3.10. За результатами, представленими на рис. 3.10, можна зробити висновок, що використання запропонованого методу безпечної маршрутизації частин повідомлення двома простими шляхами, які перетинаються, об'єднаних в єдиний композитний шлях, сприяло поліпшенню рівня мережної безпеки.



а)



б)

Рис. 3.10. Залежність виграшу за ймовірністю компрометації від використання запропонованого методу порівняно з раніше відомими рішеннями для мережної структури, наведеної на рис. 3.7, в

У цьому випадку вдалося знизити ймовірність компрометації повідомлення:

– порівняно з використанням одного простого шляху  $1 \rightarrow 3 \rightarrow 4$  в середньому на 20–55 %, якщо  $p_1^4 = 0,1 \div 0,3$  та на 5–20 % за умови  $p_1^4 = 0,5 \div 0,9$  (рис. 3.10, а);

– порівняно з використанням одного простого шляху  $1 \rightarrow 2 \rightarrow 3 \rightarrow 4$  в середньому на 5–50 % у разі  $p_1^4 = 0,1 \div 0,3$  та на 3–15 %, якщо  $p_1^4 = 0,5 \div 0,9$  (рис. 3.10, б).

Виграш за ймовірністю компрометації повідомлення, що передається, знижувався, якщо  $p_1^4 \rightarrow 1$ , оскільки будь-який з розглянутих маршрутів, і простий, і композитний, проходили через цей канал.

### **3.5.2. Дослідження методу безпечної маршрутизації повідомлень у разі використання двох різнотипних шляхів, що не перетинаються**

Аналогічно проведемо порівняльний аналіз ефективності запропонованого методу (див. підрозділ 3.4) та раніше відомих рішень (див. пункт 3.3.1) для структури мережі, представлені на рис. 3.8. За допомогою запропонованого в підрозділі 3.4 методу оцінювалася ймовірність компрометації повідомлення ( $\tilde{P}_{msg}$ ), яке передається з використанням усіх доступних каналів зв'язку, що містяться в одному композитному й одному простому шляху.

З використанням раніше відомого методу (3.2)–(3.6) оцінювалася ймовірність компрометації повідомлення, частини якого передавалися з використанням двох простих шляхів, які не перетинаються. Зокрема розглядалися два можливі випадки комбінації вибору таких шляхів. У першому випадку використовувалися шляхи  $1 \rightarrow 2 \rightarrow 4 \rightarrow 5 \rightarrow 7$  та  $1 \rightarrow 6 \rightarrow 7$ , якому відповідала ймовірність компрометації повідомлення  $P_{msg}^1$ . У другому випадку частини повідомлення передавалися іншою парою шляхів, що не перетинаються:  $1 \rightarrow 2 \rightarrow 3 \rightarrow 5 \rightarrow 7$  та  $1 \rightarrow 6 \rightarrow 7$ . Цьому рішенню відповідало значення ймовірності компрометації  $P_{msg}^2$ .

Показником ефективності безпечної маршрутизації знову була ймовірність компрометації повідомлень, які передаються, а в процесі досліджень аналізувався вплив на неї ймовірностей компрометації, наприклад,

каналів 2→4 та 1→6, які змінювалися від 0 до 1. Канал 2→4 розміщувався у композитному шляху під четвертим номером, а канал 1→6 мав перший номер у структурі простого шляху (табл. 3.4).

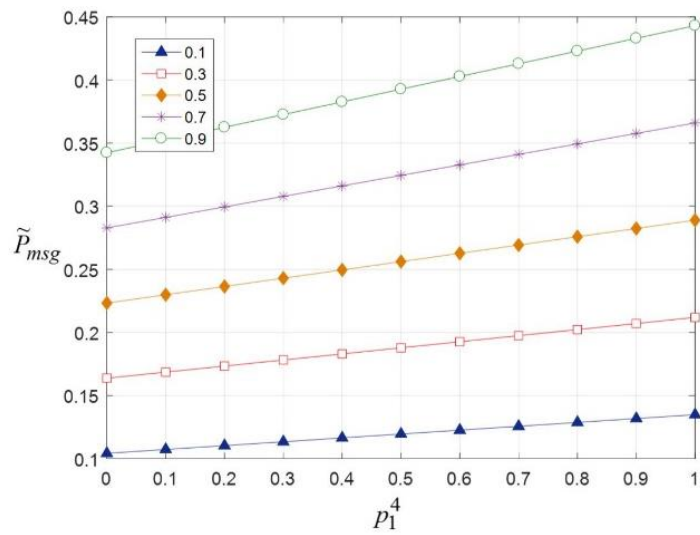
Таблиця 3.4

**Вихідні дані для дослідження випадку використання двох різнотипних шляхів, що не перетинаються**

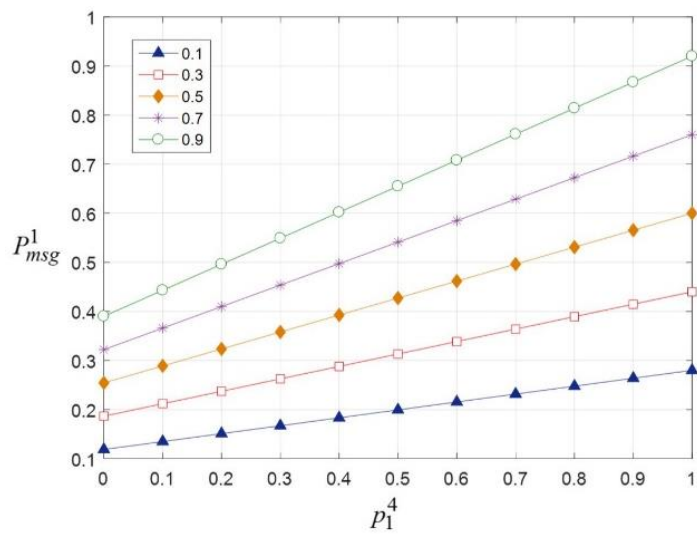
Номер шляху	1 (композитний)						2 (простий)	
	1→2	2→3	3→5	2→4	4→5	5→7	1→6	6→7
Канал зв'язку	1	2	3	4	5	6	1	2
№ каналу зв'язку в шляху	1	2	3	4	5	6	1	2
Імовірність компрометації каналу зв'язку	0,2	0,1	0,1	0÷1	0,1	0,2	0÷1	0,2
Кількість частин повідомлення	5	3	3	2	2	5	5	5

У табл. 3.4 також наведені значення ймовірностей компрометації всіх каналів, що містяться в цих двох шляхах. Останнім рядком у табл. 3.4 вказано результат розв'язання оптимізаційної задачі, пов'язаної з мінімізацією (3.19) за умови обмежень (3.12), (3.17) або (3.18), (3.20) у разі реалізації схеми Шаміра (10, 10) та  $h_1 = 2$ ,  $h_2 = 1$ . Першим (композитним) шляхом і другим (простим) шляхами передавалося по 5 частин вихідного повідомлення, тобто  $n_1 = n_2 = 5$ .

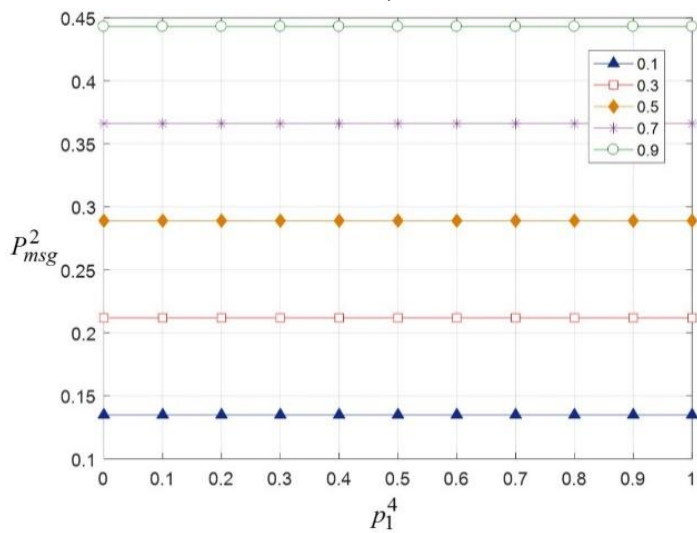
На рис. 3.11 показано залежність імовірності компрометації повідомлення, яке передається шляхами різних типів для структури, наведеної на рис. 3.8, від значень імовірності компрометації четвертого каналу композитного шляху (відкладені по осі абсцис). Кожній з множини прямих на рис. 3.11 відповідало своє значення ймовірності компрометації першого каналу простого шляху ( $p_2^1$ ). Як показано на рис. 3.11, а та б, зі зростанням  $p_2^1$  та  $p_1^4$  імовірність компрометації повідомлення, яке передається у разі використання композитного шляху та простого шляху 1→2→4→5→7 завжди зростала. З огляду на те, що прості шляхи 1→2→3→5→7 і 1→6→7, не містили канал 2→4 (рис. 3.8), то ймовірність їх компрометації залежала лише від  $p_2^1$  і не залежала від  $p_1^4$  (рис. 3.11, в).



a)



б)



в)

Рис. 3.11. Залежність імовірності компрометації повідомлення, яке передається шляхами різних типів, для мережної структури, наведеної на рис. 3.8



Проведено кількісний аналіз виграшу за ймовірністю компрометації повідомлень (рис. 3.12) від використання запропонованого методу, основанийого на використанні шляхів, що перетинаються, порівняно з раніше відомими рішеннями з використанням виразів (3.21) і (3.22). Як показано на рис. 3.12, аналізований за формулами (3.21) і (3.22) виграш за ймовірністю компрометації повідомлення, яке передається за шляхами різних типів, залежить лише від параметрів безпеки каналів, що містяться в композитному шляху. У цьому випадку це канал зв'язку 2→4, який є четвертим каналом першого (композитного) шляху з імовірністю компрометації  $p_1^4$ . Від значень імовірності компрометації каналу 1→6 ( $p_2^1 = 0,1 \div 0,9$ ), який є першим каналом другого (простого) шляху, виграш (3.21) і (3.22) не залежав (рис. 3.12).

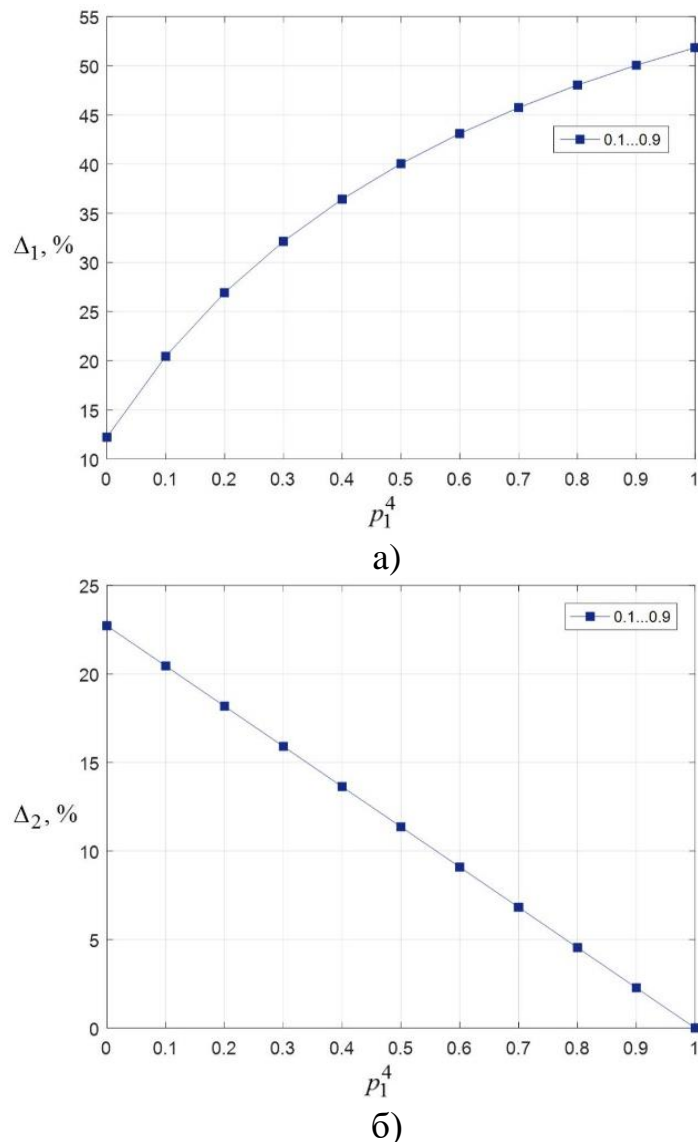


Рис. 3.12. Залежність виграшу за ймовірністю компрометації від використання запропонованого методу порівняно з раніше відомими рішеннями для мережної структури, наведеної на рис. 3.8

За результатами, представленими на рис. 3.12, також можна зробити висновок, що використання запропонованого методу безпечної маршрутизації призвело до зниження ймовірності компрометації повідомлення, яке передається:

– порівняно із застосуванням двох простих шляхів  $1 \rightarrow 2 \rightarrow 4 \rightarrow 5 \rightarrow 7$  і  $1 \rightarrow 6 \rightarrow 7$ , що не перетинаються, у середньому на 20–33 %, якщо  $p_1^4 = 0,1 \div 0,3$ , і на 40–50 % у разі  $p_1^4 = 0,5 \div 0,9$  (рис. 3.12, а);

– порівняно з використанням двох простих шляхів  $1 \rightarrow 2 \rightarrow 3 \rightarrow 5 \rightarrow 7$  і  $1 \rightarrow 6 \rightarrow 7$ , що не перетинаються, у середньому на 16–20 % за умови  $p_1^4 = 0,1 \div 0,3$  і на 3–12 %, якщо  $p_1^4 = 0,5 \div 0,9$  (рис. 3.12, б).

Таким чином, у процесі зростання ймовірності компрометації каналу, що міститься в композитному шляху, тобто якщо  $p_1^4 \rightarrow 1$ , виграш за ймовірністю компрометації повідомлення, яке передається, підвищувався порівняно з використанням простих шляхів, що містять той самий канал (рис. 3.12, а).

Якщо  $p_1^4 = 1$ , весь простий шлях  $1 \rightarrow 2 \rightarrow 4 \rightarrow 5 \rightarrow 7$  буде скомпрометований, а використання композитного шляху, що містить мережний фрагмент з паралельним з'єднанням каналів, дозволяє цього уникнути.

З іншого боку, якщо канал  $2 \rightarrow 4$  був скомпрометований, тобто  $p_1^4 = 1$ , то композитний шлях фактично втрачав свою перевагу, перетворюючись де-факто в простий шлях  $1 \rightarrow 2 \rightarrow 3 \rightarrow 5 \rightarrow 7$ . Це і призводило до зниження виграшу за ймовірністю компрометації повідомлення від застосування запропонованого методу порівняно з методом безпечної маршрутизації шляхами, що не перетинаються (рис. 3.12, б).

### **3.6. Метод безпечної швидкої перемаршрутизації повідомлень композитними шляхами: проактивний і реактивний підходи**

З метою розширення функціональних можливостей засобів безпечної маршрутизації важливо, щоб запропонований метод реалізував принципи не тільки проактивного, але й реактивного підходу. Іншими словами, у структурі методу безпечної маршрутизації важливо передбачити процедури оперативної реакції на можливі порушення рівня мережної безпеки. У цей час протоколи маршрутизації реагують на можливі зміни стану мережі в масштабі часу десятків секунд, що не є прийнятним з точки зору необхідного рівня мережної безпеки.

У зв'язку з цим усе частіше на практиці застосовуються методи та протоколи швидкої перемаршрутизації, під час яких попередньо розраховуються два типи шляхів: основний і резервний. У цьому випадку використання окремо кожного типу шляхів має сприяти задоволенню вимог щодо рівня мережної безпеки. Тоді в разі відмови основного шляху повідомлення практично миттєво (із затримкою в десятки мілісекунд) будуть передаватися з використанням резервних маршрутів. Очевидно, що основний і резервний маршрути не повинні перетинатися за елементами мережі, які скомпрометовані (маршрутизаторами, каналами зв'язку або маршрутами загалом) [49–52].

Тоді в межах безпечної швидкої перемаршрутизації (Secure Fast ReRouting, S-FRR) використання множини основних шляхів належить до рішень проактивного підходу щодо забезпечення заданого рівня мережної безпеки, а застосування резервних шляхів відповідає вимогам реактивного підходу. Зокрема в межах запропонованого методу розрахунок множини основних і резервних шляхів повинен здійснюватися максимально погоджено для підвищення ефективності кінцевих рішень.

Поділ шляхів на основні та резервні має на увазі, що частини повідомлення будуть передаватися не всіма доступними композитними та простими шляхами, а лише їхньою обмеженою кількістю, але з виконанням вимог щодо ймовірності компрометації (3.1). З огляду на те, що для підвищення рівня мережної безпеки повідомлень, які передаються, необхідно реалізувати багатошляхову маршрутизацію їх частин, то основними та резервними будуть не окремі композитні або прості шляхи, а утворені ними мультишляхи. У цьому випадку у складі як основного, так і резервного мультишляху можуть міститися кілька композитних та (або) простих шляхів.

Для розрахунку резервного мультишляху пропонується реалізувати такі дві схеми захисту основного мультишляху:

- схема захисту основного мультишляху загалом, за якої основний і резервний мультишляхи не перетинаються ні за вузлами, ні за каналами;
- схема захисту окремого шляху (композитного або простого) основного мультишляху, у разі якої резервний мультишлях не повинен містити канали та вузли шляху, що захищається.

Реалізація кожної зі схем захисту орієнтована на відновлення заданого рівня мережної безпеки за рахунок відмови від основного мультишляху та переходу до використання резервного мультишляху. У зв'язку з цим уточнимо раніше введені та введемо додаткові позначення [47]:

### Кількісні показники

$\tilde{p}_i^{pr}$  імовірність компрометації  $i$ -го композитного або простого шляху основного мультишляху ( $i = \overline{1, \tilde{M}}$ );

$\tilde{p}_i^b$  імовірність компрометації  $i$ -го композитного або простого шляху резервного мультишляху ( $i = \overline{1, \tilde{M}}$ );

$\tilde{P}_{msg}^{pr}$  імовірність компрометації повідомлення загалом у разі його передачі частинами композитними або простими шляхами основного мультишляху;

$\tilde{P}_{msg}^b$  імовірність компрометації повідомлення загалом у випадку його передачі частинами композитними або простими шляхами резервного мультишляху.

### Змінні

$n_i$  цілочисельна змінна, яка характеризує кількість частин повідомлення, що передаються  $i$ -м композитним або простим шляхом, з якого складається основний мультишлях ( $i = \overline{1, \tilde{M}}$ );

$\bar{n}_i$  цілочисельна змінна, яка характеризує кількість частин повідомлення, що передаються  $i$ -м композитним або простим шляхом, з якого складається резервний мультишлях ( $i = \overline{1, \tilde{M}}$ ).

З огляду на введені позначення для розрахунку ймовірності компрометації повідомлення, яке передається частинами множиною композитних шляхів, необхідно за аналогією до формул (3.1) і (3.13) використовувати відповідно вирази:

$$\tilde{P}_{msg}^{pr} = \prod_{i=1}^{\tilde{M}} \tilde{p}_i^{pr} \quad \text{і} \quad \tilde{P}_{msg}^b = \prod_{i=1}^{\tilde{M}} \tilde{p}_i^b. \quad (3.23)$$

Варто зазначити, що ймовірності компрометації мережних фрагментів  $\tilde{p}_i^{pr}$  і  $\tilde{p}_i^b$  є функціями від кількості частин повідомлення, що передаються ними, тобто від  $n_i$  і  $\bar{n}_i$ . Тоді з урахуванням (3.12) мають місце умови [47]:

$$\tilde{p}_i^{pr} = \begin{cases} 1 - \prod_{j=1}^{\tilde{M}_i} (1 - \tilde{p}_i^j), & n_i > 0; \\ 1, & n_i = 0, \end{cases} \quad \text{і} \quad \tilde{p}_i^b = \begin{cases} 1 - \prod_{j=1}^{\tilde{M}_i} (1 - \tilde{p}_i^j), & \bar{n}_i > 0; \\ 1, & \bar{n}_i = 0. \end{cases} \quad (3.24)$$

Системи (3.24) можуть бути записані як

$$\tilde{p}_i^{Pr} = 1 - H_0(n_i) \prod_{j=1}^{\tilde{M}_i} (1 - \tilde{p}_i^j) \quad \text{і} \quad \tilde{p}_i^b = 1 - H_0(\bar{n}_i) \prod_{j=1}^{\tilde{M}_i} (1 - \tilde{p}_i^j), \quad (3.25)$$

де  $H_0$  – функція Хевісайда, що з урахуванням виразу (3.24) розраховується таким чином:

$$H_0(n) = \begin{cases} 0, & n = 0; \\ 1, & n > 0. \end{cases}$$

Умова (3.20) з огляду на реалізацію S-FRR доповнюються виразом

$$\sum_{i=1}^{\tilde{M}} \bar{n}_i = N. \quad (3.26)$$

У свою чергу для захисту основного мультишляху, за аналогією з [53], необхідно забезпечити виконання такої умови:

$$\sum_{i=1}^{\tilde{M}} n_i \bar{n}_i = 0. \quad (3.27)$$

За необхідності захисту окремого  $i$ -го композитного шляху важливо забезпечити виконання умови

$$n_i \bar{n}_i = 0, \quad (3.28)$$

яка також є нелінійною (білінійною).

Для того щоб у використанні й основного, і резервного мультишляху виконувалися вимоги щодо ймовірності компрометації повідомлення, яке за ними передається, вводиться за аналогією з (3.1) така умова [47]:

$$P_{msg}^{Pr} \leq P_{msg}^b \leq \gamma_P. \quad (3.29)$$

Тоді в основу розроблюваного методу S-FRR може бути покладено рішення оптимізаційної задачі нелінійного цілочисельного програмування (Nonlinear Integer Programming) з критерієм оптимальності

$$J = \sum_{i=1}^{\tilde{M}} \tilde{p}_i n_i + \sum_{i=1}^{\tilde{M}} \tilde{p}_i \bar{n}_i \quad (3.30)$$

і обмеженнями, що відповідають умовам (3.17), (3.18), (3.20), (3.26), (3.27), (3.28) та (3.29). Зокрема обмеження (3.27)–(3.29) є нелінійними, а змінні  $n_i$  й  $\bar{n}_i$  мають цілочисельний характер [47]. У критерії (3.30) значення  $\tilde{p}_i$ , розраховані відповідно до виразів (3.12), є вартісними ваговими коефіцієнтами. Цим забезпечується безпечна маршрутизація в мережі, коли максимальна кількість частин повідомлення буде передаватися шляхом з мінімальною ймовірністю компрометації. Навпаки, шляхом з найвищою ймовірністю компрометації передаватиметься мінімальна кількість частин повідомлення або не буде передано жодної.

### 3.7. Дослідження методу безпечної швидкої перемаршрутизації повідомлень композитними шляхами

Продемонструємо особливості функціонування запропонованого методу безпечної швидкої перемаршрутизації конфіденційних повідомлень. Вихідна структура мережі представлена на рис. 3.13, а відповідні ймовірності компрометації каналів зв'язку наведені в табл. 3.5.

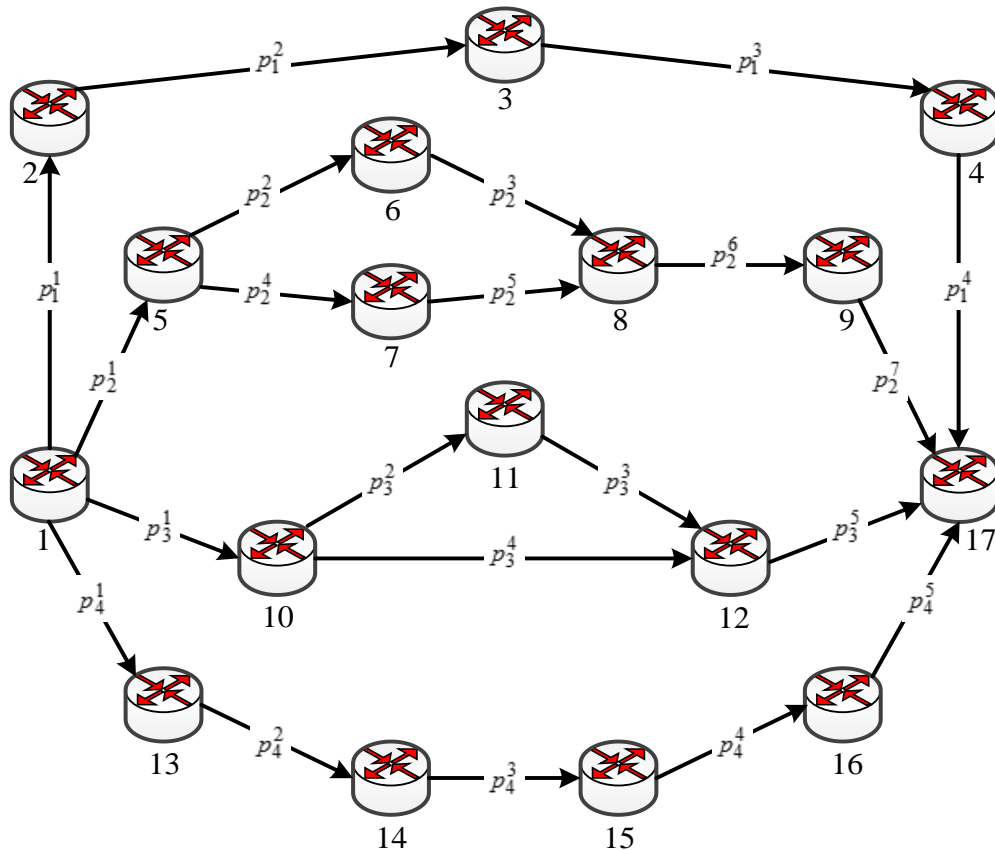


Рис. 3.13. Вихідна структура мережі

Відправником повідомлення є перший вузол, а отримувачем – сімнадцятий вузол. Суцільними лініями на рис. 3.13 показані канали зв'язку, що використовуються для формування основного та резервного мультишляхів для передачі повідомлення. Нехай за умови безпечної швидкої перемаршрутизації реалізується схема Шаміра (10, 10) і відповідно до структури шляхів, наведених на рис. 3.13,  $h_1 = 1$ ,  $h_2 = 2$ ,  $h_3 = 2$  та  $h_4 = 1$ , а допустиме значення ймовірності компрометації повідомлення, що передається, яке визначається параметром  $\gamma_P$ , так само 0,3. Тоді в процесі дослідження розглянуто два випадки, що демонструють особливості реалізації описаних у підрозділі 3.6 схем захисту:

– перший випадок пов'язаний зі схемою захисту другого (композитного) шляху;

– другий випадок описує схему захисту основного мультишляху загалом.

Розглянемо докладніше перший випадок. Тоді, відповідно до наведених у табл. 3.5 вихідних даних, ґрунтуючись на запропонованому в підрозділі 3.6 методі розрахунку, основний мультишлях містить два композитних шляхи: другий і третій, які мають найменші ймовірності компрометації: 0,5339 і 0,4061 відповідно. Параметри цих шляхів і послідовність балансування ними частин повідомлення, яке передається, наведені в табл. 3.6.

Таблиця 3.5

**Вихідні дані для дослідження безпечної швидкої перемаршрутизації**

Номер шляху	1 (простий)						
Канал зв'язку	1→2	2→3	3→4	4→17			
№ каналу зв'язку в шляху	1	2	3	4			
Ймовірність компрометації каналу зв'язку	0,15	0,19	0,17	0,2			
Номер шляху	2 (композитний)						
Канал зв'язку	1→5	5→6	6→8	5→7	7→8	8→9	9→17
№ каналу зв'язку в шляху	1	2	3	4	5	6	7
Ймовірність компрометації каналу зв'язку	0,2	0,2	0,1	0,2	0,2	0,19	0,2
Номер шляху	3 (композитний)						
Канал зв'язку	1→10	10→11	11→12	10→12	12→17		
№ каналу зв'язку в шляху	1	2	3	4	5		
Ймовірність компрометації каналу зв'язку	0,2	0,2	0,2	0,2	0,2		
Номер шляху	4 (простий)						
Канал зв'язку	1→13	13→14	14→15	15→16	16→17		
№ каналу зв'язку в шляху	1	2	3	4	5		
Ймовірність компрометації каналу зв'язку	0,2	0,18	0,1	0,15	0,1		

За третім (композитним) шляхом передавалося вісім частин повідомлення, тому що ймовірність його компрометації мінімальна та дорівнює 0,4061. За другим (композитним) шляхом передавалося дві частини повідомлення, оскільки ймовірність його компрометації була вже 0,5339, а нижній поріг для  $n_2$  відповідно до умов (3.17) становив  $h_2 = 2$ . Використання даних двох шляхів як основного мультишляху відповідно до виразу (3.23) забезпечує ймовірність компрометації повідомлення, рівну 0,2168, що задовольняє вимозі ( $\gamma_P = 0,3$ ).

У разі захисту другого (композитного) шляху основного мультишляху у складі розрахованого резервного мультишляху будуть уже перший (простий) і третій (композитний) шляхи, параметри яких наведені в табл. 3.7.

Таблиця 3.6

### Параметри основного мультишляху

Номер шляху	2 (композитний)						
Імовірність компрометації шляху	0,5339						
Кількість частин повідомлення в шляху	2						
Канал зв'язку	1→5	5→6	6→8	5→7	7→8	8→9	9→17
№ каналу зв'язку в шляху	1	2	3	4	5	6	7
Кількість частин повідомлення в каналі зв'язку	2	1	1	1	1	2	2
Номер шляху	3 (композитний)						
Імовірність компрометації шляху	0,4061						
Кількість частин повідомлення в шляху	8						
Канал зв'язку	1→10	10→11	11→12	10→12	12→17		
№ каналу зв'язку в шляху	1	2	3	4	5		
Кількість частин повідомлення в каналі зв'язку	8	4	4	4	8		

Таблиця 3.7

### Параметри резервного мультишляху (перший випадок)

Номер шляху	1 (простий)				
Імовірність компрометації шляху	0,5428				
Кількість частин повідомлення в шляху	1				
Канал зв'язку	1→2	2→3	3→4	4→17	
№ каналу зв'язку в шляху	1	2	3	4	
Кількість частин повідомлення в каналі зв'язку	1	1	1	1	
Номер шляху	3 (композитний)				
Імовірність компрометації шляху	0,4061				
Кількість частин повідомлення в шляху	9				
Канал зв'язку	1→10	10→11	11→12	10→12	12→17
№ каналу зв'язку в шляху	1	2	3	4	5
Кількість частин повідомлення в каналі зв'язку	9	5	5	4	9

За третім (композитним) шляхом передаватиметься дев'ять частин повідомлення, а за першим (простим) усього одна, тому що ймовірність



компрометації першого шляху становила 0,5428 за умови  $h_1 = 1$ . Використання резервного мультишляху також задовольняє вимоги щодо ймовірності компрометації переданого повідомлення (3.29), яка становила 0,2204.

Розглянемо докладніше другий випадок, у межах якого необхідно було захистити основний мультишлях загалом. Застосування запропонованого методу S-FRR залишило незмінним основний мультишлях (табл. 3.6). Тоді відповідно до наведених у табл. 3.5 вихідних даних резервний мультишлях містить два простих шляхи – перший і четвертий (табл. 3.8).

Таблиця 3.8

**Параметри резервного мультишляху (другий випадок)**

Номер шляху	1 (простий)				
Ймовірність компрометації шляху	0,5428				
Кількість частин повідомлення в шляху	9				
Канал зв'язку	1→2	2→3	3→4	4→17	
№ каналу зв'язку в шляху	1	2	3	4	
Кількість частин повідомлення в каналі зв'язку	9	9	9	9	
Номер шляху	4 (простий)				
Ймовірність компрометації шляху	0,5483				
Кількість частин повідомлення в шляху	1				
Канал зв'язку	1→13	13→14	14→15	15→16	16→17
№ каналу зв'язку в шляху	1	2	3	4	5
Кількість частин повідомлення в каналі зв'язку	1	1	1	1	1

Ймовірність компрометації четвертого (простого) шляху становила 0,5483. Тоді використання резервного мультишляху дозволило забезпечити значення ймовірності компрометації повідомлення, яке передається, в 0,2977 у разі  $\gamma_p = 0,3$ . За першим шляхом передавалося дев'ять частин повідомлення, тому що його ймовірність компрометації була нижчою, ніж у четвертого шляху, за яким передавалася одна частина повідомлення за умови  $h_4 = 1$ .

**Висновки до третього розділу**

1. Визначено, що залежно від часу реакції на можливу компрометацію каналів зв'язку та фрагментів мережі для забезпечення заданого рівня мережної

безпеки на практиці можуть використовуватися як проактивні, так і реактивні засоби, що повинні взаємно доповнювати один одного. Проактивні засоби застосовуються, як правило, на етапі запобігання компрометації повідомлень або мінімізації ймовірності її виникнення. Реактивні засоби використовуються тоді, коли безпека даних, що передаються, уже порушена і мережними засобами важливо оперативного відновити необхідний рівень безпеки.

2. Установлено, що одним з ефективних проактивних засобів забезпечення заданого рівня мережної безпеки є багатошляхова маршрутизація конфіденційних повідомлень, розділеного на частини відповідно до схеми Шаміра з балансуванням кількості таких частин маршрутами, що не перетинаються. На основі аналізу недоліків наявного механізму SPREAD запропоновано вдосконалення моделі розподілу фрагментів, яка була зведена до задачі оптимального балансування кількості частин повідомлення, що передається, маршрутами, які не перетинаються. Запропоновано низку критеріїв оптимальності, пов'язаних з вирішенням завдання балансування. У процесі порівняльного аналізу обґрунтований до використання на практиці критерій оптимальності, що забезпечує, з одного боку, мінімізацію верхнього динамічно керованого порога кількості частин повідомлення, які передаються окремими непересічними шляхами в мережі, а з іншого, – адаптацію до параметрів безпеки (ймовірності компрометації) окремих елементів мережі: вузлів, каналів і шляхів. Представлено числові приклади реалізації моделей з різними критеріями оптимальності отримуваних рішень, і проведено їх порівняльний аналіз. Результати порівняння (табл. 3.2) підтвердили ефективність запропонованої моделі, коли гіршим, з точки зору ймовірності компрометації, шляхом передається мінімальна кількість частин повідомлення, а кращим шляхом – їх максимальна кількість.

3. У розділі запропоновано використання особливого класу шляхів, що перетинаються, які становлять основу композитних шляхів і містять мережні фрагменти з послідовним та (або) паралельним з'єднанням каналів зв'язку мережі, що орієнтує на зниження ймовірності компрометації конфіденційних повідомлень, які передаються в ІКМ. Розроблено метод безпечної маршрутизації повідомлень шляхами, що перетинаються, який належить до класу проактивних рішень щодо забезпечення мережної безпеки. Новизна методу полягає в тому, що він, по-перше, допускає використання шляхів, які перетинаються, становлять основу композитних шляхів і містять мережні фрагменти з послідовним та (або) паралельним з'єднанням каналів зв'язку, а по-друге, оснований на оптимізації процесу вибору множини композитних

шляхів і балансування ними частин повідомлення, що передається, із забезпеченням допустимих значень його ймовірності компрометації. Проведений аналіз показав (рис. 3.10 та 3.12), що використання запропонованого методу в межах наведених розрахункових прикладів дозволяє знизити ймовірність компрометації переданих повідомлень у середньому від 5–10 % до 25–50 % з огляду на можливості використання композитних шляхів, які є одним з підкласів шляхів, що перетинаються.

4. Зазначено, що за умови зміни стану мережі, викликаного порушенням рівня безпеки конфіденційних повідомлень, що передаються в ІКМ, важливо визначити оперативну послідовність зміни множини шляхів, які використовуються для передачі його частин. Тому рішення щодо швидкої перемаршрутизації з локальним чи глобальним захистом елементів ІКМ можуть розглядатися як реалізація реактивного підходу щодо забезпечення безпечної маршрутизації. Синтезовано метод безпечної швидкої перемаршрутизації повідомлень у мережі, який орієнтує на реалізацію як проактивної, так і реактивної безпечної маршрутизації конфіденційних повідомлень. Новизна методу безпечної швидкої перемаршрутизації полягає в тому, що в разі порушення вимог мережної безпеки, викликаного підвищенням ймовірності компрометації одного або множини композитних шляхів, які містяться в основному мультишляху, багатошляхова передача частин конфіденційного повідомлення із забезпеченням заданих значень імовірності його компрометації буде здійснюватися вже заздалегідь розрахованою множиною резервних композитних шляхів, реалізуючи захист або основного мультишляху загалом, або одного чи декількох заздалегідь заданих композитних шляхів, що містить основний мультишлях.

5. У межах запропонованого методу безпечної швидкої перемаршрутизації повідомлень закладено можливість захисту як основного мультишляху загалом, так і одного або декількох заздалегідь заданих композитних шляхів, що містить цей основний мультишлях. Застосування методу S-FRR дозволяє в реальному часі забезпечувати задані значення такого важливого показника мережної безпеки, як імовірність компрометації повідомлень, що передаються, навіть в умовах динамічної зміни стану мережі (імовірності компрометації каналів і шляхів) на підставі розрахунку й оперативного переходу на використання резервних композитних шляхів за умови багатошляхової передачі частин конфіденційного повідомлення.

6. Розроблені методи безпечної маршрутизації можуть бути покладені в основу нових мережних протоколів маршрутизації та швидкої перемаршрутизації

для багатошляхової передачі частин конфіденційного повідомлення із заданими вимогами щодо граничної ймовірності його компрометації в мережі.

### **Перелік джерел посилання до третього розділу**

1. ITU-T Rec. Y.2701. Security requirements for NGN release 1. April 2007. 44 p. URL: <https://www.itu.int/rec/T-REC-Y.2701-200704-I/en>.
2. ITU-T Rec. Y.2704. Security mechanisms and procedures for NGN. January 2010. 58 p. URL: <https://www.itu.int/rec/T-REC-Y.2704-201001-I/en>.
3. ITU-T Rec. Y.2705. Minimum security requirements for the interconnection of the Emergency Telecommunications Service (ETS). March 2013. 24 p. URL: <https://www.itu.int/rec/T-REC-Y.2705-201303-I/en>.
4. ITU-T Rec. Y.2720. NGN identity management framework. January 2009. 34 p. URL: <https://www.itu.int/rec/T-REC-Y.2720-200901-I>.
5. ITU-T Rec. Y.2770. Requirements for deep packet inspection in next generation networks. December 2012. 38 p. URL: <https://www.itu.int/rec/T-REC-Y.2770-201211-I/en>.
6. Телекомунікаційні системи та мережі. Структура та основні функції / В.В. Поповський та ін. Харків: СМІТ, 2011. Т. 1. URL: <http://www.znanius.com/3534.html>.
7. Поповский В.В., Персиков А.В. Защита информации в телекоммуникационных системах: в 2 т. Харьков: СМІТ, 2006.
8. Поповский В.В., Персиков А.В. Основы криптографической защиты информации в телекоммуникационных системах: в 2 т. Харьков: СМІТ, 2010.
9. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. Киев: Арий, 2008. 464 с.
10. Оксіюк О.Г., Гаврилов Д.С., Гуржій П.М., Демідов Б.О. Метод забезпечення безпеки відеоінформаційного ресурсу на основі багаторівневої селективної обробки в телекомунікаційних системах. Наука і техніка Повітряних Сил Збройних Сил України. 2017. № 1. С. 46–48.
11. Оксіюк О.Г. Методика розрахунку часу затримки інформації управління в інформаційно-комунікаційних мережах. Вісник Черкаського державного технологічного університету. Серія: Технічні науки. 2015. № 3. С. 133–140.
12. Schneier B. Data and Goliath: The hidden battles to collect your data and control your world. WW Norton & Company, 2015. 398 p.
13. Stallings W. Cryptography and Network Security: Principles and Practice. 7th Edition. Pearson, 2016. 768 p.

14. Новиков С.Н. Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи. Москва: Горячая линия – Телеком, 2015. 128 с.
15. Björck F., Henkel M., Stirna J., Zdravkovic J. Cyber resilience-fundamentals for a definition. *New Contributions in Information Systems and Technologies*. 2015. Vol. 353. Springer, Cham. P. 311–316. DOI: [https://doi.org/10.1007/978-3-319-16486-1\\_31](https://doi.org/10.1007/978-3-319-16486-1_31).
16. Fink G.A., Griswold R.L., Beech Z.W. Quantifying cyber-resilience against resource-exhaustion attacks. *Resilient Control Systems (ISRCS) 2014: Proceedings of the 7th International Symposium, Denver, CO, USA, 19–21 August, 2014*. IEEE, 2014. P. 1–8. DOI: 10.1109/ISRCS.2014.6900093.
17. Choras M., Kozik R., Bruna M.P.T., Yautsiukhin A., Churchill A., Maciejewska I., Eguinoa I., Jomni A. Comprehensive approach to increase cyber security and resilience. *Availability, Reliability and Security (ARES) 2015: Proceedings of the 10th International Conference. Toulouse, France, 24–27 August, 2015*. IEEE, 2015. P. 686–692. DOI: 10.1109/ARES.2015.30.
18. Musman S. Assessing prescriptive improvements to a system's cyber security and resilience. *Systems Conference (SysCon) 2016: Proceedings of the Annual IEEE Conference. Orlando, FL, USA, 18–21 April, 2016*. IEEE, 2016. P. 1–6. DOI: 10.1109/SYSCON.2016.7490660.
19. Galinec D., Steingartner W. Combining cybersecurity and cyber defense to achieve cyber resilience. *Informatics 2017: Proceedings of the IEEE 14th International Scientific Conference. Poprad, Slovakia, 14–16 November, 2017*. IEEE, 2017. P. 87–93. DOI: 10.1109/INFORMATICS.2017.8327227.
20. ITU-T X-805. Security architecture for systems providing end-to-end communications. October 2003. 28 p. URL: <https://www.itu.int/rec/T-REC-X.805-200310-I/en>.
21. ISO 7498-1:1994 Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. International Standard ISO/IEC, 74981, 1994. 59 p.
22. ISO 7498-2:1989 Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture, 1989. 32 p.
23. ITU-T X-800. Security architecture for Open Systems Interconnection for CCITT applications. March 1991. 48 p. URL: <https://www.itu.int/rec/T-REC-X.800-199103-I>.

24. Santos O., Kampanakis P., Woland A. Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP. 1 edition. Cisco Press, 2016. 368 p.
25. Al-Kuwaiti M., Kyriakopoulos N., Hussein S. A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability. *IEEE Communications Surveys & Tutorials*. 2009. Vol. 11, No. 2. P. 106–124. DOI: 10.1109/SURV.2009.090208.
26. Kaur R., Kashmira P., Meena K., Mohapatra A. K. Survey on Different Techniques of Threshold Cryptography. *Journal of Electronics and Communication Engineering (IOSR-JECE)*. 2017. P. 114–119.
27. Venukumar V., Pathari V. A survey of applications of threshold cryptography – proposed and practiced. *Information Security Journal: A Global Perspective*. 2016. Vol. 25, No. 4–6. P. 180–190. DOI: 10.1080/19393555.2016.1251996.
28. Sarma K.S., Lamkuche H.S., Umamaheswari S. A Review of Secret Sharing Schemes. *Research Journal of Information Technology*. 2013. Vol. 5. P. 67–72. DOI: 10.3923/rjit.2013.67.72.
29. Lou W., Kwon Y. H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks. *IEEE Transactions on Vehicular Technology*. 2006. Vol. 55, No. 4. P. 1320–1330. DOI: 10.1109/TVT.2006.877707.
30. Lou W., Liu W., Fang Y. SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks. *INFOCOM 2004: Proceedings of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*. Hong Kong, China, 7–11 March, 2004. IEEE, 2004. P. 2404–2413. DOI: 10.1109/INFCOM.2004.1354662.
31. Alouneh S., En-Nouaary A., Agarwal A. A Multiple LSPs Approach to Secure Data in MPLS Networks. *Journal of Networks*. 2007. Vol. 2, No. 4. P. 51–58. DOI: 10.4304/jnw.2.4.51–58.
32. Alouneh S., Agarwal A., En-Nouaary A. A Novel Path Protection Scheme for MPLS Networks using Multi-path Routing. *Computer Networks: The International Journal of Computer and Telecommunications Networking*. 2009. Vol. 53, No. 9. P. 1530–1545. DOI: 10.1016/j.comnet.2009.02.001.
33. Кулаков Ю.А., Лукашенко В.В., Левчук А.В. Безопасная многопутевая маршрутизация в беспроводных сетях большой размерности. *Захист інформації*. 2011. Том 13, № 2(51). С. 5–10. DOI: 10.18372/2410-7840.13.2018.

34. Gupta D., Segal A., Panda A., Segev G., Schapira M., Feigenbaum J., Rexford J., Shenker S. A new approach to interdomain routing based on secure multi-party computation. *Hot Topics in Networks: Proceedings of the 11th ACM Workshop*. October, 2012. ACM, 2012. P. 37–42. DOI: 10.1145/2390231.2390238.
35. Gharib M., Yousefizadeh H., Movaghar A. Secure Overlay Routing for Large Scale Networks. *IEEE Transactions on Network Science and Engineering*. 2018. Vol. 1. P. 1–12. DOI: 10.1109/TNSE.2018.2812830.
36. Чевардін В.Є., Романюк В.А., Шевченко В.С. Модель загроз безпеки інформації в сучасних телекомунікаційних мережах з динамічною топологією. *Збірник наукових праць ВІТІ НТУУ «КПІ»*. 2012. № 2. С. 90–95.
37. Снегуров А.В., Чакрян В.Х. Метод формирования метрик маршрутизации, основанный на рисках информационной безопасности. *Системы управління, навігації та зв'язку*. 2012. № 4(24). С. 105–110.
38. Snihurov A., Chakrian V. Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters. *Scholars Journal of Engineering and Technology*. 2015. Vol. 3, No. 8. С. 707–714.
39. Gomes T., Martins L., Ferreira S., Pascoal M., Tipper D. Algorithms for determining a node-disjoint path pair visiting specified nodes. *Optical Switching and Networking*. 2017. Vol. 23. P. 189–204. DOI: <https://doi.org/10.1016/j.osn.2016.05.002>.
40. Myslitski K., Rak J., Kuszner Ł. Toward fast calculation of communication paths for resilient routing. *Networks*. 2017. Vol. 70, No. 4. P. 308–326. DOI: <https://doi.org/10.1002/net.21789>.
41. Natarajan M. Graph Theory Algorithms for Mobile Ad Hoc Networks. *Informatica – An International Journal of Computing and Informatics*. 2012. Vol. 36. P. 185–200.
42. Suurballe J. W. Disjoint paths in a network. *Networks*. 1974. Vol. 4, No. 2. P. 125–145.
43. Лемешко А.В., Еременко А.С. Усовершенствование модели безопасной маршрутизации сообщения с оптимальной балансировкой числа его фрагментов по непересекающимся маршрутам. *Захист інформації*. 2015. Т. 17. № 2. С. 135–142. DOI: 10.18372/2410-7840.17.8776.
44. Yeremenko O.S., Ali S.A. Secure Multipath Routing Algorithm with Optimal Balancing Message Fragments in MANET. *Radioelectronics and Informatics*. 2015. № 1(68). С. 26–29.
45. Еременко А.С. Методика расчета вероятности компрометации сообщения при использовании пересекающихся маршрутов с последовательно-

параллельной или комбинированной структурой. Наукові записки Українського науково-дослідного інституту зв'язку. 2015. № 6(40). С. 64–71.

46. Yeremenko O., Lemeshko O., Persikov A. Enhanced Method of Calculating the Probability of Message Compromising Using Overlapping Routes in Communication Network. Computer Sciences and Information Technologies (CSIT): Proceedings of the XIIth International Scientific and Technical Conference, Lviv, Ukraine, 5–8 Sept. 2017. IEEE, 2017. P. 87–90. DOI: 10.1109/STC-CSIT.2017.8098743.

47. Yeremenko O., Lemeshko O., Persikov A. Secure Routing in Reliable Networks: Proactive and Reactive Approach. Advances in Intelligent Systems and Computing II, CSIT 2017, Advances in Intelligent Systems and Computing, Springer, Cham. 2018. Vol. 689. P. 631–655. DOI: 10.1007/978-3-319-70581-1\_44.

48. Yeremenko O., Yevdokymenko M., Persikov A. Flow-aware approach of evaluating probability of compromise in combined structure network. Advanced Information and Communication Technologies (AICT): Proceedings of the 2nd International Conference, Lviv, Ukraine, 4–7 July, 2017. IEEE, 2017. P. 258–261. DOI: 10.1109/AIACT.2017.8020114.

49. Cholda P., Tapolcai J., Cinkler T., Wajda K., Jajszczyk A. Quality of resilience as a network reliability characterization tool. IEEE network. 2009. Vol. 23, No. 2. P. 11–19. DOI: 10.1109/MNET.2009.4804331.

50. Tipper D. Resilient network design: challenges and future directions. Telecommunication Systems. 2014. Vol. 56, No. 1. P. 5–16. DOI: 10.1007/s11235-013-9815-x.

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

52. Rak J., Papadimitriou D., Niedermayer H., Romero P. Information-driven network resilience: Research challenges and perspectives. Optical Switching and Networking, 2017. Vol. 23, Part 2. P. 156–178. DOI: <https://doi.org/10.1016/j.osn.2016.06.002>.

53. Lemeshko O., Romanyuk A., Kozlova H. Design schemes for MPLS Fast ReRoute. Experience of Designing and Application of CAD Systems in Microelectronics (CADSM) 2013: Proceedings of the 12th International Conference. Polyana Svalyava, Ukraine, 19–23 February, 2013. IEEE, 2013. P. 202–203.



## РОЗДІЛ 4

### ПОТОКОВІ МОДЕЛІ ТА МЕТОДИ ІЄРАРХІЧНОЇ МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

#### 4.1. Аналіз відомих теоретичних і протокольних рішень щодо ієрархічної маршрутизації в ІКМ

Як показав проведений аналіз [1, 2], досить прогресивною ідеєю в сфері інфокомунікацій є відділення рівня управління від рівня передачі даних у ІКМ. На реалізації подібної ідеї зосереджена нова концепція програмно-конфігурованих мереж, яка сьогодні активно розвивається і, на думку своїх розробників, повинна ефективно доповнити і модернізувати більшість наявних мережних технологій.

SDN-архітектура підтримує відкритий прикладний програмний інтерфейс (Application Programming Interface, API), який уможливорює реалізацію загальних мережних сервісів, керування пропускнуою здатністю, управління трафіком, оптимізацію процесорного навантаження, усі форми управління політиками та налаштування для забезпечення вимог користувачів щодо рівня якості обслуговування [2–7]. За допомогою відкритих API можна управляти мережею та процесами, що в ній протікають, реалізуючи мережні сервіси та додаткові можливості, не вдаючись у деталі їх реалізації, що дозволяє оптимізувати використання мережних та обчислювальних (серверних) ресурсів.

Таким чином, основна ідея SDN полягає у передачі низки основних функцій управління від операційних систем вузлів (маршрутизаторів і комутаторів) ІКМ до спеціального контролера (сервера) або множини таких контролерів мережної операційної системи. Концепція SDN передбачає створення єдиного, незалежного від виробника інтерфейсу обладнання між платформою управління та платформою передачі даних, а також віртуалізацією фізичних ресурсів мережі.

До основних переваг SDN належать:

- підвищення ефективності управління мережею;
- підвищення безпеки мережі;
- покращення гнучкості управління мережею та її ресурсами;
- підвищення конкурентоздатності мережного програмного забезпечення та комутаційного обладнання;
- підвищення рівня якості обслуговування.

У процесі проведеного аналізу встановлено, що на теперішній час активно використовуються декілька основних функціональних варіантів побудови SDN-архітектур, які відрізняються способом розподілу функцій контролю (управління) та передачі даних у мережі. Архітектура з розподіленим контролем (рис. 4.1, а) – це традиційна TCP/IP, мережа, в якій функції управління та передачі даних реалізуються в межах операційної системи на кожному з маршрутизаторів ІКМ окремо.

SDN-архітектура з гібридним контролем (рис. 4.1, б) передбачає делегування основних функцій контролю від маршрутизаторів до SDN-контролера. Завдяки використанню гібридного контролю деякі задачі реального масштабу часу щодо управління трафіком все ще розв'язуються на маршрутизаторах, а низка задач перекладається на SDN-контролер. У межах SDN з гібридним контролем традиційні мережні протоколи транспортної або локальної мережі та SDN-протоколи функціонують в одній і тій самій ІКМ. Подібна архітектура дозволяє впроваджувати новітні SDN-рішення, такі як OpenFlow, у дещо застарілі середовища без повної перебудови мережної архітектури.

SDN-архітектура з централізованим контролем – це базова архітектура програмно-конфігурованих мереж, в якій функції контролю повністю передані з маршрутизаторів транспортної мережі на контролери мережної операційної системи (рис. 4.1, в). SDN з централізованим контролем дозволяє значно покращити гнучкість мережі завдяки програмованості та автоматизації, значно знижуючи витрати на мережні операції. Проте централізовані рішення нерідко мають невисоку надійність і масштабованість.

З огляду на ці проблеми на практиці переходять до реалізації принципів ієрархічного контролю мережі. Ця архітектура (рис. 4.1, г) основана на введенні багаторівневої ієрархії контролерів, коли за функціональність кожного домену ІКМ відповідає окремий SDN-контролер. SDN-контролер мережі загалом здійснює координацію роботи контролерів доменів для підвищення ефективності розподіленого управління мережею. SDN-архітектура з резервним контролером, упровадження якої також спрямована на підвищення надійності мережних рішень, передбачає введення додаткового SDN-контролера, на який перекладаються функції основного контролера в разі виходу останнього з ладу (рис. 4.1, д).

Натепер сучасні ІКМ використовують досить широкий функціонал технологічних засобів щодо управління трафіком та маршрутизації з метою підвищення якості обслуговування, які реалізуються на всіх рівнях еталонної

моделі взаємодії відкритих систем (OSI). Зокрема важливо забезпечити адаптацію цих рішень під різні варіанти архітектур SDN-мереж (рис. 4.1).

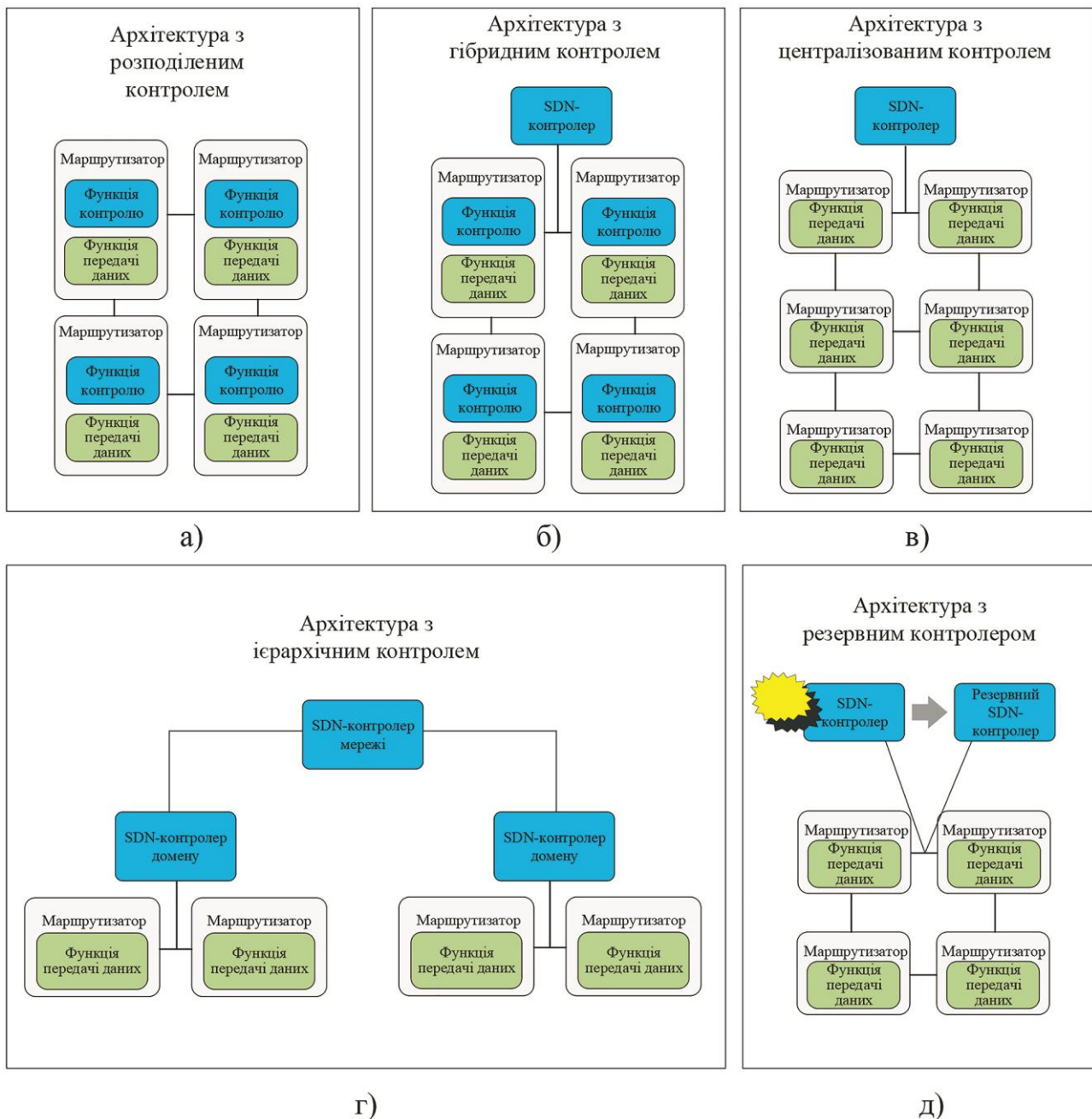


Рис. 4.1. Варіанти SDN-архітектури

Ієрархічна (багаторівнева) побудова сучасних ІКМ є адекватною реакцією на постійне зростання їх територіальної розподіленості, збільшення кількості комутаційних і термінальних пристроїв, наданих інфокомунікаційних сервісів тощо. З огляду на те що основною метою функціонування ІКМ є забезпечення заданого рівня якості обслуговування, то для підвищення масштабованості кінцевих рішень багато засобів забезпечення QoS де-факто вже мають багаторівневий характер, який підтверджують, наприклад, наявність концепцій

ієрархічних черг (Hierarchical Queuing Framework) та багаторівневого профілювання трафіку, оснований на обмеженні (Hierarchical Policing) або вирівнюванні (Hierarchical Shaping) швидкості потоку пакетів [8, 9]. Однак найбільш чутливі до проблем масштабованості саме протоколи маршрутизації, оскільки вони потребують узгодженого функціонування не одного, а цілої множини мережних пристроїв. Ієрархічна маршрутизація активно використовується в мережах IP, ATM і MPLS [10, 11], охоплюючи різні варіанти та принципи її організації.

Варто зазначити, що реалізація ієрархічних рішень у системах різного функціонального призначення, як правило [12, 13], базується, по-перше, на проведенні декомпозиції вихідної прикладної задачі, яка підлягає розв'язанню, на кілька взаємопов'язаних підзадач, об'єднаних спільною метою; по-друге, на визначенні кількості рівнів ієрархії та переліку задач, які розв'язуються на тому чи іншому ієрархічному рівні. Таким чином, залежно від особливостей організації ієрархічної маршрутизації в ІКМ її можна класифікувати за такими ознаками (рис. 4.2):

- за типом уведеної декомпозиції ІКМ ієрархічна маршрутизація може ґрунтуватися на структурній (територіальній), функціональній або структурно-функціональній декомпозиції мережі;
- за способом проведення структурної або структурно-функціональної декомпозиції ІКМ на домени виокремлюють ієрархічну маршрутизацію, коли границя доменів проходить або через маршрутизатори, або через канали зв'язку мережі;
- за способом проведення функціональної або структурно-функціональної декомпозиції ІКМ на домени розрізняють маршрутизацію з виділенням магістральної ділянки (backbone) або без організації такої ділянки;
- за місцем реалізації ієрархічної маршрутизації виокремлюють внутрішньодоменну та міждоменну маршрутизацію;
- за кількістю організованих ієрархічних рівнів розрізняють дворівневу, трирівневу та в загальному випадку  $n$ -рівневу маршрутизацію;
- за рівнем підтримки функцій міжрівневої координації може реалізуватись ієрархічна маршрутизація з координацією верхнім рівнем рішень, які отримані на нижніх рівнях, або без проведення міжрівневої координації.

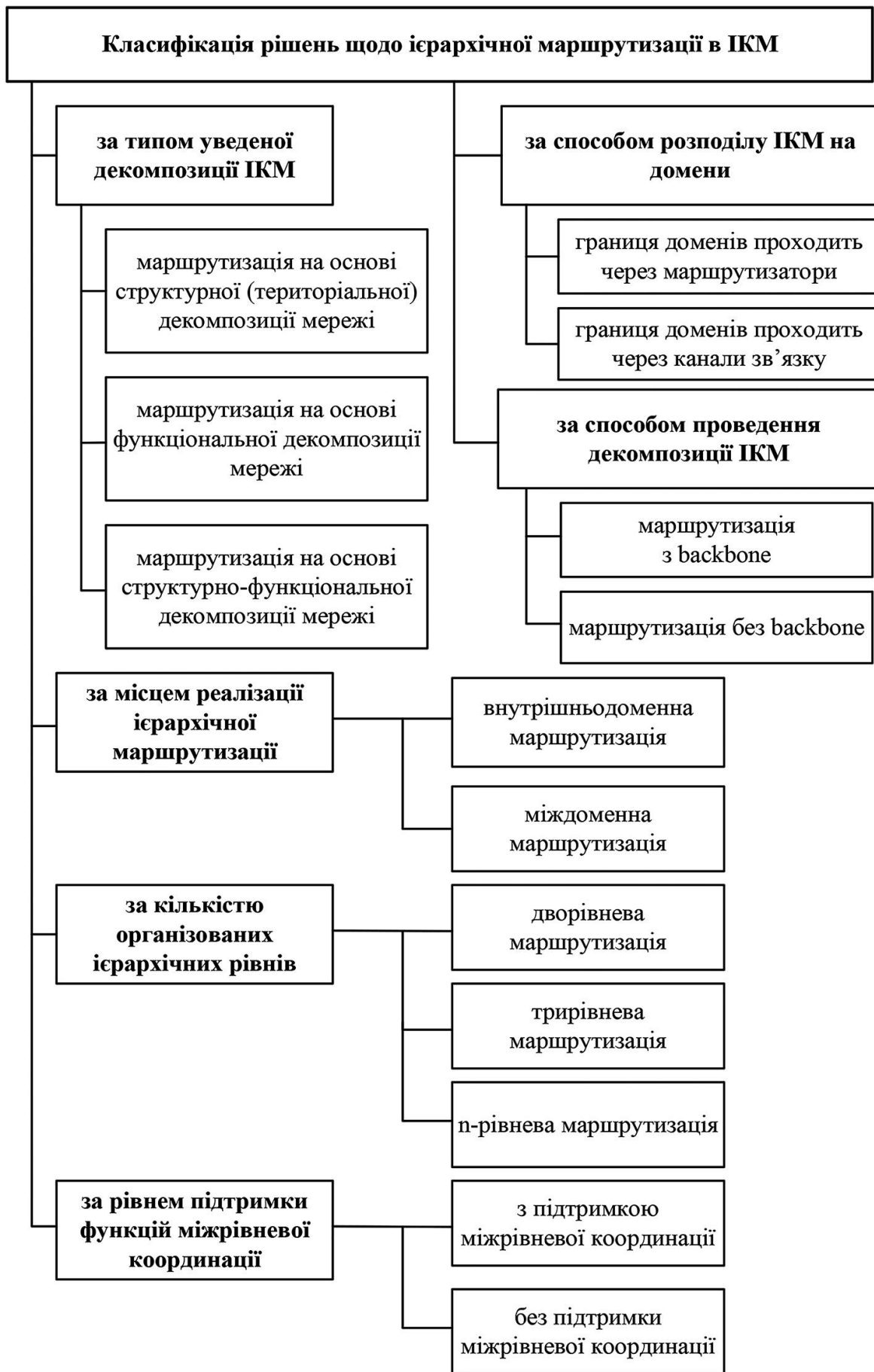


Рис. 4.2. Класифікація рішень щодо ієрархічної маршрутизації в ІКМ

У сучасних ІКМ застосовуються різні способи їх декомпозиції ІКМ. Прикладом *структурної (територіальної) декомпозиції*, яка проводиться для організації ієрархічної маршрутизації, є поділ в IP-мережі загальної маршрутної задачі на множину маршрутних підзадач, кожна з яких розв'язується в окремій підмережі – домені (area), як це реалізовано в IGP-протоколах OSPF (рис. 4.3) та IS-IS (рис. 4.4), або кластері, якщо мова йде про протокол PNNI в мережі АТМ.

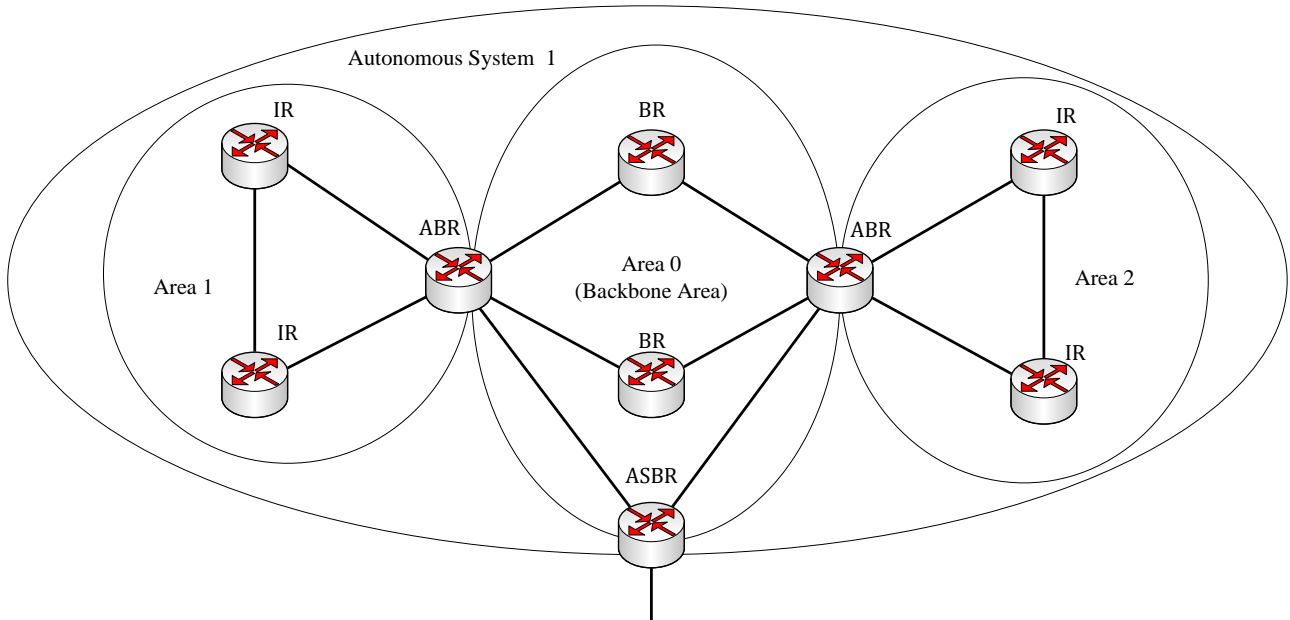


Рис. 4.3. Структурна ієрархія протоколу OSPF

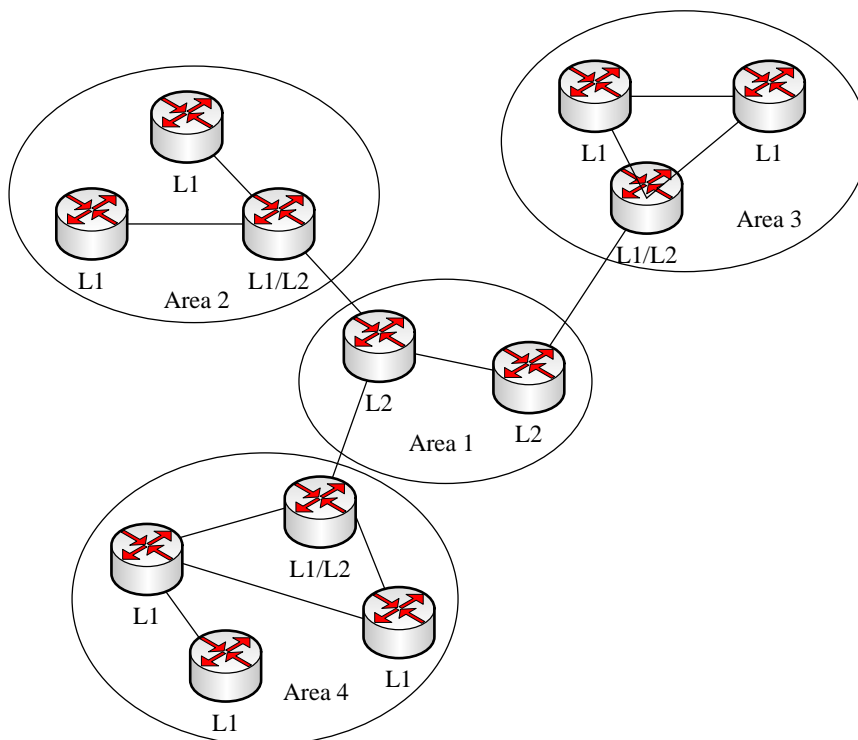


Рис. 4.4. Структурна ієрархія протоколу IS-IS

Як правило, критеріями декомпозиції мережі на домени можуть бути територіальна близькість маршрутизаторів, ступінь їх зв'язності або адміністративна підпорядкованість операторам (провайдерам) ІКМ. Окремим випадком подібної декомпозиції є розподіл маршрутних задач не між доменами, а між окремими маршрутизаторами, як це, наприклад, реалізовано в MPLS-мережах, коли функції визначення маршрутів делеговані лише приграничним маршрутизаторам – LER.

*Функціональна декомпозиція* ІКМ полягає в тому, що маршрутні підзадачі, на які здійснюється розподіл вихідної маршрутної задачі, можуть функціонально відрізнятися за своїм змістом, алгоритмом та періодичністю розв'язання. Введення функціональної ієрархії у розв'язанні задач маршрутизації може реалізуватись як на різних комутаційних пристроях, так і на центральному маршрутному сервері, наприклад контролері SDN.

У разі *структурно-функціональної декомпозиції* ІКМ одночасно реалізуються принципи як структурної, так і функціональної декомпозиції. Так, наприклад, у межах структурної декомпозиції IP-мережа розбивається на множину автономних систем (AS). Функціональна декомпозиція полягає в тому, що в кожній з AS використовується свій протокол маршрутизації внутрішнього шлюзу (Interior Gateway Protocol, IGP), а для маршрутизації між AS застосовуються протоколи зовнішнього шлюзу (Exterior Gateway Protocol, EGP), наприклад, протокол BGP (рис. 4.5) [12].

У процесі реалізації ієрархічної маршрутизації за умови проведення структурної або функціональної декомпозиції ІКМ границя між окремими доменами може проходити або через маршрутизатори, як це реалізовано у протоколі OSPF (рис. 4.3), або через канали зв'язку мережі, як, наприклад, це зроблено у протоколі IS-IS (рис. 4.4). З іншого боку, у проведенні декомпозиції ІКМ кожна автономна система IP-мережі може поділятися на підмережі різного рівня ієрархії. Верхній рівень ієрархії може визначати спеціально налаштована магістральна область (backbone), як, наприклад, це реалізовано в протоколах OSPF та IS-IS. Саме через цю область обмінюються пакетами підмережі нижнього рівня, іменовані (залежно від типу протоколу) доменами (areas), зонами (zones) або кластерами (clusters) [13]. Проте у випадку ієрархічної маршрутизації, яка базується на структурно-функціональній декомпозиції IP-мережі загалом, на множині автономних систем магістральна область (backbone) може й не організовуватися (рис. 4.5) [13].

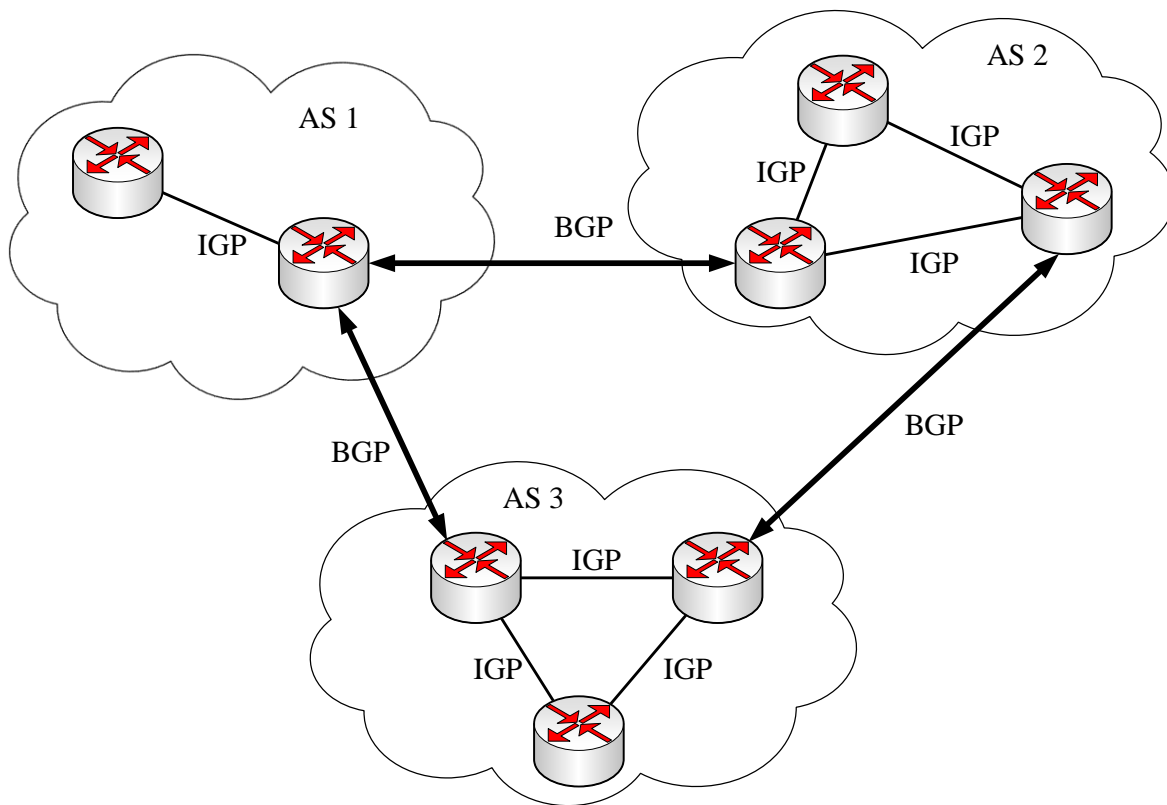


Рис. 4.5. Приклад ієрархічної побудови IP-мережі

За умови внутрішньодоменної ієрархічної маршрутизації структурна та/або функціональна ієрархія рішень може вводитися безпосередньо в межах окремого домену. У сучасних інфокомунікаційних технологіях внутрішньодоменна ієрархічна маршрутизація безпосередньо не застосовується. Проте набула широкого використання міждоменна ієрархічна маршрутизація. Так, у структурі дворівневої ієрархії протоколу OSPF завжди виокремлюється магістральний домен (*верхній рівень ієрархії*), через який відбувається взаємодія між окремими доменами (*нижній рівень ієрархії*) автономної системи загалом (рис. 4.3). Тому маршрутизатори в мережі, що використовують протокол OSPF, поділяються на декілька типів залежно від їх розташування та функцій, які вони виконують. Серед них можна виокремити:

- внутрішній маршрутизатор (Internal Router, IR) – це маршрутизатор, усі інтерфейси якого належать одному домену. IR формує та оновлює лише одну базу даних стану каналів цього домену;

- приграничний маршрутизатор (Area Border Router, ABR) – це маршрутизатор, через який з'єднується один або більше доменів з магістральним доменом. Він підтримує окрему базу даних стану каналів для кожного суміжного домену, виконуючи функції шлюзу для міждоменого трафіку, оскільки в кожного ABR завжди хоча б один інтерфейс належить магістральному домену;



– магістральний маршрутизатор (Backbone Router, BR) – маршрутизатор, у якого всі інтерфейси належать магістральному домену;

– приграничний маршрутизатор автономної системи (Autonomous System Boundary Router, ASBR) – це маршрутизатор, через який проходить обмін пакетами між цією автономною системою, що функціонує під управлінням протоколу OSPF, та іншими AS. Територіально та функціонально ASBR може розташовуватися в будь-якому місці автономної системи, а його завдання можуть вирішувати маршрутизатори IR, ABR або BR [10, 14–16].

Прикладом організації дворівневої міждоменної ієрархічної маршрутизації також може бути протокол IS-IS (рис. 4.4). Цей протокол аналогічно протоколу OSPF належить до класу протоколів стану каналів [15–17]. Маршрутизатори протоколу IS-IS, які виконують маршрутизацію тільки всередині домену, називаються маршрутизаторами 1-го рівня (L1). Маршрутизатори протоколу IS-IS, що виконують маршрутизацію між доменами, називаються маршрутизаторами 2-го рівня (L2). Маршрутизатору 1-го рівня відома тільки інформація про мережу, що стосується домену, в якому він міститься. Якщо маршрутизатор 1-го рівня на основі інформації про свій домен не знає, куди переслати пакет, то він надсилає пакет на найближчий маршрутизатор L2, який потім направляє пакет у відповідний сусідній домен.

Магістраль протоколу IS-IS не є окремим нульовим доменом, як це має місце в протоколі OSPF. Вона є групою послідовно та безперервно з'єднаних між собою маршрутизаторів 2-го рівня. Кожен маршрутизатор 2-го рівня функціонує тільки в межах окремого домену, але може мати канали, які з'єднують його з маршрутизаторами 2-го рівня іншого домену. Слід зазначити, що межею IS-IS-домена є не маршрутизатор 2-го рівня, а канал між маршрутизаторами 2-го рівня [17].

У табл. 4.1 наведено порівняння термінології, яка використовується в протоколах ієрархічної маршрутизації OSPF та IS-IS.

В IP-мережах може підтримуватися також трирівнева ієрархія, коли на рівні автономної системи реалізується дворівнева маршрутизація, організована, наприклад, за допомогою протоколу OSPF, а між автономними системами маршрутизація відбувається під управлінням, зокрема, протоколу BGP, що визначає додатковий верхній рівень ієрархії рішень (рис. 4.5).

У технології АТМ функції ієрархічної маршрутизації покладено на протокол PNNI [10, 18]. Ієрархія PNNI починається на нижньому рівні, де вузли організуються в кластери вузлів (КВ). За аналогією з традиційними мережами можна назвати КВ доменами маршрутизації, оскільки всередині кожного КВ завжди є повна інформація щодо належних йому вузлів (рис. 4.6). Також у

кожному кластері виокремлюється лідер KB (logical peer group leader), який є вузлом логічної групи (Logical Group Node, LGN) на наступному ієрархічному рівні PNNI. Усі LGN кожного KB нижнього рівня об'єднуються в KB на зазначеному рівні ієрархії PNNI. На цьому рівні у KB з LGN також обирається лідер кластеру. Кожен з лідерів цього KB створює вузол логічної групи, яка є членом групи більш високого рівня.

Таблиця 4.1

**Порівняння термінології протоколів OSPF та IS-IS**

Термінологія протоколу IS-IS	Термінологія протоколу OSPF
Домен (Area)	Домен (Area)
Кінцева система (End System)	Вузол (Host)
Проміжна система (Intermediate System)	Маршрутизатор
ISO Routing Domain	Autonomous System
Level 1 (L1)	Внутрішній маршрутизатор (IR)
Level 1/ Level 2 (L1/L2)	Приграничний маршрутизатор (ABR)
Level 2 (L2)	Магістральний маршрутизатор (BR)
Довільна проміжна система (any IS)	Приграничний маршрутизатор автономної системи (ASBR)

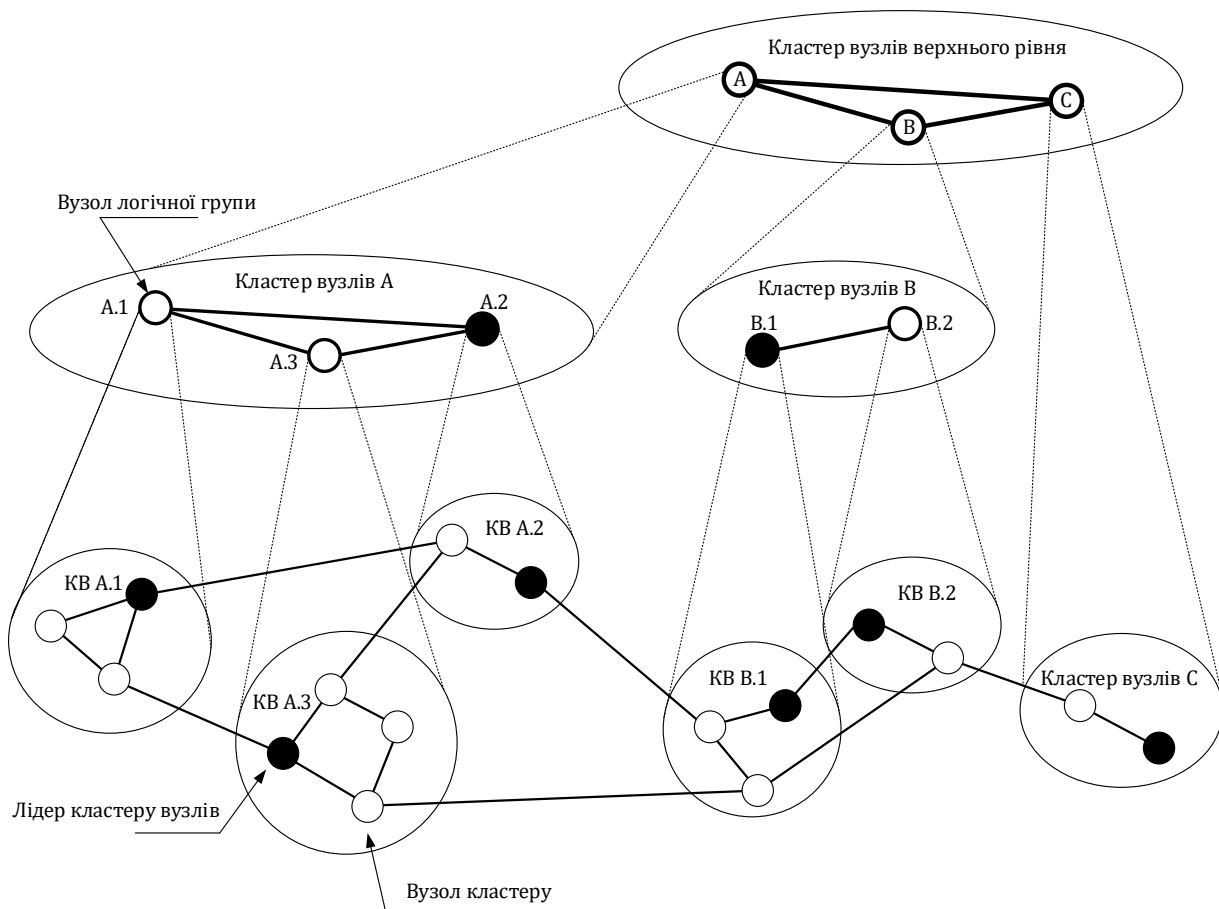


Рис. 4.6. Структурна ієрархія протоколу PNNI

Варто окремо наголосити, що проаналізовані протокольні рішення основані переважно лише на введенні структурної ієрархії без належної підтримки ієрархії функціональних задач окремих рівнів. Це проявляється в тому, що функціонально рішення, які отримуються в окремих доменах мережі, між собою не погоджуються, що негативно впливає на ефективність функціонування ІКМ загалом. З точки зору теорії ієрархічних багаторівневих систем управління [22, 23] важливим складником функціональної ієрархії маршрутних задач є саме реалізація принципів міжрівневої координації, яка проводиться для наближення ефективності ієрархічних рішень до централізованої маршрутизації з підвищенням їх масштабованості.

Алгоритми розрахунку найкоротших шляхів Дейкстри та Беллмана–Форда, які забезпечують функціональність більшості сучасних протоколів маршрутизації, безпосередньо не враховують особливостей ієрархічної побудови мережі. Інколи подібний факт, справді, не є проблемою. Зокрема це характерно для варіанта, коли кожен домен (підмережа нижнього рівня) комутується з магістральним доменом через один приграничний маршрутизатор (ABR або ASBR, наприклад, для протоколу OSPF), що є досить поширеним рішенням у сучасних мережах [10–11, 19]. У цьому випадку в розв’язанні задач маршрутизації і в доменах нижнього рівня, і в магістральному домені чітко відомі як маршрутизатор-відправник, так і маршрутизатор-отримувач. Тому жодної складності в узгодженні кінцевих рішень маршрутних завдань, що отримуються окремо в доменах різних класів, не виникає.

Проте у випадку, коли між доменами або автономними системами для підвищення відмовостійкості мережі використовуються декілька приграничних маршрутизаторів, тоді відсутність підтримки міжрівневої координації в наявних протоколах маршрутизації стає серйозною технологічною та теоретичною проблемою. Це обумовлено тим, наприклад, що в процесі реалізації одношляхової маршрутизації на міждоменній ділянці виникає неоднозначність у визначенні в кожному із суміжних доменів приграничного маршрутизатора, через який будуть передаватися пакети. За умови багатошляхової маршрутизації проблема ускладнюється ще й тим, що в кожному з доменів, в яких автономно одне від одного розв’язуються маршрутні задачі, треба визначитися не тільки з переліком використаних приграничних маршрутизаторів, але й з порядком балансування між ними мережного трафіку.

Ефективність протоколів маршрутизації і, зокрема, механізмів балансування навантаження багато в чому залежить від математичних моделей, які покладені в їх основу. Однак алгоритми Дейкстри та Беллмана–

Форда мають досить обмежені властивості щодо підтримки багатошляхових рішень та врахування характеристик потоків пакетів для забезпечення балансування навантаження в мережі [20, 21]. Причиною тому є те, що вони базуються на досить простих з функціональної точки зору графових математичних моделях пошуку найкоротшого шляху на графі, які вже не здатні адекватно описати процес маршрутизації в сучасних мультисервісних ІКМ з переважно потоковим характером мережного трафіку. Вихід з цієї ситуації ґрунтується, по-перше, на переході до декомпозиційного подання поточкових моделей, описаних у попередніх розділах, що дозволить найбільш адекватно описати процеси ієрархічної маршрутизації в сучасних ІКМ; а по-друге, на синтезі методів ієрархічної маршрутизації, які використовують теоретично обґрунтовані принципи добре апробованої теорії ієрархічних багаторівневих систем [22, 23].

Підхід, оснований на застосуванні теорії ієрархічних багаторівневих систем, уже застосовується в синтезі низки моделей і методів маршрутизації та управління трафіком [24–49]. Так, у роботах [24–30] представлені ієрархічно-координаційні рішення щодо управління каналним і буферним ресурсом ІКМ, а в статтях [32–40] описані моделі та методи щодо безпосередньо проблеми ієрархічної маршрутизації. У працях [25, 26] розглядається варіант ієрархічної маршрутизації, оснований на декомпозиційному поданні як структури ІКМ, так і функціональної моделі, описаної за допомогою системи різницевих рівнянь завантаженості буферів черг на маршрутизаторах мережі. Також пошуку підходів до ефективного та узгодженого розв'язання задач маршрутизації та розподілу каналного ресурсу присвячена досить значна кількість наукових публікацій, серед яких варто виокремити статті [31–49]. Саме в цих роботах запропоновані досить ефективні теоретичні рішення зазначених задач як у межах статичних, так і динамічних моделей [31–49]. Проте вони мають обмежені можливості щодо забезпечення збалансованого завантаження каналного ресурсу, а рішення [32, 33] більш орієнтовані на резервування ресурсів у межах IntServ. Використання теоретичних результатів, наведених у роботах [44–47], як правило, пов'язане з необхідністю розв'язання досить складних з обчислювальної точки зору оптимізаційних задач нелінійної оптимізації.

Виходячи з аналізу сучасного стану зазначеної проблеми щодо реалізації ієрархічної маршрутизації в ІКМ, основними вимогами, які висувуються до перспективних рішень у цьому напрямі є:

– орієнтація на поточкові підходи та методи, у межах яких основна увага приділяється не окремим пакетам, а характеристикам потоків пакетів;

- детальне врахування особливостей структурної та функціональної побудови ІКМ у процесі формування маршрутних метрик;
- оптимізаційне формулювання задачі ієрархічної маршрутизації, орієнтоване на максимізацію рівня QoS та/або мінімізацію використання мережного ресурсу;
- підтримка міжрівневої координації під час реалізації ієрархічної маршрутизації в ІКМ;
- забезпечення збалансованого завантаження (використання) доступного мережного ресурсу, ґрунтованого на реалізації багатошляхової маршрутизації та орієнтованого на підвищення рівня QoS;
- підвищення рівня масштабованості та погодженості рішень щодо маршрутизації, розподілу та резервування мережного ресурсу для забезпечення гарантованої якості обслуговування.

Ефективні рішення, які задовольняють перелічені вимоги та які представлені новими математичними моделями та методами ієрархічно-координаційної маршрутизації в програмно-конфігурованих інфокомунікаційних мережах, будуть запропоновані та досліджені в подальших підрозділах цього розділу.

#### **4.2. Поточкова модель і метод ієрархічно-координаційної внутрішньодоменної маршрутизації в інфокомунікаційній мережі SDN/MPLS**

У підрозділі пропонуються теоретичні рішення щодо організації ієрархічно-координаційної маршрутизації в ІКМ SDN/MPLS, що охоплюють випадок дворівневої оптимізації процесів внутрішньодоменної маршрутизації «від джерела». Особливістю запропонованої декомпозиційної моделі маршрутизації є те, що за розподілений розрахунок внутрішньодоменних маршрутів відповідають лише приграничні маршрутизатори, які, наприклад, у технології MPLS називаються LER (Label Edge Router). У цьому випадку оптимальність розрахованих маршрутів може визначатись як формою використаної маршрутної (канальної та шляхової) метрики, так і відповідністю вимогам концепції Traffic Engineering щодо забезпечення збалансованого завантаження (використання) каналних ресурсів мережі.

З метою недопущення перевантаження каналів зв'язку в MPLS-мережі, спричиненого відсутністю погодженості в діях окремих приграничних LER-маршрутизаторів, у запропонованому методі внутрішньодоменної маршрутизації вводиться дворівнева ієрархія розрахунків, коли маршрутні рішення нижнього рівня, які отримуються на приграничних маршрутизаторах, координуються SDN-контролером верхнього ієрархічного рівня. В основу

методу ієрархічно-координаційної внутрішньодоменної маршрутизації в мережі SDN/MPLS покладено принцип цільової координації, що дозволило, по-перше, коректно сформулювати та розв'язати оптимізаційні задачі нижнього та верхнього ієрархічних рівнів, а по-друге, забезпечити високу збіжність методу до оптимальних рішень, близьких за значеннями до результатів централізованих розрахунків.

#### 4.2.1. Декомпозиційна модель ієрархічно-координаційної внутрішньодоменної маршрутизації в програмно-конфігурованій інфокомунікаційній мережі SDN/MPLS

Нехай структура MPLS-мережі буде представлена у вигляді орієнтованого графа  $G = (R, E)$ , де  $R = \{R_i; i = \overline{1, m}\}$  – це множина вершин графа, що моделює маршрутизатори в мережі. У свою чергу  $E = \{E_{i, j}; i, j = \overline{1, m}; i \neq j\}$  – множина дуг, що моделює канали зв'язку, які з'єднують маршрутизатори MPLS-мережі.

За аналогією з позначеннями, уведеними в підрозділі 1.7, позначимо через  $K$  множину потоків, що циркулюють у мережі. Уведемо дві підмножини:  $K^o$  – підмножина одноадресних потоків та  $K^b$  – підмножина багатоадресних потоків,  $K^o \cup K^b = K$ . Також позначимо через  $K_r$  ( $K_r \in K$ ) множину потоків, що підлягають маршрутизації приграничним маршрутизатором  $R_r$  ( $R_r \in R$ ). Надалі в цьому розділі під  $k_r$ -м потоком ( $k_r \in K_r$ ) буде розумітися  $k$ -й потік пакетів, маршрутизація якого здійснюється приграничним маршрутизатором  $R_r$ . Так, наприклад, потік  $2_5$  – це другий потік, маршрутизацію якого здійснює п'ятий LER.

Для кожного одноадресного  $k_r$ -го потоку ( $k_r \in K^o$ ) введемо низку характеристик:

$\lambda^{k_r}$  – середня інтенсивність (швидкість передачі) пакетів, що вимірюється в пакетах за секунду (1/с);

$s_{k_r}$  – маршрутизатор-відправник;

$d_{k_r}$  – маршрутизатор-отримувач  $k_r$ -го потоку пакетів.

Для кожного багатоадресного потоку ( $k_r \in K^b$ ) множину вузлів-отримувачів позначимо як

$$d_{k_r}^* = \left\{ d_{k_r}^1, d_{k_r}^2, \dots, d_{k_r}^{m_{k_r}} \right\}. \quad (4.1)$$

Тоді для кожного приграничного маршрутизатора-відправника пакетів у MPLS-мережі шуканими є змінні  $x_{i,j}^{k_r}$ , які характеризують частку інтенсивності  $k$ -го потоку пакетів, що надходить до мережі через приграничний маршрутизатор  $R_r$  та передається каналом  $E_{i,j} \in E$ . Через  $\varphi_{i,j}$  позначимо пропускну здатність каналу зв'язку  $E_{i,j} \in E$ .

Реалізація одношляхової стратегії маршрутизації передбачає введення в модель таких умов:

$$x_{i,j}^{k_r} \in \{0,1\}. \quad (4.2)$$

Для забезпечення багатошляхової маршрутизації на маршрутні змінні накладаються обмеження у вигляді

$$0 \leq x_{i,j}^{k_r} \leq 1. \quad (4.3)$$

З метою запобігання втрат пакетів на маршрутизаторах і в MPLS-мережі загалом унаслідок реалізації одноадресної маршрутизації ( $k_r \in K^o$ ) необхідно забезпечити виконання умов збереження потоку [50–52]:

$$\left\{ \begin{array}{l} \sum_{j:E_{i,j} \in E} x_{i,j}^{k_r} - \sum_{j:E_{j,i} \in E} x_{j,i}^{k_r} = 1, \quad R_i = s_{k_r}; \\ \sum_{j:E_{i,j} \in E} x_{i,j}^{k_r} - \sum_{j:E_{j,i} \in E} x_{j,i}^{k_r} = 0, \quad R_i \neq s_{k_r}, d_{k_r}; \\ \sum_{j:E_{i,j} \in E} x_{i,j}^{k_r} - \sum_{j:E_{j,i} \in E} x_{j,i}^{k_r} = -1, \quad R_i = d_{k_r}. \end{array} \right. \quad (4.4)$$

Система рівнянь (4.4) має виконуватися для кожного потоку пакетів. Кількість умов у системі (4.4) залежить від кількості маршрутизаторів у мережі.

У реалізації багатоадресної маршрутизації, як показано в пункті 1.7.2, замість умов (4.3) та (4.4) на маршрутні змінні  $x_{i,j}^{k_r}$  (4.2) накладається низка обмежень: якщо маршрутизатор  $R_i$  є вузлом-відправником –

$$\sum_{j:E_{i,j} \in E} x_{i,j}^{k_r} \geq 1, \text{ коли } R_i = s_{k_r}, k_r \in K^o, \quad (4.5)$$

або

$$\sum_{i:E_{i,j} \in E} x_{i,j}^{k_r} = 1, \text{ якщо } R_j \in d_{k_r}^*, k_r \in K^o, \quad (4.6)$$

які вводяться для всіх вузлів-отримувачів пакетів [53–56].

Обмеження (4.5) вводяться для вузла-відправника потоку пакетів, а їх виконання орієнтоване на те, що від цього вузла потік, який надходить на обслуговування, буде переданий хоча б одному суміжному (сусідньому) вузлу-маршрутизатору. Умова (4.6) спрямована на забезпечення доставки пакетів потоку на кожен вузол-отримувач, проте потік повинен надходити на ці вузли лише з одного суміжного маршрутизатора.

Для кожного транзитного маршрутизатора  $R_j$ , яким може бути будь-який вузол MPLS-мережі, окрім відправника, у разі багатоадресної маршрутизації додатково вводяться такі умови [53–56]:

$$\sum_{i: E_{i,j} \in E} x_{i,j}^{k_r} \geq x_{j,p}^{k_r}, \text{ коли } R_j \neq s_{k_r}, k_r \in K^{\bar{b}}, \quad (4.7)$$

виконання яких робить можливим наявність потоку в будь-якому з вихідних від транзитного вузла каналі зв'язку ( $E_{j,p} \in E$ ) лише в тому випадку, коли цей потік надходить на цей вузол хоча б через один вхідний канал ( $E_{i,j} \in E$ ).

Для запобігання зациклення пакетів, тобто утворення контурів у розрахованих маршрутах, до запропонованої моделі вводяться умови такого вигляду (за кількістю контурів у мережі) [53–56]:

$$\sum_{E_{i,j} \in E_{\pi}^q} x_{i,j}^{k_r} < |E_{\pi}^q|, k_r \in K^{\bar{b}}, \quad (4.8)$$

де  $E_{\pi}^q$  – множина дуг графа, що утворюють відповідно до своєї орієнтації  $q$ -й контур ( $\pi$ );  $|E_{\pi}^q|$  – потужність множини  $E_{\pi}^q$ .

Виконання умови (4.8) гарантує, що кількість задіяних під час багатоадресної маршрутизації дуг, які створюють той чи інший контур, завжди менша від загальної кількості дуг у цьому контурі, тобто контур не входить до маршруту, який розраховується.

З метою запобігання перевантаження каналів зв'язку багатопотоковим трафіком важливо виконати умови

$$\sum_{R_r \in R} \sum_{k_r \in K_r} \lambda^{k_r} x_{i,j}^{k_r} \leq \varphi_{i,j}. \quad (4.9)$$

#### 4.2.2. Розв'язання задачі ієрархічно-координаційної внутрішньодоменої маршрутизації на основі метрик в інфокомунікаційній мережі SDN/MPLS

Умова (4.9) орієнтована на використання в процесі централізованої маршрутизації, коли всі маршрутні змінні визначаються на єдиному сервері



(контролері) маршрутів. Під час реалізації маршрутизації «від джерела» за розрахунок маршрутів відповідає множина приграничних маршрутизаторів, тому в цьому випадку умови (4.9) будуть записані в такому декомпозиційному вигляді [50–56]:

$$\sum_{k_r \in K_r} \lambda^{k_r} x_{i,j}^{k_r} \leq \varphi_{i,j} - \sum_{\substack{R_s \in R, k_s \in K_s \\ s \neq r}} \lambda^{k_s} x_{i,j}^{k_s}. \quad (4.10)$$

Фізичний зміст виразу (4.10) визначається тим, що агрегований потік, який підлягає маршрутизації вузлом  $R_r$ , не повинен за своєю інтенсивністю перевищувати пропускну здатність каналу зв'язку, яка залишилася після обслуговування потоків, що надійшли до MPLS-мережі через інші приграничні маршрутизатори. У векторно-матричній формі умови (4.10) можна записати в такому вигляді:

$$A_r \bar{x}_r \leq D_r \bar{\varphi} - \sum_{\substack{R_s \in R \\ s \neq r}} C_{rs} \bar{x}_s, \quad (4.11)$$

де  $\bar{x}_r$  – маршрутний вектор, координатами якого є змінні  $x_{i,j}^{k_r}$ ;

$\bar{\varphi}$  – вектор пропускну здатностей каналів мережі з координатами  $\varphi_{i,j}$ ;

$A_r$ ,  $D_r$ ,  $C_{rs}$  – це матриці погодження розміру, тому що розміри векторів  $\bar{x}_r$  ( $R_r \in R$ ) та вектора  $\bar{\varphi}$ , а також порядок нумерації їх координат можуть не збігатися.

У розрахунку шуканих векторів  $\bar{x}_r$  критерієм оптимальності отриманих рішень пропонується використовувати мінімум такої цільової функції:

$$F = \sum_{R_r \in R} \bar{x}_r^t H_r \bar{x}_r, \quad (4.12)$$

де  $H_r = \left\| h_{i,j}^r \right\|$  – це діагональна матриця вагових коефіцієнтів, координати якої є маршрутні метрики  $h_{i,j}^r$  каналів зв'язку MPLS-мережі;

$[\cdot]^t$  – функція транспонування вектора (матриці).

Наприклад, якщо  $h_{i,j}^r = 1$ , то в мережі буде використовуватися метрика протоколу RIP. За умови  $h_{i,j}^r = 10^7 / \varphi_{i,j}$  у мережі буде організовано маршрутизацію за аналогом метрики протоколу IGRP/EIGRP.

Для розв'язання сформульованої оптимізаційної задачі, яка пов'язана з мінімізацією виразу (4.12) за наявності обмежень (4.2)–(4.11), використовується

принцип цільової координації [22–23]. Тоді, переходячи до задачі на безумовний екстремум,

$$\min_x F = \max_\mu L$$

необхідно максимізувати за  $\bar{\mu}$  лагранжіан вигляду

$$L = \sum_{R_r \in R} \bar{x}_r^t H_r \bar{x}_r + \sum_{R_r \in R} \bar{\mu}_r^t \left( A_r \bar{x}_r - D_r \bar{\varphi} + \sum_{\substack{R_s \in R \\ s \neq r}} C_{rs} \bar{x}_s \right), \quad (4.13)$$

де  $\bar{\mu}$  – вектор множників Лагранжу;

$\bar{\mu}_r$  – підвектори вектора  $\bar{\mu}$ , що належать до кожної з умов (4.11).

У межах принципу цільової координації [22, 23] вводиться дворівнева ієрархія розрахунків: вектори маршрутних змінних пропонується визначати на нижньому рівні – розподілено на кожному з приграничних маршрутизаторів, а підвектори  $\bar{\mu}_r$  множників Лагранжа – на верхньому рівні – рівні SDN-контролера. Тоді лагранжіан (4.13) представимо у вигляді [50–56]

$$L = \sum_{R_r \in R} L_r, \quad (4.14)$$

$$L_r = \bar{x}_r^t H_r \bar{x}_r + \bar{\mu}_r^t A_r \bar{x}_r - \bar{\mu}_r^t D_r \bar{\varphi} + \sum_{\substack{R_s \in R \\ s \neq r}} \bar{\mu}_s^t C_{sr} \bar{x}_r, \quad (4.15)$$

припустивши, що  $\bar{\mu}_r$  фіксовані та формуються на верхньому рівні ієрархії.

Таким чином, цільова функція (4.14) набуває адитивної форми, а загальна проблема ієрархічної маршрутизації підлягає декомпозиції на низку маршрутних задач (4.15). Розв’язання задач, пов’язаних з мінімізацією за маршрутними змінними виразів (4.15), відбувається на нижньому рівні розрахунків. Отримані таким чином рішення визначають порядок розподіленої маршрутизації «від джерела» потоків, що надходять на кожен з приграничних LER-маршрутизаторів. Вектори  $\bar{x}_r$  передаються на верхній рівень для перевірки виконання умов (4.11).

Основною технологічною задачею верхнього ієрархічного рівня є недопущення перевантаження каналів зв’язку, тобто забезпечення виконання умов (4.11). Таким чином, на верхньому рівні розрахунків згідно з принципом цільової координації здійснюється координація рішень, отриманих на нижньому рівні, та відбувається модифікація векторів множників Лагранжа в процесі виконання ітераційної градієнтної процедури

$$\bar{\mu}_r(a+1) = \bar{\mu}_r(a) + \nabla \bar{\mu}_r, \quad (4.16)$$

де  $a$  – номер ітерації розрахунків;

$\nabla \bar{\mu}_r$  – градієнт функції, що розраховується, виходячи з отриманих на верхньому рівні результатів розв’язання задач маршрутизації на кожному конкретному маршрутизаторі-відправнику

$$\nabla \mu_r(x) \Big|_{x=x^*} = A_r \bar{x}_r^* - D_r \vec{\phi} + \sum_{\substack{R_s \in R \\ s \neq r}} C_{rs} \bar{x}_s^*, \quad (4.17)$$

де  $\bar{x}_r^*$  ( $R_r \in R$ ) – результат розрахунків, отриманий нижнім рівнем ієрархії на поточній ітерації.

Нові значення підвекторів множників Лагранжа (4.16) передаються на нижній рівень – рівень приграничних маршрутизаторів для перерозрахунку векторів маршрутних змінних. Фактично координати підвекторів (4.16) у виразі (4.15) є корекціями маршрутних метрик. Чим більший вплив здійснює той чи інший потік на перевантаження обраного каналу, тим більшого значення набуде відповідна координата вектора (4.16) та більшою стане результативна метрика перевантаженого каналу для цього потоку.

Таким чином, процес розв’язання задачі ієрархічно-координаційної внутрішньодоменної маршрутизації в ІКМ SDN/MPLS набуває ітераційного характеру. Чим менше ітерацій потребує координація маршрутних рішень (4.16), (4.17) для забезпечення виконання умов (4.11), тим менший обсяг службової інформації буде циркулювати в мережі про її стан, і тим оперативнішою буде практична реалізація отриманих результатів на приграничних маршрутизаторах. Тому актуальним завданням є аналіз впливу параметрів мережі (її топології та завантаженості), характеристик та типу трафіку на швидкість збіжності координаційної процедури (4.16), (4.17). Дослідження швидкості збіжності було проведено на різних мережних топологіях для випадків організації як одно-, так і багатоадресної маршрутизації.

### **4.2.3. Дослідження процесів ієрархічно-координаційної внутрішньодоменної маршрутизації одноадресних потоків на основі метрик в інфокомунікаційній мережі SDN/MPLS**

Для початку проаналізуємо випадок одноадресної маршрутизації на структурі мережі, зображеної на рис. 4.7. Мережа складалася з шести маршрутизаторів ( $R_1 \div R_6$ ) і дев’яти каналів зв’язку. У розривах каналів зв’язку показана їхня пропускна здатність ( $1/c$ ). Для наочності розглядалося два потоки. Перший потік пакетів передавався від маршрутизатора  $R_1$  до

маршрутизатора  $R_4$ , а вузлом-відправником та вузлом-отримувачем другого потоку були маршрутизатори  $R_3$  та  $R_4$  відповідно. Інтенсивність потоків від кожного маршрутизатора-відправника змінювалася від 0 1/с до 200 1/с.

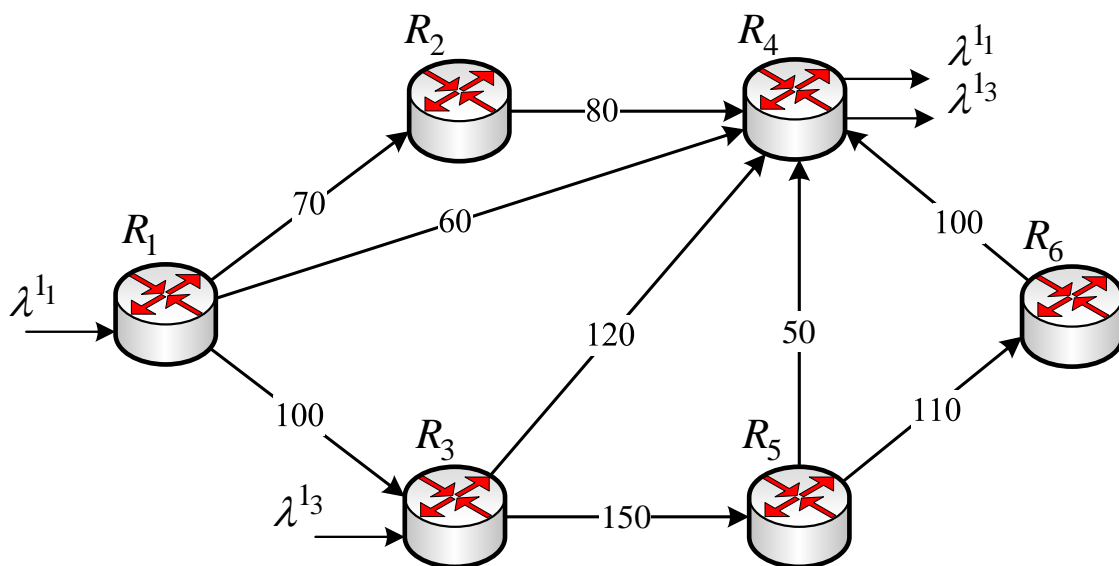


Рис. 4.7. Перший варіант структури мережі, що досліджувалась

Під час дослідження було проведено аналіз впливу завантаженості мережі, тобто значень інтенсивності потоків пакетів, на кількість ітерацій координаційної процедури (4.16), (4.17). Інтенсивність потоків змінювалася з кроком 20 1/с, загальна кількість варіантів, які були прораховані, становила 100. За результатами дослідження було зроблено висновок, що зі зростанням інтенсивності потоків збільшується ймовірність перевантаження каналів зв'язку ІКМ, тому зростає й кількість ітерацій координаційної процедури (4.16), (4.17). Для наведених вихідних даних максимальна кількість ітерацій дорівнювала 13 і спостерігалася за максимально можливою завантаженістю мережі, тобто за умови інтенсивностей 200 1/с для кожного потоку.

Розглянемо більш детально результат маршрутизації потоків для граничної завантаженості ІКМ, тобто коли інтенсивності обох потоків становили по 200 1/с. На першій ітерації результат розв'язання задачі маршрутизації нижнього рівня (4.15) показано на рис. 4.8, на якому в розривах каналів зв'язку представлено дріб з такими даними (зверху вниз): інтенсивність першого потоку (1/с), інтенсивність другого потоку (1/с), пропускна здатність каналу зв'язку (1/с).

Зважаючи на неузгодженість маршрутних рішень, отриманих на першому та п'ятому приграничних маршрутизаторах, відбувається перевантаження

каналу зв'язку, що з'єднує маршрутизатори  $R_3$  та  $R_4$ . Розподіл потоків пакетів по каналах зв'язку ІКМ, наприклад, після сьомої ітерації показано на рис. 4.9. На цій ітерації перевантаженими стають уже три канали зв'язку: між маршрутизаторами  $R_3$  та  $R_5$ ,  $R_6$  та  $R_4$ , а також між  $R_5$  та  $R_6$ .

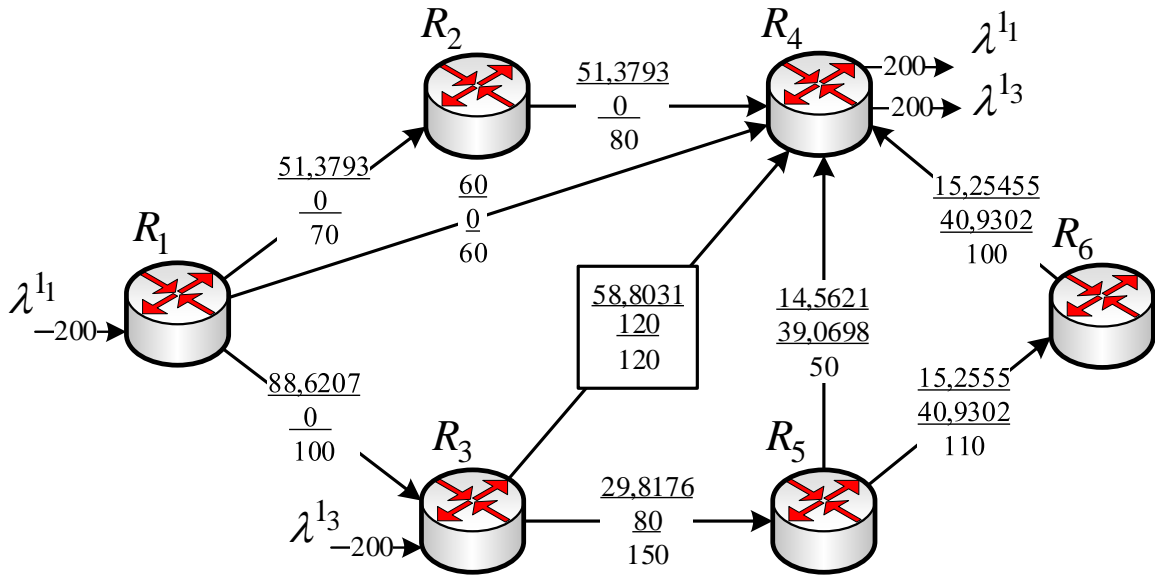


Рис. 4.8. Початковий порядок маршрутизації двох потоків в ІКМ

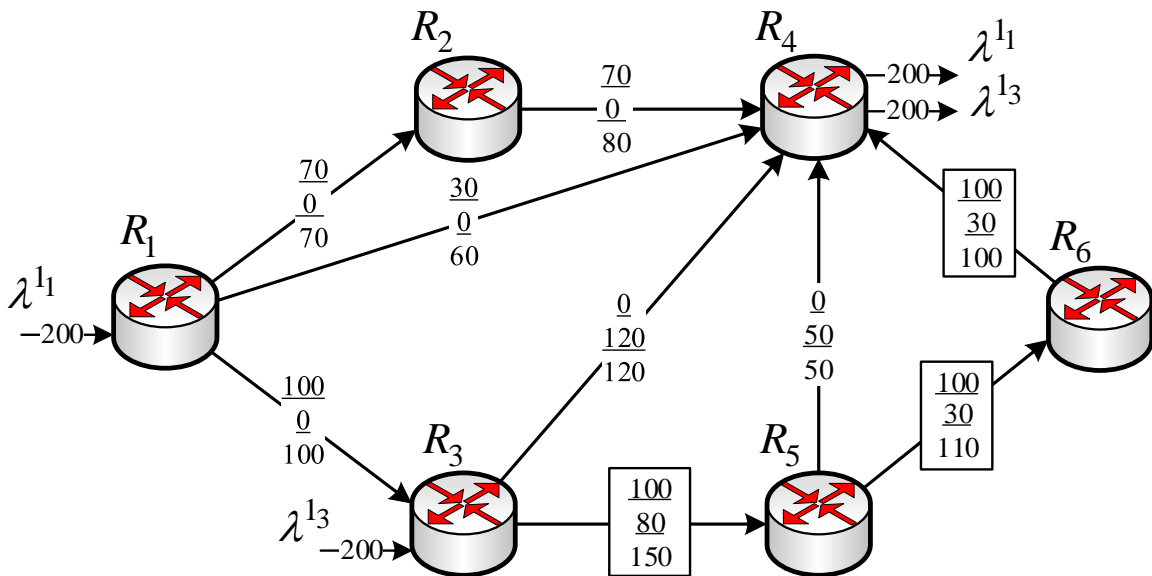


Рис. 4.9. Порядок маршрутизації потоків пакетів каналами зв'язку після сьомої ітерації

Остаточний порядок маршрутизації потоків пакетів, отриманий після тринадцятої ітерації, зображений на рис. 4.10. Зокрема жоден з каналів зв'язку під час маршрутизації двох потоків не був перевантаженим. Для вихідних даних

структури, наведеної на рис. 4.7, залежність кількості ітерацій координаційної процедури (4.16), (4.17) від інтенсивностей потоків показано на рис. 4.11.

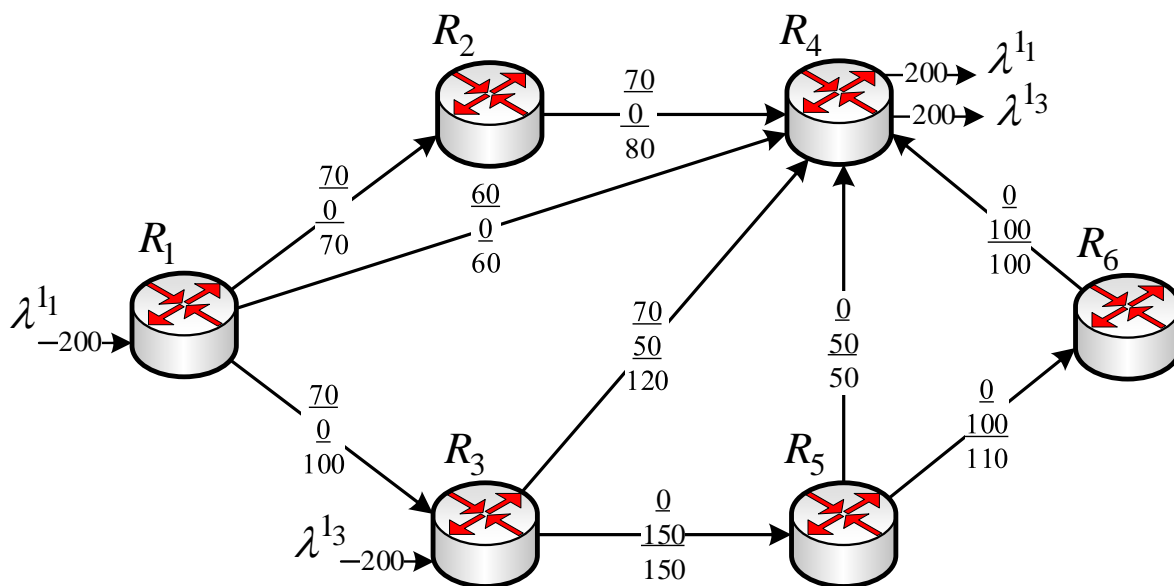


Рис. 4.10. Остаточний порядок маршрутизації потоків пакетів після тринадцятої ітерації

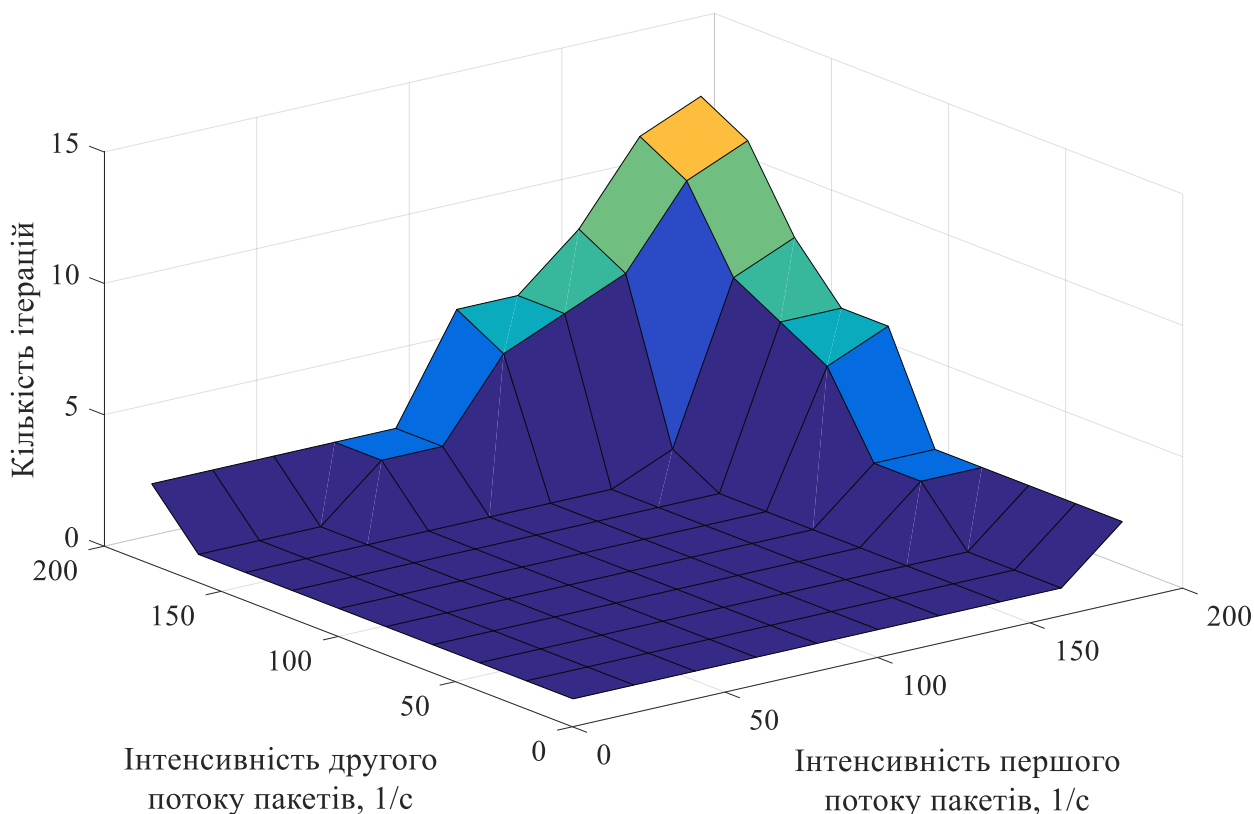


Рис. 4.11. Аналіз збіжності координаційної процедури (4.16), (4.17) за умови ієрархічно-координаційної внутрішньодоменної маршрутизації в мережі SDN/MPLS, структура якої зображена на рис. 4.7

У межах використаного принципу цільової координації кількість ітерацій координаційної процедури (4.16), (4.17) визначає інерційність процесу маршрутизації в мережі й обсяг службового трафіку, що містить дані про  $\bar{x}_r^*$  та  $\bar{\mu}_r$  ( $R_r \in R$ ). Тому важливо в процесі ієрархічної маршрутизації, яка організується в межах рішення (4.13)–(4.17), мінімізувати кількість ітерацій (4.16).

Під час дослідження встановлено (рис. 4.8–4.10), що причина зростання кількості ітерацій координаційної процедури – це перевантаження каналів зв'язку, віддалених за кількістю переприйомів від вузлів відправника або отримувача пакетів. Це обумовлено тим, що використання квадратичного критерію оптимальності (4.12) сприяє збалансованій завантаженості всіх каналів зв'язку ІКМ. У зв'язку з цим пропонується для кожного потоку пакетів до початку розрахунків забезпечити збільшення маршрутної метрики каналів зв'язку пропорційно віддаленості цих каналів (за кількістю вузлів) до відповідного вузла-відправника або отримувача пакетів. Тому для кожного потоку для модифікації маршрутних метрик пропонуються такі вирази:

$$h_{i,j}^* = h_{i,j} + g \cdot v_{i,j}^{k_r}, \quad v_{i,j}^{k_r} = \min \left( \text{hop}_{i,j}^{s_{k_r}}, \text{hop}_{i,j}^{d_{k_r}} \right), \quad (4.18)$$

де  $g$  – ваговий коефіцієнт зміни метрики ( $g > 0$ ), який регулює рівень впливу введеної модифікації на кінцеве значення маршрутної метрики;

$\text{hop}_{i,j}^{s_{k_r}}$  – мінімальна кількість вузлів між вузлом-відправником пакетів та каналом зв'язку  $E_{i,j}$ ;

$\text{hop}_{i,j}^{d_{k_r}}$  – мінімальна кількість вузлів між вузлом-отримувачем пакетів та каналом зв'язку  $E_{i,j}$ .

Таким чином, метрика каналу зв'язку  $E_{i,j}$  підлягає зміні залежно від кількості транзитних вузлів між цим каналом і вузлом-відправником (отримувачем). Канали зв'язку, що безпосередньо поєднані з відправником (отримувачем) пакетів, залишаються з номінальною метрикою, оскільки  $v_{i,j}^{k_r} = 0$  [57, 58].

Використовуючи вирази (4.18) у процесі модифікації маршрутних метрик у виразі (4.12), була також отримана залежність кількості ітерацій від інтенсивності вхідних потоків пакетів, представлена як у табл. 4.2, так і на рис. 4.12.

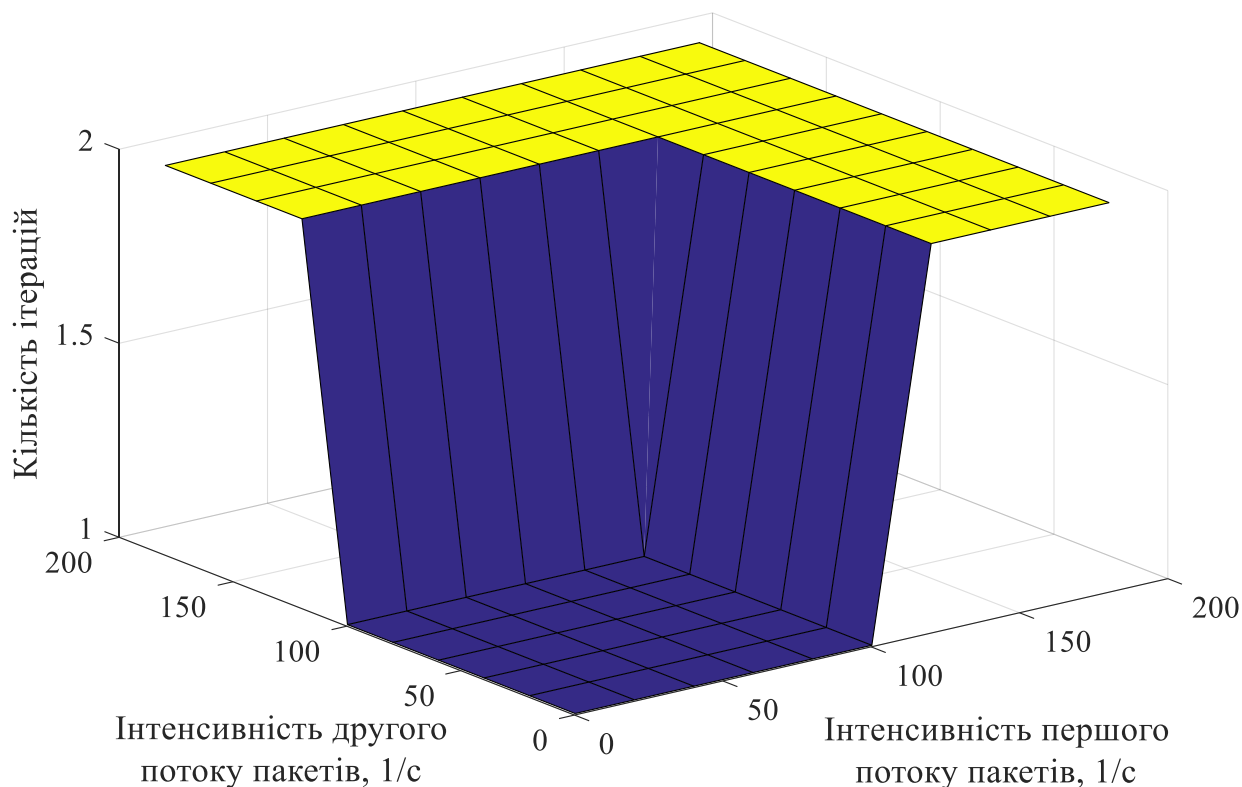


Рис. 4.12. Аналіз збіжності координаційної процедури (4.16), (4.17) за умови ієрархічно-координаційної внутрішньодоменної маршрутизації в мережі SDN/MPLS, структура якої зображена на рис. 4.7, з використанням метрики (4.18)

Модифікація метрики (4.18) каналів зв'язку значно вплинула на кількісний результат щодо збіжності координаційної процедури (4.16), (4.17), а саме: вдалося скоротити кількість ітерацій у середньому від 1,5 до 5 разів залежно від інтенсивності переданих потоків пакетів (рис. 4.13).

Проведемо додатково аналіз впливу особливостей структури ІКМ на збіжність координаційної процедури в разі реалізації ієрархічно-координаційної маршрутизації. Основними параметрами, які змінювалися в структурі мережі, були кількість каналів зв'язку та маршрутизаторів і їхня зв'язність. Як приклад розглянемо варіант структури мережі (рис. 4.14), яка містить чотири маршрутизатори ( $R_1 \div R_4$ ) та п'ять каналів зв'язку, тобто розмір ІКМ порівняно з варіантом, наведеним на рис. 4.7, знизився. Кількість потоків, що циркулюють у мережі, не змінювалася. Вузлом-відправником першого потоку пакетів був маршрутизатор  $R_1$ , вузлом-отримувачем – маршрутизатор  $R_4$ , а другий потік пакетів направлявся від маршрутизатора  $R_2$  до маршрутизатора  $R_4$ .

На рис. 4.14 у розривах каналів зв'язку показана їх пропускна здатність (1/с). У процесі дослідження інтенсивність кожного з потоків змінювалася від 0 1/с



до 180 1/с. Саме за умови максимальної інтенсивності потоків спостерігалася найбільша кількість ітерацій координаційної процедури, яка без використання виразів (4.18) дорівнювала семи. Початковий розподіл потоків у разі  $\lambda^{11} = \lambda^{12} = 180$  1/с продемонстровано на рис. 4.15, де в розривах каналів зв'язку показано дріб (зверху вниз): інтенсивність першого потоку пакетів (1/с), інтенсивність другого потоку пакетів (1/с), його пропускна здатність (1/с).

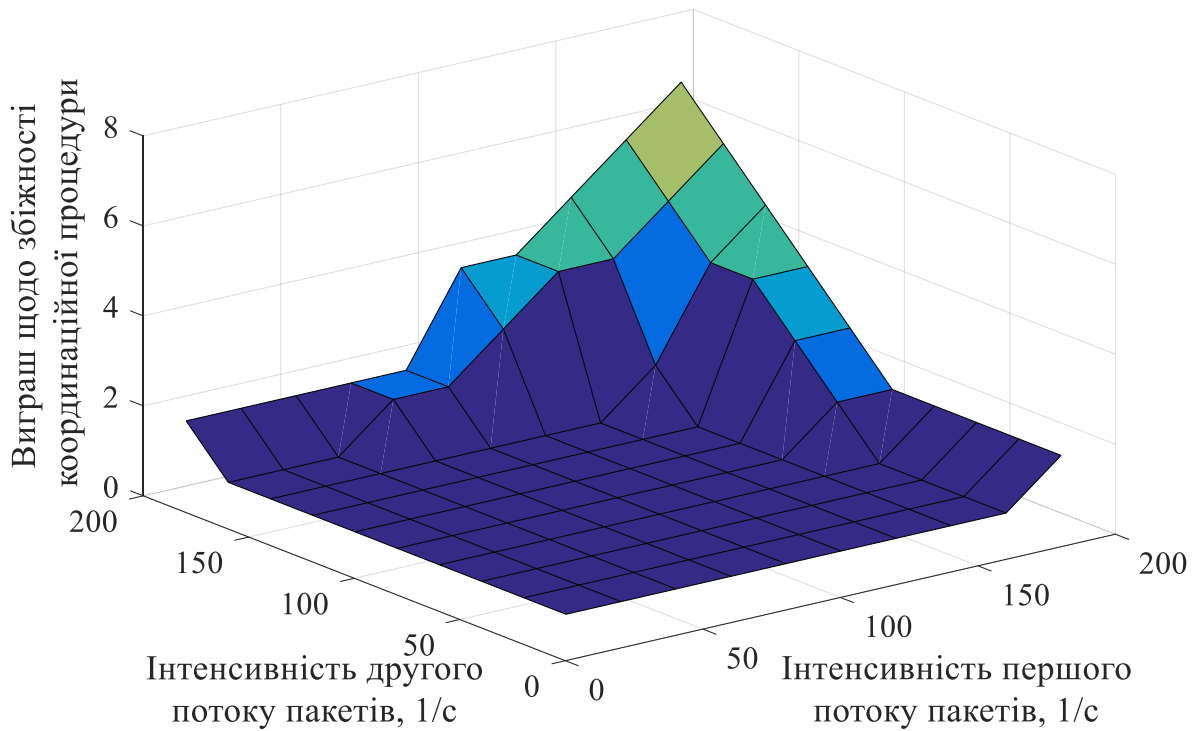


Рис. 4.13. Виграш щодо збіжності координаційної процедури (4.16), (4.17) за умови ієрархічно-координаційної внутрішньодоменної маршрутизації в мережі SDN/MPLS, структура якої зображена на рис. 4.7

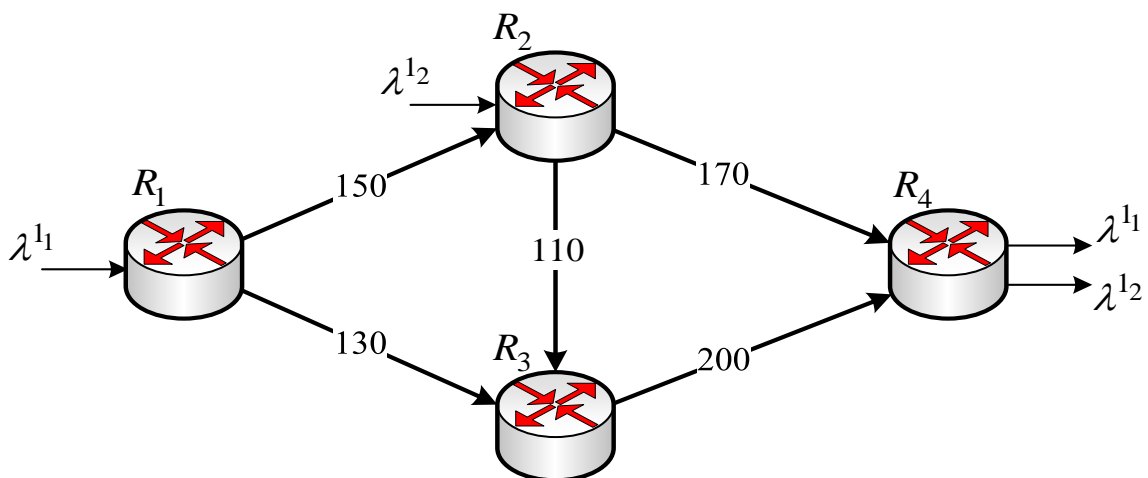


Рис. 4.14. Другий варіант структури мережі, яка досліджувалася

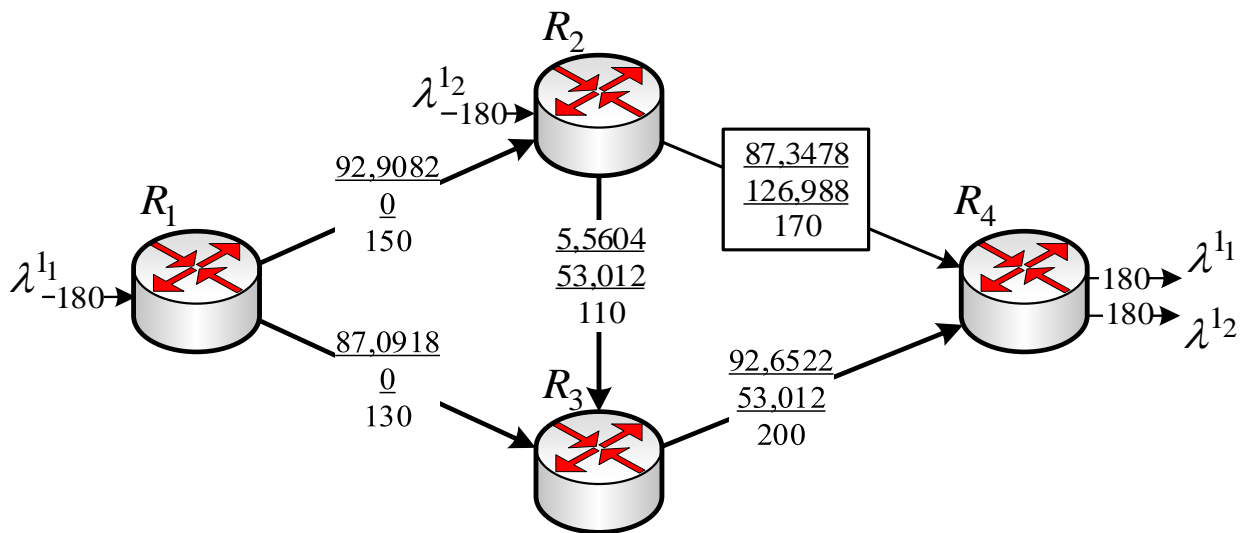


Рис. 4.15. Початковий порядок маршрутизації в ІКМ

Оскільки перший і другий маршрутизатори розраховували шляхи незалежно один від одного, то канал зв'язку між маршрутизаторами  $R_2$  та  $R_4$  виявився перевантаженими. Під час координації маршрутних рішень, що отримувалися на кожному приграничному маршрутизаторі, характер перевантаження змінювався. Так, після четвертої ітерації (рис. 4.16) перевантаженим залишився один канал, але який з'єднував маршрутизатори  $R_2$  та  $R_3$ .

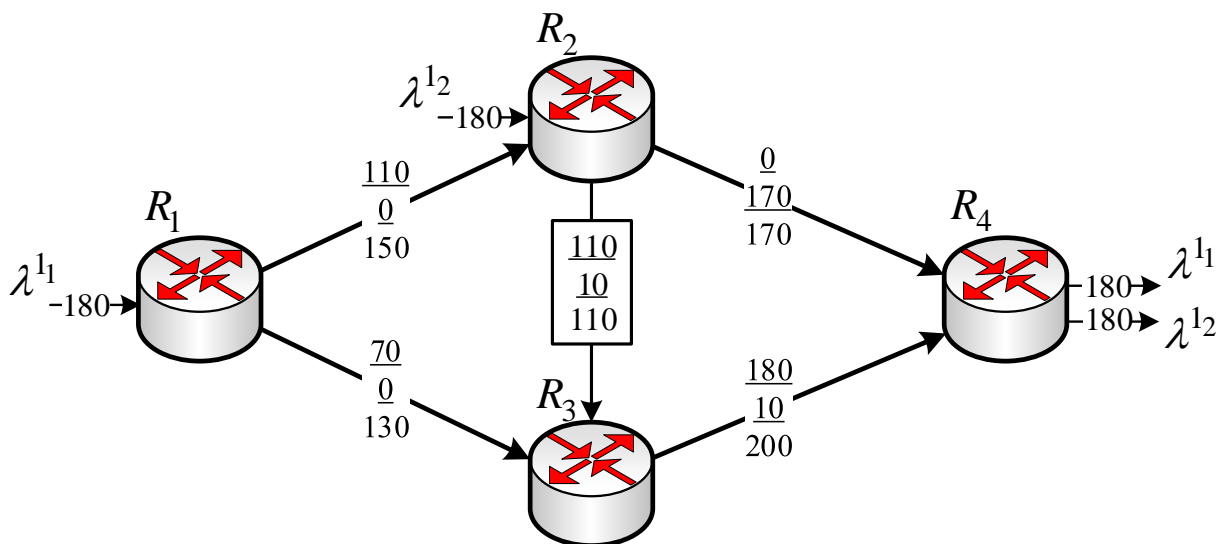


Рис. 4.16. Порядок маршрутизації потоків в ІКМ після четвертої ітерації

Остаточний порядок маршрутизації потоків в ІКМ, отриманий після завершення роботи процедури (4.16), (4.17), зображений на рис. 4.17.

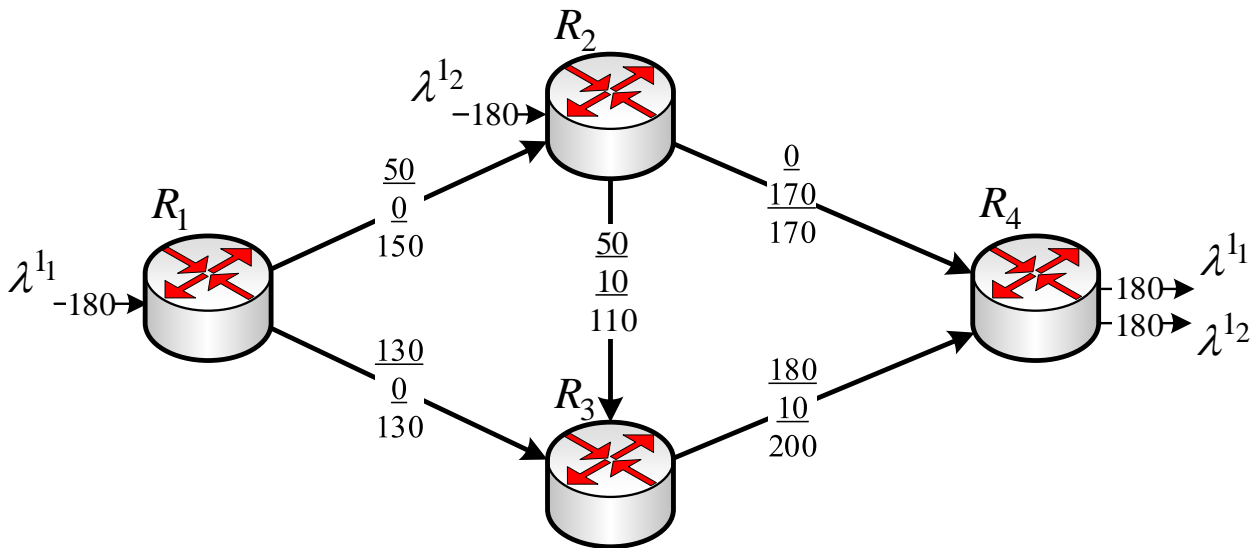


Рис. 4.17. Остаточний порядок маршрутизації потоків пакетів каналами зв'язку ІКМ (після сьомої ітерації)

Для структури, представленої на рис. 4.14, залежність кількості ітерацій координаційної процедури (4.16), (4.17) від величин інтенсивностей потоків пакетів показана на рис. 4.18.

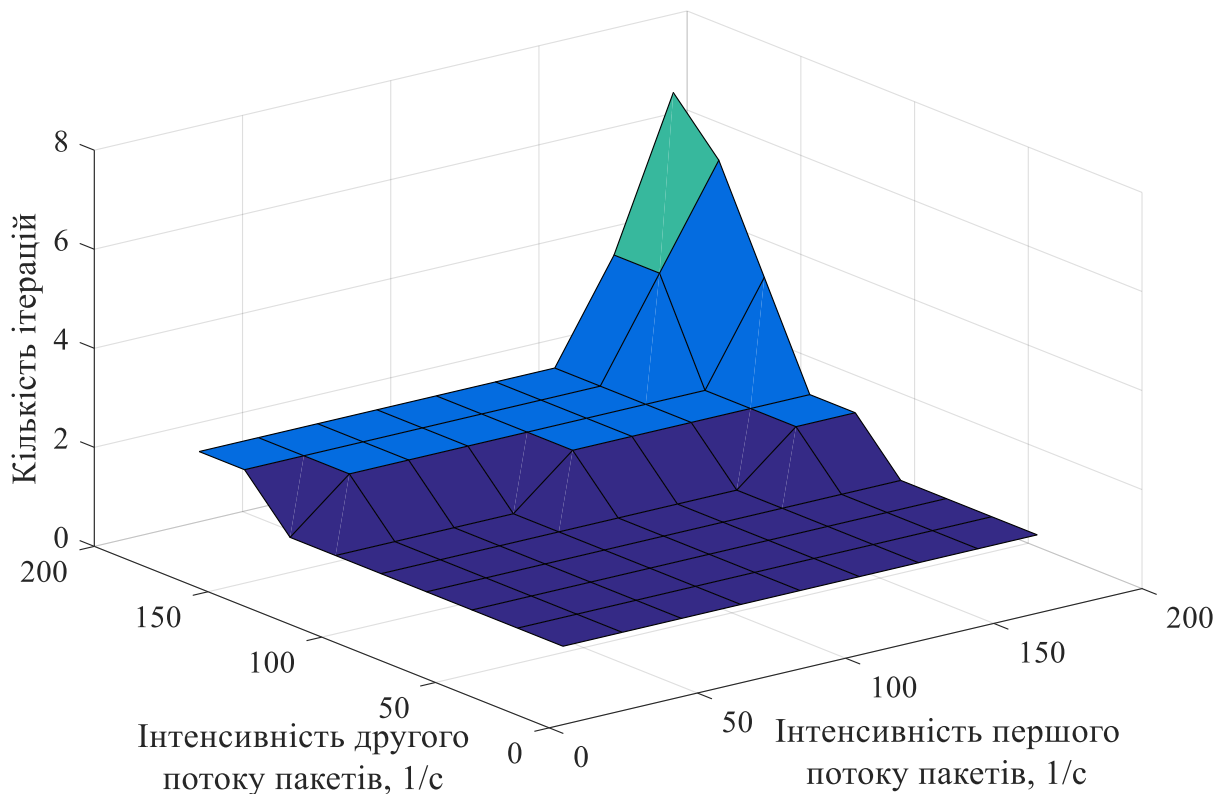


Рис. 4.18. Аналіз збіжності координаційної процедури (4.16), (4.17) за умови ієрархічно-координаційної внутрішньодоменної маршрутизації в мережі SDN/MPLS, структура якої зображена на рис. 4.14

З метою підвищення швидкості збіжності координаційної процедури маршрутна метрика також підлягала модифікації за правилом, що задано виразами (4.18). У цьому випадку для граничних значень інтенсивностей обох потоків 180 1/с максимальна кількість ітерацій дорівнювала двом (рис. 4.19). Результати аналізу роботи координаційної процедури за умови ієрархічно-координаційної внутрішньодоменної маршрутизації для структури ІКМ, зображеної на рис. 4.14, представлено на рис. 4.19 та 4.20.

Як показано на рис. 4.20, модифікація метрики каналів зв'язку (4.18) дозволяє для структури мережі, представленої на рис. 4.14, зменшити кількість ітерацій координаційної процедури в ділянці середніх і високих навантажень у середньому в 1,5–2 рази, а для граничної завантаженості мережі – до 3,5 рази.

Під час подальшого дослідження розглядалась ІКМ, структура якої у порівняно з варіантом, наведеним на рис. 4.7, має більш високу зв'язність маршрутизаторів, тобто за умови тієї ж кількості маршрутизаторів ( $m = 6$ ) кількість каналів зв'язку збільшена з 9 до 11 (рис. 4.21). На рис. 4.21 у розривах каналів зв'язку знову вказано їхні пропускні здатності (1/с). Кількість і характеристики потоків, порівняно з першим прикладом (рис. 4.7), не змінювалися.

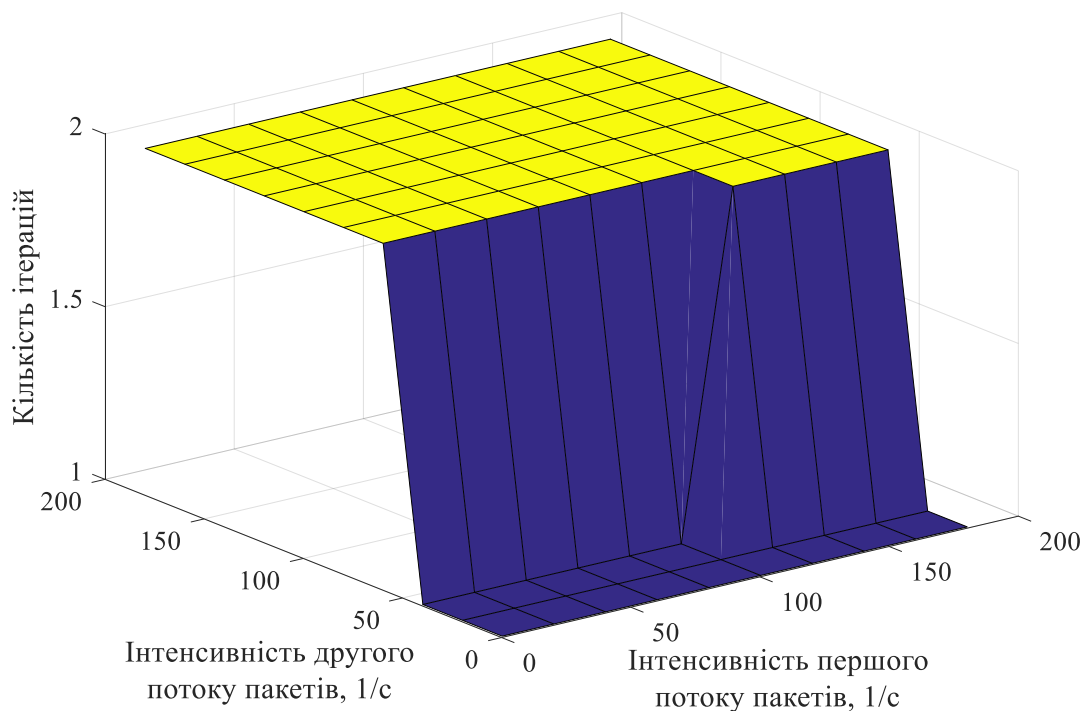


Рис. 4.19. Аналіз збіжності координаційної процедури (4.16), (4.17) за умови ієрархічно-координаційної внутрішньодоменної маршрутизації в мережі SDN/MPLS, структура якої зображена на рис. 4.14, з використанням метрики (4.18)

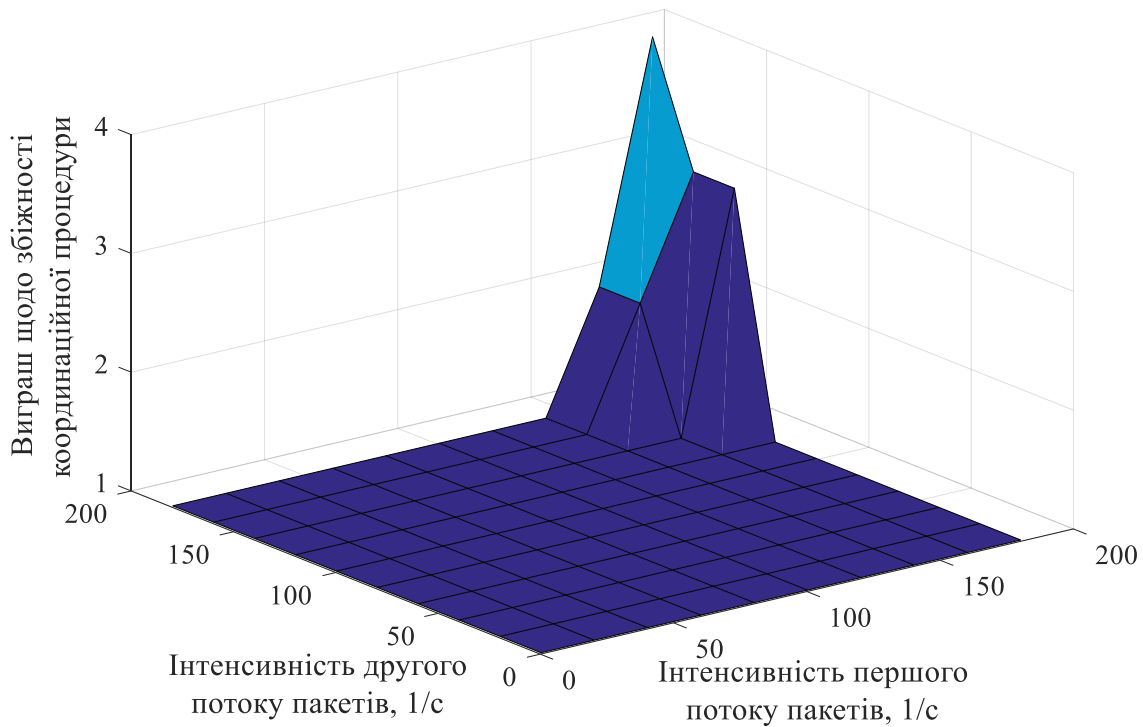


Рис. 4.20. Виграш щодо збіжності координаційної процедури (4.16), (4.17) за умови ієрархічно-координаційної внутрішньодоменної маршрутизації в мережі SDN/MPLS, структура якої зображена на рис. 4.14

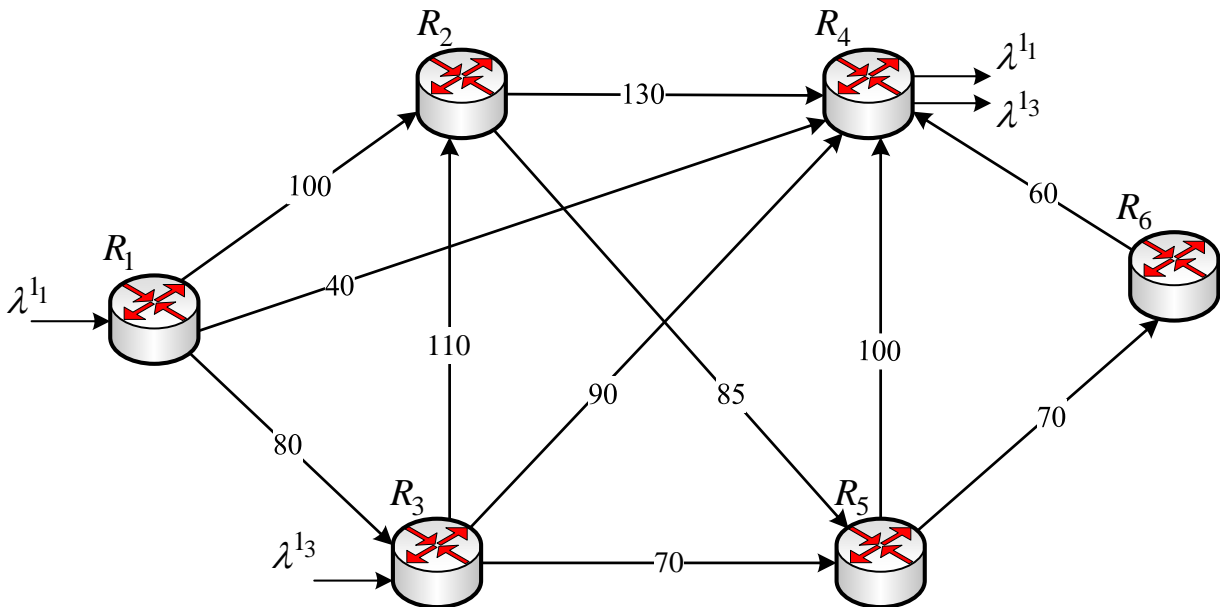


Рис. 4.21. Третій варіант структури мережі, яка досліджувалася

Реалізація ієрархічно-координаційної внутрішньодоменної маршрутизації на основі принципу цільової координації (4.13)–(4.17) дозволила забезпечити збіжність координаційної процедури (4.16), (4.17) за 15 ітерацій. У цьому випадку на першій ітерації перевантаженим був канал зв'язку, що з'єднує маршрутизатори  $R_3$  та  $R_4$  (рис. 4.22).

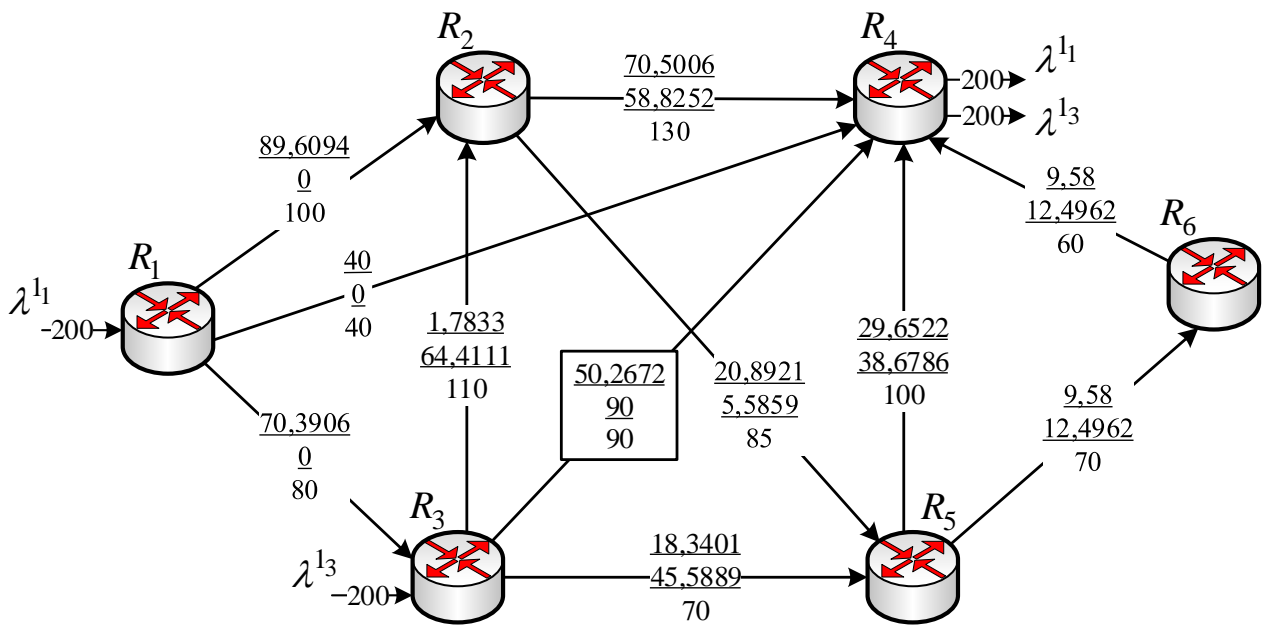


Рис. 4.22. Початковий порядок маршрутизації потоків в ІКМ

На рис. 4.22 в розривах каналів зв'язку вказано (зверху вниз): інтенсивність першого потоку (1/с), інтенсивність другого потоку (1/с), його пропускна здатність (1/с). Після сьомої ітерації перевантаженим став канал між маршрутизаторами  $R_2$  та  $R_3$  (рис. 4.23). Після завершення роботи координаційної процедури (4.16), (4.17), тобто після п'ятнадцятої ітерації, остаточний порядок маршрутизації потоків в ІКМ, структура якої представлена на рис. 4.21, зображений на рис. 4.24. Жоден з 11 каналів зв'язку перевантажений не був.

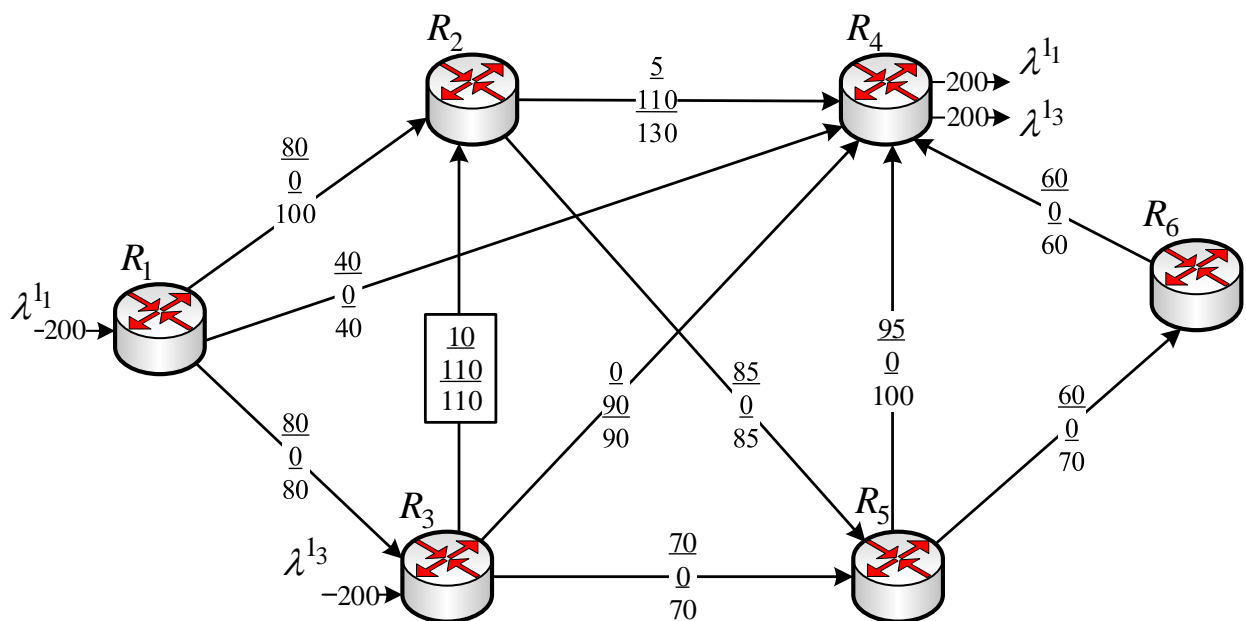


Рис. 4.23. Порядок маршрутизації потоків в ІКМ після сьомої ітерації

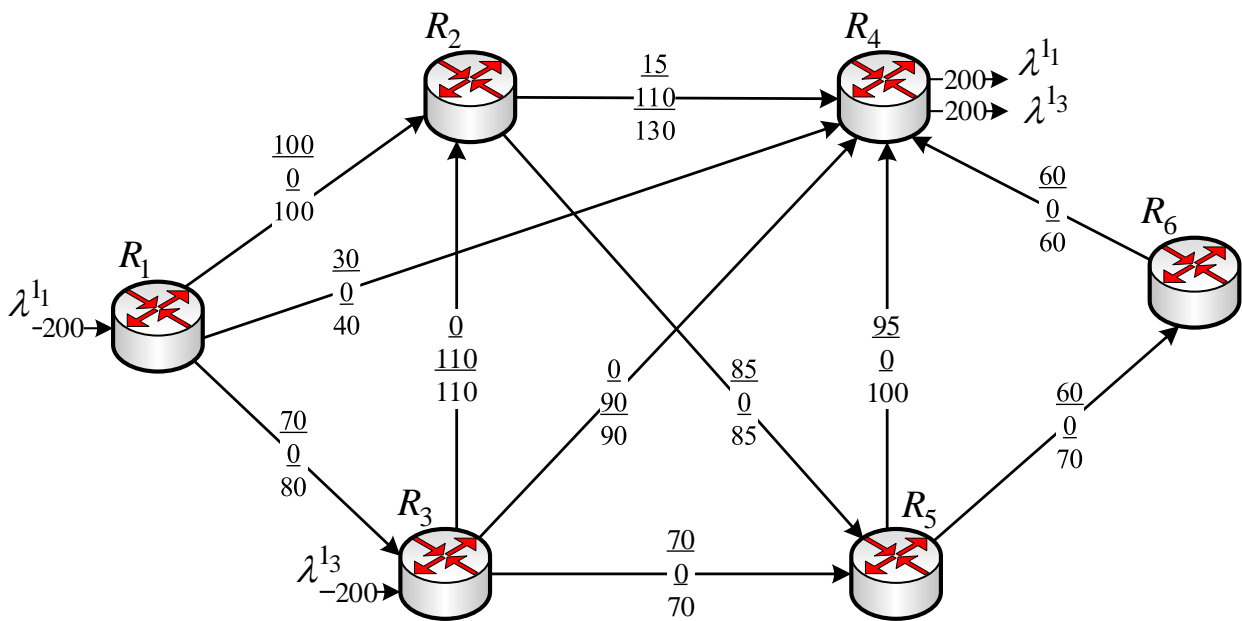


Рис. 4.24. Остаточний порядок маршрутизації потоків пакетів каналами зв'язку ІКМ (після п'ятнадцятої ітерації)

На рис. 4.25 показано результати аналізу збіжності координаційної процедури (4.16), (4.17) у разі зміни завантаженості ІКМ, структура якої представлена на рис. 4.21.

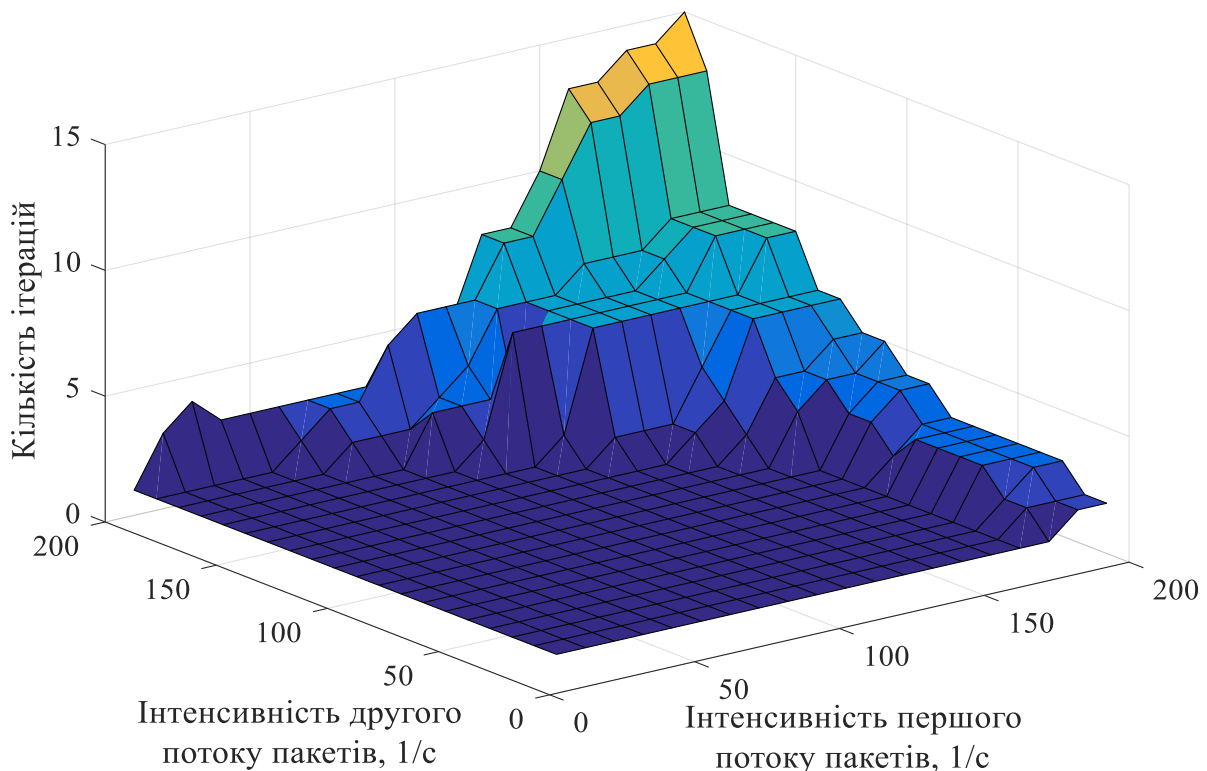


Рис. 4.25. Аналіз збіжності координаційної процедури (4.16), (4.17) за умови ієрархічно-координаційної внутрішньодоменної маршрутизації в мережі SDN/MPLS, структура якої зображена на рис. 4.21

У процесі модифікації маршрутної метрики за правилом (4.18) вдалося зменшити кількість ітерацій процедури (4.16), (4.17) до восьми (рис. 4.26), тобто практично удвічі (рис. 4.27) порівняно з початковими рішеннями.

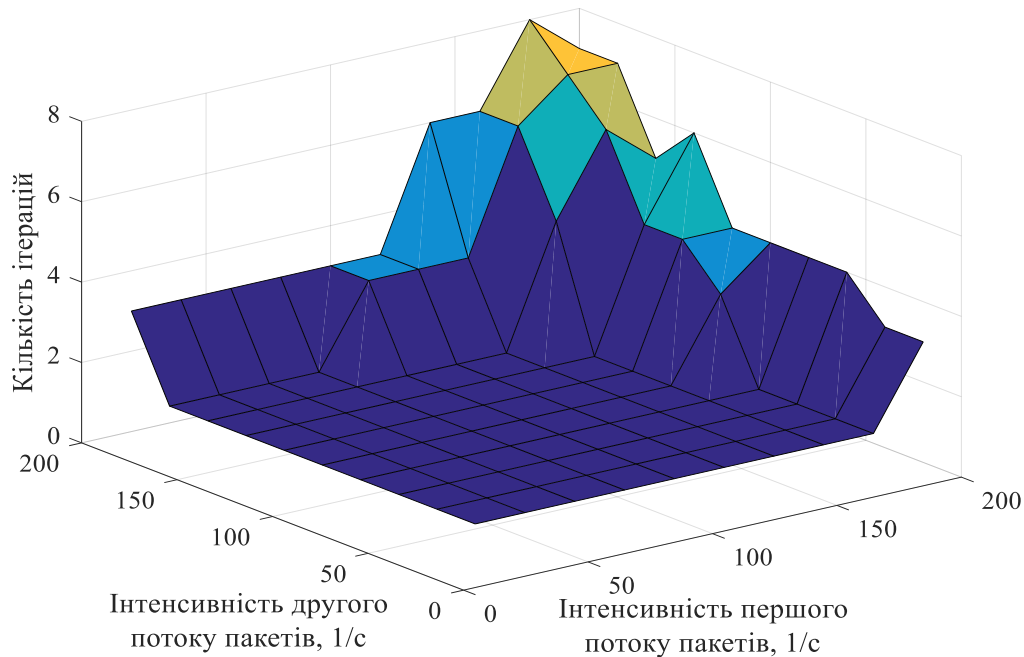


Рис. 4.26. Аналіз збіжності координаційної процедури (4.16), (4.17) за умови ієрархічно-координаційної внутрішньодоменної маршрутизації в мережі SDN/MPLS, структура якої зображена на рис. 4.17, з використанням метрики (4.18)

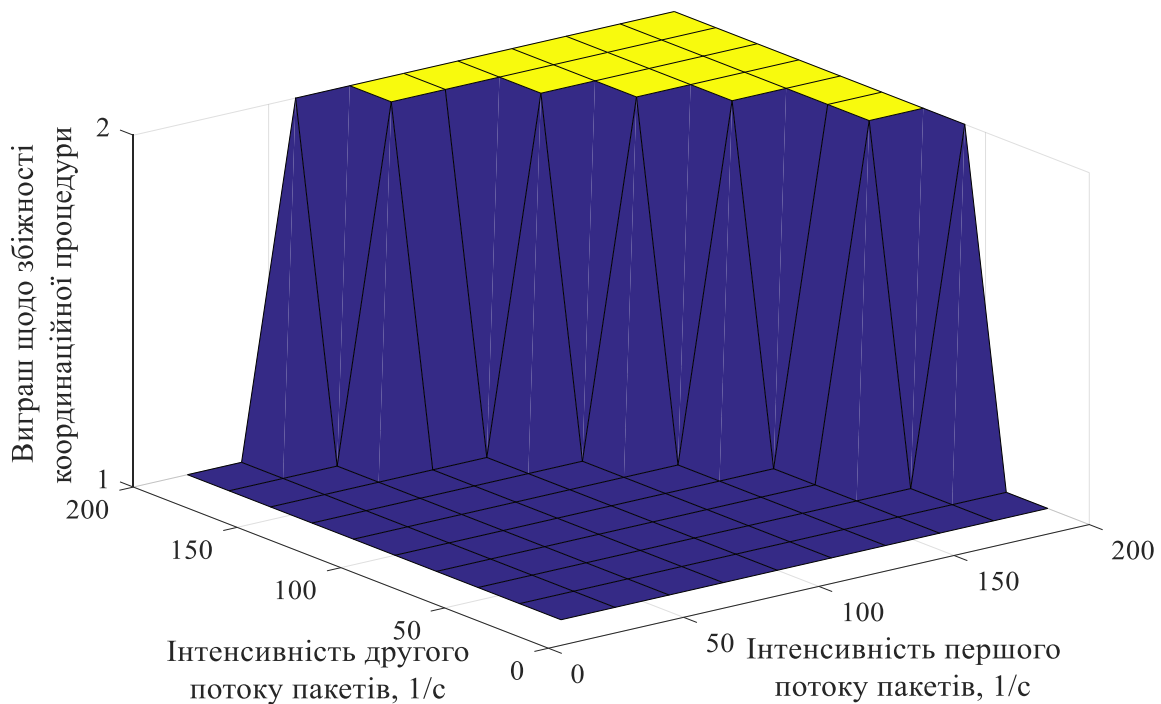


Рис. 4.27. Виграш щодо збіжності координаційної процедури під час реалізації ієрархічно-координаційної внутрішньодоменної маршрутизації для структури ІКМ, що наведена на рис. 4.17



Отже, зі збільшенням завантаженості мережі, її розміру та зв'язності маршрутизаторів кількість ітерацій координаційної процедури (4.16), (4.17) збільшується, що призводить до відповідного зростання часу розв'язання маршрутних задач та обсягів службового трафіку в мережі. Застосування виразів для визначення маршрутних метрик (4.18) дозволяє суттєво (у середньому від 1,5 до 4 разів) підвищити швидкість збіжності отриманих рішень до оптимальних значень.

#### 4.2.4. Розв'язання задачі ієрархічно-координаційної внутрішньодоменої маршрутизації одноадресних потоків з балансуванням навантаження в інфокомунікаційній мережі SDN/MPLS-TE

З метою задоволення вимог концепції Traffic Engineering [59–62] щодо забезпечення балансування навантаження в мережі SDN/MPLS-TE під час реалізації ієрархічно-координаційної внутрішньодоменої маршрутизації в моделі (4.1)–(4.11), заснованої на маршрутних метриках, змінюється форма запису умов запобігання перевантаження каналів зв'язку (4.9). Як показано в роботах [63–67], ці умови представлені в такому вигляді:

$$\sum_{R_r \in R} \sum_{k_r \in K} \lambda^{k_r} x_{i,j}^{k_r} \leq \alpha \varphi_{i,j}, E_{i,j} \in E, \quad (4.19)$$

де  $\alpha$  – змінна балансування, яка кількісно визначає верхній поріг завантаженості каналів зв'язку мережі.

На змінну  $\alpha$  накладається умова у вигляді [63–67]

$$0 \leq \alpha \leq 1. \quad (4.20)$$

Саме мінімізація цього порогового значення  $\alpha$  є метою маршрутизації з балансуванням навантаження за вимогами концепції Traffic Engineering. Однак варто врахувати, що в процесі розподіленого розрахунку маршрутних змінних на кожному окремому приграничному маршрутизаторі вимоги умов (4.19) виконати досить важко. Це обумовлено тим, що кожен приграничний маршрутизатор у мережі приймає рішення щодо маршрутизації потоків, які надходять на нього, в умовах відсутності інформації про результати розрахунків на інших приграничних маршрутизаторах. У зв'язку з цим кожна з умов (4.19) розділимо на дві умови-нерівності: на умови (4.10) та умови

$$\sum_{k_r \in K_r} \lambda^{k_r} x_{i,j}^{k_r} \leq \alpha_r \varphi_{i,j}, \quad (4.21)$$

де  $\alpha_r$  – верхній поріг завантаженості каналів зв'язку потоками, які підлягають маршрутизації приграничним маршрутизатором  $R_r$ .

На змінні  $\alpha_r$  також накладаються обмеження, аналогічні до (4.20),

$$0 \leq \alpha_r \leq 1. \quad (4.22)$$

Умови (4.21) вводяться для забезпечення балансування навантаження, а нерівності (4.10) – для запобігання перевантаження каналів зв'язку ІКМ. Умови (4.21) можна виконати для кожного з приграничних маршрутизаторів окремо, натомість виконання умов (4.10) потребує координації роботи множини приграничних вузлів. Тому надалі умови (4.10) знову будуть використовуватись у векторно-матричній формі (4.11).

Варто зазначити, що на практиці завжди буде виконуватися нерівність

$$\alpha \leq \sum_{R_r \in R} \alpha_r. \quad (4.23)$$

Тому для розрахунку множини шуканих маршрутних змінних, представленої векторами  $\vec{x}_r$  ( $R_r \in R$ ), критерієм оптимальності отримуваних рішень обрано мінімум такої цільової функції:

$$F = \sum_{R_r \in R} \alpha_r, \quad (4.24)$$

яка вже записана в адитивній формі, що дуже важливо для забезпечення координації маршрутних рішень, які розподілено отримуються на приграничних маршрутизаторах мережі MPLS-TE.

Таким чином, розв'язання задачі ієрархічно-координаційної внутрішньодоменової маршрутизації в ІКМ SDN/MPLS-TE буде пов'язано з мінімізацією цільової функції (4.24) за наявності обмежень (4.2)–(4.8), (4.21), (4.22). Для цього знову використаємо принцип цільової координації [22, 23], у межах якого переходимо до двоїстої задачі

$$\min_{\vec{x}, \alpha_r} F = \max_{\mu} L,$$

де лагранжیان має такий вигляд:

$$L = \sum_{R_r \in R} \alpha_r + \sum_{R_r \in R} \vec{\mu}_r^t \left( A_r \vec{x}_r - D_r \vec{\phi} + \sum_{\substack{R_s \in R, \\ s \neq r}} C_{rs} \vec{x}_s \right). \quad (4.25)$$

Тоді, за аналогією з пунктом 4.2.2, у межах принципу цільової координації [22, 23] лагранжیان (4.25) представимо у вигляді

$$L = \sum_{R_r \in R} L_r, \quad (4.26)$$

$$L_r = \alpha_r + \vec{\mu}_r^t A_r \vec{x}_r - \vec{\mu}_r^t D_r \vec{\phi} + \sum_{\substack{R_s \in R, \\ s \neq r}} \vec{\mu}_s^t C_{sr} \vec{x}_r, \quad (4.27)$$

для того щоб усі маршрутні змінні належали до індексу  $r$ .

Таким чином, лагранжіан (4.26) набуває адитивної форми, а загальна проблема маршрутизації виявилася поділеною на кілька окремих маршрутних задач. Розв'язання задачі щодо мінімізації виразу (4.27) за наявності обмежень (4.2)–(4.4) та (4.21), (4.22) відбувається на нижньому рівні розрахунків. Унаслідок визначається послідовність маршрутизації потоків на кожному окремо взятому приграничному маршрутизаторі. Основна задача верхнього рівня залишилася незмінною – це координація рішень (4.16), (4.17), отриманих на нижньому рівні, з метою запобігання перевантаження каналів зв'язку (4.11).

Як зазначалось у пункті 4.2.2, у разі невиконання умов (4.11) координатор змінює градієнт функції (4.17), тим самим збільшуючи значення координат вектора множників Лагранжа (4.16) у виразі (4.27). Нові значення векторів множників Лагранжа координатор спрямовує на приграничні маршрутизатори. Тим самим фактично координатор змінює метрику перевантажених каналів, ініціюючи зменшення навантаження на цей канал зв'язку. Чим більше значення в перевантаженні каналу мають потоки, що надходять у мережу через маршрутизатор  $R_r$ , тим вищим є значення маршрутної метрики, яка залежить від  $\bar{\mu}_r$  (4.27).

На нижньому рівні приграничні LER-маршрутизатори розраховують нові значення маршрутних змінних, ґрунтуючись на модифікації векторів множників Лагранжа ( $\bar{\mu}_r$ ). Ці значення маршрутних змінних знову спрямовуються на верхній рівень для перевірки умов запобігання перевантаження каналів зв'язку (4.11) та подальшої координації рішень нижнього рівня (4.16), (4.17). Процес координації набуває ітераційного характеру, повторюючись доти, поки є проблема перевантаження каналів зв'язку.

#### **4.2.5. Дослідження процесів ієрархічно-координаційної внутрішньодоменної маршрутизації одноадресних потоків з балансуванням навантаження в інфокомунікаційній мережі SDN/MPLS-TE**

Дослідження процесів ієрархічно-координаційної внутрішньодоменної маршрутизації одноадресних потоків у мережі SDN/MPLS-TE проводилось у межах запропонованої моделі (4.1)–(4.4), (4.11), (4.16), (4.17), (4.19)–(4.27) для різних мережних структур зі змінюваною кількістю вузлів (маршрутизаторів) і каналів зв'язку. Для моделювання та розгляду всіх аспектів запропонованих рішень як приклад була обрана мережа, структура якої представлена на рис. 4.7. Вхідні дані щодо характеристик потоків залишилися незмінними.

На рис. 4.28 зображена залежність кількості ітерацій координаційної процедури (4.16), (4.17) від інтенсивностей потоків. Як показано на рис. 4.28, зі збільшенням навантаження на мережу ймовірність виникнення перевантаження каналів у зв'язку з розподіленим характером розв'язання задачі маршрутизації «від джерела» на нижньому рівні зростає. Тому й збільшується кількість ітерацій координаційної процедури (4.16), (4.17). Максимальна кількість ітерацій становила 10 і спостерігалася у разі гранично можливої завантаженості мережі, тобто коли інтенсивності кожного з потоків дорівнювали 200 1/с.

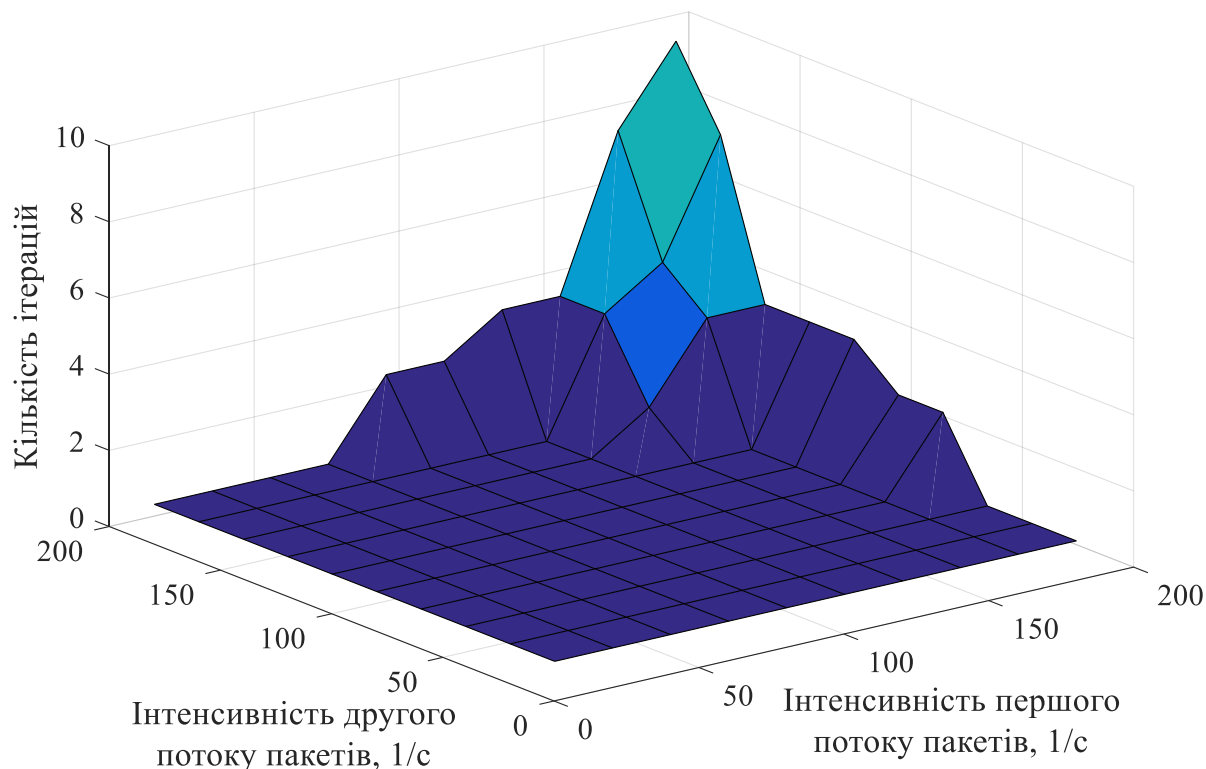


Рис. 4.28. Залежність кількості ітерацій координаційної процедури (4.16), (4.17) під час реалізації ієрархічно-координаційної маршрутизації з балансуванням навантаження в мережі від інтенсивностей потоків

Як і у випадку, описаному в пункті 4.2.2, причиною зростання кількості ітерацій координаційної процедури є перевантаження каналів зв'язку, що віддалені за кількістю переприйомів від вузлів відправника або отримувача пакетів. У зв'язку з цим для кожного приграничного маршрутизатора за умови балансування потоків пакетів пропонується використовувати не номінальні, а модифіковані значення пропускних здатностей каналів зв'язку, які беруть участь у розрахунках (4.21)

$$\varphi_{i,j}^r = \varphi_{i,j} v_{i,j}^{k_r}, \quad (4.28)$$

$$0 \leq v_{i,j}^{k_r} \leq 1, \quad (4.29)$$

де  $v_{i,j}^{k_r}$  – ваговий коефіцієнт, що характеризує пропорційну віддаленість каналу  $E_{i,j} \in E$  (за кількістю вузлів) від відповідного маршрутизатора-відправника або отримувача пакетів  $k_r$ -го потоку пакетів. Для розрахунку цього коефіцієнта пропонується використовувати вираз:

$$v_{i,j}^{k_r} = \frac{1}{\min\left(hop_{i,j}^{s_{k_r}}, hop_{i,j}^{d_{k_r}}\right) + 1}, \quad (4.30)$$

де  $hop_{i,j}^{s_{k_r}}$  – мінімальна кількість вузлів між маршрутизатором-відправником  $k_r$ -го потоку пакетів і каналом зв'язку  $E_{i,j}$ ;

$hop_{i,j}^{d_{k_r}}$  – мінімальна кількість вузлів між маршрутизатором-отримувачем  $k_r$ -го потоку пакетів і каналом зв'язку  $E_{i,j}$ .

Залежно від місця розташування каналу зв'язку в мережі можливі такі значення вагового коефіцієнта:

$v_{i,j}^{k_r} = 1$ , коли канал зв'язку  $E_{i,j} \in E$  є інцидентним до маршрутизатора-відправника або маршрутизатора-отримувача пакетів  $k_r$ -го потоку;

$v_{i,j}^{k_r} \rightarrow 1$ , чим ближче канал зв'язку  $E_{i,j} \in E$  до маршрутизатора-відправника або маршрутизатора-отримувача пакетів  $k_r$ -го потоку;

$v_{i,j}^{k_r} \rightarrow 0$ , чим далі канал зв'язку  $E_{i,j} \in E$  до маршрутизатора-відправника або маршрутизатора-отримувача пакетів  $k_r$ -го потоку ( $k_r \in K_r$ ).

На рис. 4.29 показано, що використання (4.28)–(4.30) в умовах балансування навантаження (4.21) під час реалізації ієрархічно-координаційної маршрутизації дозволило для аналізованої структури мережі (рис. 4.7) значно знизити кількість ітерацій координаційної процедури (до  $1 \div 2$ ), що в середньому від 1,5 до 5 разів менше, ніж без використання виразів (4.28)–(4.30) (рис. 4.28). Максимальна кількість ітерацій, як і в раніше розглянутому випадку (рис. 4.28), спостерігалася у разі граничної завантаженості мережі.

На рис. 4.30 представлений виграш щодо збіжності координаційної процедури (4.16), (4.17) за умови реалізації ієрархічно-координаційної внутрішньодоменої маршрутизації в мережі SDN/MPLS-TE з використанням (4.28)–(4.30) в умовах балансування навантаження (4.21).

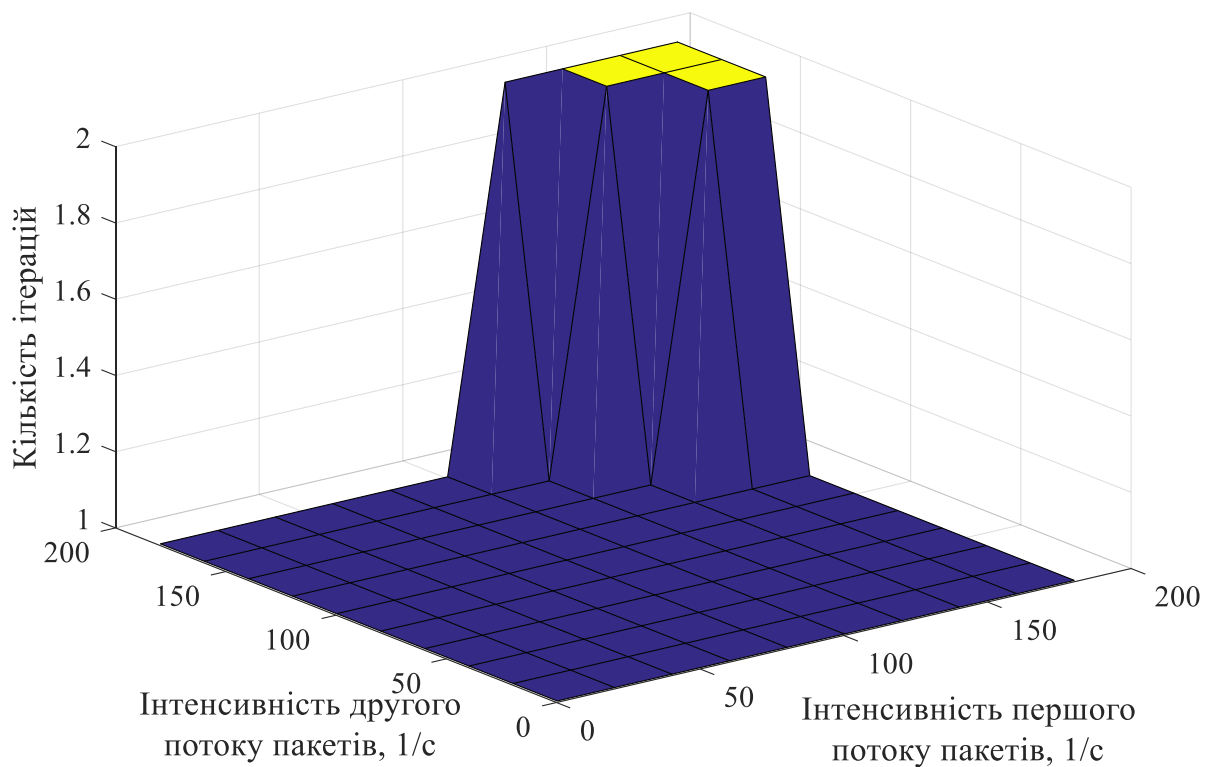


Рис. 4.29. Залежність кількості ітерацій координаційної процедури (4.16), (4.17) за умови ієрархічно-координаційної маршрутизації з балансуванням навантаження в мережі SDN/MPLS-TE від інтенсивностей потоків пакетів з використанням виразів (4.28)–(4.30) в умовах балансування (4.21)

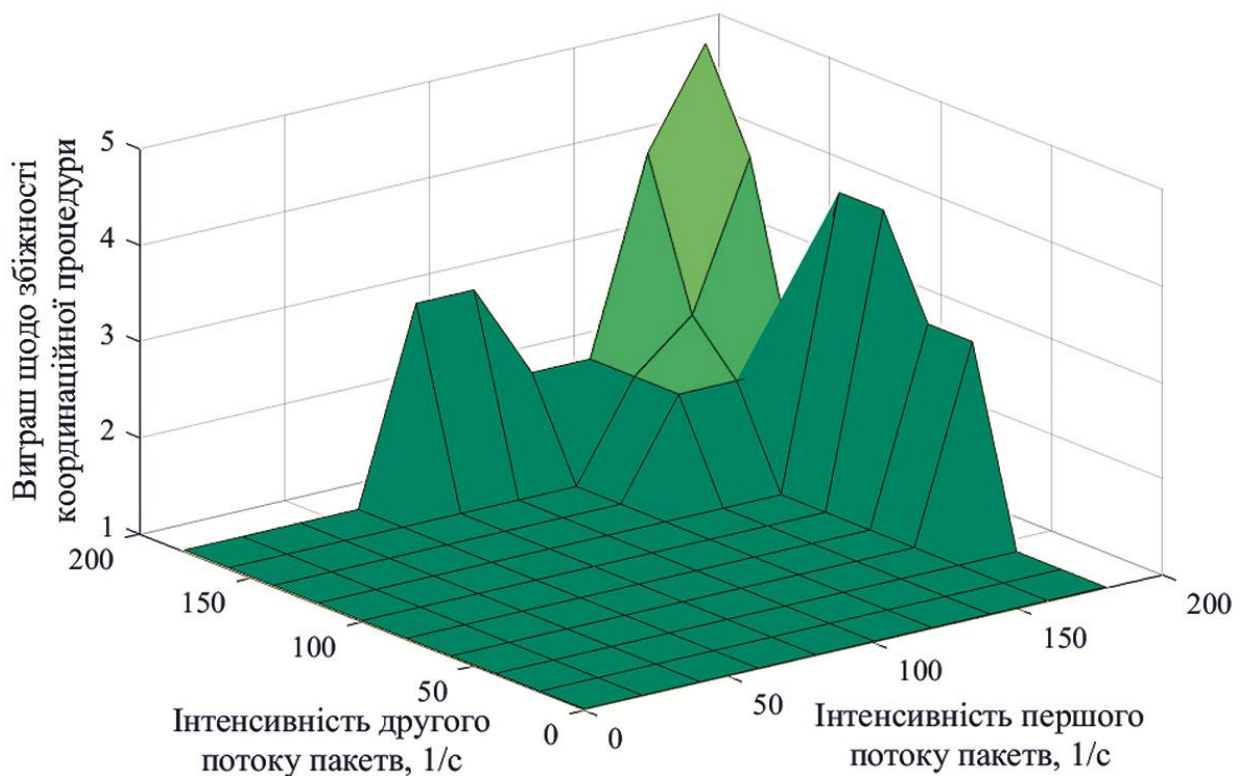


Рис. 4.30. Виграш щодо збіжності координаційної процедури (4.16), (4.17) за умови реалізації ієрархічно-координаційної внутрішньодоменної маршрутизації в мережі SDN/MPLS-TE, структура якої зображена на рис. 4.7

Результати дослідження процесів ієрархічно-координаційної внутрішньодоменної маршрутизації одноадресних потоків, а саме вплив завантаженості мережі на збіжність процедур координації (4.16), (4.17), наведено в табл. 4.2. У цій таблиці відтворено результати розрахунків, коли порівнювалися швидкість збіжності координаційної процедури (4.16), (4.17) з використанням маршрутних метрик (4.12) та ТЕ-критерію (4.24), орієнтованого на забезпечення балансування навантаження в ІКМ.

Таблиця 4.2

**Результати порівняння швидкості збіжності  
координаційної процедури (4.16), (4.17) за умови використання  
різних критеріїв оптимальності розв'язань задачі  
ієрархічно-координаційної внутрішньодоменної маршрутизації**

Інтенсивність першого потoku пакетів, 1/с	Інтенсивність другого потoku пакетів, 1/с	Кількість ітерацій у разі використання критерію (4.12)		Кількість ітерацій у разі використання критерію (4.24)	
		без вико- ристання умов (4.18)	з вико- ристанням умов (4.18)	без вико- ристання умов (4.28)–(4.30)	з вико- ристання умов (4.28)–(4.30)
20	20	1	1	1	1
40	20	1	1	1	1
60	20	1	1	1	1
...	...			...	...
100	100	1	1	1	1
...	...	...	...	...	...
140	160	4	2	1	1
140	180	6	2	4	1
140	200	6	2	4	2
...	...			...	...
200	40	2	2	1	1
200	60	2	2	1	1
200	80	2	2	3	1
200	100	2	2	3	1
...	...			...	...
200	160	9	2	8	2
200	180	12	2	8	2
200	200	13	2	10	2

Результати дослідження показали, що мережа може впоратися з максимальним навантаженням 400 л/с, тобто коли кожен потік мав інтенсивність, яка дорівнювала 200 л/с. З табл. 4.2 видно, що за умови завантаженості мережі меншої ніж на 60% у процесі реалізації ієрархічної внутрішньодоменної маршрутизації координація рішень приграничних маршрутизаторів не відбувалася, оскільки їх розподілені дії не призводили до перевантаження каналів зв'язку мережі. У подальшому зростанні завантаженості мережі розподілений характер рішень, отриманих на кожному з приграничних маршрутизаторів, неминуче спричиняв перевантаження каналів зв'язку та викликав необхідність координації цих рішень SDN-контролером верхнього рівня ієрархії.

Використання ТЕ-критерію оптимальності (4.24) та виразів (4.28)–(4.30) дозволяє знизити кількість ітерацій координаційної процедури (4.16), (4.17) від 1,5–2 до 3,5–5 разів, а в низці випадків і до 8 разів. Це на практиці призводить до пропорційного зниження часу розв'язання маршрутних задач та обсягів службового трафіку, що циркулює в мережі SDN/MPLS-TE. Особливо це характерно для розмірних мереж в умовах їх високої завантаженості, що і визначає ділянку переважного використання запропонованих рішень на практиці шляхом заміни наявних або впровадження нових протоколів маршрутизації в мережах SDN/MPLS та SDN/MPLS-TE.

#### **4.2.6. Дослідження процесів ієрархічно-координаційної внутрішньодоменної маршрутизації багатоадресних потоків в інфокомунікаційній мережі SDN/MPLS-TE**

Проведено аналіз процесу збіжності рішень ієрархічно-координаційної внутрішньодоменної маршрутизації до оптимальних рішень, але вже для передачі пакетів багатоадресних потоків. Дослідження стосувалося випадків використання двох критеріїв оптимальності: (4.12) та (4.24), а також охоплювало різні мережні структури з варійованою кількістю вузлів (маршрутизаторів) і каналів зв'язку. Для прикладу розглянемо структуру ІКМ, представлену на рис. 4.31. Мережа містить п'ять вузлів ( $R_1 \div R_5$ ) та сім каналів зв'язку, у розривах яких вказана їх пропускна здатність (л/с).

Кількість потоків та їх характеристики, які є вихідними даними для розрахунків, наведено в табл. 4.3.

У використанні критерію оптимальності (4.12) з  $h_{i,j}^r = 10^7 / \varphi_{i,j}$  на нульовій ітерації, тобто до початку роботи координаційної процедури,



дерево маршрутів для першого потоку представлено на рис. 4.32. У цьому випадку в розривах каналів зв'язку показано дріб, де в чисельнику наведено інтенсивність першого багатоадресного потоку пакетів, а в знаменнику – пропускна здатність цього каналу зв'язку. На рис. 4.33 вказані ті самі дані розрахунків, але для другого багатоадресного потоку пакетів. На рис. 4.34 представлено розв'язання задачі багатоадресної маршрутизації одночасно для двох потоків, яке відповідає нульовій ітерації, тобто до початку роботи координаційної процедури (4.16), (4.17). Зокрема на рис. 4.34 в розривах каналів зв'язку (зверху вниз) представлені такі дані: сумарна інтенсивність двох потоків (1/с), пропускна здатність каналу зв'язку.

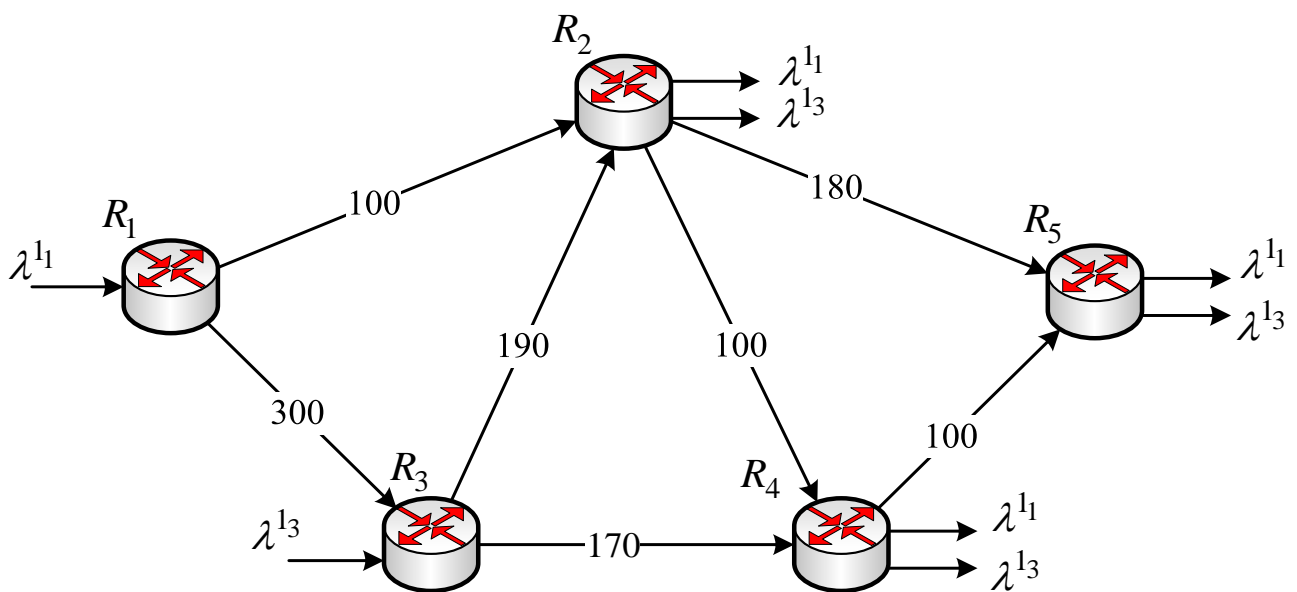


Рис. 4.31. Перша структура ІКМ, яка досліджувалася для багатоадресного випадку

Таблиця 4.3

### Характеристики багатоадресних потоків

№ потоку	Інтенсивність потоку, 1/с	Вузол-відправник	Вузли-отримувачі
1	$\lambda^{11} = 100$	$R_1$	$R_2, R_4, R_5$
2	$\lambda^{13} = 100$	$R_3$	$R_2, R_4, R_5$

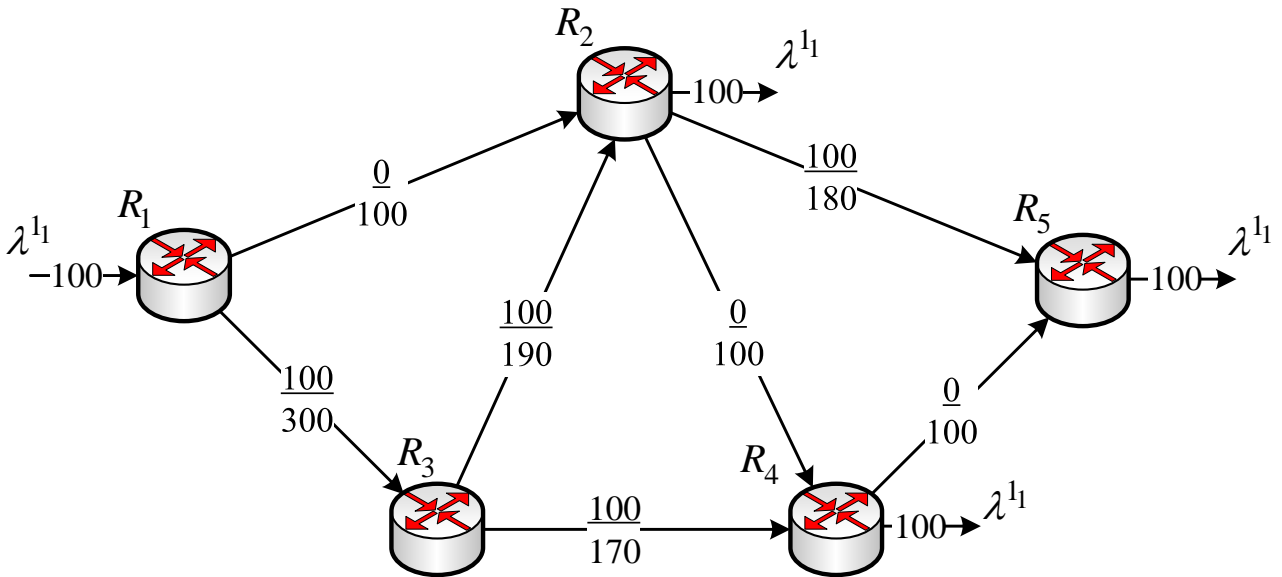


Рис. 4.32. Дерево маршрутів для першого потоку пакетів, розраховане на нульовій ітерації (до початку роботи координаційної процедури)

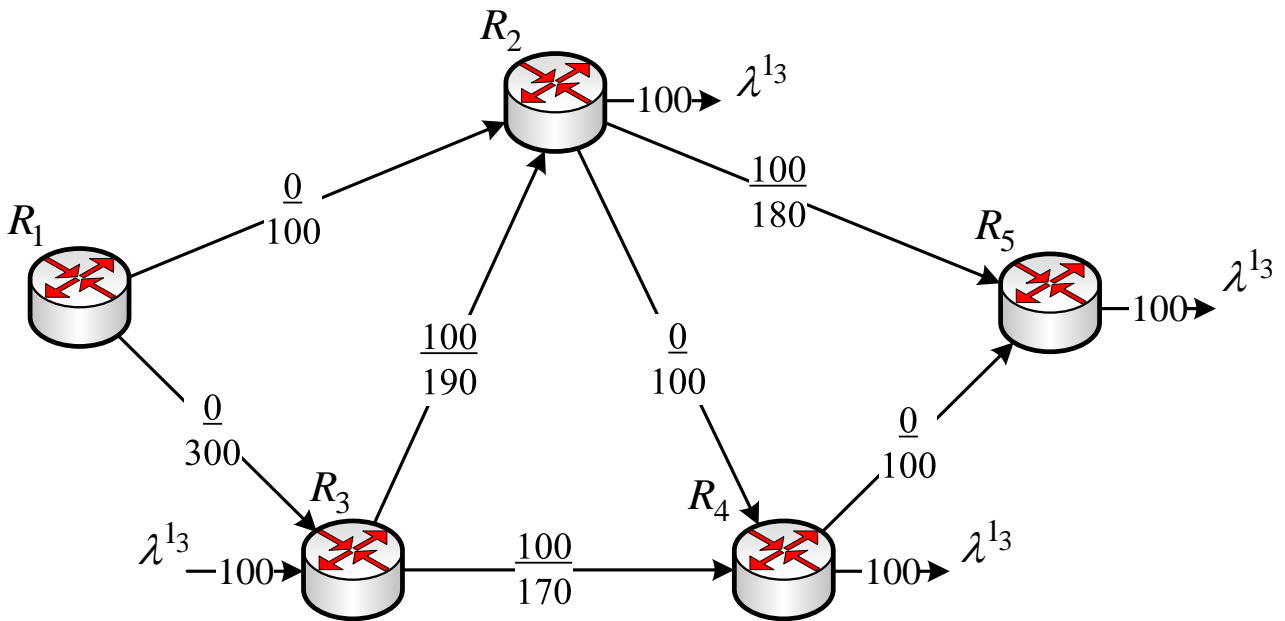


Рис. 4.33. Дерево маршрутів для другого потоку пакетів, розраховане на нульовій ітерації (до початку роботи координаційної процедури)

Як видно з рис. 4.34, через неузгодженість рішень, які було отримано на першому та п'ятому вузлах-відправниках, відбувається перевантаження трьох каналів зв'язку: між маршрутизаторами  $R_3$  та  $R_2$ ,  $R_3$  та  $R_4$ ,  $R_2$  та  $R_5$ . Для запобігання перевантаження цих каналів зв'язку і мережі загалом

відповідно до виразів (4.13)–(4.17) відбувається координація маршрутних рішень на верхньому рівні ієрархії. Для цієї структури (рис. 4.31) уже після першої координаційної ітерації (4.16), (4.17) у межах багатоадресної маршрутизації двох розглянутих потоків перевантаженню мережі вдалося запобігти: на рис. 4.35 та 4.36 зображено порядок маршрутизації відповідно першого та другого багатоадресних потоків (за аналогією до рис. 4.32 та 4.64), а на рис. 4.37 (за аналогією до рис. 4.34) представлено остаточне розв’язання задачі багатоадресної маршрутизації одночасно для двох потоків.

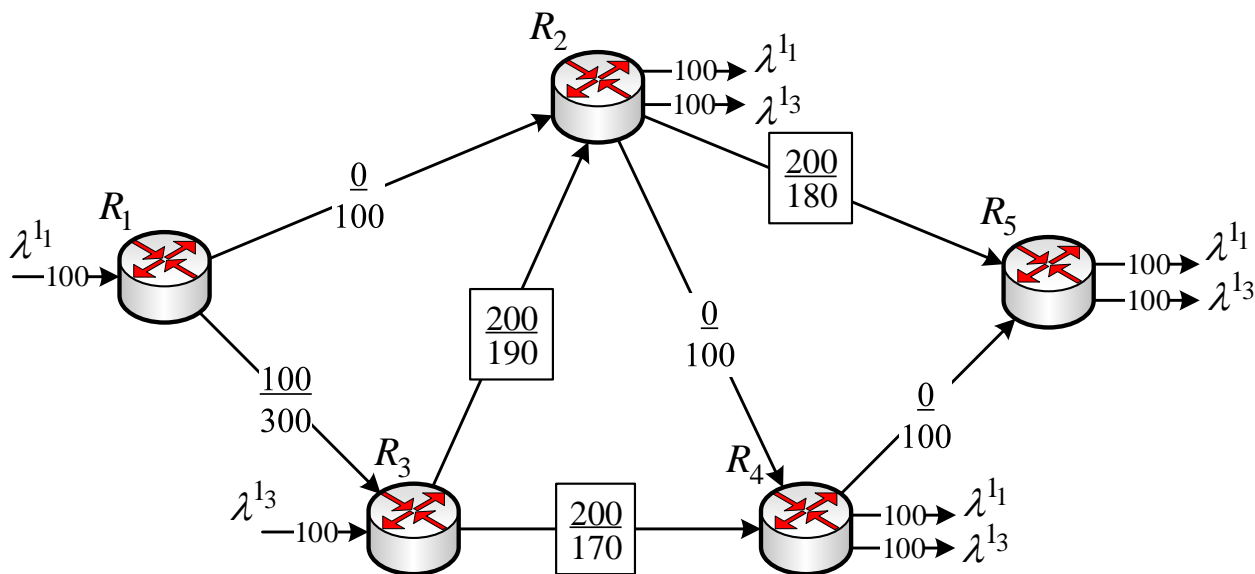


Рис. 4.34. Розв’язання задачі багатоадресної маршрутизації одночасно для двох потоків до початку роботи координаційної процедури

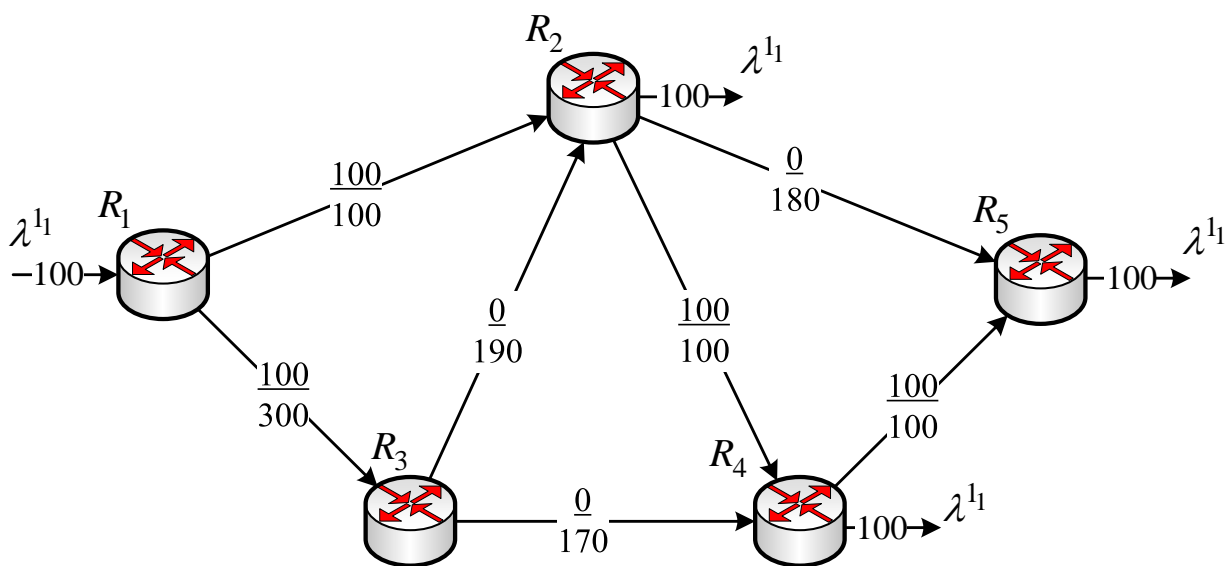


Рис. 4.35. Дерево маршрутів для першого потоку пакетів

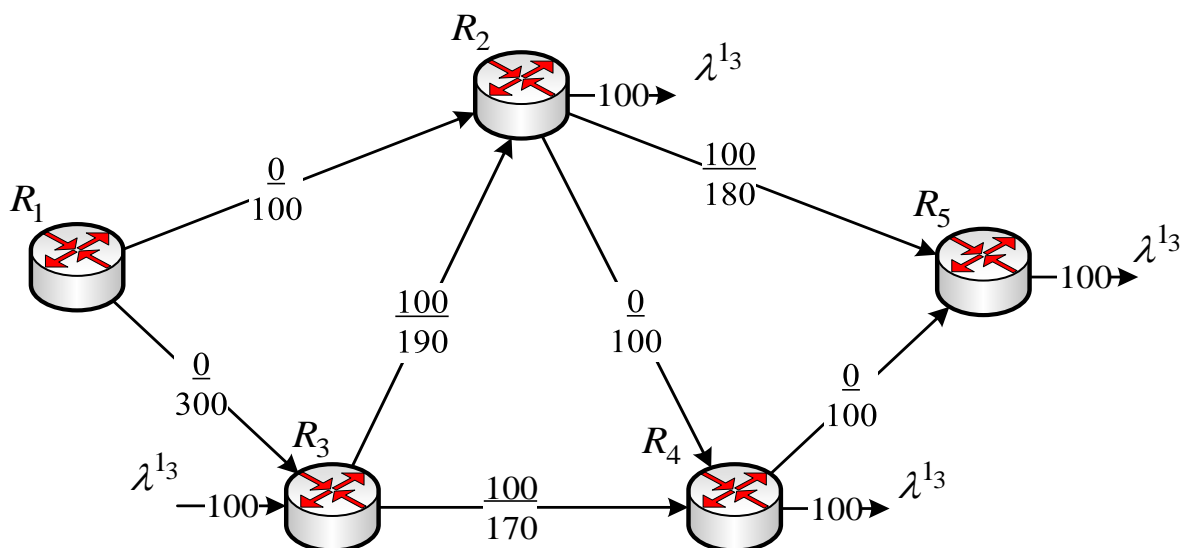


Рис. 4.36. Дерево маршрутів для другого потоку пакетів

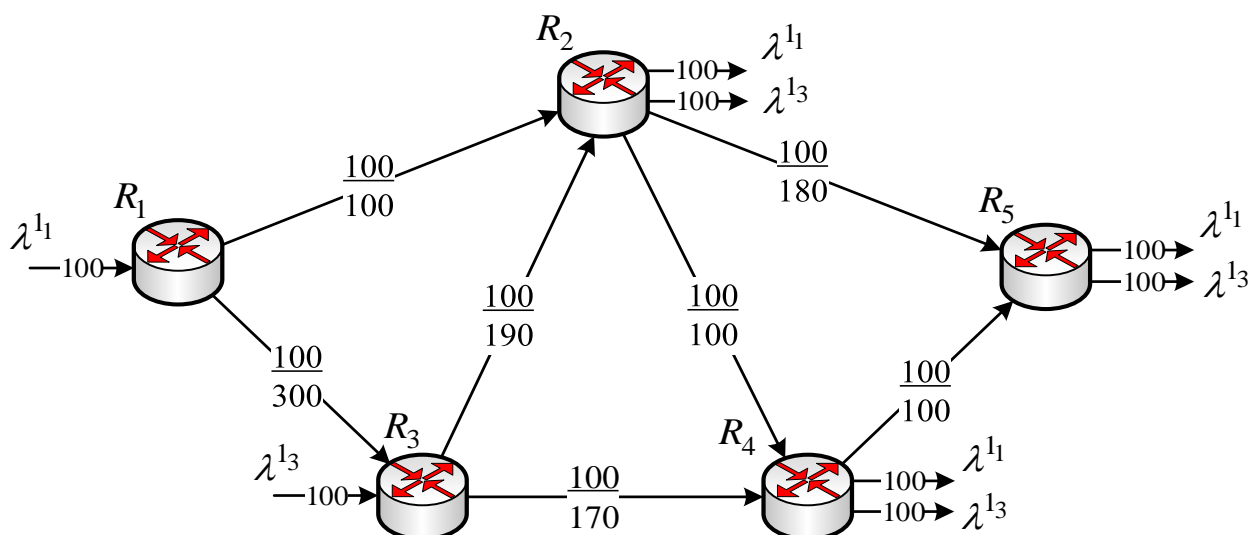


Рис. 4.37. Кінцеве розв'язання задачі багатоадресної маршрутизації одночасно для двох потоків

Однак, за результатами дослідження [53–56], збіжність до оптимального рішення за одну координаційну ітерацію – це швидше виняток, характерний для цього випадку, ніж правило. Традиційно на збіжність ієрархічних методів маршрутизації впливають розмірність і зв'язність вузлів мережі, завантаженість каналів зв'язку, кількість та інтенсивності потоків. Розглянемо, як буде впливати розмірність мережі на збіжність координаційної процедури (4.16), (4.17) у розв'язанні задачі багатоадресної маршрутизації. Використаємо варіант мережі, структура якої представлена на рис. 4.38. Мережа складається з шести маршрутизаторів ( $R_1 \div R_6$ ) та дев'яти каналів зв'язку, у розривах яких

указана їх пропускна здатність (1/с). Кількість потоків та їх характеристики, які були вихідними даними для розрахунків, наведені в табл. 4.4.

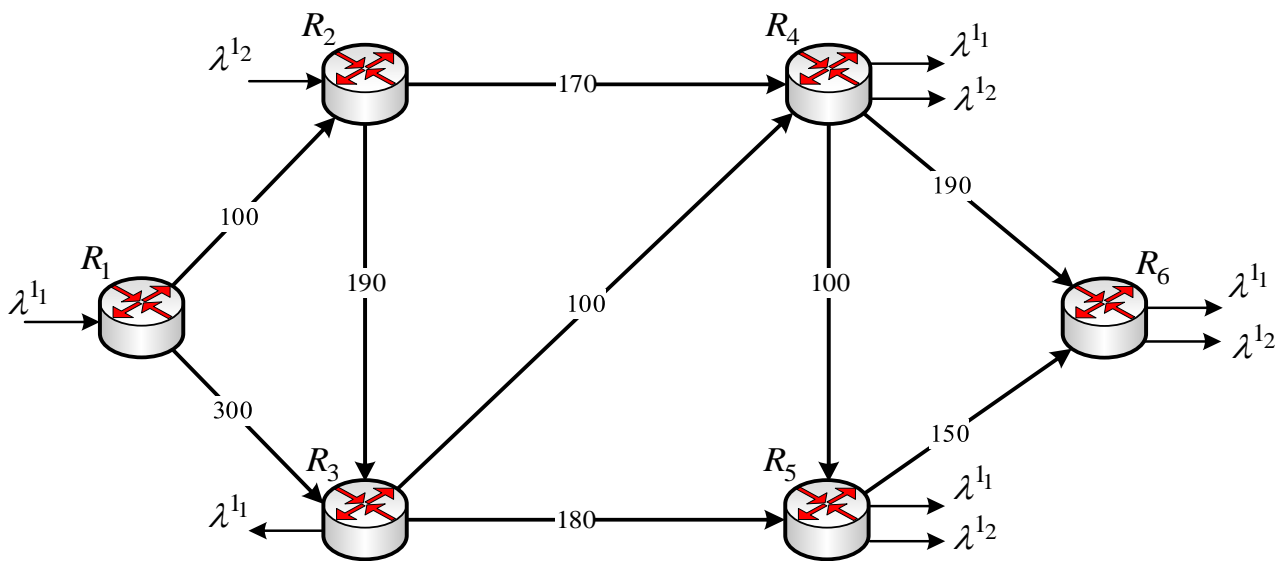


Рис. 4.38. Друга структура мережі, яка була використана для дослідження процесів ієрархічно-координаційної маршрутизації багатоадресних потоків у мережі SDN/MPLS

Таблиця 4.4

### Характеристики багатоадресних потоків

№ потоку	Інтенсивність потоку, 1/с	Вузол-відправник	Вузли-отримувачі
1	$\lambda^1 = 10 \div 100$	$R_1$	$R_3, R_4, R_5, R_6$
2	$\lambda^2 = 10 \div 100$	$R_2$	$R_4, R_5, R_6$

Під час дослідження було проведено аналіз впливу завантаженості каналів зв'язку та ІКМ загалом на кількість ітерацій координаційної процедури (4.16), (4.17). Інтенсивність потоків змінювалася з кроком п'ять пакетів за секунду (1/с) від 10 до 100 1/с. Тоді загальна кількість прорахованих варіантів вихідних даних щодо завантаженості мережі становила 200. Результати аналізу збіжності координаційної процедури (4.16), (4.17) за різних умов використання критеріїв оптимальності (4.12) і (4.24) розв'язань задачі ієрархічно-координаційної внутрішньодоменної маршрутизації багатоадресних потоків наведено в табл. 4.5.

Результати моделювання показали, що мережа може впоратися з максимальним навантаженням 200 1/с, тобто коли кожен потік мав інтенсивність 100 1/с. З табл. 4.5 видно, що в разі завантаженості мережі менш ніж на 70–75% приграничні маршрутизатори забезпечували розрахунок

маршрутів від відправників до отримувачів, не перевантажуючи канали зв'язку мережі, тобто в цьому випадку координація їх рішень не була потрібна.

Таблиця 4.5

**Результати дослідження процесів  
ієрархічно-координаційної внутрішньодоменної  
маршрутизації багатоадресних потоків**

Інтенсивність першого потоку пакетів, 1/с	Інтенсивність другого потоку пакетів, 1/с	Кількість ітерацій у разі використання критерію оптимальності (4.12)	
		без використання умов (4.18)	з використанням умов (4.18)
20	20	1	1
40	20	1	1
...	...	...	...
55	20	1	1
...	...	...	...
100	50	1	1
100	55	1	1
100	60	1	1
...	...	...	...
80	95	2	2
85	95	2	2
90	95	3	2
95	95	3	2
95	100	3	3
100	100	3	3

У подальшому зростанні завантаженості мережі розподілений характер рішень, які було отримано від кожного приграничного маршрутизатора, неодмінно спричиняв перевантаження каналів зв'язку. Для запобігання перевантаження каналів зв'язку та мережі загалом на верхньому рівні ієрархії відбувалася координація отриманих з нижнього рівня рішень під час розрахунку множників Лагранжа (4.16), які у вигляді штрафних коефіцієнтів спускалися на нижній рівень, ініціюючи новий перерахунок маршрутних змінних. Таким чином, процес координації набував ітераційного характеру, а кількість таких ітерацій із зростанням завантаженості мережі також збільшувалася. Максимальна кількість координаційних ітерацій для розглянутого прикладу становила 11 і спостерігалася за умови інтенсивності кожного з потоків пакетів 100 1/с. Розглянемо докладніше процес координації рішень багатоадресної маршрутизації для цього (двохсотого) варіанта вихідних даних (табл. 4.5).

На рис. 4.39 представлено дерево маршрутів до початку роботи координаційної процедури для першого багатоадресного потоку. У розривах каналів зв'язку показано дріб, де в чисельнику наведена інтенсивність першого потоку пакетів, а в знаменнику – пропускна здатність даного зв'язку. На рис. 4.40 ті самі дані зображені для другого багатоадресного потоку.

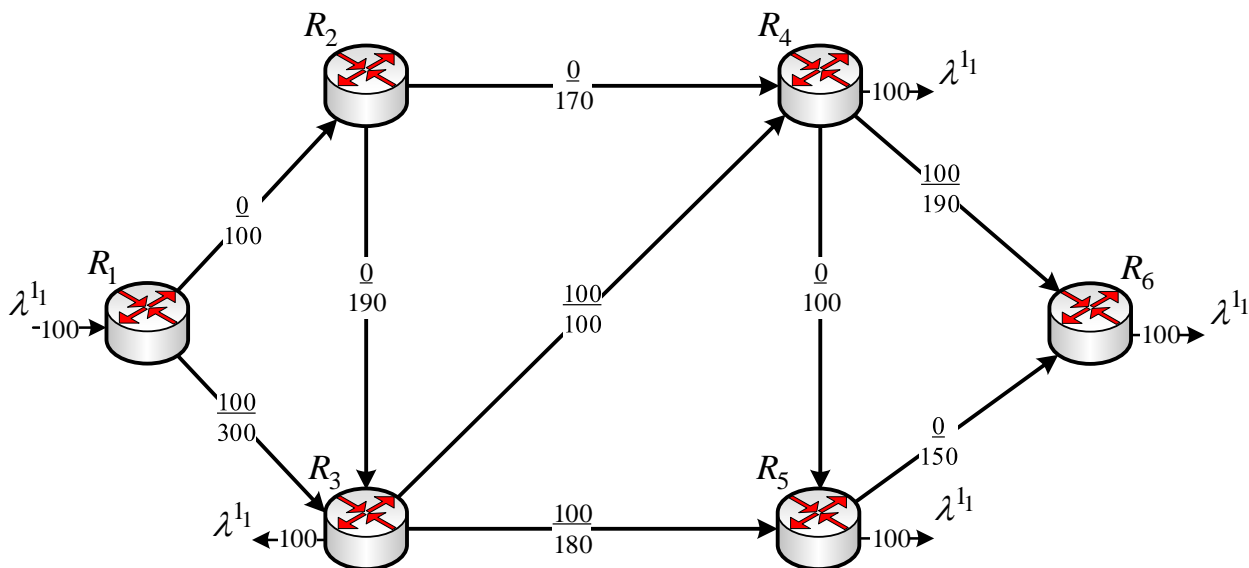


Рис. 4.39. Дерево маршрутів до початку роботи координаційної процедури для першого багатоадресного потоку

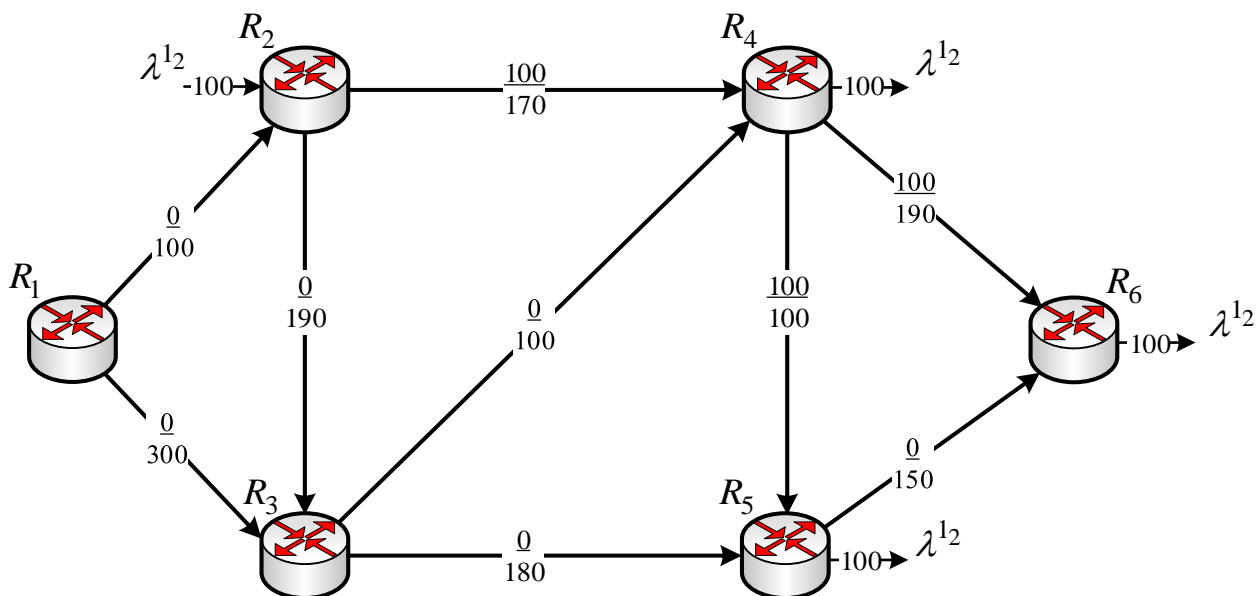


Рис. 4.40. Дерево маршрутів до початку роботи координаційної процедури для другого багатоадресного потоку

На рис. 4.41 представлено роз'язання задачі багатоадресної маршрутизації для двох розглянутих потоків після першої координаційної ітерації. У розривах каналів зв'язку показано дріб, де в чисельнику наведено

сумарну інтенсивність двох багатоадресних потоків пакетів, а в знаменнику – пропускна здатність каналу зв'язку.

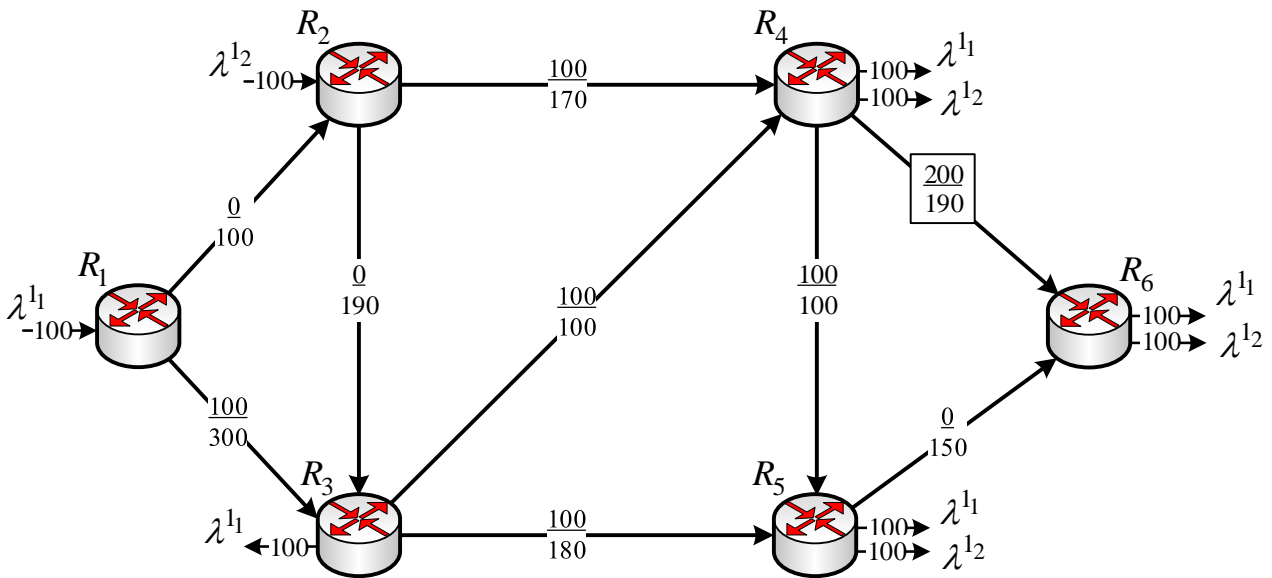


Рис. 4.41. Розв'язання задачі багатоадресної маршрутизації для двох розглянутих потоків до початку роботи координаційної процедури

Як видно з рис. 4.41, після першої ітерації спостерігається перевантаження каналу зв'язку між маршрутизаторами  $R_4$  та  $R_6$  через неузгоджену (децентралізовану) роботу приграничних вузлів-відправників. Після п'ятої координаційної ітерації порядок маршрутизації першого і другого багатоадресних потоків показано на рис. 4.42 та 4.43 відповідно, позначення на яких аналогічні до рис. 4.39 та 4.40.

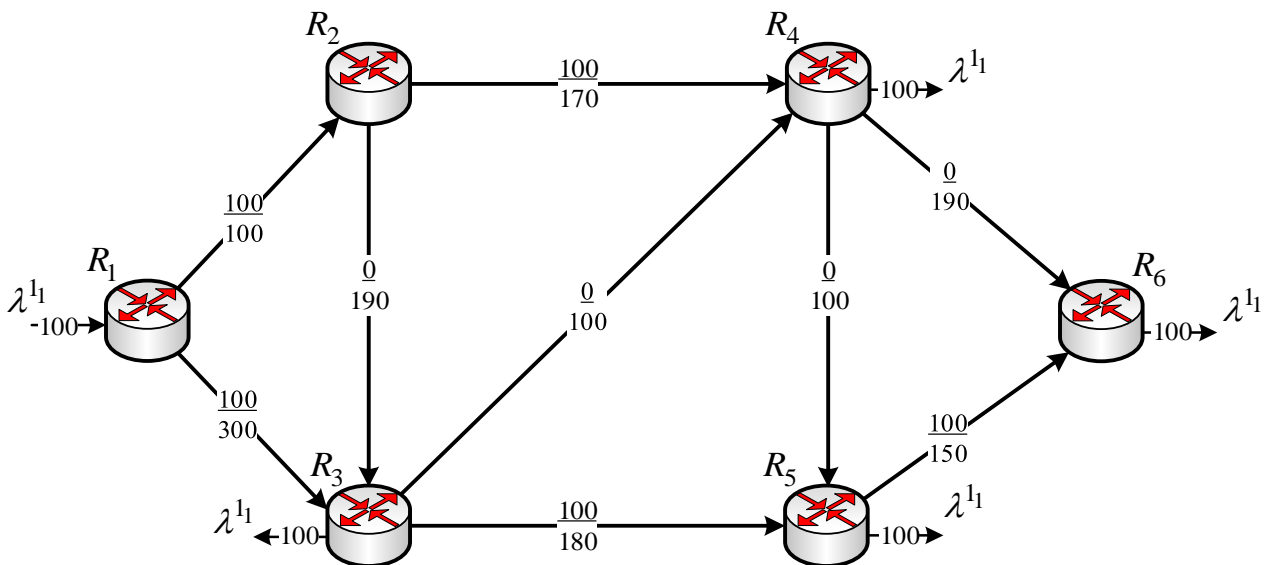


Рис. 4.42. Порядок маршрутизації першого багатоадресного потоку після другої координаційної ітерації



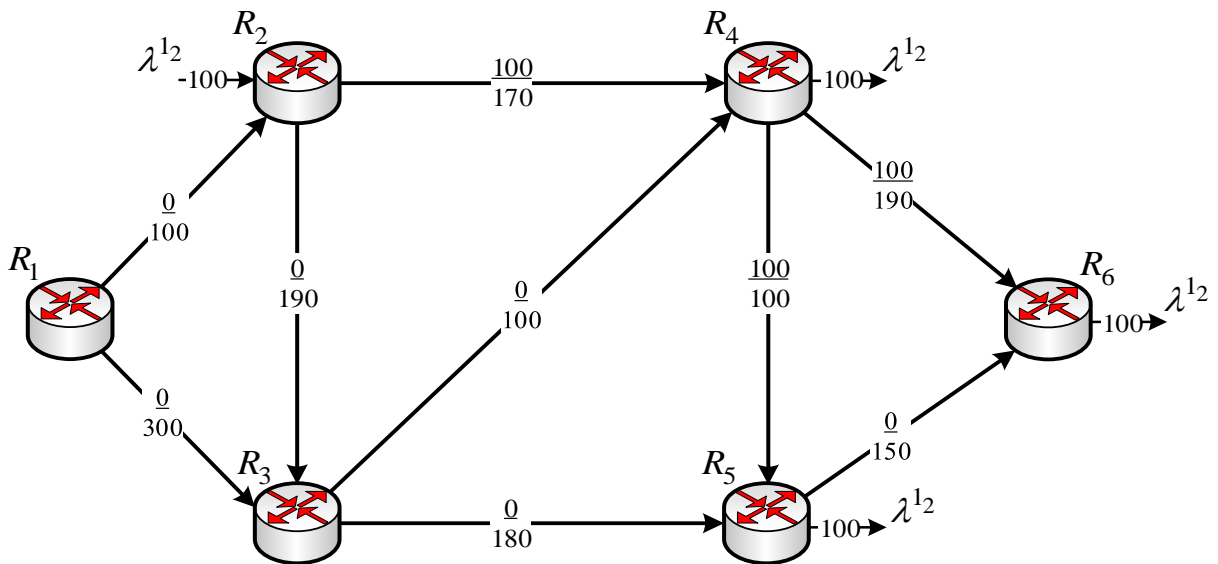


Рис. 4.43. Порядок маршрутизації другого багатоадресного потоку після другої координаційної ітерації

На рис. 4.44 представлено розв'язання задачі багатоадресної маршрутизації для двох потоків після другої ітерації. У розривах каналів зв'язку показано (як і на рис. 4.41) дріб, де в чисельнику наведено сумарну інтенсивність потоків пакетів, а в знаменнику – пропускну здатність каналу зв'язку. Після другої координаційної ітерації вдалося запобігти перевантаженню проблемного каналу зв'язку між маршрутизаторами  $R_4$  та  $R_6$  (рис. 4.41), однак виникло перевантаження іншого каналу – уже між маршрутизаторами  $R_2$  та  $R_4$  (рис. 4.44).

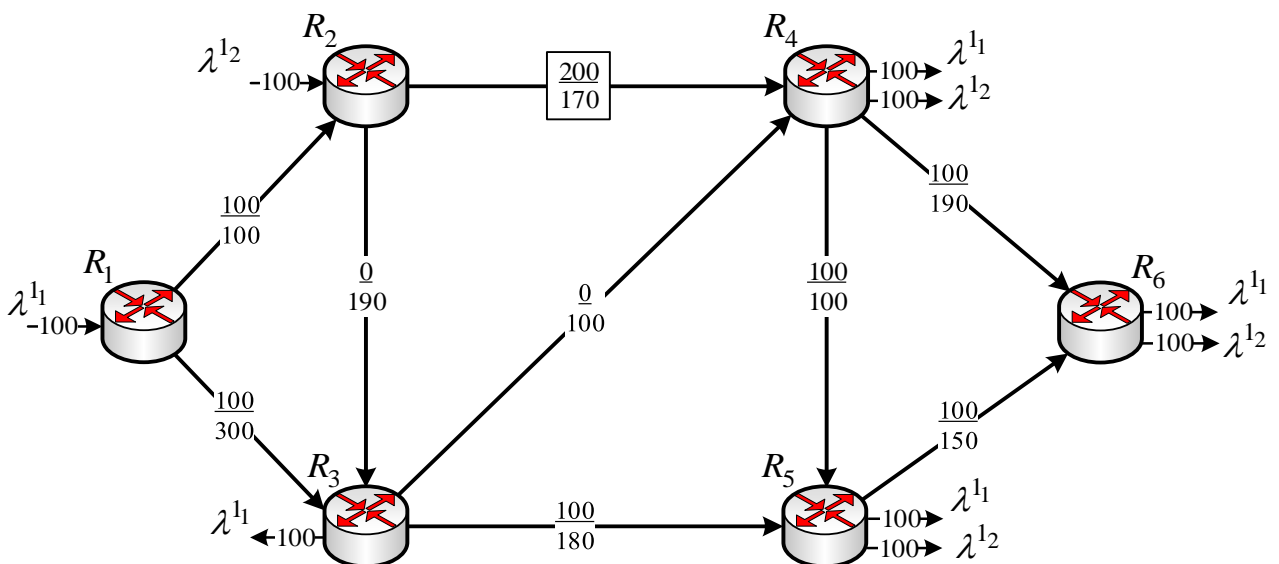


Рис. 4.44. Розв'язання задачі багатоадресної маршрутизації для двох потоків після другої координаційної ітерації

На рис. 4.45 та 4.46 (за аналогією до рис. 4.39 і 4.40) показані дерева маршрутів відповідно для першого і другого багатоадресних потоків після завершення координації, тобто після третьої координаційної ітерації.

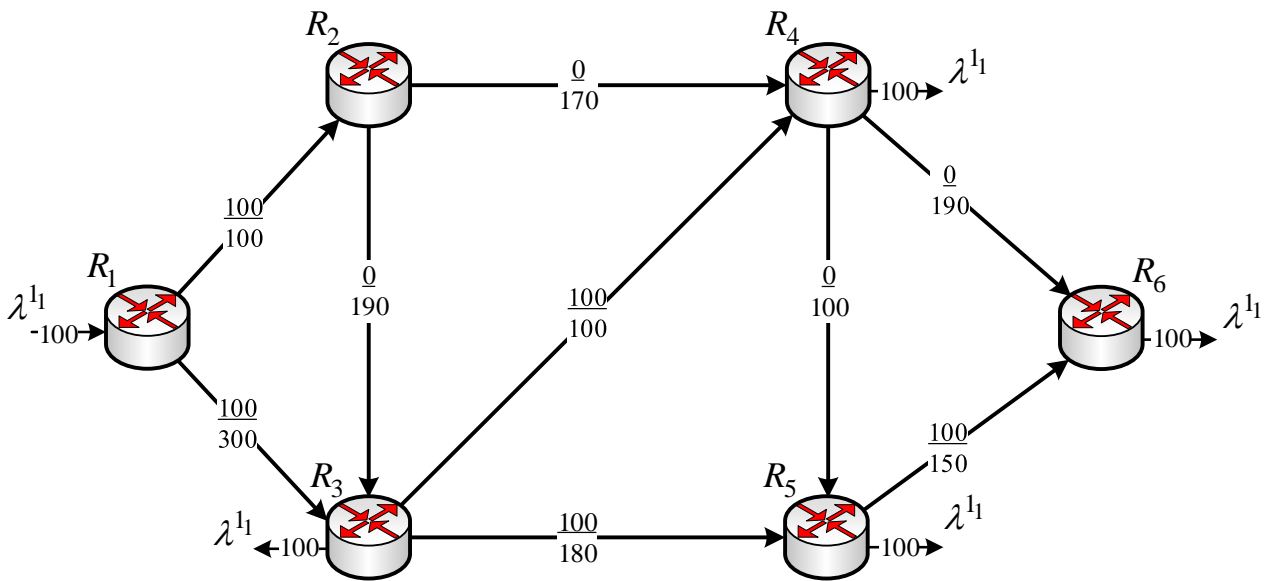


Рис. 4.45. Дерево маршрутів для першого багатоадресного потоку після завершення координації (після третьої координаційної ітерації)

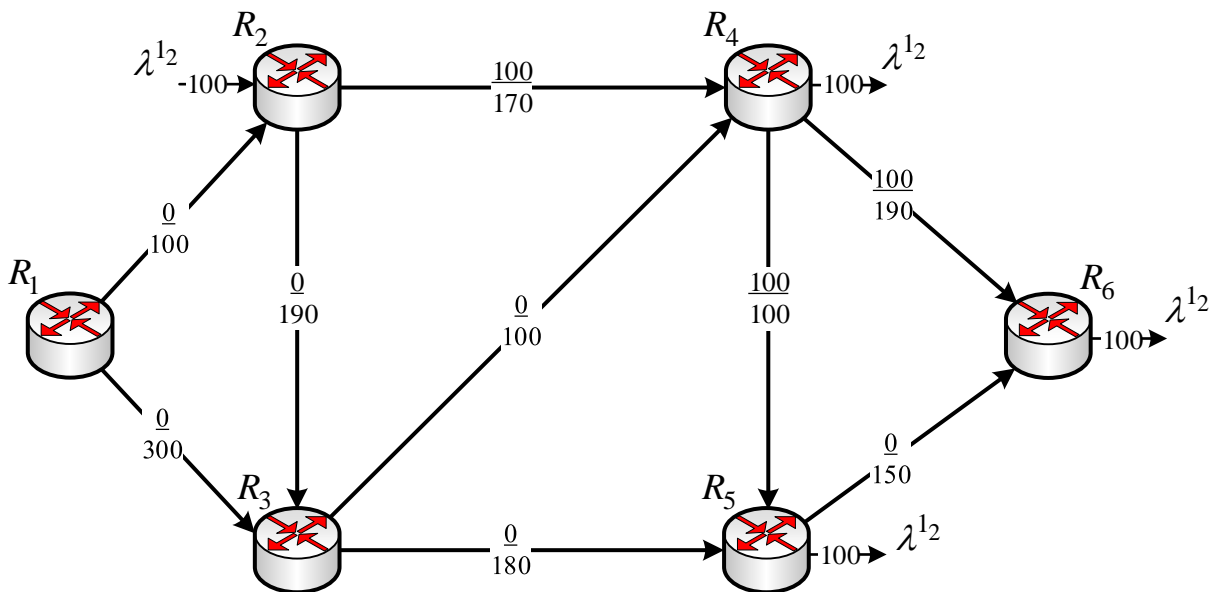


Рис. 4.46. Дерево маршрутів для другого багатоадресного потоку після завершення координації (після третьої координаційної ітерації)

На рис. 4.47 представлено остаточне (скоординоване) розв'язання задачі ієрархічно-координаційної внутрішньодоменної маршрутизації для варіанта, коли інтенсивність кожного багатоадресного потоку пакетів становила 100 1/с.

У розривах каналів зв'язку показано дріб, де в чисельнику наведена сумарна інтенсивність двох багатоадресних потоків пакетів, а в знаменнику – пропускна здатність каналу зв'язку.

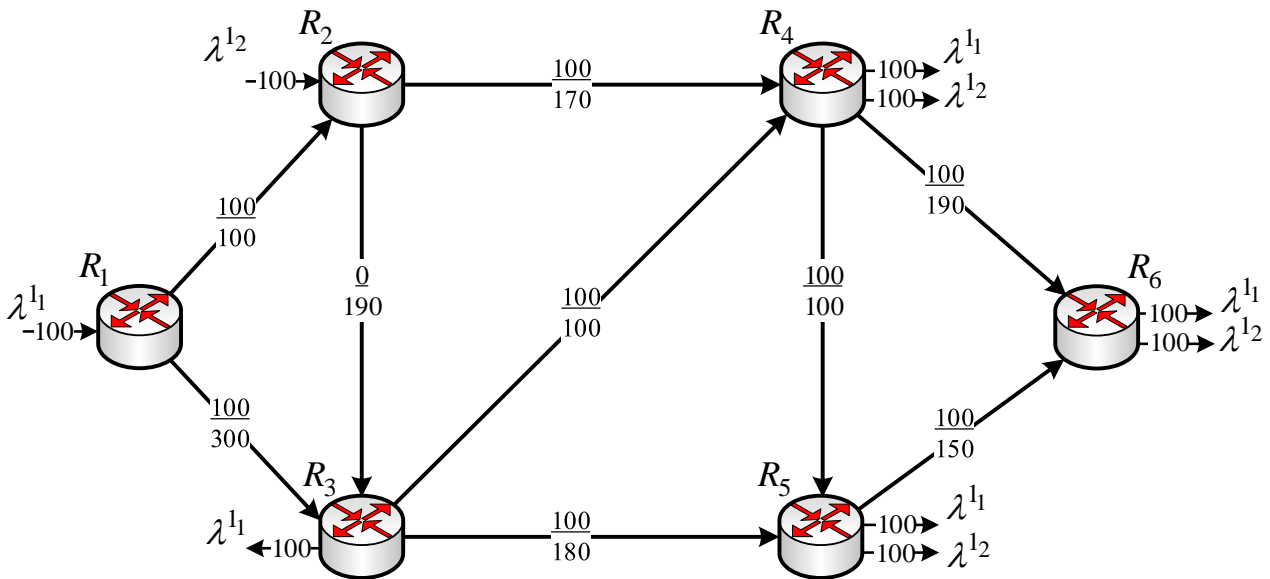


Рис. 4.47. Остаточне розв'язання задачі багатоадресної маршрутизації для варіанта, коли інтенсивність кожного потоку пакетів становила 100 1/с

Як і в попередньому випадку (табл. 4.2), використання запропонованих умов (4.18), (4.30)–(4.32) та ТЕ-критерію оптимальності маршрутних рішень також дозволило зменшити кількість ітерацій координаційної процедури (4.16), (4.17) у середньому в 1,5–2 рази (табл. 4.5), що особливо характерно за умови високої завантаженості мережі SDN/MPLS.

#### 4.2.7. Структура методу ієрархічно-координаційної внутрішньодоменної маршрутизації в інфокомунікаційній мережі SDN/MPLS

Ґрунтуючись на запропонованій у пункті 4.2.2 декомпозиційній моделі маршрутизації та результатах, проведених у пунктах 4.2.3–4.2.4 досліджень, пропонується метод ієрархічно-координаційної внутрішньодоменної маршрутизації в ІКМ SDN/MPLS, який містить етапи функціонування, наведені в рис. 4.48.

**Етап 1. Збір та аналіз вихідних даних.** Це стосується інформації про топологію MPLS-мережі, кількість приграничних маршрутизаторів, пропускні здатності каналів зв'язку та характеристики потоків.

**Етап 2. Розв'язання задач нижнього ієрархічного рівня.** Розрахунок на кожному з приграничних LER-маршрутизаторів векторів маршрутних змінних  $\vec{x}_r$ , що відбувається під час розв'язання відповідних оптимізаційних

задач (табл. 4.6). Забезпечення врахування виразів (4.18) або (4.28)–(4.30) для підвищення швидкості збіжності координаційної процедури (4.16), (4.17) на верхньому рівні ієрархії. Передача з кожного приграничного маршрутизатора розрахованих маршрутних векторів  $\vec{x}_r$  на SDN-контролер верхнього рівня для проведення подальшої координації.

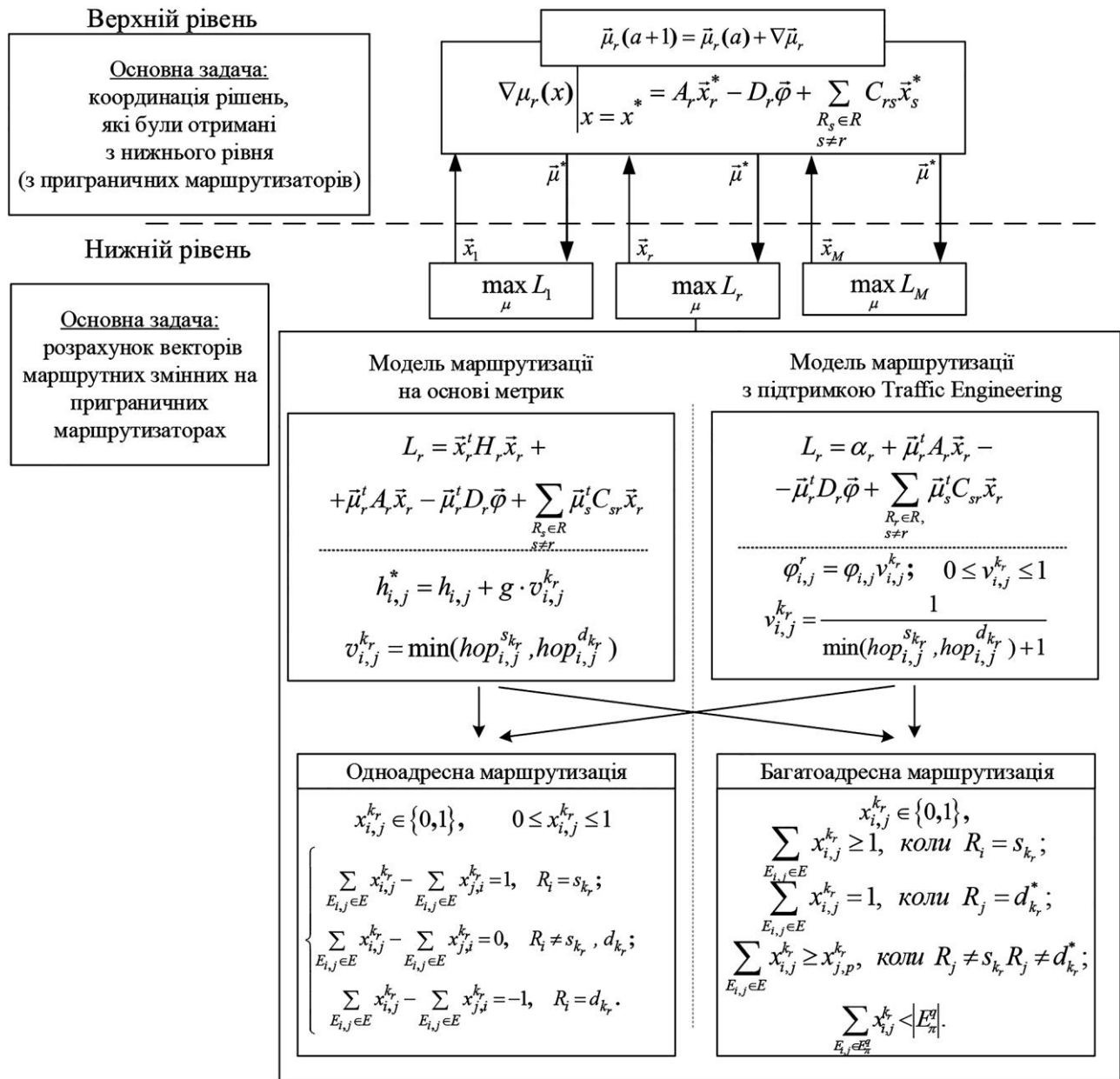


Рис. 4.48. Структура методу ієрархічно-координаційної внутрішньодоменної маршрутизації в ICM SDN/MPLS

**Характеристика оптимізаційних задач нижнього рівня  
запропонованого методу внутрішньодоменної маршрутизації**

Стратегія маршрутизації		Критерій оптимальності	Обмеження	Тип оптимізаційної задачі	
ОАМ	ОШМ	На основі маршрутних метрик	(4.12)	(4.2), (4.4), (4.9), (4.10)	ЗЦНП
		Traffic Engineering	(4.24)	(4.2), (4.4), (4.9), (4.19)–(4.23)	ЗЦЛП
	БШМ	На основі маршрутних метрик	(4.12)	(4.3), (4.4), (4.9), (4.10)	КП
		Traffic Engineering	(4.24)	(4.3), (4.4), (4.9), (4.19)–(4.23)	ЛП
БАМ	ОШМ	На основі маршрутних метрик	(4.12)	(4.2), (4.5)–(4.8), (4.9), (4.10)	ЗЦНП
		Traffic Engineering	(4.24)	(4.2), (4.5)–(4.8), (4.9), (4.19)–(4.23)	ЗЦЛП

ОАМ – одноадресна маршрутизація; БАМ – багатоадресна маршрутизація; ОШМ – одношляхова маршрутизація; БШМ – багатошляхова маршрутизація; ЛП – лінійне програмування; ЗЦЛП – змішане цілочисельне ЛП; КП – квадратичне програмування; ЗЦНП – змішане цілочисельне нелінійне програмування.

**Етап 3.** *Перевірка виконання умов запобігання перевантаження каналів зв'язку та координація маршрутних рішень на верхньому ієрархічному рівні.* У разі недотримання умов (4.11) на SDN-контролері виконується координаційна процедура (4.16), (4.17) для запобігання перевантаження каналів зв'язку MPLS-мережі на основі аналізу змісту маршрутних векторів  $\vec{x}_r$ . Формування векторів множників Лагранжа  $\vec{\mu}_r$  та передача їх на нижній ієрархічний рівень для модифікації лагранжіанів (4.15) або (4.27).

Якщо умови щодо запобігання перевантаження каналів зв'язку (4.11) виконуються, то процес координації завершується, а актуальні маршрутні вектори  $\vec{x}_r$  реалізуються в MPLS-мережі шляхом формування таблиць комутації за позначками на приграничних (LER) та транзитних маршрутизаторах (LSR) за допомогою сигнальних протоколів, наприклад, LDP (Label Distribution Protocol) або RSVP-TE (Resource ReServation Protocol TE).

Запропоноване рішення відповідає архітектурі SDN, наведеній на рис. 4.1, б, коли SDN-контролери завантажуються мінімально. У цьому випадку на них покладаються лише задачі щодо координації маршрутних рішень, отриманих на приграничних маршрутизаторах MPLS-мережі. Проте цей метод може бути адаптований і під SDN-архітектуру, наведену на рис. 4.1, в, коли задачі ієрархічних рівнів розв'язуються на SDN-контролері. Зокрема за розрахунок векторів маршрутних змінних  $\bar{x}_r$ , під час розв'язання відповідних оптимізаційних задач (4.15) або (4.27) можуть відповідати окремі процесори (ядра) обчислювальної системи SDN-контролера. Використання багатопроцесорних (багатоядерних) архітектур маршрутизаторів [66–67] з розпаралелюванням розрахунків сприяє підвищенню обчислювальної потужності SDN-контролера та масштабованості SDN-архітектури загалом.

### 4.3. Синтез і дослідження математичної моделі та методу ієрархічно-координаційної міждоменної маршрутизації в програмно-конфігурованій ІКМ

#### 4.3.1. Декомпозиційна модель міждоменної маршрутизації в програмно-конфігурованій ІКМ, що складається з множини послідовно з'єднаних доменів

Нехай структура ІКМ буде представлена у вигляді орієнтованого графа

$$G = (R, E), \quad (4.31)$$

де  $R$  – це множина вершин, що моделює маршрутизатори, а  $E$  – множина дуг графа, яка описує канали зв'язку мережі.

Позначимо через  $K$  множину потоків, що циркулюють у мережі, тоді  $|K| = \tilde{K}$  – потужність множини, що кількісно характеризує загальне число потоків в ІКМ. Для кожного  $k$ -го потоку ( $k \in K$ ) вважається відомою його середня швидкість пакетів (інтенсивність) –  $\lambda^k$ , яка вимірюється в пакетах за секунду (1/с).

У ході синтезу декомпозиційної моделі міждоменної маршрутизації припустимо, що ІКМ складається з  $N$  взаємопов'язаних між собою підмереж – доменів. Тоді нехай кожен окремий  $p$ -й домен в ІКМ описується за допомогою підграфа  $G^p = (R^p, E^p)$  графа  $G$ , де  $R^p = \{R_i^p; i = \overline{1, m_p}\}$  – множина маршрутизаторів  $p$ -го домену, а  $m_p$  – їх загальна кількість у домені;

$E^P = \{E_{i,j}^P; i, j = \overline{1, m_p}, i \neq j\}$  – це множина каналів, що з'єднують маршрутизатори  $p$ -го домену (рис. 4.49).

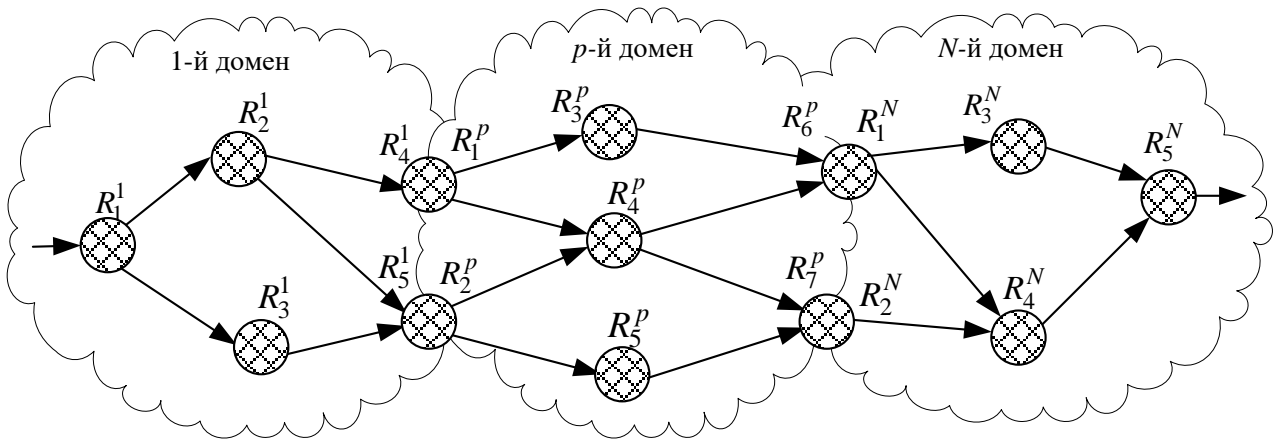


Рис. 4.49. Подання структури ІКМ, що містить декілька послідовно з'єднаних доменів, у вигляді орієнтованого графа

У процесі декомпозиції ІКМ границя між доменами проходила через маршрутизатори мережі, як це реалізовано, наприклад, у протоколі OSPF [10, 14]:

$$R^P \cap R^Q \neq 0 \text{ та } E^P \cap E^Q = 0, \quad (4.32)$$

тобто деякі маршрутизатори ІКМ можуть належати одночасно кільком суміжним доменам. Також для кожного  $p$ -го домену визначимо множину приграничних маршрутизаторів  $B^P$  ( $B^P \in R^P$ ). У свою чергу всю множину приграничних маршрутизаторів  $p$ -го домену можна поділити на дві підмножини:  $B_{in}^{P,k}$  – підмножина приграничних маршрутизаторів, через які пакети  $k$ -го потоку надходять до  $p$ -го домену;  $B_{out}^{P,k}$  – підмножина приграничних маршрутизаторів, через які пакети  $k$ -го потоку вибувають з  $p$ -го домену. Для кожного каналу зв'язку  $E_{i,j}^P$  через  $\varphi_{i,j}^P$  позначимо його пропускну здатність, яка вимірюється в пакетах за секунду (1/с).

Нехай унаслідок розв'язання задачі ієрархічно-координаційної міждоменної маршрутизації для кожного  $p$ -го домену необхідно розрахувати маршрутні змінні  $x_{i,j}^{p,k}$ , які характеризують частку інтенсивності  $k$ -го потоку

пакетів, що протікає в каналі  $E_{i,j}^p \in E^p$ . Тоді для кожного маршрутизатора  $p$ -го домену необхідно виконати умови збереження  $k$ -го потоку для забезпечення зв'язності внутрішньодоменних ділянок міждоменних маршрутів. Якщо  $p$ -й домен є транзитним для  $k$ -го потоку пакетів, то подібні умови мають вигляд

$$\left\{ \begin{array}{l} \sum_{B_{in}^{p,k} \in B^p} \left( \sum_{E_{i,j}^p \in E^p} x_{i,j}^{p,k} - \sum_{E_{j,i}^p \in E^p} x_{j,i}^{p,k} \right) = 1; \\ \sum_{E_{i,j}^p \in E^p} x_{i,j}^{p,k} - \sum_{E_{j,i}^p \in E^p} x_{j,i}^{p,k} = 0; \\ \sum_{B_{out}^{p,k} \in B^p} \left( \sum_{E_{i,j}^p \in E^p} x_{i,j}^{p,k} - \sum_{E_{j,i}^p \in E^p} x_{j,i}^{p,k} \right) = -1. \end{array} \right. \quad (4.33)$$

Система рівнянь (4.33) повинна виконуватися для кожного  $k$ -го потоку пакетів окремо. Перша умова системи (4.33) охоплює всі приграничні маршрутизатори, через які  $k$ -й потік надходить до  $p$ -го домену; друга умова в (4.33) вводиться для внутрішніх маршрутизаторів  $p$ -го домену, які для  $k$ -го потоку є транзитними; третя умова має виконуватися для всіх приграничних маршрутизаторів, через які  $k$ -й потік вибуває з  $p$ -го домену.

Якщо  $k$ -й потік пакетів надійшов в ІКМ через  $p$ -й домен, а його джерелом є, наприклад, маршрутизатор  $R_i^p$ , то для цієї мережі перша умова системи (4.33) дещо спроститься і набуде вигляду

$$\sum_{E_{i,j}^p \in E^p} x_{i,j}^{p,k} = 1.$$

Решта рівнянь у системі (4.33) залишиться незмінною.

У разі, коли маршрутизатор  $R_j^p$  з  $p$ -го домену є отримувачем пакетів  $k$ -го потоку, то спроститься лише останнє рівняння системи (4.33) та матиме такий вигляд:

$$\sum_{E_{j,i}^p \in E^p} x_{j,i}^{p,k} = 1.$$



Крім того, з метою запобігання перевантаження каналів зв'язку  $p$ -го домену мережі важливо виконати такі умови:

$$\sum_{k \in K} \lambda^k x_{i,j}^{p,k} \leq \varphi_{i,j}^p, \quad p = \overline{1, N}. \quad (4.34)$$

Для реалізації одношляхової маршрутизації на маршрутні змінні накладаються обмеження вигляду

$$x_{i,j}^{p,k} \in \{0,1\}, \quad (4.35)$$

а за умови реалізації багатошляхової маршрутизації – такі умови:

$$0 \leq x_{i,j}^{p,k} \leq 1. \quad (4.36)$$

Змінні (4.35), (4.36) є координатами маршрутних векторів, які відповідно до проведеної структурної декомпозиції (рис. 4.49) підлягають функціональній декомпозиції

$$\vec{x} = \begin{bmatrix} \bar{x}_1 \\ \bar{x}_2 \\ \vdots \\ \bar{x}_p \\ \vdots \\ \bar{x}_N \end{bmatrix}, \quad \bar{x}_p = \begin{bmatrix} \bar{x}_p^1 \\ \bar{x}_p^2 \\ \vdots \\ \bar{x}_p^k \\ \vdots \\ \bar{x}_p^{\tilde{K}} \end{bmatrix}, \quad \bar{x}_p^k = \begin{bmatrix} x_{1,2}^{p,k} \\ x_{1,3}^{p,k} \\ \vdots \\ x_{i,j}^{p,k} \\ \vdots \\ x_{m_p, m_p-1}^{p,k} \end{bmatrix}, \quad (4.37)$$

де  $\vec{x}$  – це вектор маршрутних змінних, які визначають порядок маршрутизації потоків в ІКМ загалом;  $\bar{x}_p$  – це маршрутний вектор, що визначає порядок маршрутизації всіх потоків, які циркулюють в  $p$ -му домені;  $\bar{x}_p^k$  – це маршрутний вектор, який визначає результат розв'язання задачі маршрутизації  $k$ -го потоку в  $p$ -му домені.

У разі розподіленого розрахунку векторів  $\bar{x}_p$  та  $\bar{x}_p^k$  у межах кожного окремого  $p$ -го домену важливо забезпечити структурну та функціональну зв'язність міждоменних маршрутів, тобто маршрутів, що проходять через множину маршрутизаторів різних доменів. Структурна зв'язність міждоменних маршрутів полягає в тому, що закінчення маршруту в одному домені має збігатися з початком цього ж маршруту в сусідньому домені. Функціональна зв'язність міждоменного маршруту буде забезпечуватись у тому випадку, коли порядок балансування навантаження на граничних (міждоменних)

маршрутизаторах, який визначений у сусідніх доменах, буде однаковим. Тобто для функціональної зв'язності міждоменного маршруту необхідно виконати умову щодо його структурної зв'язності. Для забезпечення структурної та функціональної зв'язності міждоменного маршруту в модель (4.31)–(4.37) вводяться умови міждоменної взаємодії:

$$C_{p,q}^k \bar{x}_p^k = C_{q,p}^k \bar{x}_q^k, \quad p, q = \overline{1, N}, \quad p \neq q, \quad k \in K, \quad (4.38)$$

де  $C_{p,q}^k$  – матриця взаємодії  $p$ -го та  $q$ -го доменів, яка має розмір  $m_{p,q} \times m_x^{p,k}$ ;  $m_{p,q} = |R^p \cap R^q|$  – кількість маршрутизаторів, через які проходить границя між  $p$ -м і  $q$ -м доменами;  $m_x^{p,k}$  – число координат  $x_{i,j}^{p,k}$  вектора  $\bar{x}_p^k$ .

Для отримання більш наочного уявлення про структуру та зміст матриць взаємодії доменів (4.38), що вводяться до запропонованої моделі, розглянемо приклади їх формування на кількох мережних структурах. Нехай у першому випадку розглядається структура мережі, яка представлена на рис. 4.50 та складається з двох доменів. Границя доменів, що була визначена під час структурної декомпозиції ІКМ, проходить через два маршрутизатори, які належать цим доменам. У позначеннях першого домену (рис. 4.50) це маршрутизатори  $R_5^1$  та  $R_6^1$ , а в позначеннях другого –  $R_1^2$  та  $R_2^2$ .

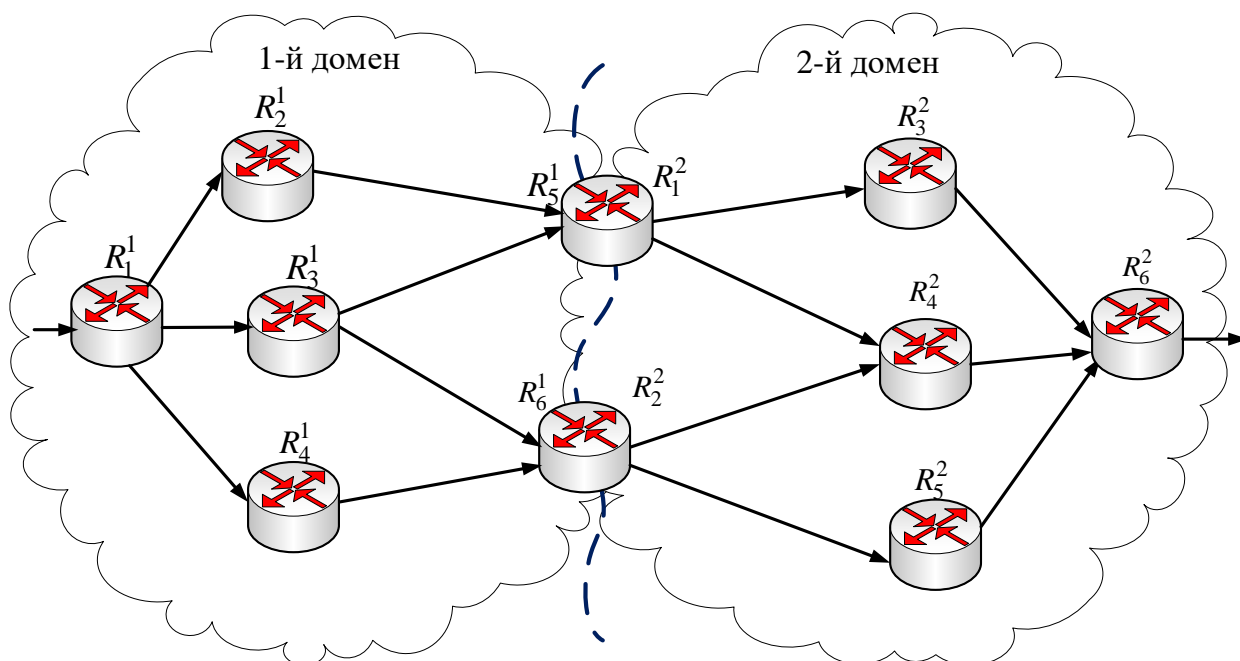


Рис. 4.50. Приклад першої структури ІКМ, що досліджувалася

Необхідно розв'язати задачу міждоменної маршрутизації потоку пакетів, який передається, наприклад, між маршрутизаторами  $R_1^1$  та  $R_6^2$ .

На рис. 4.50 показано випадок, коли будь-який з двох приграничних маршрутизаторів містить по два інтерфейси в кожному домені. Тоді вектори  $\vec{x}_1$  та  $\vec{x}_2$ , що визначають результат розв'язання задачі маршрутизації одного потоку в першому і другому доменах відповідно, набуватимуть такого вигляду:

$$\vec{x}_1 = \begin{bmatrix} x_{1,2}^{1,1} \\ x_{1,3}^{1,1} \\ x_{1,4}^{1,1} \\ x_{2,5}^{1,1} \\ x_{3,5}^{1,1} \\ x_{3,6}^{1,1} \\ x_{4,6}^{1,1} \end{bmatrix} \quad \text{та} \quad \vec{x}_2 = \begin{bmatrix} x_{1,3}^{2,1} \\ x_{1,4}^{2,1} \\ x_{2,4}^{2,1} \\ x_{2,5}^{2,1} \\ x_{3,6}^{2,1} \\ x_{4,6}^{2,1} \\ x_{5,6}^{2,1} \end{bmatrix}.$$

З урахуванням уведених позначень і проведеної декомпозиції умови взаємодії (4.38) першого та другого доменів (рис. 4.50) мають такий вигляд:

$$\text{для маршрутизатора } R_5^1 \left( R_1^2 \right): \quad x_{1,3}^{2,1} + x_{1,4}^{2,1} = x_{2,5}^{1,1} + x_{3,5}^{1,1};$$

$$\text{для маршрутизатора } R_6^1 \left( R_2^2 \right): \quad x_{2,4}^{2,1} + x_{2,5}^{2,1} = x_{3,6}^{1,1} + x_{4,6}^{1,1}.$$

У зв'язку з цим матриці міждоменної взаємодії для випадку симетричної структури доменів мають розмір  $(2 \times 7)$  та можуть бути записаними у формі

$$C_{2,1}^1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \quad \text{та} \quad C_{1,2}^1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

а умови (4.38) для розглянутого випадку (рис. 4.50) допускають запис

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_{1,3}^{2,1} \\ x_{1,4}^{2,1} \\ x_{2,4}^{2,1} \\ x_{2,5}^{2,1} \\ x_{3,6}^{2,1} \\ x_{4,6}^{2,1} \\ x_{5,6}^{2,1} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_{1,2}^{1,1} \\ x_{1,3}^{1,1} \\ x_{1,4}^{1,1} \\ x_{2,5}^{1,1} \\ x_{3,5}^{1,1} \\ x_{3,6}^{1,1} \\ x_{4,6}^{1,1} \end{bmatrix}.$$

Випадок, коли ІКМ представлена двома доменами, але які мають один щодо іншого асиметричну структуру, показано на рис. 4.51. Границя між доменами також проходить через два приграничні маршрутизатори:  $R_5^1$  ( $R_1^2$ ) та  $R_6^1$  ( $R_2^2$ ). Для цього варіанта (рис. 4.51) характерно, що приграничні маршрутизатори мають різну кількість інтерфейсів, які належать різним доменам: два інтерфейси – першому домену та один інтерфейс – другому.

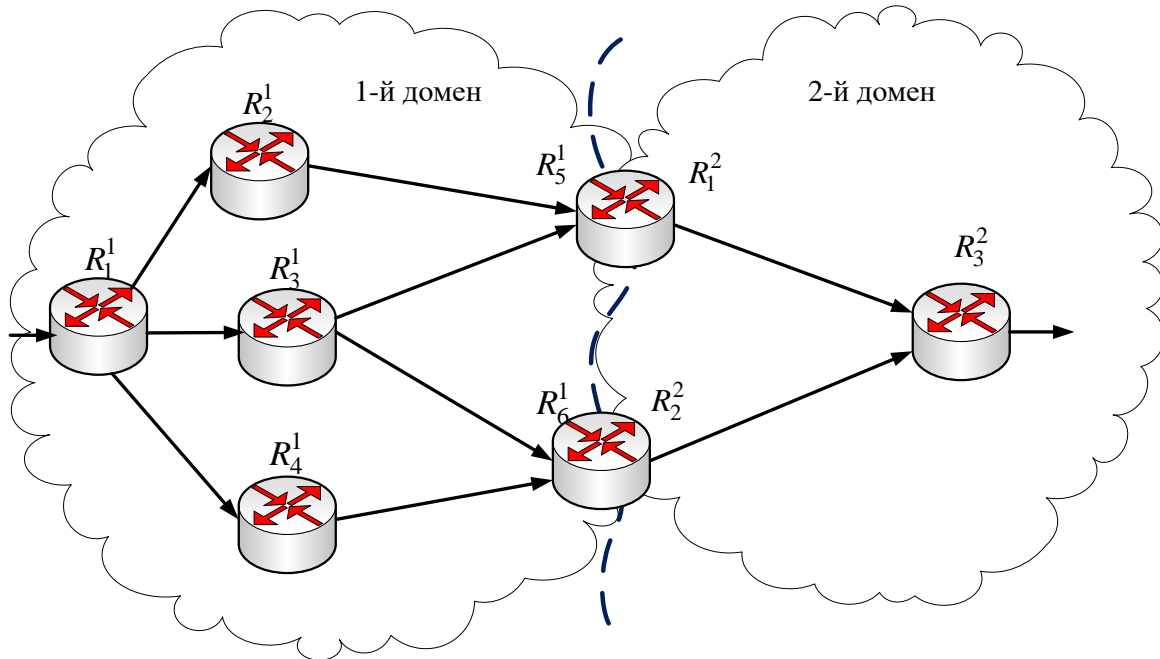


Рис. 4.51. Приклад другої структури ІКМ, що досліджувалася

Результат розв'язання задачі маршрутизації в першому та другому доменах (рис. 4.51) можна представити у вигляді відповідних маршрутних векторів:

$$\vec{x}_1 = \begin{bmatrix} x_{1,1}^{1,1} \\ x_{1,2}^{1,1} \\ x_{1,3}^{1,1} \\ x_{1,4}^{1,1} \\ x_{2,5}^{1,1} \\ x_{3,5}^{1,1} \\ x_{3,6}^{1,1} \\ x_{4,6}^{1,1} \end{bmatrix} \quad \text{та} \quad \vec{x}_2 = \begin{bmatrix} x_{1,3}^{2,1} \\ x_{2,3}^{2,1} \end{bmatrix}.$$

Тоді умови взаємодії доменів у скалярному вигляді можна записати таким чином:

$$x_{1,3}^{2,1} = x_{2,5}^{1,1} + x_{3,5}^{1,1}; \quad x_{2,3}^{2,1} = x_{3,6}^{1,1} + x_{4,6}^{1,1},$$

у зв'язку з чим матриці взаємодії доменів для випадку асиметричної структури доменів ІКМ можуть бути записані у такій формі:

$$C_{2,1}^1 = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} \quad \text{та} \quad C_{1,2}^1 = \begin{vmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{vmatrix},$$

маючи розміри  $2 \times 2$  і  $2 \times 7$  відповідно.

У матричній формі умови взаємодії доменів (4.38) для структури ІКМ, наведеної на рис. 4.51, набуватимуть такого вигляду:

$$\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} \cdot \begin{bmatrix} x_{1,3}^{2,1} \\ x_{2,3}^{2,1} \end{bmatrix} = \begin{vmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{vmatrix} \cdot \begin{bmatrix} x_{1,2}^{1,1} \\ x_{1,3}^{1,1} \\ x_{1,4}^{1,1} \\ x_{2,5}^{1,1} \\ x_{3,5}^{1,1} \\ x_{3,6}^{1,1} \\ x_{4,6}^{1,1} \end{bmatrix}$$

або в спрощеній формі  $\bar{x}_2^1 = C_{1,2}^1 \bar{x}_1^1$ .

#### 4.3.2. Метод ієрархічно-координаційної міждоменної маршрутизації в програмно-конфігурованій ІКМ

Ґрунтуючись на математичній моделі (4.33)–(4.38), що була запропонована в пункті 4.3.1, в основу методу ієрархічно-координаційної міждоменної маршрутизації буде покладено розв'язання оптимізаційної задачі щодо розрахунку векторів маршрутних змінних  $\bar{x}_p^k$  ( $p = \overline{1, N}, k \in K$ ) за умови дотримання обмежень (4.33)–(4.36), (4.38) з використанням такого критерію оптимальності маршрутних рішень:

$$\min F, \quad F = \sum_{p \in N} \sum_{k \in K} \left( \bar{x}_p^k \right)^t H_p^k \bar{x}_p^k, \quad (4.39)$$

де  $H_p^k$  – діагональна матриця вагових коефіцієнтів, координатами якої, як правило [70–74], є маршрутні метрики каналів зв'язку  $p$ -го домену ІКМ.

Цільова функція  $F$  кількісно характеризує умовні сумарні витрати на організацію процесу міждоменної маршрутизації в ІКМ. Для надання шуканим рішенням властивостей ієрархічно-координаційної маршрутизації в ході розв'язання оптимізаційної задачі, пов'язаної з мінімізацією виразу (4.39) за наявності обмежень (4.33)–(4.36), (4.38), буде використано принцип цільової координації [22, 23]. Тоді, переходячи до задачі на безумовний екстремум

$$\min_{\bar{x}} F = \max_{\bar{\mu}} L,$$

необхідно максимізувати за  $\bar{\mu}$  лагранжіан вигляду:

$$L = \sum_{p=1}^N \sum_{k \in K} \left( \bar{x}_p^k \right)^t H_p^k \bar{x}_p^k + \sum_{p=1}^N \sum_{q=1}^N \sum_{\substack{k \in K \\ q \neq p}} \left( \bar{\mu}_{p,q}^k \right)^t \left( C_{p,q}^k \bar{x}_p^k - C_{q,p}^k \bar{x}_q^k \right), \quad (4.40)$$

де  $\bar{\mu}$  – вектор множників Лагранжа;

$\bar{\mu}_{p,q}$  – підвектори вектора  $\bar{\mu}$ , що належать до кожної з векторно-матричних умов взаємодії доменів (4.38).

З тієї причини, що в межах принципу цільової координації вектори множників Лагранжа  $\bar{\mu}$  розраховуються на верхньому рівні та для нижнього рівня є відомими значеннями, то вираз (4.40) можна представити в такій декомпозиційній формі:

$$L = \sum_{p=1}^N L_p,$$

$$L_p = \sum_{k \in K} \left( \bar{x}_p^k \right)^t H_p^k \bar{x}_p^k + \sum_{\substack{q=1 \\ p \neq q}}^N \sum_{k \in K_p^+} \left( \bar{\mu}_{p,q}^k \right)^t C_{p,q}^k \bar{x}_p^k - \sum_{\substack{q=1 \\ p \neq q}}^N \sum_{k \in K_p^-} \left( \bar{\mu}_{q,p}^k \right)^t C_{p,q}^k \bar{x}_p^k, \quad (4.41)$$

де  $K_p^+$  – підмножина потоків, які надходять до  $p$ -го домену з інших доменів;

$K_p^-$  – підмножина потоків, які виходять з  $p$ -го домену ( $K_p^+, K_p^- \subset K$ ).

Якщо  $k$ -й потік надходить в ІКМ через  $p$ -й домен, то  $k \in K_p^+$ . Відповідно до проведеної функціональної декомпозиції у виразі (4.41) усі складники належать до  $p$ -го домену, а другий і третій складники в цьому виразі відповідають за узгодження порядку маршрутизації відповідно вихідних і вхідних потоків для  $p$ -го домену ІКМ. Таким чином, у межах пропонованого методу загальна проблема ієрархічно-координаційної міждоменної маршрутизації формулюється як задача дворівневої оптимізації. Сам метод

ієрархічно-координаційної міждоменної маршрутизації передбачає таку послідовність дій (рис. 4.52):

1. На нижньому ієрархічному рівні SDN-контролери доменів проводять збір та аналіз інформації про їх стан – топологію, пропускні здатності каналів зв'язку, характеристики потоків, що циркулюють у мережі. Це дозволяє сформувати матриці маршрутних метрик  $H_p^k$  та міждоменної взаємодії  $C_{p,q}^k$ , що містяться у виразі (4.41), та структуру обмежень (4.33).

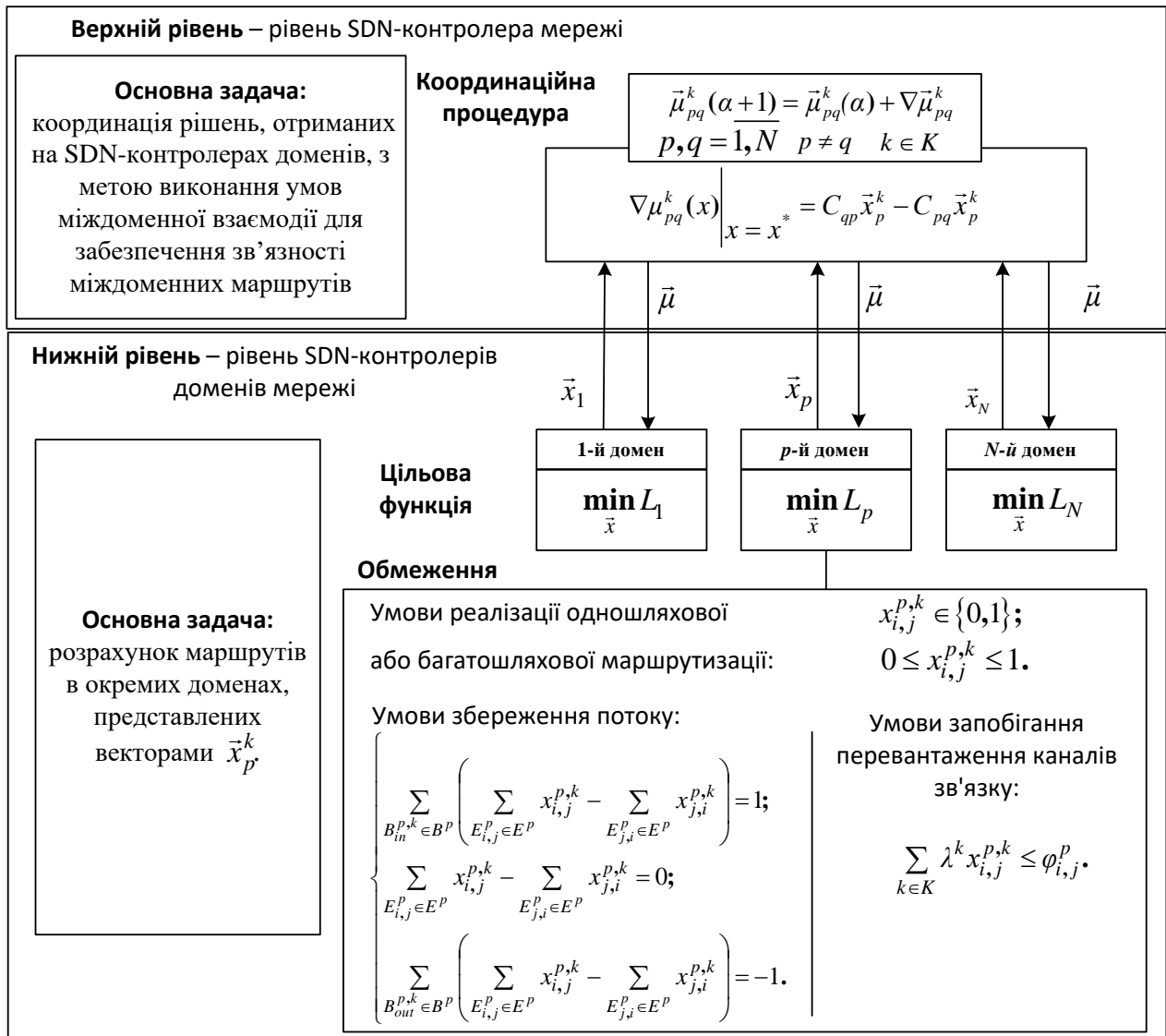


Рис. 4.52. Структура дворівневого методу ієрархічно-координаційної міждоменної маршрутизації в програмно-конфігурованій ІКМ

2. Відповідно до результатів проведеного аналізу SDN-контролери доменів здійснюють розрахунок маршрутних змінних, представлених векторами  $\bar{x}_p^k$  ( $p = \overline{1, N}$ ,  $k \in K$ ), у процесі мінімізації лагранжіанів (4.41) за

умови обмежень (4.33)–(4.36). Результати розрахунків спрямовуються на верхній рівень – на SDN-контролер програмно-конфігурованої мережі загалом.

3. На верхньому рівні SDN-контролер мережі координує рішення, отримані на нижньому рівні SDN-контролерами доменів, з метою забезпечення виконання умов міждоменної взаємодії (4.38) шляхом модифікації векторів множників Лагранжа в процесі виконання градієнтної ітераційної процедури

$$\bar{\mu}_{p,q}^k(a+1) = \bar{\mu}_{p,q}^k(a) + \nabla \bar{\mu}_{p,q}^k, \quad (4.42)$$

де  $a$  – номер ітерації;  $\nabla \bar{\mu}_{p,q}^k$  – градієнт функції (4.41), який розраховується відповідно до отриманих на нижньому рівні результатів розв’язання задач маршрутизації  $\bar{x}_p^{k*}$  ( $p = \overline{1, N}$ ,  $k \in K$ ) у кожному конкретному домені

$$\nabla \bar{\mu}_{p,q}^k(x) \Big|_{x = x^*} = C_{p,q} \bar{x}_p^k - C_{q,p} \bar{x}_q^k. \quad (4.43)$$

4. Модифіковані значення векторів множників Лагранжа  $\bar{\mu}_{p,q}^k$  передаються на нижній рівень (на SDN-контролери доменів) для розрахунку нових маршрутних векторів  $\bar{x}_p^k$ . За аналогією до рішень, висвітлених у підрозділі 4.2, координати векторів множників Лагранжа  $\bar{\mu}_{p,q}^k$  були модифікаціями маршрутних метрик для каналів зв’язку, що не утворювали зв’язний маршрут (маршрути). Процес розрахунків набуває ітераційного характеру. Зв’язність міждоменних маршрутів буде забезпечуватися в разі наближення значень координат градієнта (4.43) до нуля.

Таким чином, запропонований метод ієрархічно-координаційної міждоменної маршрутизації дозволяє відмовитися від централізації управління мережею, а також розподілити управління між SDN-контролерами доменів, що позитивно впливає на масштабованість маршрутних рішень. Проте ефективність запропонованого методу ієрархічно-координаційної міждоменної маршрутизації з точки зору оптимальності та оперативності отриманих рішень багато в чому залежить від швидкості збіжності координаційної процедури (4.42), (4.43). З технологічної точки зору мінімізація кількості ітерацій процедури (4.42), (4.43) для отримання шуканого оптимального рішення орієнтує на скорочення обсягу службового трафіку, що передається між ієрархічними рівнями про результати розрахунків на кожній з ітерацій, і на зменшення загального часу розв’язання задачі міждоменної маршрутизації в ІКМ загалом [70–74].



### 4.3.3. Дослідження запропонованого методу ієрархічно-координаційної міждоменної маршрутизації в програмно-конфігурованій ІКМ

Проведемо дослідження запропонованого методу ієрархічно-координаційної міждоменної маршрутизації в ІКМ з метою підтвердження його працездатності, адекватності та ефективності отриманих результатів розрахунку. Під час дослідження методу також проаналізуємо вплив на швидкість збіжності градієнтної процедури координації (4.42), (4.43) основних топологічних і функціональних параметрів ІКМ: структури мережі та зв'язності її доменів, характеристик потоків, а також типу реалізованої стратегії маршрутизації – одно- або багатопляхової.

У межах першого розглянутого прикладу проаналізуємо характер рішень задачі ієрархічно-координаційної міждоменної маршрутизації для варіанта структури ІКМ, яка представлена на рис. 4.53.

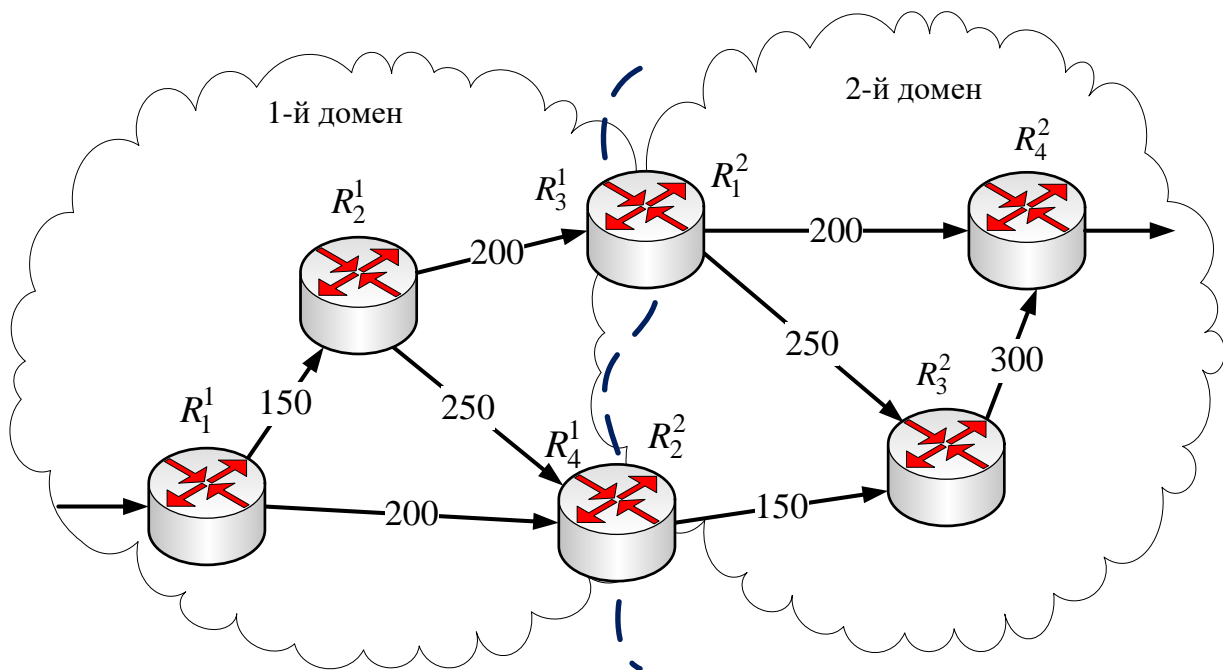


Рис. 4.53. Структура першої мережі, що досліджується

Мережа складається з двох доменів (рис. 4.53). Перший і другий домени містять по чотири маршрутизатори:  $R^1 = \{R_1^1, R_2^1, R_3^1, R_4^1\}$ ,  $R^2 = \{R_1^2, R_2^2, R_3^2, R_4^2\}$ . Взаємодія між доменами здійснюється через маршрутизатори  $R_3^1$  ( $R_1^2$ ) та  $R_4^1$  ( $R_2^2$ ). Нехай вузлом-джерелом пакетів буде маршрутизатор  $R_1^1$ , що розміщений у першому домені, а вузол-отримувач – маршрутизатор  $R_4^2$ , який

міститься відповідно в другому домені. У розривах каналів зв'язку (рис. 4.53) показана їх пропускна здатність (1/с). На головній діагоналі матриці  $H_p^k$  (4.39) розташовані величини  $10^8/\phi_{i,j}^p$  за аналогією до значень маршрутних метрик, характерних для протоколу OSPF [10, 14].

У розрахунках інтенсивність потоку пакетів змінювалася від 10 1/с до 300 1/с. Так, наприклад, у разі інтенсивності потоку 30 1/с на рис. 4.54 представлено початкове розв'язання задачі міждоменної маршрутизації, тобто до початку процесу координації. На цьому рисунку в розривах каналів зв'язку вказано дріб: у чисельнику представлена інтенсивність потоку пакетів, який передається, а в знаменнику – пропускна здатність каналу зв'язку.

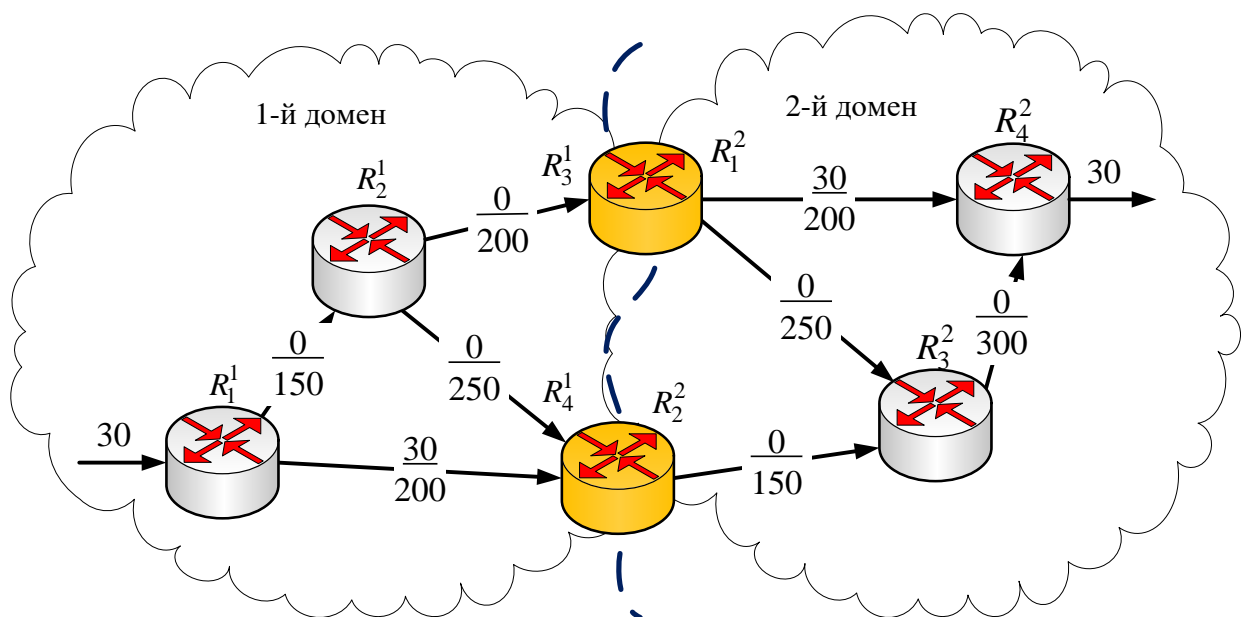


Рис. 4.54. Початкове розв'язання задачі міждоменної маршрутизації потоку інтенсивністю 30 1/с в ІКМ

З огляду на те що розрахунок маршрутів у різних доменах проводився незалежно один від одного, то зв'язність міждоменного маршруту не забезпечувалась (рис. 4.54), тобто умови міждоменної взаємодії (4.38) не були виконані. Так, з першого домену потік виходив через маршрутизатор  $R_4^1$  ( $R_2^2$ ), а до другого домену надходив через маршрутизатор  $R_1^2$  ( $R_3^1$ ). Початковий вибір маршрутів у кожному з доменів пояснюється тим, що саме вони є оптимальними, тобто «найкоротшими» в межах обраної метрики. Ці маршрути в доменах є, з одного боку, найбільш продуктивними, а з іншого, – містять мінімальну кількість переприйомів (hops), тому що використаний критерій оптимальності (4.41) має адитивний характер.

Проведена на верхньому рівні ієрархії запропонованого методу координація маршрутних рішень, отриманих в окремих доменах, яка спрямована на забезпечення виконання умов взаємодії (4.38), призводить до того, що зв'язність єдиного розрахованого міждоменного маршруту була забезпечена вже після третьої координаційної ітерації (рис. 4.55). Подібна ситуація була характерна і під час збільшення інтенсивності потоку до 150 1/с. У цьому випадку також була реалізована одношляхова стратегія маршрутизації, а координація здійснювалася знову ж за три ітерації.

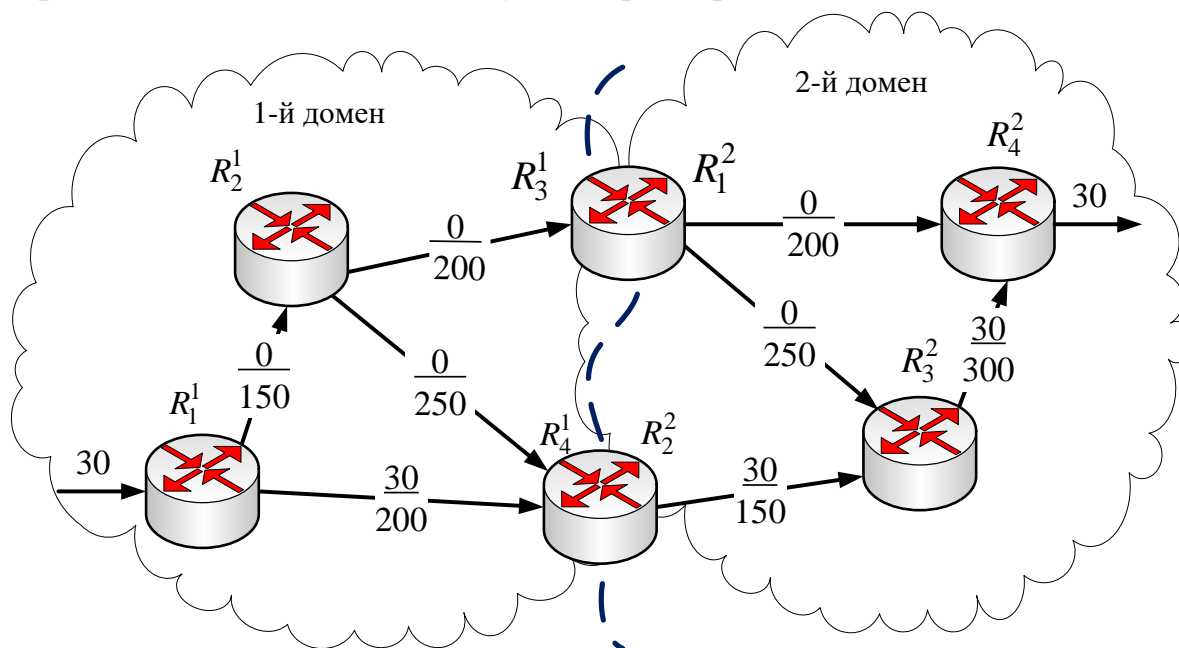


Рис. 4.55. Кінцеве (скоординоване) розв'язання задачі міждоменної маршрутизації потоку з інтенсивністю 30 1/с в ІКМ

У подальшому збільшенні інтенсивності того ж потоку за тими самими вихідними даними щодо структури мережі та пропускних здатностей каналів зв'язку (рис. 4.53) збіжність координаційної процедури забезпечувалася вже після п'ятої ітерації, а маршрутні рішення мали багатошляховий характер. Зокрема на рис. 4.56 показано початкове (до початку роботи координаційної процедури) розв'язання задачі міждоменної маршрутизації за інтенсивності потоку 300 1/с. Позначення в розривах каналів зв'язку є ідентичними до наведених на рис. 4.54 та 4.55. У кожному з доменів реалізується багатошляхова маршрутизація, тому що жоден з каналів не впорається з навантаженням 300 1/с. Однак через відсутність координації маршрутних рішень, що були отримані в окремих доменах, зв'язність міждоменних маршрутів не забезпечувалася (рис. 4.56).

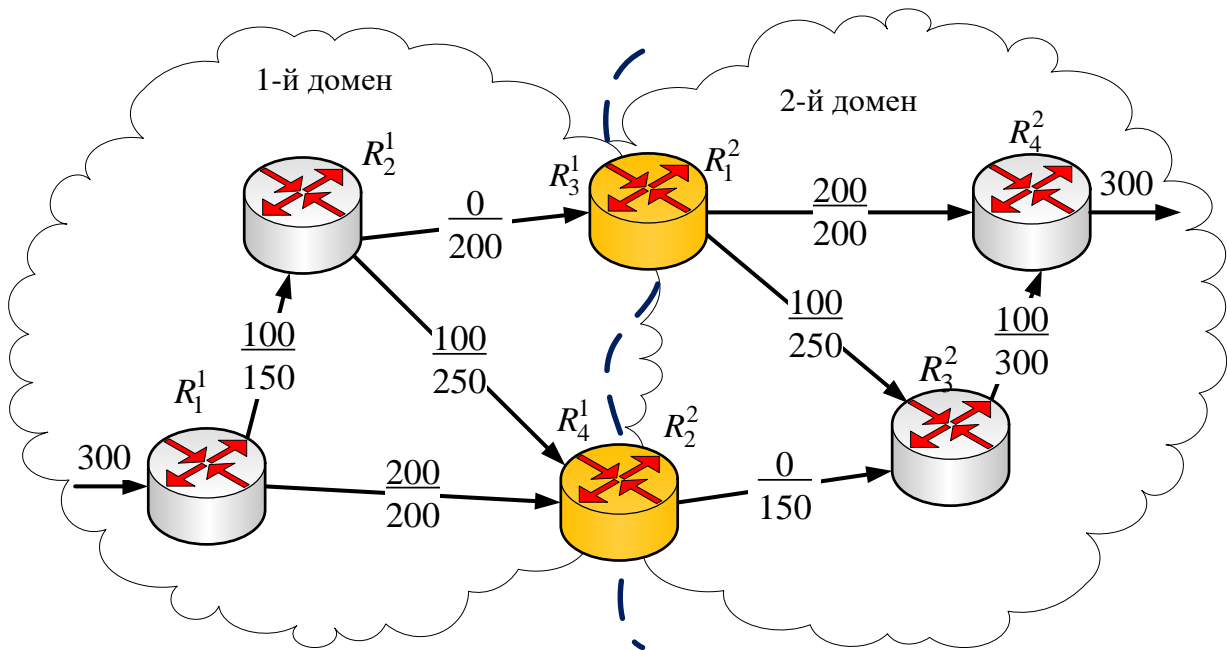


Рис. 4.56. Початкове розв'язання задачі міждоменної маршрутизації потоку інтенсивністю 300 1/с в ІКМ

На рис. 4.57 показано проміжне розв'язання задачі ієрархічно-координаційної міждоменної маршрутизації, яке було отримано після третьої ітерації. У межах цього маршрутного рішення все ще не виконуються умови міждоменної взаємодії (4.38), але спостерігається менша розбіжність у результатах розрахунків, отриманих у різних доменах ІКМ, порівняно з початковим рішенням (рис. 4.56).

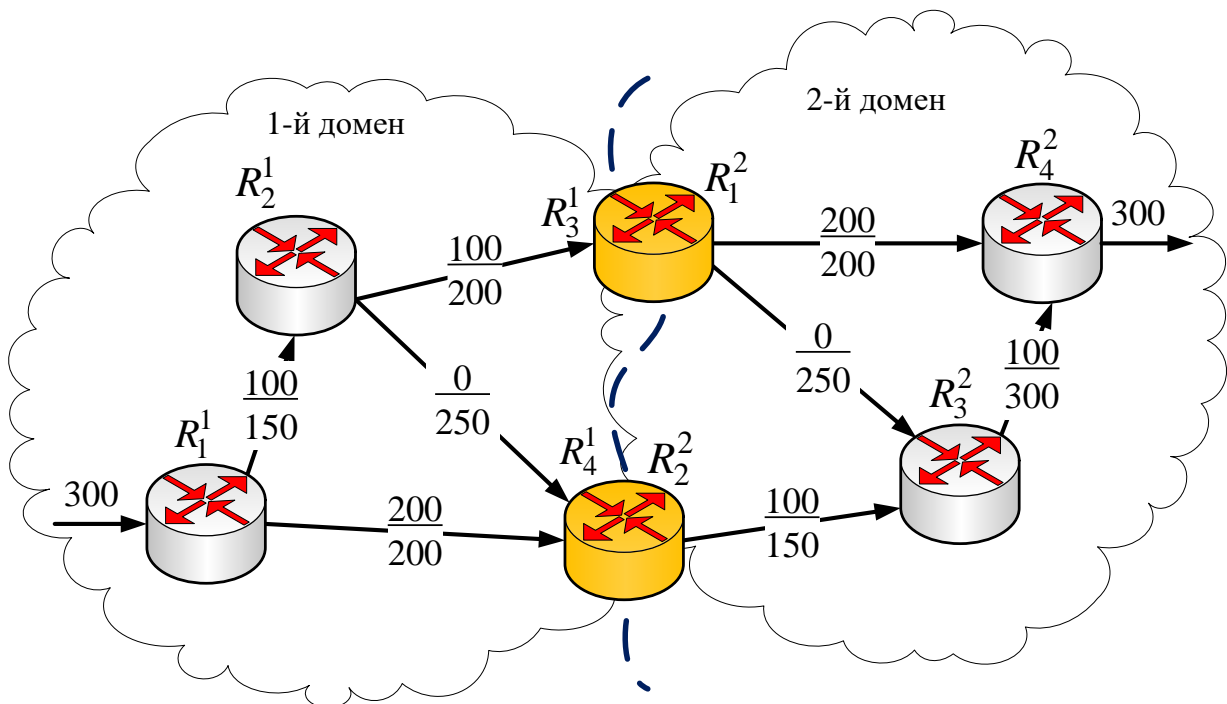


Рис. 4.57. Проміжне розв'язання задачі міждоменної маршрутизації потоку інтенсивністю 300 1/с в ІКМ (після третьої координаційної ітерації)

На рис. 4.58 наведений кінцевий порядок міждоменної маршрутизації після п'ятої координаційної ітерації роботи запропонованого методу, що приводить до виконання умов міждоменної взаємодії (4.38). Зростання кількості ітерацій координаційної процедури для отримання шуканого рішення за умови збільшення інтенсивності потоку викликано необхідністю реалізації багатопляхової стратегії маршрутизації як усередині доменів, так і між ними, що передбачало розширення кількості варіантів допустимих рішень поставленої задачі.

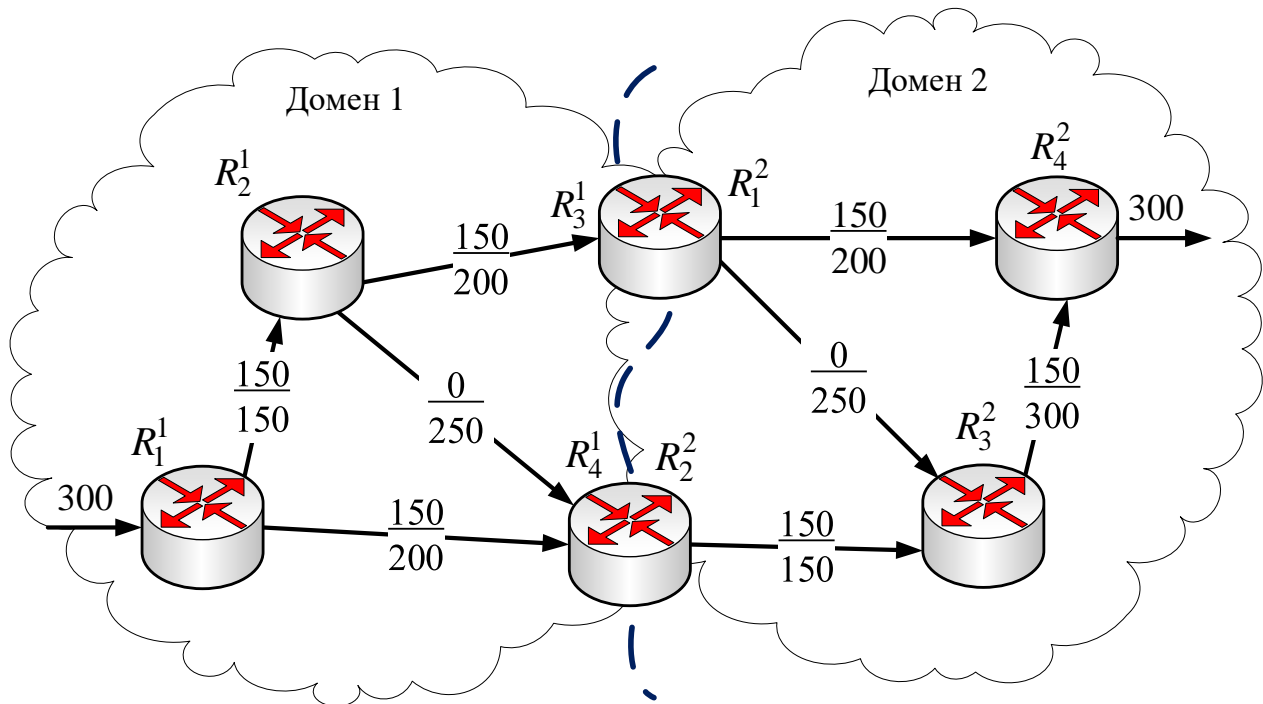


Рис. 4.58. Кінцеве (скоординоване) розв'язання задачі міждоменної маршрутизації потоку інтенсивністю 300 1/с в ІКМ

Далі буде проаналізовано вплив зростання розміру доменів і зв'язності приграничних маршрутизаторів (кількості залучених на них інтерфейсів) на характер рішень ієрархічно-координаційної міждоменної маршрутизації та швидкість збіжності координаційної процедури. Для цього була досліджена структура ІКМ (рис. 4.59), яка складалася також з двох доменів. Проте, на відміну від раніше розглянутої структури ІКМ (рис. 4.53), перший домен містить більшу кількість маршрутизаторів і каналів зв'язку, що призвело до зростання залучених інтерфейсів на приграничних маршрутизаторах цих доменів. На рис. 4.59 у розривах каналів зв'язку вказані їх пропускні здатності (1/с).

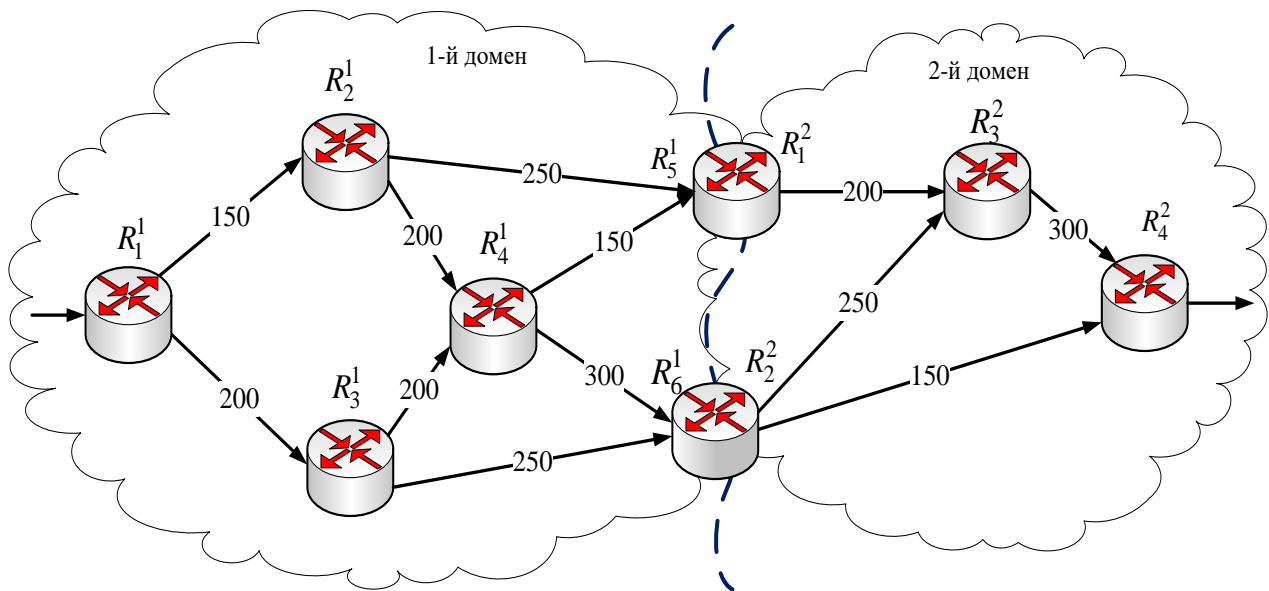


Рис. 4.59. Структура другої мережі, що досліджується

Таким чином, перший домен містить шість маршрутизаторів  $R^1 = \{R_1^1, R_2^1, R_3^1, R_4^1, R_5^1, R_6^1\}$ , а другий – чотири маршрутизатори  $R^2 = \{R_1^2, R_2^2, R_3^2, R_4^2\}$ . Взаємодія між цими доменами здійснюється через маршрутизатори  $R_5^1$  ( $R_1^2$ ) та  $R_6^1$  ( $R_2^2$ ). Нехай відправником пакетів є маршрутизатор  $R_1^1$ , що розташований у першому домені, а отримувачем – маршрутизатор  $R_4^2$ , що належить другому домену ІКМ.

Під час дослідження інтенсивність потоку змінювалася від 10 до 350 1/с. Зокрема кількість ітерацій координаційної процедури зростала від однієї до трьох пропорційно завантаженості мережі. Так, за умови інтенсивності потоку 200 1/с (рис. 4.60) зв'язність міждоменного маршруту забезпечувалась уже після першої ітерації координаційної процедури, що насамперед пов'язано з реалізацією одношляхової стратегії маршрутизації. На рис. 4.60 у розривах каналів зв'язку представлено дріб, де чисельник – це інтенсивність потоку пакетів, що протікає в каналі зв'язку, а знаменник – його пропускна здатність.

Для реалізації багатошляхової міждоменної маршрутизації, наприклад, у разі інтенсивності потоку 300 1/с запропонований метод забезпечував збіжність до оптимального рішення за три ітерації координаційної процедури. На рис. 4.61 представлено початкове розв'язання задачі міждоменної маршрутизації потоку інтенсивністю 300 1/с в ІКМ, структуру якої наведено на рис. 4.59. У межах початкового розв'язання сформульованої задачі, тобто до початку роботи координаційної процедури, зв'язність міждоменного маршруту

не була забезпечена (рис. 4.61), тому що перший домен прагнув передати пакети як через маршрутизатор  $R_5^1$  ( $R_1^2$ ), так і через  $R_6^1$  ( $R_2^2$ ) з інтенсивностями відповідно 100 1/с та 200 1/с, а другий домен намагався приймати пакети від першого домену лише через маршрутизатор  $R_6^1$  ( $R_2^2$ ).

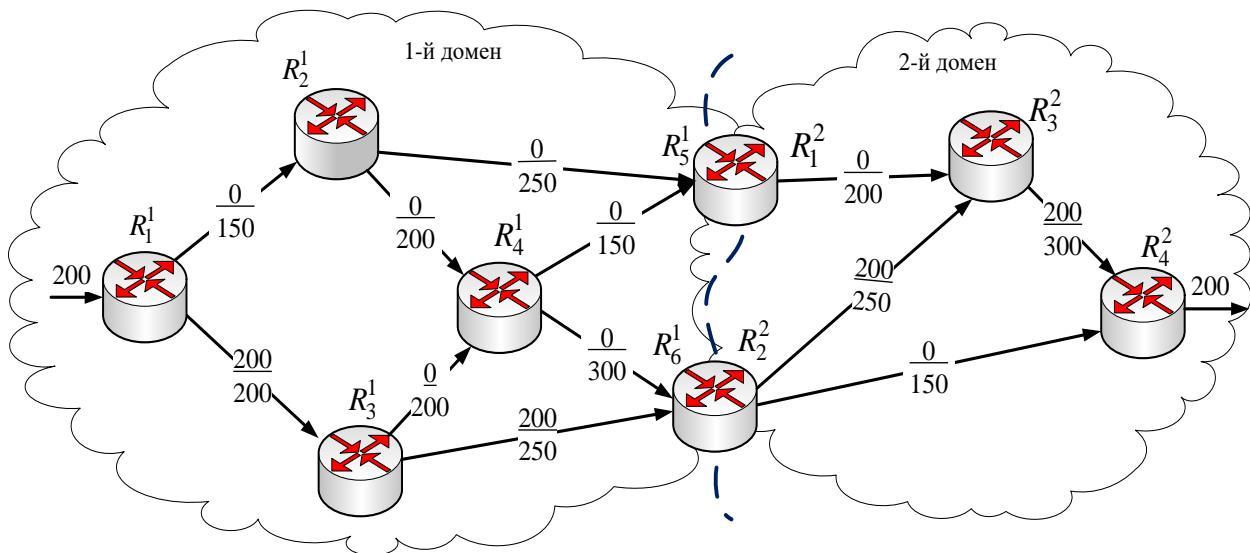


Рис. 4.60. Кінцеве (скоординоване) розв'язання задачі міждоменної маршрутизації потоку інтенсивністю 200 1/с в ІКМ

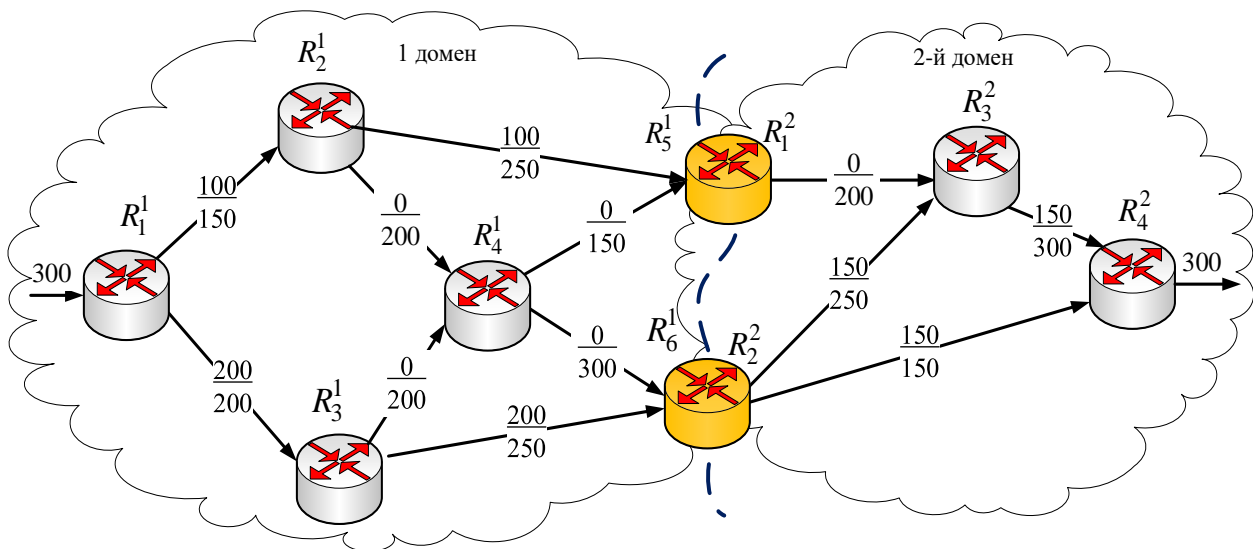


Рис. 4.61. Початкове розв'язання задачі міждоменної маршрутизації потоку інтенсивністю 300 1/с в ІКМ

Після завершення роботи координаційної процедури (4.42), (4.43), а саме після третьої ітерації, забезпечувалося виконання умов міждоменної взаємодії (4.38), як показано на рис. 4.62.

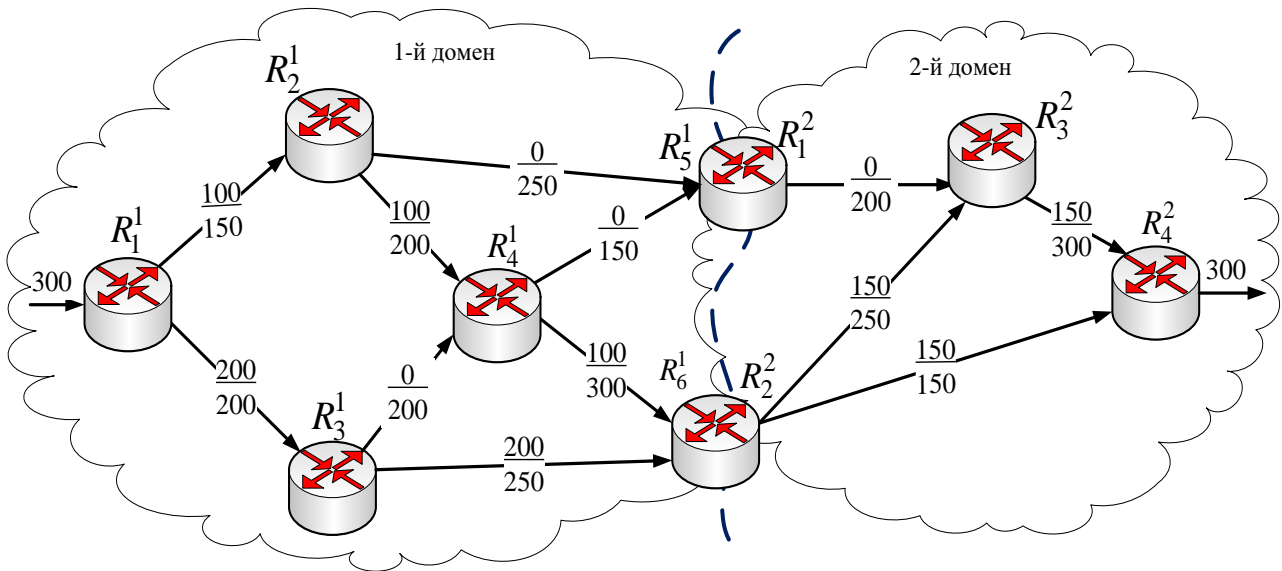


Рис. 4.62. Скоординоване розв'язання задачі міждоменної маршрутизації потоку інтенсивністю 300 1/с в ІКМ

Подальше дослідження було спрямоване на визначення ступеня впливу на збіжність координаційної процедури (4.42), (4.43) кількості приграничних маршрутизаторів, через які відбувалася взаємодія сусідніх доменів. Для цього підлягала дослідженню структура ІКМ, що представлена на рис. 4.63, у межах якої було виокремлено два домени. Кожен з доменів містив по сім маршрутизаторів:

$$R^1 = \{R_1^1, R_2^1, R_3^1, R_4^1, R_5^1, R_6^1, R_7^1\};$$

$$R^2 = \{R_1^2, R_2^2, R_3^2, R_4^2, R_5^2, R_6^2, R_7^2\}.$$

Взаємодія між цими доменами здійснювалася вже через три маршрутизатори  $R_5^1$  ( $R_1^2$ ),  $R_6^1$  ( $R_2^2$ ) та  $R_7^1$  ( $R_3^2$ ). Нехай відправником пакетів є маршрутизатор  $R_1^1$ , що розміщений у першому домені, а отримувачем – маршрутизатор  $R_7^2$ , який належить другому домену. На рис. 4.63 в розривах каналів зв'язку вказані їх пропускні здатності (1/с).

У процесі дослідження інтенсивність потоку змінювалася від 10 1/с до 300 1/с. Зокрема кількість ітерацій для збіжності координаційної процедури змінювалася залежно від інтенсивності потоку і реалізованої стратегії маршрутизації. За умови інтенсивності потоку до 120 1/с була реалізована одношляхова стратегія маршрутизації, а збіжність координаційної процедури була забезпечена за 1–2 ітерації. У зростанні інтенсивності потоку вже реалізовувалася багатошляхова стратегія маршрутизації, а кількість



ітерацій координаційної процедури варіювалася від 3 до 4. Так, наприклад, на рис. 4.64 показано початкове рішення задачі міждоменної маршрутизації (до початку роботи координаційної процедури) у разі інтенсивності потоку 250 1/с, зокрема в розривах каналів зв'язку представлено дріб, де чисельник – це інтенсивність потоку пакетів, що протікає в каналі зв'язку, а знаменник – його пропускну здатність.

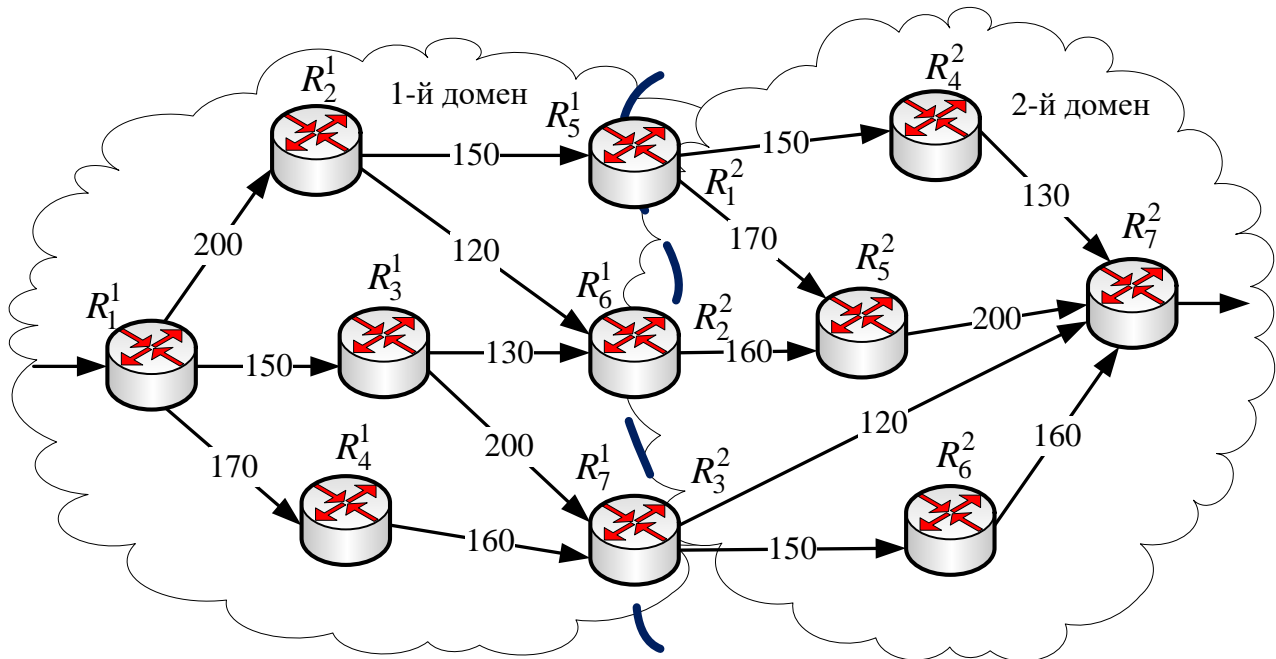


Рис. 4.63. Структура третьої мережі, що досліджується

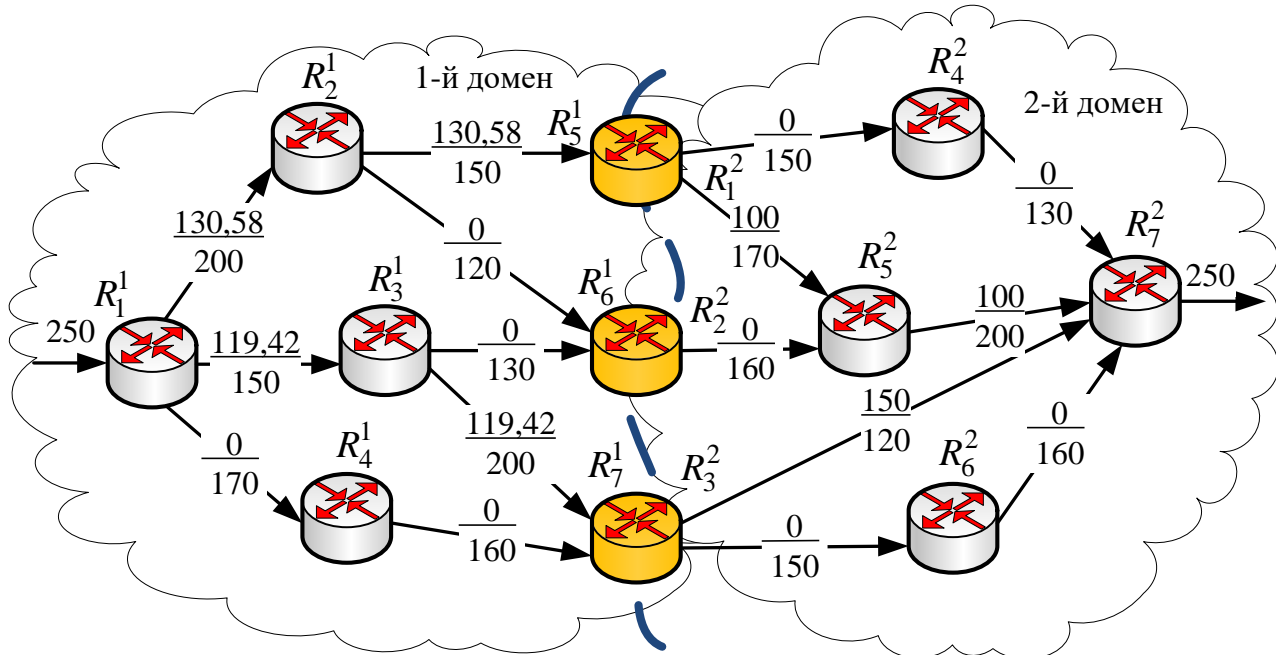


Рис. 4.64. Початкове розв'язання задачі міждоменної маршрутизації потоку інтенсивністю 250 1/с в ІКМ

У межах початкового розв'язання сформульованої маршрутної задачі зв'язність міждоменного маршруту не була забезпечена (рис. 4.64), тому що перший домен прагнув передати пакети через маршрутизатори  $R_5^1$  ( $R_1^2$ ) і  $R_7^1$  ( $R_3^2$ ) з інтенсивностями відповідно 130,58 1/с та 119,42 1/с, а другий домен намагався приймати пакети від першого домену через ті самі маршрутизатори  $R_5^1$  ( $R_1^2$ ) та  $R_7^1$  ( $R_3^2$ ), але з інтенсивностями 100 1/с та 150 1/с відповідно. Тобто забезпечувалася структурна, але не функціональна зв'язність міждоменного маршруту, бо порядок балансування навантаження на граничних (міждоменних) маршрутизаторах, який визначався SDN-контролером першого домену, відрізнявся від подібного порядку балансування, що був визначений на контролері другого домену.

Виконання умов міждоменної взаємодії (4.38) було забезпечено після завершення роботи координаційної процедури (4.42), (4.43), а саме після її третьої ітерації, як показано на рис. 4.65.

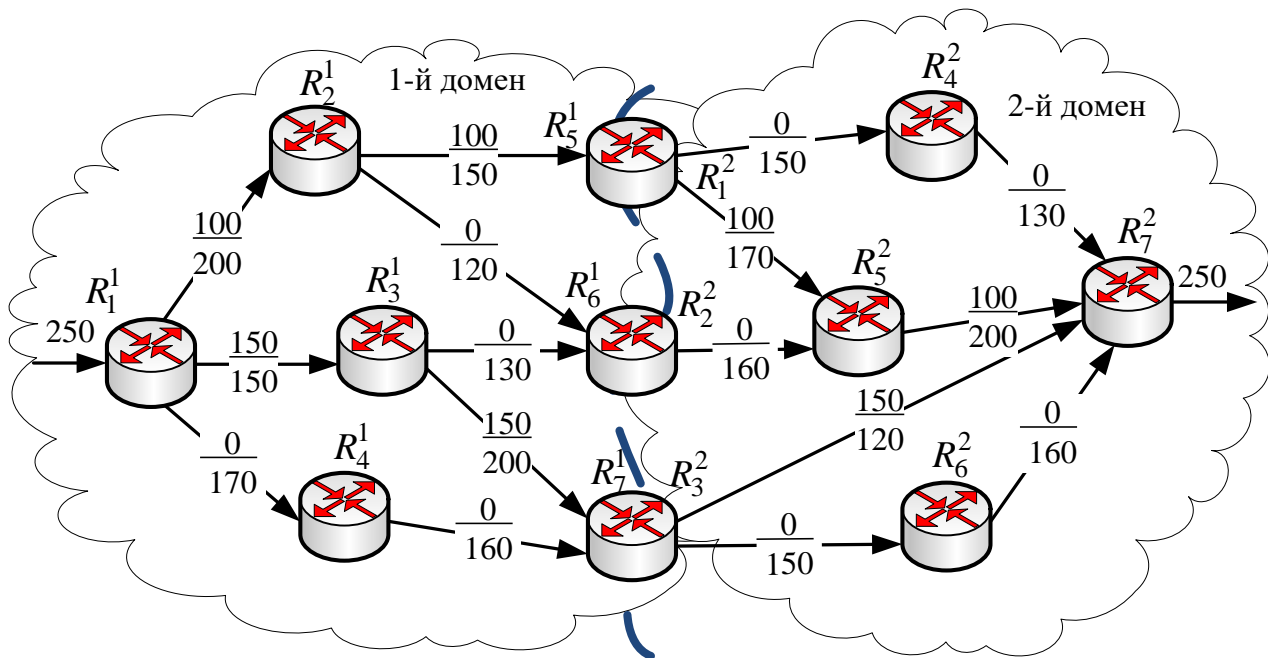


Рис. 4.65. Скоординоване розв'язання задачі міждоменної маршрутизації потоку інтенсивністю 250 1/с в ІКМ

Для скоординованого рішення у разі побудови міждоменного мультишляху були залучені два приграничні вузли  $R_5^1$  ( $R_1^2$ ) та  $R_7^1$  ( $R_3^2$ ), через які передавалися пакети інтенсивностями 100 1/с та 150 1/с відповідно. Для цих

маршрутів були характерними висока пропускна здатність і мінімальна кількість переприємів, що визначалося особливістю використовуваної маршрутної метрики.

Отже, як показали результати дослідження [75, 76], на швидкість збіжності координаційної процедури (4.42), (4.43), впливали такі основні чинники: кількість доменів, структура та розмір доменів у мережі, кількість приграничних маршрутизаторів, завантаженість мережі та стратегія маршрутизації (одно- чи багатошляхова). У процесі збільшення кількості приграничних маршрутизаторів та при реалізації багатошляхової стратегії маршрутизації загалом випадку число ітерацій координаційної процедури (4.42), (4.43) зростало (табл. 4.7). У табл. 4.7 наведені результати дослідження, коли число маршрутизаторів на границі доменів дорівнювала двом.

Таблиця 4.7

**Залежність кількості ітерацій координаційної процедури від реалізованої стратегії маршрутизації та кількості доменів в ІКМ**

Кількість доменів у мережі	2	3	4
Стратегія маршрутизації			
Одношляхова маршрутизація (4.35)	1–3	2–4	3–6
Багатошляхова маршрутизація (4.36)	2–5	2–6	3–7

Рішення, які представлені в цьому підрозділі, мають відношення до випадку, коли централізоване розв’язання маршрутних задач у кожному окремому домені покладалося на відповідний SDN-контролер домену (рис. 4.52). Якщо ж на рівні транспортної мережі використовується технологія MPLS, то для розрахунку внутрішньодоменних маршрутів «від джерела» на приграничних маршрутизаторах (LER) можна застосувати дворівневий метод, запропонований у підрозділі 4.2 цієї роботи. Тоді загальне розв’язання задачі міждоменної маршрутизації набуває тривірневої архітектури, як буде показано в наступному пункті.

**4.3.4. Тривірневий метод ієрархічно-координаційної маршрутизації в багатодоменній ІКМ**

Нехай для синтезу тривірневого методу структура ІКМ представляється у вигляді орієнтованого графа (4.31). Позначимо через  $K_r$  ( $K_r \in K$ ) множину потоків, що підлягають маршрутизації  $r$ -м приграничним маршрутизатором

$p$ -го домену:  $R_r^P$  ( $R_r^P \in R$ ). Для кожного  $k_r$ -го потоку ( $k_r \in K_r$ ) вважається відомою його середня швидкість пакетів (інтенсивність) –  $\lambda^{k_r}$  (1/с). Також для кожного  $p$ -го домену визначимо множину приграничних маршрутизаторів  $B^P$ , де  $B^P \in R^P$ , через які потоки пакетів надходять до цього домену або вибувають з нього. У свою чергу всю множину приграничних маршрутизаторів  $p$ -го домену можна поділити на дві підмножини:  $B_{in}^{p,k_r}$  ( $k_r \in K_r$ ) – підмножина приграничних маршрутизаторів, через які  $k_r$ -й потік надходить до  $p$ -го домену;  $B_{out}^{p,k_r}$  – підмножина приграничних маршрутизаторів, через які  $k_r$ -й потік вибуває з  $p$ -го домену. Для кожного каналу зв'язку  $p$ -го домену  $E_{i,j}^P$  через  $\varphi_{i,j}^P$  позначимо його пропускну здатність (1/с).

Нехай унаслідок розв'язання задачі ієрархічно-координаційної міждоменної маршрутизації «від джерела» для кожного  $p$ -го домену необхідно розрахувати маршрутні змінні  $x_{i,j}^{p,k_r}$ , які характеризують частку інтенсивності  $k_r$ -го потоку пакетів, що протікає в каналі  $E_{i,j}^P \in E^P$ . Для кожного маршрутизатора  $p$ -го домену необхідно виконати умови збереження для кожного  $k_r$ -го потоку. Якщо  $p$ -й домен є транзитним для  $k_r$ -го потоку пакетів, то подібні умови мають вигляд

$$\left\{ \begin{array}{l} \sum_{B_{in}^{p,k_r} \in B^P} \left( \sum_{E_{i,j}^P \in E^P} x_{i,j}^{p,k_r} - \sum_{E_{j,i}^P \in E^P} x_{j,i}^{p,k_r} \right) = 1; \\ \sum_{E_{i,j}^P \in E^P} x_{i,j}^{p,k_r} - \sum_{E_{j,i}^P \in E^P} x_{j,i}^{p,k_r} = 0; \\ \sum_{B_{out}^{p,k_r} \in B^P} \left( \sum_{E_{i,j}^P \in E^P} x_{i,j}^{p,k_r} - \sum_{E_{j,i}^P \in E^P} x_{j,i}^{p,k_r} \right) = -1. \end{array} \right. \quad (4.44)$$

Перша умова системи (4.44) справедлива для всіх приграничних маршрутизаторів, через які  $k_r$ -й потік надходить до  $p$ -го домену; друга умова вводиться для тих маршрутизаторів  $p$ -го домену, що для  $k_r$ -го потоку

є транзитними; третя умова має виконуватися для всіх приграничних маршрутизаторів, через які  $k_r$ -й потік вибуває з  $p$ -го домену.

Якщо  $k_r$ -й потік пакетів згенеровано в  $p$ -му домені, а його джерелом є, наприклад, маршрутизатор  $R_i^p$ , то для цієї мережі перша умова системи (4.44) дещо спроститься і набуде вигляду

$$\sum_{E_{i,j}^p \in E^p} x_{i,j}^{p,k_r} = 1.$$

Решта рівнянь у системі (4.44) залишиться незмінною. У разі, коли маршрутизатор  $R_i^p$   $p$ -го домену є отримувачем пакетів  $k_r$ -го потоку, то спроститься лише останнє рівняння системи (4.44), приймаючи такий вигляд:

$$\sum_{E_{j,i}^p \in E^p} x_{j,i}^{p,k_r} = 1.$$

З метою запобігання перевантаження каналів зв'язку  $p$ -го домену мультипотокним трафіком важливо виконати такі умови:

$$\sum_{R_r^p \in R^p} \sum_{k_r \in K_r} \lambda^{k_r} x_{i,j}^{p,k_r} \leq \varphi_{i,j}^p.$$

Ця умова орієнтована на централізовану маршрутизацію, коли розрахунок змінних  $x_{i,j}^{p,k_r}$  відбувається на єдиному SDN-контролері домену. Якщо за розрахунок внутрішньодомених маршрутів відповідає декілька, як правило, приграничних маршрутизаторів з множини  $R^p$ , то в цьому випадку умови запобігання перевантаження матимуть такий вигляд:

$$\sum_{k_r \in K_r} \lambda^{k_r} x_{i,j}^{p,k_r} \leq \varphi_{i,j}^p - \sum_{\substack{R_s^p \in R^p \\ s \neq r}} \sum_{k_s \in K_s} \lambda^{k_s} x_{i,j}^{p,k_s}, \quad p = \overline{1, N}. \quad (4.45)$$

Під час реалізації одношляхової маршрутизації на маршрутні змінні накладаються обмеження вигляду

$$x_{i,j}^{p,k_r} \in \{0,1\}, \quad (4.46)$$

а в разі забезпечення реалізації багатошляхової маршрутизації – умови вигляду

$$0 \leq x_{i,j}^{p,k_r} \leq 1. \quad (4.47)$$

Маршрутні змінні (4.46), (4.47) є координатами маршрутних векторів, які відповідно до проведеної структурної декомпозиції підлягають функціональній декомпозиції:

$$\vec{x}_p = \begin{bmatrix} \vec{x}_p^1 \\ \vec{x}_p^2 \\ \vdots \\ \vec{x}_p^r \\ \vdots \\ \vec{x}_p^{M^p} \end{bmatrix}, \quad \vec{x}_p^r = \begin{bmatrix} \vec{x}_p^{k_1} \\ \vec{x}_p^{k_2} \\ \vdots \\ \vec{x}_p^{k_r} \\ \vdots \\ \vec{x}_p^{\tilde{K}_r} \end{bmatrix}, \quad \vec{x}_p^{k_r} = \begin{bmatrix} x_{1,2}^{p,k_r} \\ x_{1,3}^{p,k_r} \\ \vdots \\ x_{i,j}^{p,k_r} \\ \vdots \\ x_{m_p,m_p-1}^{p,k_r} \end{bmatrix}. \quad (4.48)$$

У векторно-матричній формі умови (4.45) можна представити у вигляді

$$\sum_{k_r \in K_r} A_r^p \vec{x}_p^{k_r} \leq D_r^p \vec{\varphi}_p - \sum_{\substack{R_s^p \in R^p \\ s \neq r}} \sum_{k_s \in K_s} C_{rs}^p \vec{x}_p^{k_s}, \quad (4.49)$$

де  $\vec{x}_p^{k_r}$  – вектор, координатами якого є шукані змінні  $x_{i,j}^{p,k_r}$ ;

$\vec{\varphi}_p$  – вектор пропускних здатностей каналів ІКМ з координатами  $\varphi_{i,j}^p$ ;

$A_r^p$ ,  $D_r^p$ ,  $C_{rs}^p$  – матриці для погодження, тому що розміри векторів  $\vec{x}_p^{k_r}$  ( $R_r^p \in R^p$ ) та  $\vec{\varphi}_p$ , а також нумерація їх координат загалом можуть не збігатися.

За умови розподіленого (децентралізованого) розрахунку вектора  $\vec{x}_p^{k_r}$  на приграничних маршрутизаторах у межах кожного окремого  $p$ -го домену важливо забезпечити зв'язність міждомених маршрутів, тобто маршрутів, що проходять через множину маршрутизаторів різних доменів. Це стосується введення до структури моделі (4.45)–(4.49) умов міждоменної взаємодії

$$C_{p,q}^{k_r} \vec{x}_p^{k_r} = C_{q,p}^{k_r} \vec{x}_q^{k_r}, \quad p, q = \overline{1, N}, \quad p \neq q, \quad k_r \in K_r, \quad (4.50)$$

де  $C_{p,q}^{k_r}$  – матриця взаємодії  $p$ -го та  $q$ -го доменів, що має розмір  $m_{p,q} \times m_x^{p,k_r}$ ;

$m_{p,q} = |R^p \cap R^q|$  – кількість маршрутизаторів, через які проходить межа між  $p$ -м та  $q$ -м доменами;

$m_x^{p,k_r}$  – кількість координат  $x_{i,j}^{p,k_r}$  у векторі  $\vec{x}_p^{k_r}$ .

Ґрунтуючись на запропонованій вище математичній моделі (4.44)–(4.50), в основу трирівневого методу ієрархічно-координаційної міждоменної

маршрутизації буде покладено розв'язання оптимізаційної задачі щодо розрахунку векторів маршрутних змінних  $\bar{x}_p^{k_r}$  ( $p = \overline{1, N}$ ,  $k_r \in K_r$ ) за умови дотримання обмежень (4.44)–(4.47), (4.50) у використанні наступного критерію оптимальності отримуваних рішень [77–79]:

$$\min F, \quad F = \sum_{p \in N} \sum_{R_r^p \in R^p} \sum_{k_r \in K_r} \left( \bar{x}_p^{k_r} \right)^t H_p^{k_r} \bar{x}_p^{k_r}, \quad (4.51)$$

де  $H_p^{k_r}$  – діагональна матриця вагових коефіцієнтів, координатами якої, зазвичай, є маршрутні метрики каналів зв'язку в  $p$ -му домені ІКМ. Цільова функція  $F$  кількісно характеризує сумарні умовні витрати на організацію процесу міждоменної маршрутизації в ІКМ.

Для надання шуканим рішенням властивостей ієрархічно-координаційної маршрутизації в розв'язанні сформульованої оптимізаційної задачі, пов'язаної з мінімізацією виразу (4.51) за наявності обмежень (4.44)–(4.47), (4.50), буде використано принцип цільової координації [22, 23]. Тоді, переходячи до задачі на безумовний екстремум

$$\min_x F = \max_{\mu, \eta} L,$$

необхідно максимізувати за векторами множників Лагранжа  $\vec{\mu}$  та  $\vec{\eta}$  лагранжіан вигляду [77–79]:

$$\begin{aligned} L = & \sum_{p \in N} \sum_{R_r^p \in R^p} \sum_{k_r \in K_r} \left( \bar{x}_p^{k_r} \right)^t H_p^{k_r} \bar{x}_p^{k_r} + \\ & + \sum_{p=1}^N \sum_{\substack{q=1 \\ q \neq p}}^N \sum_{R_r^p \in R^p} \sum_{k_r \in K_r} \left( \vec{\mu}_{p,q}^{k_r} \right)^t \left( C_{p,q}^{k_r} \bar{x}_p^{k_r} - C_{q,p}^{k_r} \bar{x}_q^{k_r} \right) + \\ & + \sum_{p=1}^N \sum_{R_r^p \in R^p} \left( \vec{\eta}_p^{k_r} \right)^t \left( \sum_{k_r \in K_r} A_r^p \bar{x}_p^{k_r} - D_r^p \vec{\varphi}_p + \sum_{\substack{R_s^p \in R^p \\ s \neq r}} \sum_{k_s \in K_s} C_{rs}^p \bar{x}_p^{k_s} \right), \quad (4.52) \end{aligned}$$

де  $\vec{\mu}_{p,q}^{k_r}$  – підвектор вектора  $\vec{\mu}$ , що належить до векторно-матричної умови взаємодії  $p$ -го та  $q$ -го доменів, представлених виразом (4.50);

$\vec{\eta}_p^{k_r}$  – підвектор вектора  $\vec{\eta}$ , який належить до кожної з умов (4.49), представлених у кожному  $p$ -му домені.

Відповідно до змісту дворівневих методів, запропонованих у пунктах 4.2.2 та 4.3.2, загальна проблема міждоменної маршрутизації

«від джерела» формулюється як задача ієрархічно-координаційної трирівневої оптимізації. Зокрема задачі введених трьох ієрархічних рівнів маршрутизації полягають у такому:

- нульовий (нижній) рівень має забезпечувати розрахунок векторів маршрутних змінних  $\vec{x}_p^{k_r}$  ( $p = \overline{1, N}$ ,  $k_r \in K_r$ ) на кожному з приграничних маршрутизаторів доменів ІКМ;
- перший рівень відповідає за запобігання перевантаження каналів зв'язку в кожному з доменів ІКМ шляхом розрахунку вектора множників Лагранжа  $\vec{\eta}$ ;
- другий (верхній) рівень відповідає за забезпечення зв'язності міждоменних маршрутів шляхом розрахунку вектора множників Лагранжа  $\vec{\mu}$ .

Оскільки вектори множників Лагранжа  $\vec{\mu}$  та  $\vec{\eta}$  розраховуються на верхніх ієрархічних рівнях і для нульового рівня є фіксованими параметрами, то вираз (4.52) можна представити в такій декомпозиційній формі:

$$\begin{aligned}
 L &= \sum_{p=1}^N \sum_{R_r^p \in R^p} L_r^p, \\
 L_r^p &= \sum_{k_r \in K_r} \left( \vec{x}_p^{k_r} \right)^t H_p^{k_r} \vec{x}_p^{k_r} + \\
 &+ \sum_{\substack{q=1 \\ p \neq q}}^N \sum_{k_r \in K_r^+} \left( \vec{\mu}_{p,q}^{k_r} \right)^t C_{p,q}^{k_r} \vec{x}_p^{k_r} - \sum_{\substack{q=1 \\ p \neq q}}^N \sum_{k_r \in K_r^-} \left( \vec{\mu}_{q,p}^{k_r} \right)^t C_{p,q}^{k_r} \vec{x}_p^{k_r} + \\
 &+ \left( \vec{\eta}_p^{k_r} \right)^t \left( \sum_{k_r \in K_r} A_r^p \vec{x}_p^{k_r} - D_r^p \vec{\phi}_p + \sum_{\substack{R_s^p \in R^p \\ s \neq r}} \sum_{k_s \in K_s} \left( \vec{\eta}_p^{k_s} \right)^t C_{sr}^p \vec{x}_p^{k_r} \right). \quad (4.53)
 \end{aligned}$$

Отже, на нульовому рівні кожен  $r$ -й приграничний маршрутизатор  $p$ -го домену буде формувати маршрутні змінні, представлені векторами  $\vec{x}_p^{k_r}$  ( $p = \overline{1, N}$ ,  $R_r^p \in R^p$ ,  $k_r \in K_r$ ), шляхом мінімізації лагранжіану (4.53).

На першому рівні методу відбувається координація рішень, отриманих з нульового рівня, для запобігання перевантаження каналів зв'язку (4.43) в кожному окремо взятому домені

$$\vec{\eta}_p^{k_r}(a+1) = \vec{\eta}_p^{k_r}(a) + \nabla \vec{\eta}_p^{k_r}, \quad (4.54)$$

де  $a$  – номер ітерації роботи координатора першого рівня, яким є SDN-контролер кожного окремого домену;



$\nabla \vec{\eta}_p^{k_r}$  – градієнт функції (4.54), який розраховується відповідно до отримуваних з нижнього рівня результатів розв’язання задач маршрутизації  $\vec{x}_p^{k_r*}$  ( $p = \overline{1, N}$ ,  $R_r^p \in R^p$ ,  $k_r \in K_r$ ) у кожному конкретному домені

$$\nabla \vec{\eta}_p^{k_r}(x) \Big|_{x=x^*} = \sum_{k_r \in K_r} A_r^p \vec{x}_p^{k_r} - D_r^p \vec{\varphi}_p + \sum_{\substack{R_s^p \in R^p \\ s \neq r}} \sum_{k_s \in K_s} C_{rs}^p \vec{x}_p^{k_s}. \quad (4.55)$$

За умови наближення координат градієнта  $\nabla \vec{\eta}_p^{k_r}$  до нуля буде забезпечуватися виконання умов запобігання перевантаження каналів (4.49) у кожному з доменів ІКМ.

Завдання координатора другого рівня полягає в забезпеченні виконання умов міждоменної взаємодії (4.50) шляхом модифікації векторів множників Лагранжа такої градієнтної ітераційної процедури:

$$\vec{\mu}_{p,q}^{k_r}(b+1) = \vec{\mu}_{p,q}^{k_r}(b) + \nabla \vec{\mu}_{p,q}^{k_r}, \quad (4.56)$$

де  $b$  – номер ітерації роботи координатора другого рівня;

$\nabla \vec{\mu}_{p,q}^{k_r}$  – градієнт функції (4.56), який розраховується відповідно до отримуваних з першого рівня результатів розв’язання задач маршрутизації  $\vec{x}_p^{k_r*}$  ( $p = \overline{1, N}$ ,  $k_r \in K_r$ ) під час виконання умов (4.49) у кожному конкретному домені

$$\nabla \vec{\mu}_{p,q}^{k_r}(x) \Big|_{x=x^*} = C_{p,q}^{k_r} \vec{x}_p^{k_r} - C_{q,p}^{k_r} \vec{x}_q^{k_r}. \quad (4.57)$$

У разі наближення значень координат градієнта (4.57) до нуля буде забезпечуватися зв’язність міждомених маршрутів. Загальний оптимум досягається, коли  $\nabla \vec{\eta}_p^{k_r}(x)$  та  $\nabla \vec{\mu}_{p,q}^{k_r}(x)$  наблизяться до нуля.

Ефективність запропонованого трирівневого методу ієрархічно-координаційної міждоменної маршрутизації з точки зору оптимальності та оперативності отримуваних рішень багато в чому залежить від швидкості збіжності процедур координації (4.54), (4.55) та (4.56), (4.57). З технологічного боку, чим менше ітерацій потрібно для отримання шуканого оптимального рішення, тим меншим є обсяг службового трафіку, який передається між ієрархічними рівнями про результати розрахунків на кожній з ітерацій, та нижчим є час розв’язання задачі міждоменної маршрутизації в ІКМ загалом. На рис. 4.66 наведено структуру трирівневого методу ієрархічно-координаційної маршрутизації.

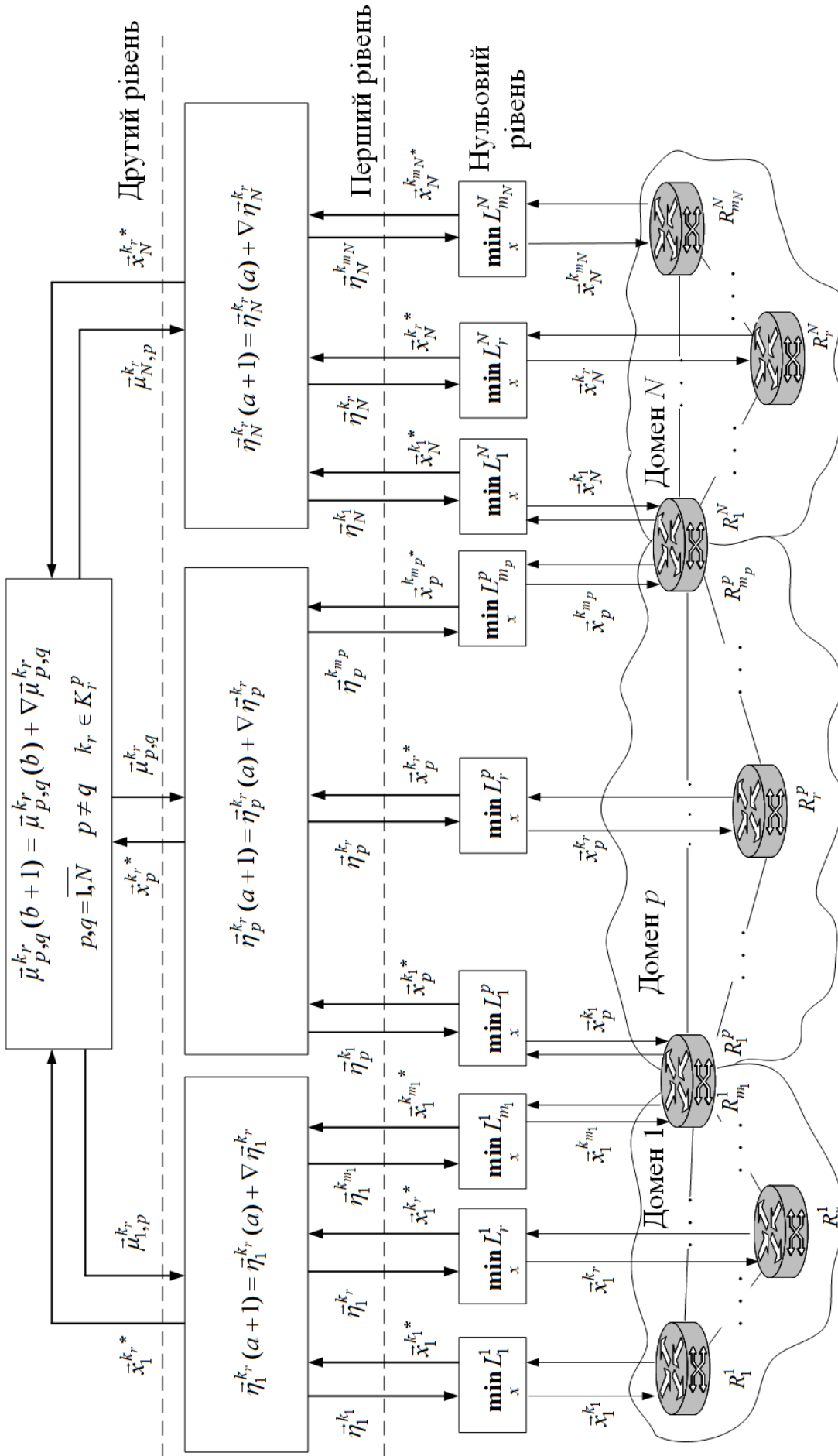


Рис. 4.66. Структура тривірневого методу ієрархічно-координатної маршрутизації

#### 4.4. Синтез і дослідження математичної моделі та методу ієрархічної міждоменної швидкої перемаршрутизації в ІКМ

Як зазначалось у першому розділі, відмінною властивістю функціонування протоколів маршрутизації OSPF та IS-IS є використання мультидоменних рішень. Зокрема маршрутизатори різних доменів (ділянок, кластерів, підмереж) можуть обмінюватися пакетами через один (опорний) домен, що, як правило, має нульовий номер. Важливо врахувати, що застосування єдиного приграничного маршрутизатора для зв'язку звичайного та опорного доменів істотно знижує відмовостійкість ТКМ загалом [46–49, 82]. У разі, коли приграничний маршрутизатор не в змозі забезпечити свою функціональність (перевантаження, збій, компрометація), то підключений через нього домен стає блокованим щодо опорного домену, а також до інших доменів мережі.

У зв'язку з цим для підвищення відмовостійкості мережних рішень на практиці все частіше для зв'язку звичайних доменів та опорного домену ІКМ використовуються кілька приграничних маршрутизаторів [82, 83]. У випадку відмови одного з них трафік може передаватися через працездатні маршрутизатори. Однак у процесі розв'язання задач маршрутизації міждоменних потоків виникає низка важливих особливостей, які варто врахувати.

*Перша особливість* пов'язана з тим, що у розв'язанні задач міждоменної маршрутизації треба передбачити реалізацію схем захисту приграничних маршрутизаторів у разі їх відмов з причин, наведених у підрозділі 2.1. Таким чином, поряд з множиною основних маршрутів необхідно розрахувати і множину резервних шляхів, які є обхідними щодо маршрутизатора, який захищається.

*Друга особливість* полягає в тому, що з'являється неоднозначність у порядку використання приграничних маршрутизаторів, який визначається, з одного боку, в опорному домені, а з іншого, у звичайних доменах мережі. Це може супроводжуватися порушенням зв'язності міждоменних маршрутів на границі «опорний домен – звичайний домен», а за умови багатошляхової маршрутизації неоднозначність може проявлятися також у неузгодженому балансуванні трафіку на приграничних маршрутизаторах.

Тому актуальним є завдання, пов'язане з підвищенням узгодженості (координованості) рішень щодо швидкої перемаршрутизації, отримуваних у звичайних доменах та опорному домені. Це може бути досягнуто на підставі перегляду математичних моделей і методів, покладених в основу відповідних протоколів ієрархічної маршрутизації. Для забезпечення високого рівня теоретичного обґрунтування шуканих рішень пропонується використовувати

положення, принципи та постулати теорії багаторівневих ієрархічних систем, запропонованої Месаровичем [22] та розвиненої Сінгхом і Тітлі [23]. Подібний підхід уже застосовується для вирішення завдань ієрархічного управління трафіком [50, 70].

#### 4.4.1. Декомпозиційна модель ієрархічної міждоменної швидкої перемаршрутизації в ІКМ

Припустимо, що структура ієрархічної ІКМ (рис. 4.67), як показано в пункті 4.3.1, представлена орієнтованим графом  $\Gamma = (R, E)$ . Тоді в разі синтезу декомпозиційної моделі ієрархічної міждоменної швидкої перемаршрутизації припустимо, що ІКМ складається з  $P$  доменів, пов'язаних між собою за принципом побудови IP-мереж.

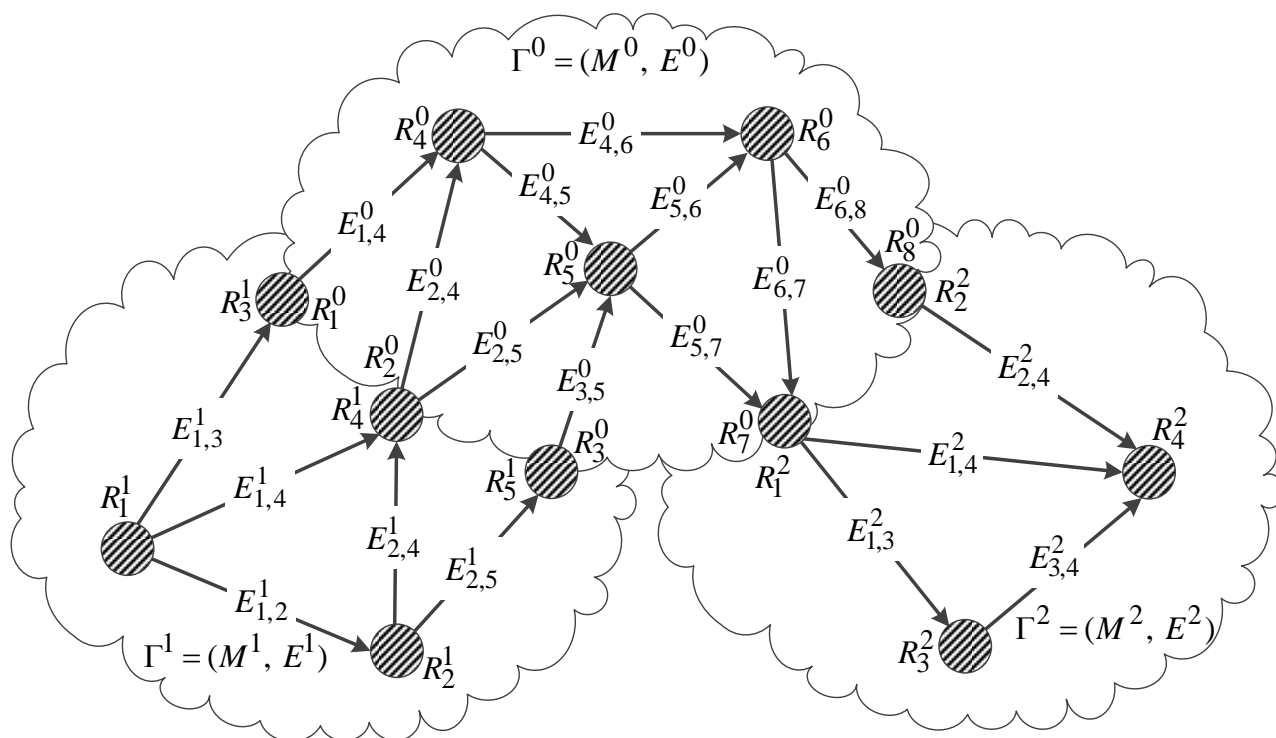


Рис. 4.67. Приклад структури ієрархічної мультидоменної мережі

Нехай кожен окремий  $p$ -й домен мережі описується підграфом  $\Gamma^p = (R^p, E^p)$  графа  $\Gamma$ , де  $R^p = \{R_i^p; i = \overline{1, m_p}\}$  – множина маршрутизаторів  $p$ -го домену, а  $m_p$  – загальна кількість маршрутизаторів у домені;  $E^p = \{E_{i,j}^p; i, j = \overline{1, m_p}, i \neq j\}$  – множина каналів зв'язку, які з'єднують маршрутизатори  $p$ -го домену ( $p = \overline{0, P}$ ). У цьому випадку нульовий номер надається опорному домену (backbone area), який задається підграфом  $\Gamma^0 = (R^0, E^0)$ . Інші  $P$  доменів обмінюються пакетами через цей опорний домен.

Припустимо, що за умови декомпозиції мережі границя між доменами проходить через маршрутизатори, як у протоколі OSPF [10, 14]. Тоді на основі введеної структурної моделі мережі мають місце такі умови:

$$\begin{cases} R^p \cap R^q = 0, & p, q = \overline{1, P}, p \neq q; \\ R^0 \cap R^p \neq 0, & p = \overline{1, P}; \\ E^p \cap E^q = 0, & p, q = \overline{0, P}, p \neq q. \end{cases} \quad (4.58)$$

Реалізація умов (4.58) визначає те, що тільки опорний домен може мати спільні маршрутизатори з іншими доменами. Крім того, кожен окремий канал зв'язку мережі належить лише одному домену. З метою підвищення відмовостійкості мережі кількість приграничних маршрутизаторів між доменами має бути рівною двом або більше. Зокрема, якщо один з подібних маршрутизаторів відмовить, усі потоки будуть переспрямовані на інші приграничні маршрутизатори.

Також для кожного  $p$ -го домену визначимо множину приграничних маршрутизаторів  $B^p$  ( $B^p \subset R^p$ ), через які потоки надходять до нього або виходять. Таким чином, уся множина приграничних маршрутизаторів  $p$ -го домену може бути поділена на дві підмножини, де  $B_{in}^{p,k}$  – підмножина приграничних маршрутизаторів, через які  $k$ -й потік надходить до  $p$ -го домену, а  $B_{out}^{p,k}$  – підмножина приграничних маршрутизаторів, через які  $k$ -й потік виходить з  $p$ -го домену. З кожним каналом зв'язку  $p$ -го домену пов'язана його пропускна здатність  $\varphi_{i,j}^p$  (1/с). Позначимо через  $R_{i*}^p \subset R^p / B_{out}^{p,k}$  множину маршрутизаторів, суміжних з маршрутизатором  $R_i^p$ .

Припустимо, що для структури мережі, представленої на рис. 4.67, джерелом  $k$ -го потоку є один з маршрутизаторів першого домену, а отримувачем – маршрутизатор другого домену. Тоді введені підмножини приграничних маршрутизаторів мають такий вигляд:

$$B_{out}^{1,k} = \{R_3^1, R_4^1, R_5^1\}; B_{in}^{0,k} = \{R_1^0, R_2^0, R_3^0\}; B_{out}^{0,k} = \{R_7^0, R_8^0\}; B_{in}^{2,k} = \{R_1^2, R_2^2\}.$$

Задамо множину маршрутизаторів, суміжних з маршрутизатором  $R_4^1$  першого домену:  $R_{4*}^1 = \{R_1^1, R_2^1\}$ . Той самий маршрутизатор  $R_4^1$  позначається як  $R_2^0$  у нульовому домені, для якого множина суміжних маршрутизаторів є такою:  $R_{2*}^0 = \{R_4^0, R_5^0\}$ . Розв'язуючи задачу ієрархічної міждоменної

маршрутизації для кожного  $p$ -го домену, необхідно розрахувати маршрутні змінні  $x_{i,j}^{p,k}$ , які характеризують частку інтенсивності  $k$ -го потоку в каналі зв'язку  $E_{i,j}^p \in E^p$ . Для кожного маршрутизатора  $p$ -го домену необхідно виконати умови збереження кожного  $k$ -го потоку, щоб забезпечити зв'язність розрахованих міждоменних маршрутів у мережі. Якщо  $p$ -й домен є опорним доменом для  $k$ -го потоку, то ці умови мають такий вигляд:

$$\left\{ \begin{array}{l} \sum_{B_{in}^{0,k} \in B^0} \left( \sum_{E_{i,j}^0 \in E^0} x_{i,j}^{0,k} - \sum_{E_{j,i}^0 \in E^0} x_{j,i}^{0,k} \right) = 1; \\ \sum_{E_{i,j}^0 \in E^0} x_{i,j}^{0,k} - \sum_{E_{j,i}^0 \in E^0} x_{j,i}^{0,k} = 0; \\ \sum_{B_{out}^{0,k} \in B^0} \left( \sum_{E_{i,j}^0 \in E^0} x_{i,j}^{0,k} - \sum_{E_{j,i}^0 \in E^0} x_{j,i}^{0,k} \right) = -1. \end{array} \right. \quad (4.59)$$

Перше рівняння в системі (4.59) вводиться для всіх маршрутизаторів опорного домену, через які  $k$ -й потік надходить до цього домену. Друге рівняння вводиться для всіх маршрутизаторів опорного домену, які є транзитними для  $k$ -го потоку в опорному домені. Тоді як третє рівняння в системі (4.59) вводиться для всіх маршрутизаторів опорного домену, через які  $k$ -й потік виходить з опорного домену.

Якщо  $k$ -й потік надходить до мережі через  $p$ -й домен, а його джерелом є, наприклад, маршрутизатор  $R_i^p$ , то для цього випадку умови збереження мають такий вигляд:

$$\left\{ \begin{array}{l} \sum_{E_{i,j}^p \in E^p} x_{i,j}^{p,k} = 1; \\ \sum_{E_{i,j}^p \in E^p} x_{i,j}^{p,k} - \sum_{E_{j,i}^p \in E^p} x_{j,i}^{p,k} = 0; \\ \sum_{B_{out}^{p,k} \in B^p} \left( \sum_{E_{i,j}^p \in E^p} x_{i,j}^{p,k} - \sum_{E_{j,i}^p \in E^p} x_{j,i}^{p,k} \right) = -1. \end{array} \right. \quad (4.60)$$

Коли маршрутизатор  $R_i^p$  в  $p$ -му домені є отримувачем  $k$ -го потоку, то мають місце такі умови збереження для кожного  $k$ -го потоку:

$$\left\{ \begin{array}{l} \sum_{B_{in}^{p,k} \in B^p} \left( \sum_{E_{i,j}^p \in E^p} x_{i,j}^{p,k} - \sum_{E_{j,i}^p \in E^p} x_{j,i}^{p,k} \right) = 1; \\ \sum_{E_{i,j}^p \in E^p} x_{i,j}^{p,k} - \sum_{E_{j,i}^p \in E^p} x_{j,i}^{p,k} = 0; \\ \sum_{E_{j,i}^p \in E^p} x_{j,i}^{p,k} = 1. \end{array} \right. \quad (4.61)$$

У разі одношляхової маршрутизації потоків мають місце такі умови:

$$x_{i,j}^{p,k} \in \{0, 1\}, \quad (4.62)$$

а для реалізації багатошляхової стратегії маршрутизації маршрутні змінні мають відповідати умовам:

$$0 \leq x_{i,j}^{p,k} \leq 1. \quad (4.63)$$

У цьому випадку маршрутні змінні (4.62), (4.63) є координатами відповідних маршрутних векторів:

$$\vec{x} = \begin{bmatrix} \bar{x}_1 \\ \bar{x}_2 \\ \vdots \\ \bar{x}_p \\ \vdots \\ \bar{x}_N \end{bmatrix}, \quad \vec{x}_p = \begin{bmatrix} \bar{x}_p^1 \\ \bar{x}_p^2 \\ \vdots \\ \bar{x}_p^k \\ \vdots \\ \bar{x}_p^{|K|} \end{bmatrix}, \quad \vec{x}_p^k = \begin{bmatrix} x_{1,2}^{p,k} \\ x_{1,3}^{p,k} \\ \vdots \\ x_{i,j}^{p,k} \\ \vdots \\ x_{m_p, m_p-1}^{p,k} \end{bmatrix}, \quad (4.64)$$

де  $\vec{x}$  – вектор маршрутних змінних, що визначає основні маршрути в мережі загалом;

$\vec{x}_p$  – вектор маршрутних змінних, який визначає основні маршрути в  $p$ -му домені;

$\vec{x}_p^k$  – вектор маршрутних змінних, що визначає основний шлях (шляхи) для  $k$ -го потоку в  $p$ -му домені.

У разі розподіленого (децентралізованого) розрахунку векторів  $\vec{x}_p$  та  $\vec{x}_p^k$  у кожному окремому домені важливо забезпечити зв'язність міждоменних

маршрутів, які проходять через множину маршрутизаторів у різних доменах. Відповідно до результатів, отриманих у пункті 4.3.1, це означає необхідність уведення в структуру моделі (4.58)–(4.64) додаткових умов міждоменної взаємодії

$$C_{p,0}^k \bar{x}_p^k = C_{0,p}^k \bar{x}_0^k, \quad p = \overline{1, P}, \quad k \in K, \quad (4.65)$$

де  $C_{p,0}^k$  – матриця взаємодії між  $p$ -м та опорним доменами під час передачі пакетів  $k$ -го потоку, яка має розмір  $m_{p,0} \times m_x^{p,k}$ ;

$m_{p,0} = |R^p \cap R^0|$  – кількість маршрутизаторів, що є граничними між  $p$ -м та опорним доменами;

$m_x^{p,k}$  – кількість координат  $x_{i,j}^{p,k}$  вектора  $\bar{x}_p^k$ .

#### 4.4.2. Умови захисту приграничних маршрутизаторів під час ієрархічно-координативної міждоменної швидкої перемаршрутизації в ІКМ

Для розв'язання задачі відмовостійкої міждоменної маршрутизації поряд з розрахунком основних маршрутів необхідно розрахувати і множину резервних шляхів. Тому вводяться додаткові маршрутні змінні  $\bar{x}_{i,j}^{p,k}$ .

За аналогією з виразами (4.64) змінні  $\bar{x}_{i,j}^{p,k}$  також можна представити у вигляді координат відповідних векторів  $\bar{\bar{x}}$ ,  $\bar{\bar{x}}_p$  і  $\bar{\bar{x}}_p^k$ , зокрема для резервних маршрутів також необхідно виконати умови міждоменної взаємодії

$$C_{p,0}^k \bar{\bar{x}}_p^k = C_{0,p}^k \bar{\bar{x}}_0^k, \quad p = \overline{1, P}, \quad k \in K. \quad (4.66)$$

У цій роботі пропонуються схеми захисту приграничного маршрутизатора шляхом захисту множини каналів зв'язку, інцидентних вузлу, що захищається. Якщо ж один з маршрутизаторів  $p$ -го домену є джерелом  $k$ -го потоку, тоді в процесі реалізації одношляхової маршрутизації для захисту приграничного маршрутизатора  $R_i^p \in B_{out}^{p,k}$  треба виконати такі умови:

$$\bar{x}_{j,i}^{p,k} \in \{0; \delta_{j,i}^{p,k}\} \quad \forall R_j^p \in R_{i*}^p, \quad \text{якщо } R_{i*}^p \subset R^p \setminus B_{out}^{p,k}, \quad (4.67)$$

де

$$\delta_{j,i}^{p,k} = \begin{cases} 0, & \text{за умови захисту каналу зв'язку } E_{j,i}^p; \\ 1, & \text{в іншому випадку.} \end{cases} \quad (4.68)$$



Під час багатошляхової маршрутизації мають виконуватися умови

$$0 \leq \bar{x}_{j,i}^{p,k} \leq \delta_{j,i}^{p,k} \quad \forall R_j^p \in R_{i^*}^p, \text{ якщо } R_{i^*}^p \subset R^p \setminus B_{out}^{p,k}, \quad (4.69)$$

де вибір значень  $\delta_{j,i}^{p,k}$  також підпорядковується умові (4.68).

У позначеннях опорного домену (backbone area) для приграничного маршрутизатора  $R_z^0 \in B_{in}^{0,k}$ , який підлягає захисту, у разі одношляхової маршрутизації ці ж умови записуються в такому вигляді:

$$\bar{x}_{z,j}^{0,k} \in \{0; \delta_{z,j}^{0,k}\} \quad \forall R_j^0 \in R_{z^*}^0, \text{ коли } R_{z^*}^0 \subset R^0 \setminus B_{in}^{0,k}. \quad (4.70)$$

Тоді як для багатошляхової маршрутизації вводяться умови

$$0 \leq \bar{x}_{z,j}^{0,k} \leq \delta_{z,j}^{0,k} \quad \forall R_j^0 \in R_{z^*}^0, \text{ якщо } R_{z^*}^0 \subset R^0 \setminus B_{in}^{0,k}. \quad (4.71)$$

Якщо ж один з маршрутизаторів  $p$ -го домену є отримувачем пакетів  $k$ -го потоку, то для одношляхової маршрутизації у процесі захисту приграничного маршрутизатора  $R_i^p \in B_{in}^{p,k}$  необхідне виконання нижченаведених умов:

$$\bar{x}_{i,j}^{p,k} \in \{0; \delta_{i,j}^{p,k}\} \quad \forall R_j^p \in R_{i^*}^p, \text{ коли } R_{i^*}^p \subset R^p \setminus B_{in}^{p,k}, \quad (4.72)$$

де

$$\delta_{i,j}^{p,k} = \begin{cases} 0, & \text{за умови захисту каналу зв'язку } E_{i,j}^p; \\ 1, & \text{в іншому випадку.} \end{cases} \quad (4.73)$$

У разі багатошляхової маршрутизації мають виконуватися умови

$$0 \leq \bar{x}_{i,j}^{p,k} \leq \delta_{i,j}^{p,k} \quad \forall R_j^p \in R_{i^*}^p, \text{ якщо } R_{i^*}^p \subset R^p \setminus B_{in}^{p,k}, \quad (4.74)$$

де вибір значень  $\delta_{i,j}^{p,k}$  підпорядковується умові (4.68).

У позначеннях опорного домену для маршрутизатора  $R_z^0 \in B_{out}^{0,k}$ , що захищається, для одношляхової маршрутизації ці умови записуються у вигляді

$$\bar{x}_{j,z}^{0,k} \in \{0; \delta_{j,z}^{0,k}\} \quad \forall R_j^0 \in R_{z^*}^0, \text{ якщо } R_{z^*}^0 \subset R^0 \setminus R_{out}^{0,k}. \quad (4.75)$$

У процесі реалізації стратегії багатошляхової маршрутизації маємо умови:

$$0 \leq \bar{x}_{j,z}^{0,k} \leq \delta_{j,z}^{0,k} \quad \forall R_j^0 \in R_{z^*}^0, \text{ коли } R_{z^*}^0 \subset R^0 \setminus R_{out}^{0,k}. \quad (4.76)$$

За необхідності здійснення резервування пропускної здатності мережі, а також з метою запобігання можливого перевантаження каналів зв'язку під час реалізації стратегій як одношляхової, так і багатошляхової маршрутизації в модель за аналогією до (2.20) вводяться такі умови:

$$\frac{1}{2} \sum_{k \in K} \lambda^k \left[ x_{i,j}^{p,k} + \bar{x}_{i,j}^{p,k} + \left| x_{i,j}^{p,k} - \bar{x}_{i,j}^{p,k} \right| \right] \leq \varphi_{i,j}^p, \quad p = \overline{0, P}. \quad (4.77)$$

#### 4.4.3. Метод ієрархічно-координаційної міждоменної швидкої перемаршрутизації в ІКМ

Ураховуючи запропоновану вище математичну модель (4.58)–(4.77), основою методу ієрархічної міждоменної швидкої перемаршрутизації в ІКМ, що пропонується, є розв’язок оптимізаційної задачі на підставі розрахунку векторів маршрутних змінних  $\vec{x}_p^k$  та  $\overleftarrow{x}_p^k$  ( $p = \overline{0, P}$ ,  $k \in K$ ) з урахуванням обмежень (4.59)–(4.63), (4.65)–(4.77) під час використання такого критерію оптимальності:

$$\min_{x, \bar{x}} F, F = \sum_{p=0}^P \sum_{k \in K} \left[ \left( \vec{x}_p^k \right)^t H_p^k \vec{x}_p^k + \left( \overleftarrow{x}_p^k \right)^t H_p^k \overleftarrow{x}_p^k \right], \quad (4.78)$$

де  $H_p^k$  – діагональна матриця вагових коефіцієнтів, координатами якої, як правило, є маршрутні метрики каналів зв’язку  $p$ -го домену. Цільова функція  $F$  характеризує сумарну умовну вартість організації ієрархічної міждоменної швидкої перемаршрутизації в ІКМ.

Цільову функцію (4.64) можна представити в адитивній формі

$$F = \sum_{p=0}^P F_p, F_p = \sum_{k \in K} \left[ \left( \vec{x}_p^k \right)^t H_p^k \vec{x}_p^k + \left( \overleftarrow{x}_p^k \right)^t H_p^k \overleftarrow{x}_p^k \right]. \quad (4.79)$$

Особливістю формулювання та подальшого розв’язання оптимізаційної задачі (4.79) є те, що розрахунок векторів  $\vec{x}_p^k$  та  $\overleftarrow{x}_p^k$  з метою підвищення масштабованості маршрутних рішень можна здійснювати за кожним доменом окремо, мінімізуючи  $F_p$ . Первинний вибір маршрутів у кожному з доменів пояснюється тим, що вони оптимальні, тобто «найкоротші» в межах вибраних метрик  $H_p^k$ . Якщо на головній діагоналі матриці  $H_p^k$  (4.79) розташовані величини  $10^8 / \varphi_{i,j}^p$  за аналогією до значень маршрутних метрик у протоколі OSPF [10, 14], то ці маршрути є, з одного боку, найбільш продуктивними, з іншого, – вони містять мінімальну кількість переприйомів, оскільки застосовується адитивний критерій.

Проте якщо розрахунок основних і резервних маршрутів у різних доменах здійснюється незалежно один від одного, то зв’язність міждоменних шляхів може не забезпечуватися, тобто умови міждоменної взаємодії (4.65), (4.66) можуть порушуватися. З метою забезпечення виконання умов

міждоменної взаємодії (4.65), (4.66) у збереженні децентралізації розрахунку  $\bar{x}_p^k$  та  $\bar{\bar{x}}_p^k$  за окремими доменами пропонується використати принцип цільової координації [22, 23]. Тоді, переходячи до задачі на безумовний екстремум

$$\min_{x, \bar{x}} F = \max_{\mu, \eta} L,$$

необхідно максимізувати за  $\bar{\mu}$  та  $\bar{\eta}$  такий лагранжیان:

$$\begin{aligned} L = & \sum_{p=0}^P \sum_{k \in K} \left[ \left( \bar{x}_p^k \right)^t H_{p, \bar{x}_p^k}^k + \left( \bar{\bar{x}}_p^k \right)^t H_{p, \bar{\bar{x}}_p^k}^k \right] + \\ & + \sum_{p=1}^P \sum_{k \in K} \left( \bar{\mu}_{p,0}^k \right)^t \left( C_{p,0}^k \bar{x}_p^k - C_{0,p}^k \bar{\bar{x}}_0^k \right) + \\ & + \sum_{p=1}^P \sum_{k \in K} \left( \bar{\eta}_{p,0}^k \right)^t \left( C_{p,0}^k \bar{\bar{x}}_p^k - C_{0,p}^k \bar{\bar{x}}_0^k \right), \end{aligned} \quad (4.80)$$

де  $\bar{\mu}$  – вектор множників Лагранжа для основного маршруту;

$\bar{\eta}$  – вектор множників Лагранжа для резервного маршруту;

$\bar{\mu}_{p,0}^k$  – підвектори вектора  $\bar{\mu}$ , що мають відношення до кожної з векторно-матричних умов міждоменної взаємодії (4.65) для основного маршруту;

$\bar{\eta}_{p,0}^k$  – підвектори вектора  $\bar{\eta}$ , що мають відношення до кожної з векторно-матричних умов міждоменної взаємодії (4.66) для резервного маршруту.

У межах принципу цільової координації пропонується ввести таку ієрархію розрахунків: на нижньому рівні в кожному з доменів окремо розраховувати маршрутні вектори  $\bar{x}_p^k$  та  $\bar{\bar{x}}_p^k$ , а на верхньому рівні обчислювати вектори множників Лагранжа  $\bar{\mu}$  та  $\bar{\eta}$  для забезпечення виконання умов міждоменної взаємодії (4.65) та (4.66). Тоді, зважаючи на те, що в межах принципу цільової координації вектори множників Лагранжа розраховуються на верхньому рівні та для нижнього рівня є відомими значеннями, вираз (4.80) можна представити в такій декомпозиційній формі:

$$\begin{aligned} L &= \sum_{p=0}^P L_p, \\ L_0 &= \sum_{k \in K} \left[ \left( \bar{x}_0^k \right)^t H_{0, \bar{x}_0^k}^k + \left( \bar{\bar{x}}_0^k \right)^t H_{0, \bar{\bar{x}}_0^k}^k \right], \end{aligned}$$

$$\begin{aligned}
L_p = & \sum_{k \in K} \left[ \left( \bar{x}_p^k \right)^t H_p^k \bar{x}_p^k + \left( \bar{\bar{x}}_p^k \right)^t H_p^k \bar{\bar{x}}_p^k \right] + \\
& + \sum_{k \in K_p^+} \left( \bar{\mu}_{p,0}^k \right)^t C_{p,0}^k \bar{x}_p^k - \sum_{k \in K_p^-} \left( \bar{\mu}_{q,0}^k \right)^t C_{p,0}^k \bar{x}_p^k + \\
& + \sum_{k \in K_p^+} \left( \bar{\eta}_{p,0}^k \right)^t C_{p,0}^k \bar{\bar{x}}_p^k - \sum_{k \in K_p^-} \left( \bar{\eta}_{q,0}^k \right)^t C_{p,0}^k \bar{\bar{x}}_p^k, \quad p = \overline{1, P}, \quad (4.81)
\end{aligned}$$

де  $K_p^+$  – підмножина потоків, що надходять з інших доменів мережі до  $p$ -го домену, який є доменом маршрутизатора-отримувача для  $k$ -го потоку;

$K_p^-$  – підмножина потоків, що виходять з  $p$ -го домену, який є доменом маршрутизатора-джерела для  $k$ -го потоку ( $K_p^+, K_p^- \in K$ ).

Згідно з проведеною декомпозицією у виразі (4.81) усі складники належать до  $p$ -го домену, зокрема другий, третій, четвертий та п'ятий складники в цьому виразі відповідають за узгодження порядку маршрутизації для основного та резервного шляхів вихідних і вхідних потоків відповідно для  $p$ -го домену ІКМ.

Таким чином, загальна проблема міждоменної швидкої перемаршрутизації сформульована як задача ієрархічно-координаційної дворівневої оптимізації. На нижньому ієрархічному рівні відбувається розрахунок маршрутних змінних, представлених векторами  $\bar{x}_p^k$  та  $\bar{\bar{x}}_p^k$  ( $p = \overline{0, P}$ ,  $k \in K$ ), у процесі мінімізації (4.81).

Водночас головним завданням верхнього рівня запропонованого методу є координація рішень, отриманих на нижньому рівні, з метою забезпечення виконання умов міждоменної взаємодії (4.65) та (4.66) шляхом модифікації векторів множників Лагранжа у виконанні градієнтної ітераційної процедури [22, 23]:

$$\bar{\mu}_{p,0}^k(i+1) = \bar{\mu}_{p,0}^k(i) + \nabla \bar{\mu}_{p,0}^k; \quad \bar{\eta}_{p,0}^k(i+1) = \bar{\eta}_{p,0}^k(i) + \nabla \bar{\eta}_{p,0}^k, \quad (4.82)$$

де  $i$  – номер координаційної ітерації;

$\nabla \bar{\mu}_{p,0}^k$  і  $\nabla \bar{\eta}_{p,0}^k$  – градієнти, які розраховуються, виходячи з отримуваних на нижньому рівні результатів розв'язання задач маршрутизації  $\bar{x}_p^{k*}$  та  $\bar{\bar{x}}_p^{k*}$  у кожному конкретному домені ( $p \neq 0$ ):

$$\begin{cases} \left. \nabla \bar{\mu}_{p,0}^k(x) \right|_{x = x^*} = C_{p,0}^k \bar{x}_p^k - C_{0,p}^k \bar{x}_0^k; \\ \left. \nabla \bar{\eta}_{p,0}^k(\bar{x}) \right|_{\bar{x} = \bar{x}^*} = C_{p,0}^k \bar{\bar{x}}_p^k - C_{0,p}^k \bar{\bar{x}}_0^k. \end{cases} \quad (4.83)$$

За умови наближення значень градієнтів (4.83) до нуля буде забезпечуватися зв'язність міждоменних основних і резервних маршрутів. Ефективність запропонованого методу міждоменної швидкої перемаршрутизації з точки зору оптимальності та оперативності отримуваних рішень багато в чому залежить від швидкості збіжності координаційної процедури (4.82)–(4.83). З технологічної точки зору, чим менше ітерацій потрібно для отримання шуканого оптимального рішення, тим нижчий обсяг службового трафіку, що циркулює в мережі та передається між ієрархічними рівнями щодо результатів розрахунків на кожній з ітерацій, і меншим є час розв'язання задач ієрархічної маршрутизації в ІКМ загалом.

#### 4.4.4. Дослідження методу ієрархічно-координаційної міждоменної швидкої перемаршрутизації в ІКМ

Особливості роботи та ефективність запропонованого методу з підтвердженням адекватності математичної моделі, покладеної в його основу, буде продемонстровано на наступному числовому прикладі. Для цього було обрано структуру ІКМ, яка показана на рис. 4.68 та складається з трьох доменів: нульового, першого та другого.

Маршрутизатори, розміщені в 1, 2 та 0-му доменах відповідно, зручно представити у вигляді таких множин:  $R^1 = \{R_1^1, R_2^1, R_3^1, R_4^1, R_5^1\}$ ;  $R^2 = \{R_1^2, R_2^2, R_3^2, R_4^2\}$ ;  $R^0 = \{R_1^0, R_2^0, R_3^0, R_4^0, R_5^0, R_6^0, R_7^0, R_8^0\}$ . Взаємодія між першим та опорним доменами здійснюється через маршрутизатори  $R_3^1 (R_1^0)$ ,  $R_4^1 (R_2^0)$  та  $R_5^1 (R_3^0)$ . Тоді як взаємодія між опорним та другим доменами реалізується через маршрутизатори  $R_7^0 (R_1^2)$  та  $R_8^0 (R_2^2)$ . Припустимо, що вузлом-джерелом є маршрутизатор  $R_1^1$ , розташований у першому домені, а вузлом-отримувачем є маршрутизатор  $R_4^2$ , розміщений у другому домені. Крім того, на рис. 4.68 у розривах каналів зв'язку мережі показано їх пропускну здатність  $\varphi_{i,j}^p$  (1/с).

Під час дослідження інтенсивність потоку пакетів, що передавався в мережі, за умови реалізації стратегії одношляхової маршрутизації змінювалася від 10 1/с до 100 1/с, а в разі багатошляхової маршрутизації – від 10 1/с до 200 1/с.

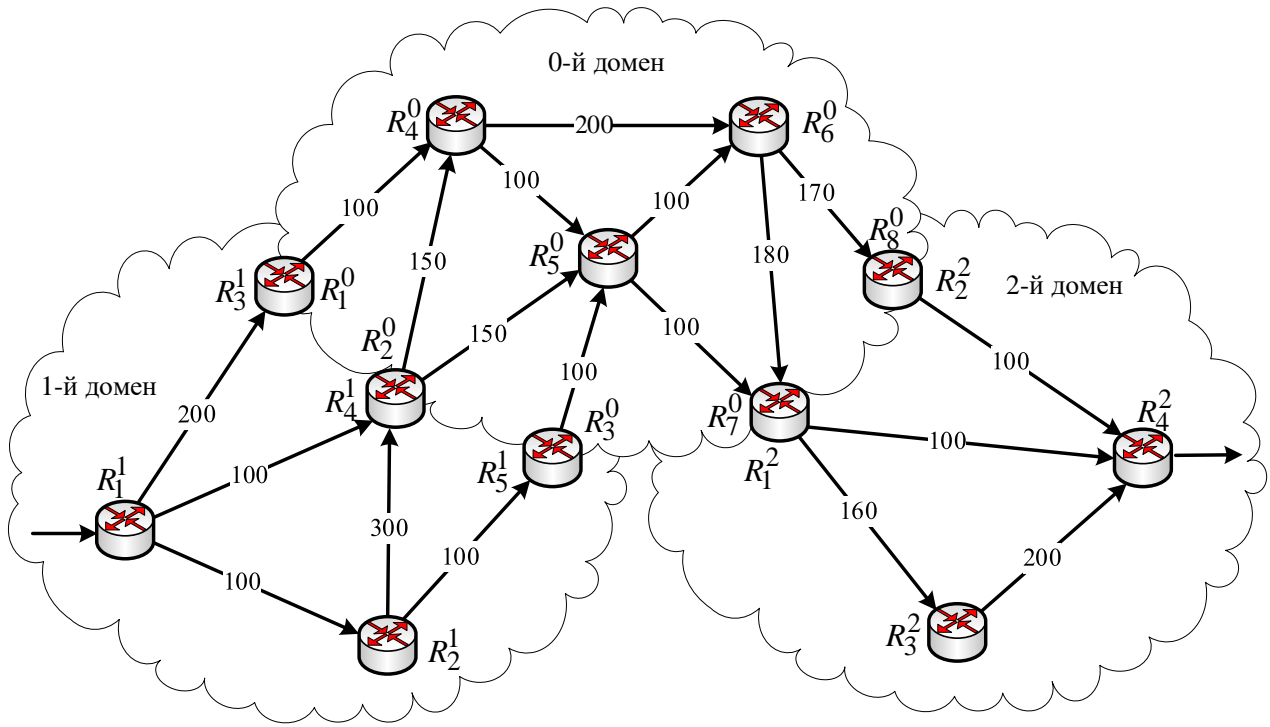


Рис. 4.68. Структура мережі, яка використовувалася в дослідженні методу

Нехай в мережі, структура якої наведена на рис. 4.68, необхідно захистити приграничний маршрутизатор  $R_4^1$  ( $R_2^0$ ), що розміщений на межі першого й опорного доменів. У випадку інтенсивності потоку в межах від 10 1/с до 100 1/с реалізовувалася одношляхова маршрутизація. Скоординоване розв'язання задачі міждоменної швидкої перемаршрутизації, представлене основним маршрутом, показано на рис. 4.69, а резервним – на рис. 4.70.

Розрахований (основний або резервний) шлях представлений суцільною лінією, тоді як невикористовувані канали зв'язку зображені напівпрозорими лініями. На рис. 4.69 та 4.70 у розривах каналів зв'язку вказаний дріб, де в чисельнику представлена інтенсивність потоку пакетів, що передається, а в знаменнику – пропускна здатність каналу зв'язку. Розрахований основний шлях (рис. 4.69) містить такі маршрутизатори різних доменів, зокрема приграничний маршрутизатор  $R_4^1$  ( $R_2^0$ ):

$$R_1^1 \rightarrow R_4^1 (R_2^0) \rightarrow R_5^0 \rightarrow R_7^0 (R_1^2) \rightarrow R_4^2.$$

Резервний маршрут представлений на рис. 4.70:

$$R_1^1 \rightarrow R_2^1 \rightarrow R_5^1 (R_3^0) \rightarrow R_5^0 \rightarrow R_7^0 (R_1^2) \rightarrow R_4^2.$$

Він не містить приграничний маршрутизатор  $R_4^1$  ( $R_2^0$ ), який захищається.

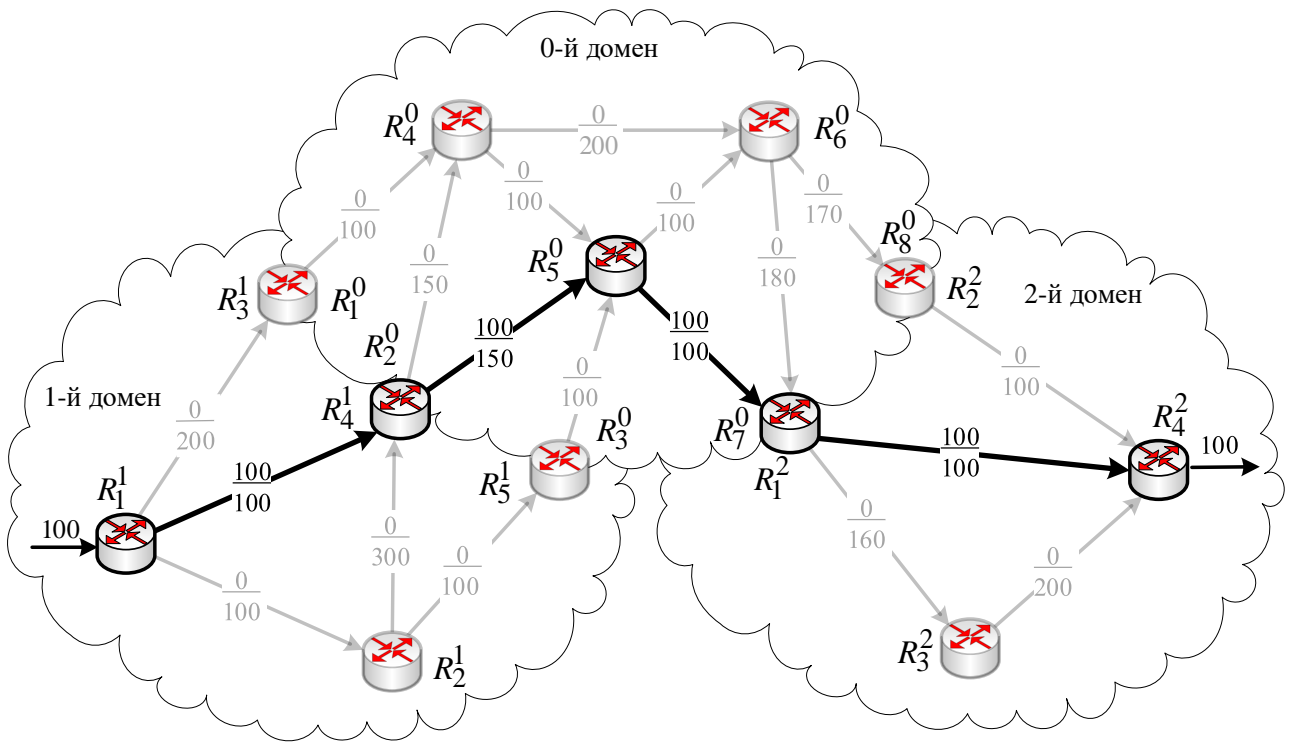


Рис. 4.69. Скоординоване розв'язання задачі міждоменної одношляхової маршрутизації потоку інтенсивністю 100 1/с, представлене основним маршрутом

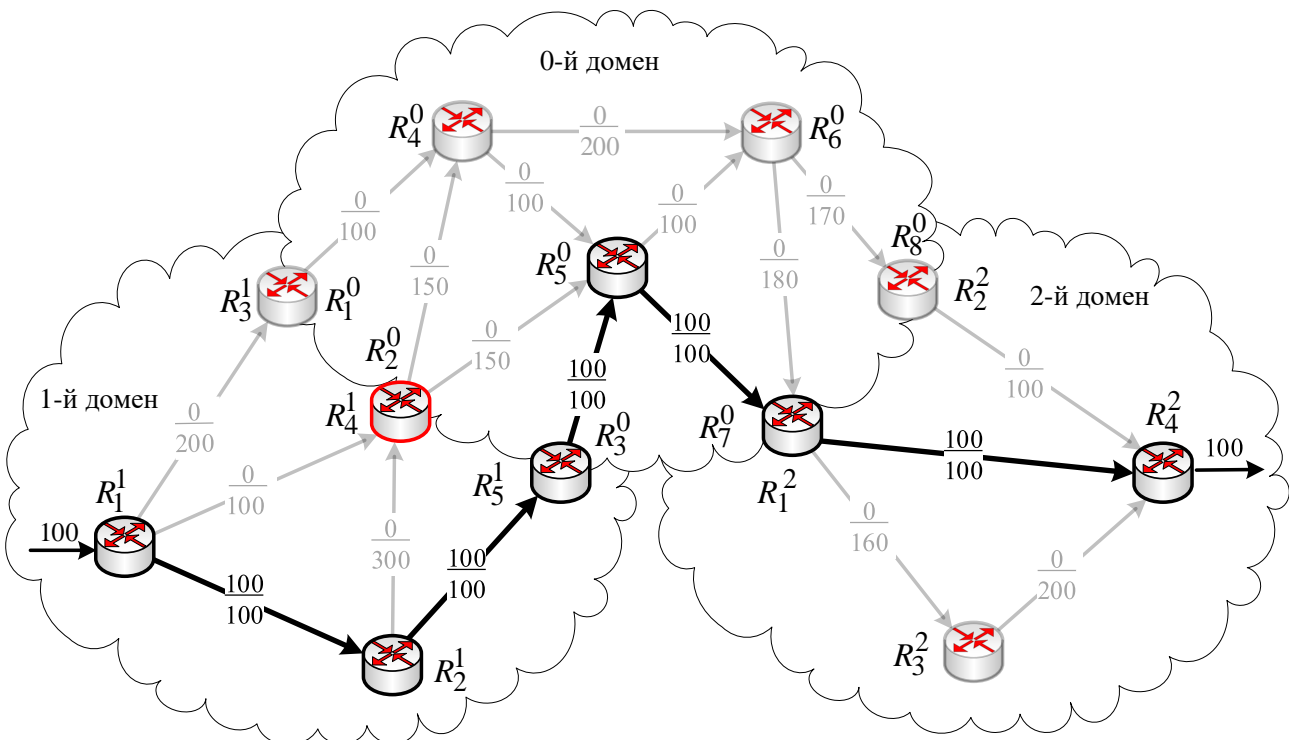


Рис. 4.70. Скоординоване розв'язання задачі міждоменної одношляхової маршрутизації потоку інтенсивністю 100 1/с, представлене резервним маршрутом

Кожен з розрахованих маршрутів відповідно до умови (4.77) надає потоку, що передається, необхідну пропускну здатність. Це рішення було отримано після другої координаційної ітерації (4.82), (4.83), оскільки у початковому розрахунку не була забезпечена зв'язність міждоменного маршруту, тому що умови міждоменної взаємодії (4.65) та (4.66) не виконувалися.

Нехай, як і раніше, необхідно забезпечити захист приграничного маршрутизатора  $R_4^1 (R_2^0)$  за умови подальшого збільшення інтенсивності того ж потоку до 200 1/с в ІКМ, структура якої представлена на рис. 4.68. Для реалізації багатошляхової швидкої перемаршрутизації збіжність координаційної процедури забезпечувалася вже після третьої ітерації. Скоординоване рішення показано на рис. 4.71 та 4.72 для основного та резервного маршрутів відповідно. На цих рисунках позначення в розривах каналів зв'язку ідентичні тим, що наведені на рис. 4.69 та 4.70. Основний мультишлях для передачі потоку 200 1/с від маршрутизатора-джерела пакетів до маршрутизатора-отримувача містить два шляхи, якими передаються потоки з однаковою інтенсивністю 100 1/с (рис. 4.71):

- $R_1^1 \rightarrow R_4^1 (R_2^0) \rightarrow R_4^0 \rightarrow R_6^0 \rightarrow R_7^0 (R_1^2) \rightarrow R_4^2$ ;
- $R_1^1 \rightarrow R_2^1 \rightarrow R_4^1 (R_2^0) \rightarrow R_5^0 \rightarrow R_7^0 (R_1^2) \rightarrow R_3^2 \rightarrow R_4^2$ .

Резервний мультишлях, який використовується для захисту приграничного вузла  $R_4^1 (R_2^0)$ , також складається з двох шляхів (рис. 4.72), кожним з яких передається потік інтенсивністю 100 1/с:

- $R_1^1 \rightarrow R_3^1 (R_1^0) \rightarrow R_4^0 \rightarrow R_6^0 \rightarrow R_7^0 (R_1^2) \rightarrow R_4^2$ ;
- $R_1^1 \rightarrow R_2^1 \rightarrow R_5^1 (R_3^0) \rightarrow R_5^0 \rightarrow R_7^0 (R_1^2) \rightarrow R_3^2 \rightarrow R_4^2$ .

Ефективність практичної реалізації запропонованого методу багато в чому залежить від швидкості збіжності координаційної процедури (4.82), (4.83). Мінімізація кількості координаційних ітерацій дозволяє, по-перше, пропорційно зменшити обсяги циркулюючої службової інформації про стан мережі, а по-друге, підвищити оперативність вирішення маршрутних завдань загалом. У процесі дослідження встановлено, що на швидкість збіжності координаційної процедури впливало багато різних чинників:

- реалізована стратегія маршрутизації: одношляхова чи багатошляхова;
- кількість приграничних маршрутизаторів;
- завантаженість мережі;



- структура доменів, зокрема опорного;
- зв'язність та кількість доменів.

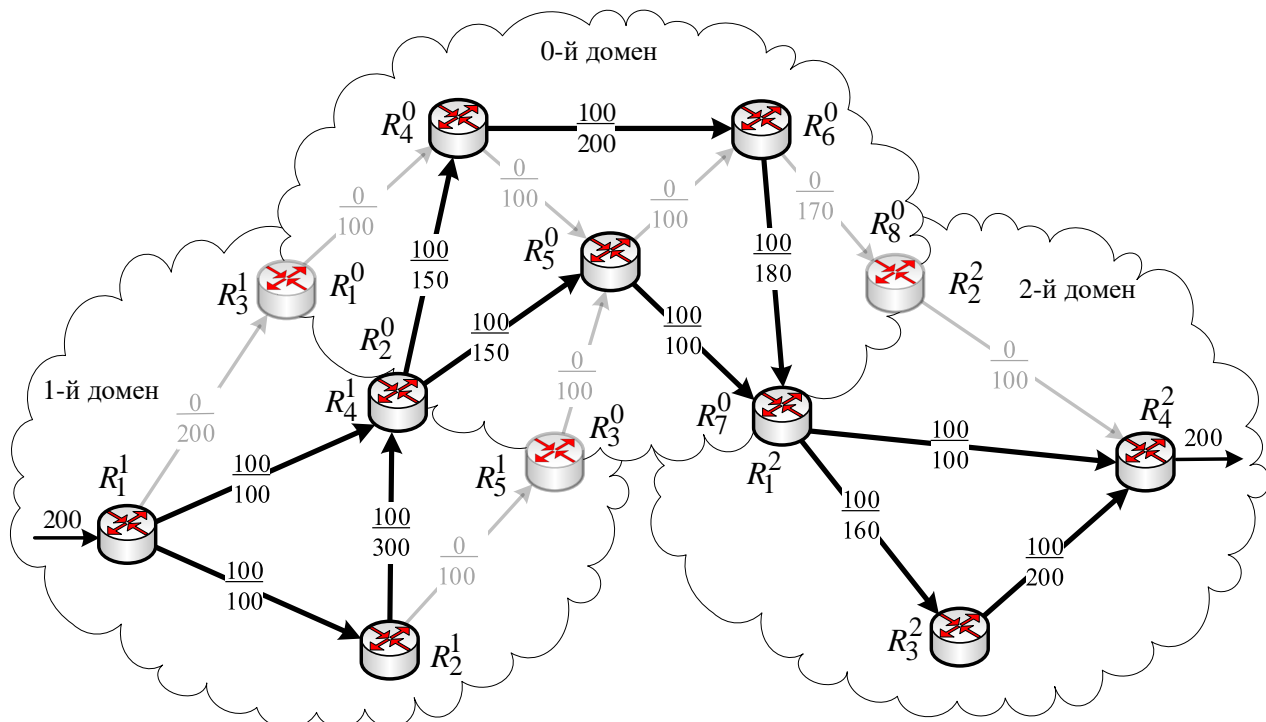


Рис. 4.71. Скоординоване розв'язання задачі міждоменної багатопляхової маршрутизації потоку інтенсивністю 200 1/с, представлене основним мультишляхом

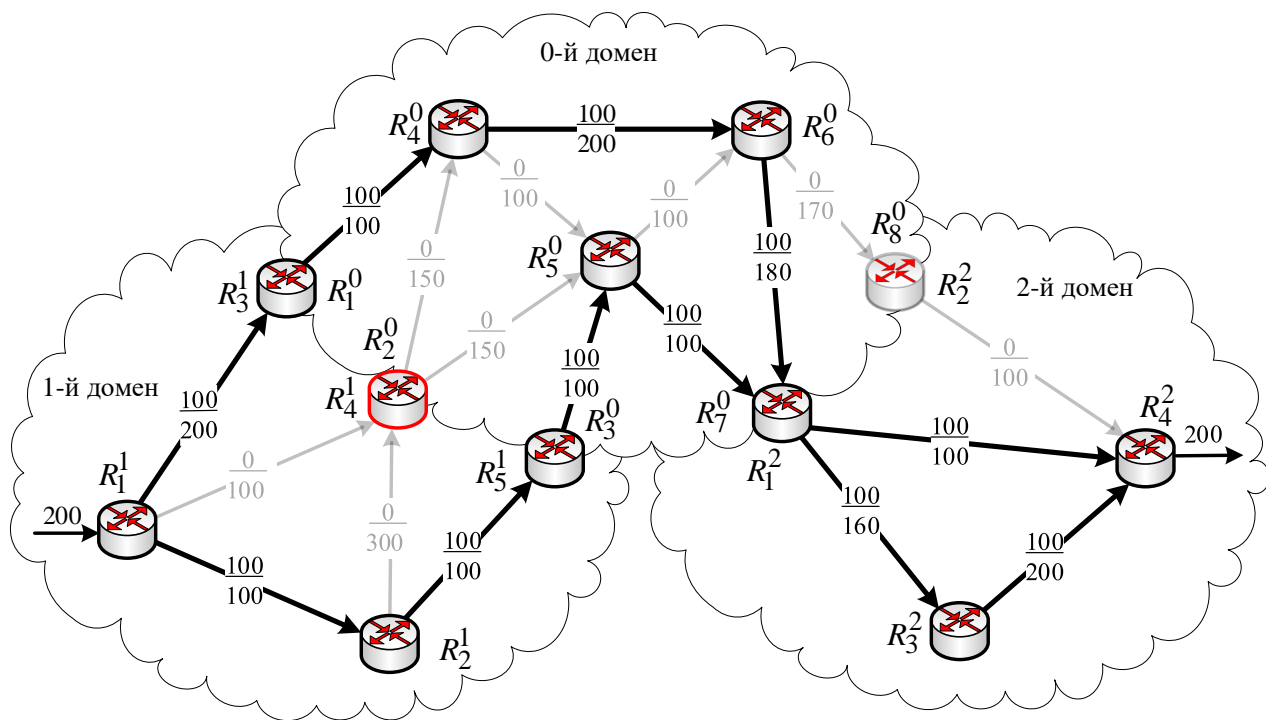


Рис. 4.72. Скоординоване розв'язання задачі міждоменної багатопляхової маршрутизації потоку інтенсивністю 200 1/с, представлене резервним мультишляхом

Представлений перелік чинників упорядкований за ступенем зниження впливу на швидкість збіжності процедури (4.82), (4.83). Тобто найбільша кількість координаційних ітерацій залежала від реалізованої стратегії маршрутизації та кількості приграничних маршрутизаторів, і меншою мірою – від структури доменів та їх зв'язності. Загалом у використанні двох приграничних маршрутизаторів кожним з доменів кількість координаційних ітерацій становила в середньому  $1 \div 2$  у разі використання одношляхової маршрутизації або  $2 \div 3$  – за умови багатошляхової маршрутизації (табл. 4.8).

Таблиця 4.8

**Результати аналізу впливу кількості приграничних маршрутизаторів і використаної стратегії маршрутизації на кількість ітерацій координаційної процедури (4.82), (4.83) запропонованого методу**

Кількість приграничних маршрутизаторів у домені	Стратегія маршрутизації	
	Одношляхова	Багатошляхова
2	$1 \div 2$	$2 \div 3$
3	$2 \div 3$	$3 \div 4$

Якщо структура доменів містила три приграничних маршрутизатора, то середня кількість координаційних ітерацій у процедурі (4.82), (4.83) зростала до  $2 \div 3$  за умови одношляхової або до  $3 \div 4$  – багатошляхової маршрутизації (табл. 4.8). Зростання кількості ітерацій було обумовлено тим, що зі збільшенням кількості приграничних маршрутизаторів і переходом до багатошляхової маршрутизації зростала і кількість варіантів рішень, що отримуються в окремих доменах, які треба узгодити за допомогою координаційної процедури (4.82), (4.83). Під час досліджень також встановлено, що розміри доменів та зв'язність внутрішньодомених маршрутизаторів на швидкість збіжності координаційної процедури (4.82), (4.83) істотно не впливали.

**Висновки до четвертого розділу**

1. У процесі проведеного аналізу встановлено, що дієвим засобом підвищення масштабованості ІКМ є використання ієрархічної маршрутизації, яка на сьогоднішній день представлена множиною протокольних рішень. Проте наявні протоколи ієрархічної маршрутизації (OSPF, IS-IS, EGP/BGP) оснований лише на введенні структурної ієрархії мережі та використанні досить простих комбінаторних алгоритмів пошуку найкоротшого шляху на

графі, за допомогою якого описується структура ІКМ. Це значно знижує ефективність функціонування ІКМ і передбачає перегляд і вдосконалення наявних моделей і методів ієрархічної маршрутизації, на яких основані відомі протокольні рішення.

2. У цьому розділі запропоновано декомпозиційну модель ієрархічно-координаційної внутрішньодоменної маршрутизації одно- або багатоадресних потоків у програмно-конфігурованій інфокомунікаційній мережі SDN/MPLS-TE. Залежно від постановки задачі та множини вихідних даних запропонована модель може бути адаптована під випадок використання маршрутних метрик (4.12) та вимог концепції Traffic Engineering (4.24). Для реалізації стратегії маршрутизації «від джерела», яка є характерною для MPLS-мереж, здійснена декомпозиція умов запобігання перевантаження каналів зв'язку (4.10), (4.11) та балансування навантаження (4.19).

3. Удосконалено метод ієрархічно-координаційної внутрішньодоменної маршрутизації «від джерела» в інфокомунікаційній мережі SDN/MPLS-TE. В основу методу покладено розв'язання сформульованої в межах запропонованої декомпозиційної моделі оптимізаційної задачі щодо розрахунку векторів маршрутних змінних на кожному з приграничних маршрутизаторів MPLS-мережі. Для розв'язання оптимізаційної задачі з критеріями оптимальності (4.12) або (4.24) використано принцип цільової координації з уведенням дворівневої ієрархії розрахунків. На нижньому рівні кожним з приграничних маршрутизаторів розраховувався вектор маршрутних змінних для потоків, які надходили через нього до мережі. На верхньому рівні здійснювалася координація рішень нижнього рівня для запобігання перевантаження каналів зв'язку MPLS-мережі, оскільки приграничні маршрутизатори розраховують маршрутні вектори незалежно один від одного. У межах запропонованого методу процес пошуку оптимальних маршрутних векторів набував ітераційного характеру.

4. Установлено, що для мінімізації часу розв'язання маршрутних задач та з метою зниження обсягів службового трафіку, що циркулює в мережі, важливо забезпечити високу швидкість збіжності координаційної процедури (4.16), (4.17). У зв'язку з цим проведено кількісний аналіз чинників, що впливають на збіжність координаційної процедури методу ієрархічно-координаційної внутрішньодоменної маршрутизації. З'ясовано, що із збільшенням розміру мережі, зв'язності її маршрутизаторів і навантаженості ІКМ загалом кількість ітерацій координаційної процедури зростає. Показано, що за умови

завантаженості мережі менш ніж на 50% перевантаження каналів зв'язку не спостерігалось (табл. 4.2), а метод досягав оптимуму за одну ітерацію. Однак у разі збільшення завантаженості мережі від 55% і більше кількість ітерацій координаційної процедури нелінійно зростала у зв'язку з можливим перевантаженням каналів зв'язку через непогодженість роботи окремих приграничних маршрутизаторів.

5. За результатами проведеного дослідження було визначено, що причина зростання кількості ітерацій координаційної процедури (4.16), (4.17) – це перевантаження віддалених за кількістю переприйомів від маршрутизатора-відправника або отримувача каналів зв'язку. Це обумовлено тим, що використання квадратичного критерію оптимальності (4.12) та ТЕ-критерію (4.24) сприяє збалансованій завантаженості всіх каналів зв'язку ІКМ. У зв'язку з цим у роботі запропоновано використовувати модифікацію маршрутної метрики для каналів зв'язку мережі, представленої виразом (4.18). Використання модифікації маршрутної метрики (4.18) у методі (4.13)–(4.17) дозволило, як показали чисельні результати розрахунку для множини мережних структур та різної завантаженості мережі, знизити кількість ітерацій координаційної процедури в середньому від 1,5 до 4 разів (рис. 4.13, 4.20, 4.27). Використання ТЕ-критерію оптимальності (4.24) та виразів (4.28)–(4.30) дозволяє зменшити кількість ітерацій координаційної процедури (4.16), (4.17) від 1,5–2 до 3,5–5 разів, а в деяких випадках і до 8 разів (рис. 2.24). За умови маршрутизації багатоадресних потоків використання запропонованих рішень дозволило підвищити збіжність координаційної процедури в середньому в 1,5–2 рази (табл. 4.5). Це особливо характерно для високої завантаженості мережі, що і визначає ділянку переважного використання пропонуваного рішення на практиці шляхом зміни наявних або розроблення нових протоколів маршрутизації.

6. Запропоновані маршрутні рішення мають високу масштабованість, що дозволило: значно знизити розмір маршрутних задач (пропорційно кількості приграничних маршрутизаторів) та обчислювальну складність їх розв'язання, покращити збіжність координаційної процедури (4.16), (4.17) з відповідним зниженням обсягів службової інформації, що циркулює в мережі, про її стан, та максимального часу оновлення маршрутних векторів. Крім того, запропонований метод може бути адаптований і на випадок, коли задачі ієрархічних рівнів розв'язуються на SDN-контролері з багатопроекторною (багатоядерною) архітектурою. Тобто за розрахунок векторів маршрутних змінних  $\vec{x}_r$  у

розв'язанні відповідних оптимізаційних задач (4.15) або (4.27) можуть відповідати окремі процесори (ядра) обчислювальної системи SDN-контролера. Розпаралелювання розрахунків також сприяє підвищенню обчислювальної потужності SDN-контролера та масштабованості SDN-архітектури загалом.

7. Під час розрахунків також оцінювалося у відсотковому вираженні розбіжність між значеннями критеріїв оптимальності, які отримувалися за умови ієрархічно-координаційної (4.12) та централізованої маршрутизації. Розбіжність була в межах від 2% до 5% у разі зростання завантаженості мережі для структур з невеликим розміром (рис. 4.14) і становила від 3% до 11% для структур з більшим розміром (рис. 4.7, 4.21). За ТЕ-показниками (4.20) та (4.24) отримані ієрархічно-координаційні рішення відрізнялися від централізованих не більше ніж на 3–7%.

8. У розділі запропоновано математичну модель та метод ієрархічно-координаційної міждоменної маршрутизації у програмно-конфігурованій ІКМ. Новизна моделі полягає в тому, що на основі її декомпозиційного представлення щодо кожного окремого домену, по-перше, набули нової форми умови збереження потоку (4.33) для доменів різних типів: відправників, отримувачів пакетів та транзитних доменів; по-друге, вдалося коректно сформулювати умови міждоменної взаємодії (4.38), виконання яких гарантувало структурну та функціональну зв'язність міждоменних маршрутів.

9. Обґрунтовано вибір принципу цільової координації як основи запропонованого методу ієрархічно-координаційної міждоменної маршрутизації, наблизивши якість розподіленої маршрутизації за доменами до результатів централізованої маршрутизації. Водночас вдалося суттєво знизити розмірність маршрутної задачі, що в підсумку сприяє підвищенню масштабованості рішень щодо міждоменної маршрутизації. Використання запропонованого методу гарантувало збіжність координаційної процедури (4.42), (4.43) за кінцеве число ітерацій, що було підтверджено у розрахункових прикладах.

10. У процесі дослідження запропонованого методу ієрархічно-координаційної міждоменної маршрутизації в програмно-конфігурованій інфокомунікаційній мережі проаналізовано вплив структури мережі, зв'язності маршрутизаторів, кількості приграничних маршрутизаторів, реалізованої стратегії маршрутизації (одно або багатопляхової) та завантаженості ІКМ на збіжність координаційної процедури (4.42), (4.43). Результати дослідження виявили, що до збільшення кількості ітерацій координаційної процедури (4.42), (4.43) призводило, насамперед, зростання завантаженості ІКМ, реалізація

багатошляхової стратегії маршрутизації, а також збільшення кількості приграничних маршрутизаторів. Це пояснювалося розширенням кількості можливих варіантів розв'язання задачі маршрутизації в окремих доменах, що і призводило до збільшення кількості ітерацій (до 3÷4) координаційної процедури. Інші особливості структури доменів ІКМ на збіжність методу значно не впливали. У процесі реалізації одношляхової маршрутизації метод забезпечував зв'язність міждоменного маршруту в середньому за 1÷2 ітерації роботи координаційної процедури.

11. У розділі запропоновано трирівневий метод ієрархічно-координаційної маршрутизації «від джерела» в ІКМ. Запропонований метод є удосконаленням методу міждоменної маршрутизації в мережі SDN, у межах якого розрахунок маршрутних змінних усередині доменів проводився централізовано на відповідних SDN-контролерах. Метод може застосовуватись у SDN/MPLS-мережах, коли в кожному з доменів реалізується розподілена маршрутизація «від джерела» на приграничних маршрутизаторах. В основу методу покладено принцип цільової координації, за допомогою якого вдалося розділити задачу розрахунку маршрутних змінних для передачі пакетів від маршрутизатора-відправника до маршрутизатора-отримувача на три рівні з послідовною координацією рішень. На нульовому рівні відбувається розрахунок маршрутних змінних приграничними маршрутизаторами кожного домену; на першому рівні здійснюється координація рішень нульового рівня для запобігання перевантаження каналів зв'язку в кожному окремому домені; а основне завдання координатора другого рівня полягає в забезпеченні структурної та функціональної зв'язності міждоменних маршрутів.

12. З'ясовано, що застосування запропонованих дворівневого та трирівневого методів міждоменної маршрутизації в мережі SDN дозволяє підвищити масштабованість маршрутних рішень, знизити обчислювальну складність розрахунків, зменшивши розмір задач маршрутизації (пропорційно кількості доменів в ІКМ) без суттєвої втрати якості балансування навантаження в SDN/MPLS-мережі. Мінімізація кількості ітерацій координаційної процедури сприяє також зменшенню, по-перше, обсягів службової інформації про стан мережі, що циркулює в ІКМ, по-друге, загального часу розв'язання задачі міждоменної маршрутизації в SDN/MPLS-мережі.

13. З метою підвищення масштабованості та відмовостійкості маршрутних рішень у розділі запропоновано математичну модель та метод ієрархічної міждоменної швидкої перемаршрутизації в ІКМ. Представлений

метод оснований на декомпозиційному поданні потокової моделі маршрутизації (4.44)–(4.50) з уведенням умов взаємодії доменів (4.51), (4.52) для забезпечення зв'язності міждоменних маршрутів – основних та резервних. Крім того, у модель включено умови резервування приграничних маршрутизаторів, адаптованих як під реалізацію одношляхової, так і багатошляхової маршрутизації (4.53)–(4.63). В основу запропонованого методу міждоменної швидкої перемаршрутизації покладено розв'язання оптимізаційної задачі, пов'язаної з мінімізацією завантаженості каналів зв'язку мережі (4.64). Запропонований метод (4.65)–(4.69) використовує принцип цільової координації для забезпечення узгодженості маршрутних рішень, отримуваних за окремими доменами. У межах розглянутого прикладу продемонстровано працездатність запропонованого методу з точки зору збіжності координаційної процедури (4.68), (4.69) і забезпечення захисту приграничних маршрутизаторів під час реалізації одношляхової або багатошляхової маршрутизації.

14. Доведено, що використання запропонованого методу дозволяє підвищити якість вирішення маршрутних завдань у мережах ієрархічної структури, а саме істотно знизити розміри маршрутних таблиць та обчислювальну складність отримуваних рішень за рахунок зменшення розміру розв'язуваної оптимізаційної задачі у визначенні маршрутних векторів. У процесі досліджень встановлено, що на ефективність запропонованого методу з точки зору швидкості збіжності координаційної процедури (4.68), (4.69) найсильніше впливала кількість приграничних маршрутизаторів і реалізована стратегія маршрутизації. Загалом метод збігався до оптимальних рішень за  $1 \div 2$  ітерації процедури (4.68), (4.69) під час реалізації одношляхової маршрутизації, за  $2 \div 3$  ітерації – за умови багатошляхової маршрутизації через два приграничних маршрутизатори і за  $3 \div 4$  ітерації – у разі багатошляхової маршрутизації через три приграничних маршрутизатори.

15. У процесі розрахунків також оцінено у відсотковому відношенні розбіжність між значеннями критеріїв оптимальності, які отримувалися за умови ієрархічно-координаційної маршрутизації (4.39) та розрахованих для випадку централізованої маршрутизації. Розбіжність збільшувалася в разі збільшення кількості доменів у межах від 5% до 12% для мережних структур з невеликим розміром (рис. 4.53) і в межах від 8% до 17% для структур з більшим розміром (рис. 4.59, 4.63). За ТЕ-показниками (4.20) та (4.24) отримані ієрархічні рішення відрізнялися від централізованих не більше ніж на 5–9%.

## Перелік джерел посилання до четвертого розділу

1. Поповский В.В. Основы теории телекоммуникационных систем. LAPLAMBERT Academical Publishing. 2018. 565 с.
2. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. 1st Edition. Pearson Education Inc., 2016. 510 p.
3. RFC 7426 – Software-Defined Networking (SDN): Layers and Architecture Terminology / E. Haleplidis, K. Pentikousis, S. Denazis and other. IETF. proposed standard, January 2015. 35 p.
4. QoS-aware Adaptive Routing in Multi-Layer Hierarchical Software Defined Networks: A Reinforcement Learning Approach / S.C. Lin, I.F. Akyildiz, P. Wang, M. Luo. 2016 IEEE International Conf. on Services Computing (San Francisco, CA, USA, 27 June–2 July 2016). San Francisco, 2016. P. 25–33.
5. Amin R., Reisslein M., Shah N. Hybrid SDN Networks: A Survey of Existing Approaches. IEEE Communications Surveys & Tutorials. 2018. 48 p. DOI: 10.1109/COMST.2018.2837161.
6. Duan Q., Toy M. Virtualized Software-Defined Networks and Services. Boston-London: Artech house, 2016. 319 p.
7. Blial O., Mamoun M. Ben, Benaini R. An Overview on SDN Architectures with Multiple Controllers. Journal of Computer Networks and Communications. 2016. Vol. 2016, Article ID 9396525. P. 1–8.
8. Вегешна III. Качество обслуживания в сетях IP / пер. с англ. Москва: Вильямс, 2003. 368 с.
9. Barreiros M., Lundqvist P. QoS-Enabled Networks: Tools and Foundations. Wiley Series on Communications Networking & Distributed Systems, 2nd Edition: Wiley, 2016. 254 p.
10. Uyles D. Black. IP routing protocols: RIP, OSPF, BGP, PNNI and Cisco routing protocols. Prentice Hall PTR, 2000. 287 p.
11. Misra S., Goswami S. Network Routing: Fundamentals, Applications, and Emerging Technologies 1st Edition. Wiley, 2017. 536 p.
12. RFC 4271 – A Border Gateway Protocol 4 (BGP-4) / Y. Rekhter, T. Li, S. Hares. IETF. PROPOSED STANDARD, January 2006. 104 p.
13. Гольдштейн А.Б., Гольдштейн Б.С. Технология и протоколы MPLS. Санкт-Петербург, БХВ, 2005. 304 с.
14. Moy J. RFC 1247 – OSPF Version 2. IETF proposed standard, July 1991. 189 p.



15. Обзор и сравнительный анализ основных моделей и алгоритмов многопутевой маршрутизации в мультисервисных телекоммуникационных сетях / В.В. Поповский, А.В. Лемешко, Л.И. Мельникова, Д.В. Андрушко. Прикладная радиоэлектроника. 2005. Т. 4. Вып. № 4. С. 372–382.
16. Новиков С.Н. Классификация методов маршрутизации в мультисервисных сетях связи. Вестник СибГУТИ. 2013. № 1. С. 57–67.
17. Oran D. RFC 1142 – OSI IS-IS Intra-domain Routing Protocol. IETF proposed standard, February 1990. 157 p.
18. Af-pnni-0055.000. Private Network-Network Interface. Specification Version 1.0 (PNNI 1.0). March 1996. 366 p.
19. Rak J. Resilient Routing in Communication Networks (Computer Communications and Networks), 1st edition. Springer, 2015. 181 p.
20. Medhi D., Ramasamy K. Network Routing, Second Edition: Algorithms, Protocols, and Architectures (The Morgan Kaufmann Series in Networking) 2nd Edition. Cambridge, MA, USA: Elsevier Inc., 2018. 1018 p.
21. Marsic I. Computer Networks: Performance and Quality of Service. Rutgers University, 2013. 500 p.
22. Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем. Москва: Мир, 1973. 344 с.
23. Сингх М., Титли А. Системы: декомпозиция, оптимизация и управление. Москва: Машиностроение, 1986. 494 с.
24. Лемешко А.В. Алгоритм иерархическо-координационного управления информационным обменом в сети передачи данных. Открытые информационные и компьютерные интегрированные технологии. 1998. Вып. № 1. С. 323–328.
25. Лемешко А.В., Семеняка М.В. Модель и метод предотвращения перегрузки с активным управлением очередью на узлах телекоммуникационной сети. Проблеми телекомунікацій. 2014. № 2 (14). С. 91–104. URL: [http://pt.journal.kh.ua/2014/2/1/142\\_lemeshko\\_aqm.pdf](http://pt.journal.kh.ua/2014/2/1/142_lemeshko_aqm.pdf).
26. Лемешко А.В., Симоненко Д.В. Динамическая модель балансировки буферных и канальных ресурсов транспортной сети телекоммуникационной системы. Проблеми телекомунікацій. 2010. № 2 (2). С. 42–49. URL: [http://pt.journal.kh.ua/2010/2/2/102\\_lemeshko\\_dynamic.pdf](http://pt.journal.kh.ua/2010/2/2/102_lemeshko_dynamic.pdf).
27. Lemeshko O.V., Ahmad M. Hailan, Starkova O.V. Multi-level traffic management in the MPLS-TE DiffServ network. The experience of designing and application of CAD systems in microelectronics: 11th International Conference (Polyana-Svalyava-(Zakarpattia), 23–25 February 2011). Polyana–Svalyava, 2011. P. 118–120.

28. Ghosh S., Rajkumar R., Hansen J., Lehoczky J. Scalable QoS-based resource allocation in hierarchical networked environment. Real Time and Embedded Technology and Applications: 11th IEEE Symposium (Porto, Portugal, 7–10 March 2005). Porto, 2005. P. 256–267.
29. Capelle M., Abdellatif S., Huguet M. Online virtual links resource allocation in Software-Defined Networks. 2015 IFIP Networking Conference (Toulouse, France, May 2015). Toulouse, 2015. P. 1–9.
30. Alhihi M. Method of Distribution Network Resources after Restoration, the Networks MPLS-TE Use of Various Telecommunications Technologies to Construct Backbone Networks. Int. J. Communications, Network and System Sciences. Vol. 10. 2017. P. 251–260.
31. QoS in the MPLS-DiffServ network / A. Saika, R. El Kouch, B. Raouyane, M. Bellafkih, M.M. Himmi. Sciences of Electronics, Technologies of Information and Telecommunications (SETIT): 6th International Conference (Sousse, Tunisia, 21–24 March 2012). Sousse, 2012. P. 507–510.
32. Лемешко А.В., Ахмад М. Хайлан, Семеняка М.В. Модель и метод иерархической маршрутизации на основе резервирования ресурсов в сети IP/IntServ. Радиотехника: Всеукр. межвед. науч.-техн. сб. 2010. Вып. 163. С. 79–84.
33. Lemeshko A., Hailan Ahmad M., Yevsyeyeva O. Mathematical Model and Method of Routing with Resources Reservation in IP/IntServ Network. Proceedings of International Conference on Modern Problem of Radio Engineering, Telecommunications and Computer Science (TCSET'2012) (Lviv–Slavske, Ukraine, 21–24 Feb. 2012). Lviv–Slavske, 2012. P. 325–326.
34. An efficient dynamic multicast routing algorithm with advance resource reservation awareness / P. Pavarangkoon, A. Gunabhibal, C. Pomavalai, R. Varakulsiripunth. Advanced Communication Technology: 6th International Conference on (Phoenix Park, Korea, 9–11 Feb. 2004). Phoenix Park, 2004. P. 651–655
35. End-to-End Resource Reservations in Distributed Embedded Systems / M. Ashjaei, S. Mubeen, M. Behnam, L. Almeida, T. Nolte. 22nd International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA) (Daegu, South Korea 17–19 Aug. 2016). Daegu, 2016. P. 1–11.
36. Евсева О.Ю. Решение задачи иерархическо-координационной маршрутизации в телекоммуникационных сетях методом предсказания взаимодействия. Открытые информационные и компьютерные интегрированные технологии. 2003. Вып. 21. С. 102–111.

37. Abe J.F., Mantar H.A. Multipath Routing and Brokering in Inter-Domain or Inter-AS with SDN: A Model. 2017 Advances in Wireless and Optical Communications (RTUWO'17): proceedings of Conference (Riga, Latvia, November 2017). Riga, 2017. P. 192–197.
38. Lemeshko O., Ahmad M. Hailan, Ali S. Ali. A flow-based model of two-level routing in multiservice network. Modern Problems of Radio Engineering, Telecommunications and Computer Science. Proceedings of the international Conference TCSET'2010. (Lviv–Slavsko, 2010). Lviv, 2010. P. 225.
39. Fakhrali S., Zarandi H.R. FXY: a hierarchical routing algorithm to balance performance and fault tolerance in networks-on-chip. Journal of Circuits, Systems and Computers, Vol. 23. Issue 10. December 2014. P. 1450146-1-23.
40. Лемешко А.В., Ахмад М. Хайлан. Многоуровневое управление трафиком в сети MPLS–TE DiffServ на основе координационного принципа прогнозирования взаимодействий. Проблеми телекомунікацій. 2010. № 1 (1). С. 35–44. URL: [http://pt.journal.kh.ua/2010/1/1/101\\_lemeshko\\_traffic.pdf](http://pt.journal.kh.ua/2010/1/1/101_lemeshko_traffic.pdf).
41. Gholamian M.R., Heydari M. An inventory model with METRIC approach in location-routing-inventory problem. Advances in Production Engineering & Management. Vol. 12. N 2. June 2017. P. 115–126.
42. Lemeshko O.V., Yeremenko O.S. Dynamics Analysis of Multipath QoS-Routing Tensor Model with Support of Different Flows Classes. Smart Systems and Technologies (SST): 2016 International Conference (Josip Juraj Strossmayer University of Osijek, Croatia. 12–14 Oct. 2016). Croatia, 2016. P. 225–230.
43. Research Challenges for Traffic Engineering in Software Defined Networks / I.F. Akyildiz, A. Lee, P. Wang and other. IEEE Network. Vol. 30. Issue 3. P. 52–58.
44. Stochastic time-dependent vehicle routing problem: Mathematical models and ant colony algorithm / Zh. Duan, Sh. Sun, Sh. Sun, W. Li. Advances in Mechanical Engineering. 2015. Vol. 7(11). P. 1–16.
45. Domain clustering for inter-domain path computation speed-up / L. Maggi, J. Leguay, J. Cohen, P. Medagliani. An international Journal Networks. 2017. Vol. 71, Issue 3. P. 1–19.
46. IP Fast Rerouting for Multi-Link Failures / T. Elhourani, A. Gopalan and other. IEEE/ACM Transactions on Networking. 2016. P. 3014–3025.
47. Kwon D., Park J.H., Kim D.K. Hierarchical multicast transmission for single cell point-to-multipoint (SC-PTM) in cellular networks. Information and Communication Technology Convergence (ICTC), 2017 International Conference on (Jeju, South Korea, 18–20 Oct. 2017). Jeju, 2017. P. 737–741.

48. Мерсни А. Двухуровневый метод многопутевой маршрутизации многоадресных потоков в телекоммуникационной сети. Наукові записки УНДІЗ. 2017. № 2(46). С. 98–106.

49. Lemeshko O., Yeremenko O., Hailan A.M. Two-level Method of Fast ReRouting in Software-Defined Networks. Proc. Fourth International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), (Kharkiv, 10–13 October 2017). Kharkiv, 2017. P. 376–379.

50. Лемешко А.В., Невзорова Е.С., Арус К.М. Анализ сходимости координационной процедуры при реализации иерархической маршрутизации в телекоммуникационной сети. Проблеми телекомунікацій. 2015. № 1 (16). С. 54–71. URL: [http://pt.journal.kh.ua/2015/1/1/151\\_lemeshko\\_coordination.pdf](http://pt.journal.kh.ua/2015/1/1/151_lemeshko_coordination.pdf).

51. Nevzorova O., Hasan A.K., Korshets O.A. Convergence Analysis of the Hierarchical Routing Method. Modern Problems of Radio Engineering, Telecommunications, and Computer Science: proc. of XII International Conf. (Lviv–Slavske, 25 February–1 March 2014). Lviv–Slavske, 2014. P. 587–589.

52. Невзорова Е.С. Анализ сходимости метода иерархической маршрутизации. Радиоэлектроника и молодежь в XXI веке: материалы 18-го Международного мол. форума (Харьков, 14–16 апреля 2014). Харьков: ХНУРЭ, 2014. С. 71–72.

53. Nevzorova Ye.S., Arous K.M., Salakh M.T.R. Method for hierarchical coordinated multicast routing in a telecommunication network. Telecommunication and Radio Engineering. 2016. Vol. 75. P. 1137–1151.

54. Nevzorova O., Arous K., Hailan A. Flow-based model of hierarchical multicast routing. Problems of Infocommunications Science and Technology, PICS&T'2015: proceedings of Second International Scientific-Practical Conference (Kharkiv, 13–15 Oct. 2015). Kharkiv, 2015. P. 50–53.

55. Невзорова Е.С., Арус К.М. Анализ модели двухуровневой многоадресной маршрутизации в телекоммуникационной сети. Современные информационно-телекоммуникационные технологии: материалы научно-технической конф. (Київ, 17–20 ноября 2015). Киев, 2015. С. 98–100.

56. Nevzorova O., Arous K.M., Ali A.S. Research of the flow-based model of hierarchical multicast routing. Modern Problems of Radio Engineering, Telecommunications, and Computer Science: proceedings of XIII International Conference (Lviv–Slavske, 23–26 Feb. 2016). Lviv–Slavske, 2016. P. 889–892.

57. Lemeshko O., Nevzorova O., Hailan A. The increasing convergence of coordination procedure in the implementation of multipath hierarchical routing. Problems of Infocommunications Science and Technology PICS&T'2014:

proceedings of First International Scientific-Practical Conference (Kharkiv, Ukraine, 14–17 Oct. 2014). Kharkiv, 2014. P. 45–48.

58. Спосіб підвищення збіжності координаційної процедури в ході оптимізації процесу ієрархічної маршрутизації в телекомунікаційній мережі: патент Україна: МПК (2015.01) G 06 G 3/00. № u201412829; заявка 01.12.2014; опуб. 25.05.2015, бюл. № 10. 7 с.

59. RFC 3272 – Overview and Principles of Internet Traffic Engineering / D. Awduche, A. Chiu, A. Elwalid, I. Widjaja and other. IETF proposed standard, May 2002. 70 p.

60. Simha A., Osborne E. Traffic Engineering with MPLS. Cisco Press, 2002. 608 p.

61. Seok Yo., Lee Yo., Choi Ya., Kim C. A constrained multipath traffic engineering scheme for MPLS networks. Proc. of IEEE ICC 2002. (New York, 2002). New York, 2002. P. 2431–2436.

62. Wang Y., Wang Z. Explicit routing algorithms for Internet Traffic Engineering. Computer Communications and Networks: Proceedings Eight International Conference. (Boston, USA, 11–13 Oct. 1999). Boston, 1999. P. 582–588.

63. Невзорова О.С. Розробка та дослідження методу ієрархічно-координаційної внутрішньодоменної маршрутизації в телекомунікаційній мережі MPLS-TE. Проблеми телекомунікацій. 2017. № 2 (21). С. 3–15. URL: [http://pt.journal.kh.ua/2017/2/1/172\\_nevzorova\\_hierarchical.pdf](http://pt.journal.kh.ua/2017/2/1/172_nevzorova_hierarchical.pdf)

64. Невзорова Е.С., Тарики Надия. Анализ сходимости иерархической маршрутизации с использованием технологии Traffic Engineering // Радиоэлектроника и молодежь в XXI веке: материалы 19-го Международного молодежного форума: сб. материалов форума. Т. 4. (Харьков: ХНУРЭ, 20–22 апреля 2015). Харьков, 2015. С. 75–76.

65. Nevzorova O., Vavenko T., Arif F.A.R. Hierarchical method of load-balancing routing in MPLS network. Problems of Infocommunications. Science and Technology (PIC S&T): 4th International Scientific-Practical Conference (Kharkov, Ukraine, 10–13 Oct. 2017). Kharkov, 2017. P. 434–438.

66. Lemeshko O., Nevzorova O., Rossikhin V., Hailan A.M. Hierarchical Method of Load Balancing Routing on SDN Controllers with Multicore Architecture. Problems of Infocommunications. Science and Technology (PIC S&T): International Scientific-Practical Conference (Kharkiv, Ukraine, 9–12 Oct. 2018). Kharkiv, 2018. P. 1–4.

67. Невзорова О.С., Шаповалова А.С., Обиденнова М.С. Ієрархічно-координаційний метод маршрутизації в програмно-конфігурованій мережі.

Фізико-технологічні проблеми передавання, оброблення та збереження інформації в інформаційних системах (PREDT): матеріали VII Міжнародної науково-практичної конференції (Чернівці, Україна, 8–10 листопада 2018). Чернівці, 2018. С. 104–105.

68. Невзорова Е.С. Исследование сходимости иерархическо-координационного метода маршрутизации. Проблемы експлуатації та захисту інформаційно-комунікаційних систем: тези науково-практичної конференції (Київ, 2–4 червня 2015). Київ, 2015. С. 157–158.

69. Lemeshko O., Nevzorova O., Mersni A., Nailan A.M., Ali A.S., Harkusha S. Improved two-level method of multicast routing in MPLS-TE network // 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), July 2–6, 2019. Lviv, Ukraine. P. 846–850.

70. Лемешко А.В., Невзорова Е.С., Ильяшенко А.Е. Разработка и анализ метода иерархическо-координационной междоменной маршрутизации в телекоммуникационной сети. Наукові записки Українського науково-дослідного інституту зв'язку. 2016. № 4 (44). С. 49–67.

71. Лемешко А.В., Ильяшенко А.Е., Коваленко Т.Н., Невзорова Е.С. Разработка и анализ диакоптического метода междоменной маршрутизации с балансировкой нагрузки в телекоммуникационной сети. Проблемы телекомунікацій. 2018. № 1(22). С. 3–24. URL: [http://pt.journal.kh.ua/2018/1/1/181\\_lemeshko\\_diacoptic.pdf](http://pt.journal.kh.ua/2018/1/1/181_lemeshko_diacoptic.pdf).

72. Lemeshko O., Nevzorova O., Vavenko T. Hierarchical coordination method of inter-area routing in telecommunication network. Radio Electronics & Info Communications (UkrMiCo): proceedings of International Conference (Kyiv, 11–16 Sept. 2016). Kyiv, Ukraine, 2016. P. 1–4.

73. Lemeshko O., Nevzorova O., Vavenko T. Two-level method of hierarchical inter-area routing in network. Physical and technological problems of transmission, processing and storage of information in infocommunication systems: proceedings of V International Scientific Practical Conference (Chernivtsi, 3–5 november 2016). Chernivtsi, 2016. P. 154–155.

74. Невзорова Е.С., Ильяшенко А.Е. Метод иерархической междоменной маршрутизации на основе принципа целевой координации. Інформатика, математика, автоматика: матеріали науково-технічної конференції (Суми, 17–21 квітня 2017). Суми, 2017. С. 106.

75. Lemeshko O., Nevzorova O., Nailan A.M. Research of hierarchical coordination method of inter-area routing in telecommunication network. Problems

of infocommunications Science and Technology (PIC S&T'2016): III Intern. Scientific-Practical Conf. (Kharkiv, 4–6 Oct.2016). Kharkiv, 2016. P. 135–138.

76. Невзорова Е.С., Ильяшенко А.Е. Исследование метода иерархической междоменной маршрутизации. Радиоелектроніка та молодь у XXI столітті: матеріали 21-го міжнародного молодіжного форуму (Харків, 25–27 квітня 2017). Харків, 2017. С. 57–58.

77. Лемешко А.В., Невзорова Е.С. Разработка трехуровневого метода иерархической маршрутизации на основе принципа целевой координации. Радиоелектроника и информатика. 2017. № 2 (77). С. 15–19.

78. Невзорова Е.С., Ильяшенко А.Е. Трехуровневый метод иерархической маршрутизации. Перспективи розвитку інформаційно-телекомунікаційних технологій та систем ПРІТС 2017: тези допов. ІХ Міжнародна науково-технічна конференція студентів та аспірантів (Київ НТУУ «КПІ ім. Ігоря Сікорського»), 2017). Київ, 2017. С. 475.

79. Lemeshko O., Yeremenko O., Nevzorova O., Vavenko T. Three-level Method of Hierarchical Coordination Routing in Multi-Area Network. Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017): IEEE The Second International Conference, (Kyiv, 11–15 Sept. 2017) Kyiv, 2017. P. 1–4.

80. Lemeshko O., Yeremenko O., Nevzorova O. Hierarchical Method of Inter-Area Fast Rerouting. Transport and Telecommunication Journal. 2017 18(2). P. 155–167.

81. Yeremenko O., Nevzorova O., Ali Salem Ali. Two-level method of fault-tolerant inter-area routing. The Experience of Designing and Application of CAD System in Microelectronic (CADSM): 14th International Conference (Polyana-Svalyava (Zakarpattya), 21–25 February 2017). Polyana–Svalyava, 2017. P. 105–108.

82. Tiso J., Teare D. Designing Cisco Network Service Architectures (ARCH): Foundation Learning Guide. Cisco press. 2011. 733 p.

83. Cisco Networking Academy (Ed.). Routing Protocols Companion Guide. Pearson Education. 2014. 792 p.

## ВИСНОВКИ

1. Під час проведених досліджень встановлено, що окрім вимог до якості обслуговування, які вже стали класичними функціями сучасних ІКМ, на перший план також виходить функціонал щодо забезпечення високого рівня відмовостійкості, масштабованості та мережної безпеки, що особливо важливо у функціонуванні ІКМ в умовах постійних деструктивних (випадкових та антагоністичних) впливів, які призводять до суттєвої зміни як структурних, так і функціональних параметрів і властивостей мережі: її топології, пропускну здатності, керованості, стійкості тощо.

2. Незважаючи на високий науковий та прикладний рівень досягнутих у сфері управління трафіком в ІКМ результатів, до перспективних мережних рішень усе ж висунуто низку важливих концептуальних засад:

- комплексне врахування вимог щодо відмовостійкості мережі з підтримкою на алгоритмічно-програмному рівні наявних і новітніх схем перемаршрутизації та захисту елементів мережі, їх пропускну здатності та рівня QoS загалом як на рівні доступу (Fault-Tolerant Routing), так і на рівні ядра мережі (Fast ReRouting);

- підвищення рівня мережної безпеки під час передачі різноманітних конфіденційних даних, зокрема сесійних ключів, інформації щодо автентифікації, критично важливих для користувача повідомлень тощо;

- оптимізація використання доступного мережного ресурсу, підвищення масштабованості отриманих мережних рішень, оснований зокрема на реалізації ієрархічних стратегій маршрутизації та управління трафіком в ІКМ загалом.

Виконання наведених вимог пов'язано з необхідністю вдосконалення наявних та розроблення нових моделей та методів, які б слугували подальшою теоретичною основою перспективних протоколів маршрутизації та технологічних засобів управління трафіком в ІКМ.

3. Подальшого розвитку набула система поточних моделей відмовостійкої маршрутизації без резервування елементів інфокомунікаційної мережі шляхами, що не перетинаються або перетинаються лише у вузлах. Новизною рішень є введення до структури моделей нелінійних умов використання шляхів заданого типу в процесі балансування навантаження. Як показали проведені дослідження, загалом запропоновані рішення



дозволили забезпечити підвищення продуктивності мережі приблизно в 1,7 разів. У цьому випадку зі зростанням розміру мережі та зв'язності маршрутизаторів вираш за продуктивністю збільшувався до 2,5–4 разів.

4. Отримала подальший розвиток потокова модель швидкої перемаршрутизації. Новизна моделі полягає, по-перше, у лінійній формі умов захисту каналу та вузла під час реалізації багатошляхової маршрутизації; по-друге, у введенні системи критеріїв оптимальності рішень щодо відмовостійкої маршрутизації з установленням ієрархії співвідношень вагових коефіцієнтів у відповідних цільових функціях. Це дозволило підвищити продуктивність ІКМ і масштабованість рішень щодо швидкої перемаршрутизації, а також знизити обчислювальну складність їх протокольної реалізації.

5. Уперше запропоновано дворівневий метод швидкої перемаршрутизації з балансуванням навантаження в програмно-конфігурованих мережах. Новизна методу полягає, по-перше, у введенні за принципом прогнозування взаємодій дворівневої ієрархії розрахунків маршрутних змінних, що відповідають за формування основних і резервних шляхів з реалізацією схем захисту каналу, вузла, шляху та їх пропускної здатності; а по-друге, у забезпеченні збалансованої завантаженості каналів зв'язку мережі потоками, які протікають як основними, так і резервними маршрутами, що відповідає вимогам концепції Traffic Engineering.

6. Уперше представлено лінійну оптимізаційну модель багатошляхової швидкої перемаршрутизації з балансуванням навантаження в ІКМ із захистом каналу, вузла та пропускної здатності. Новизною запропонованої моделі є те, що узгоджене рішення завдань щодо балансування навантаження і швидкої перемаршрутизації із захистом каналу, вузла та пропускної здатності забезпечується у розв'язанні задачі лінійного програмування. Це дозволило знизити обчислювальну складність розрахунку маршрутних змінних, відповідальних за формування основного та резервного шляхів, і забезпечити збалансовану завантаженість каналів зв'язку мережі за вимогами концепції Traffic Engineering. У роботі показано, що вираш від реалізації багатошляхової стратегії маршрутизації за умови TE FRR дозволив знизити верхній поріг завантаженості каналів зв'язку в середньому від 37,12% до 59,41% у разі захисту каналу та від 31,5% до 56,3% у випадку захисту вузла, що позитивно позначається і на рівні якості обслуговування в мережі загалом.

7. Уперше запропоновано систему поточкових моделей відмовостійкої маршрутизації із захистом шлюзу за замовчуванням. Новизною рішень є,

по-перше, реалізація функцій відмовостійкості шляхом уведення додаткових керуючих змінних, відповідальних за вибір основного та резервного шлюзів за замовчуванням з балансуванням навантаження між ними, по-друге, забезпечення погодженого розв'язання задач щодо захисту шлюзу за замовчуванням і швидкої перемаршрутизації в транспортній мережі, що дозволило підвищити рівень відмовостійкості ІКМ засобами маршрутизації.

8. Уперше представлено методи безпечної маршрутизації повідомлень шляхами, які перетинаються, що належать до класу проактивних і реактивних рішень щодо забезпечення заданого рівня мережної безпеки. Новизна методу безпечної маршрутизації полягає в тому, що він, по-перше, допускає використання особливого класу шляхів, які перетинаються і становлять основу композитних шляхів, а також містять мережні фрагменти з послідовним та (або) паралельним з'єднанням каналів зв'язку мережі, а по-друге, оснований на оптимізації процесу вибору множини композитних шляхів і балансування ними частин повідомлення, що передається, із забезпеченням допустимих значень його ймовірності компрометації. Як показав проведений аналіз, використання запропонованого методу в межах поданих розрахункових прикладів дозволяє поліпшити ймовірність компрометації повідомлень, які передаються, у середньому від 5–10% до 25–50% з огляду на можливість використання композитних шляхів, які є підкласом шляхів, що перетинаються.

9. З'ясовано, що новизна методу безпечної швидкої перемаршрутизації полягає в тому, що в разі порушення вимог мережної безпеки, викликаного підвищенням ймовірності компрометації одного або множини композитних шляхів, які містять основний мультишлях, багатопляхова передача частин конфіденційного повідомлення із забезпеченням заданих значень ймовірності його компрометації здійснюватиметься вже за заздалегідь розрахованою множиною резервних композитних шляхів, реалізуючи захист або основного мультишляху загалом, або одного чи декількох заданих композитних шляхів, що розміщені в цьому основному мультишляху.

10. Під час проведеного в роботі аналізу встановлено, що дієвим засобом підвищення якості обслуговування та масштабованості ІКМ є використання ієрархічної маршрутизації, яка на сьогодні представлена множиною протокольних рішень. Проте наявні протоколи ієрархічної маршрутизації оснований лише на структурній ієрархії мережі та на досить простих комбінаторних алгоритмах пошуку найкоротшого шляху на графі, за допомогою якого описується структура ІКМ. Це значно знижує ефективність функціонування

ІКМ і передбачає перегляд і вдосконалення наявних моделей і методів ієрархічної маршрутизації, на яких оснований відомі протокольні рішення.

11. Удосконалено потокову модель та метод ієрархічно-координаційної внутрішньодоменної маршрутизації «від джерела» в ІКМ SDN/MPLS-TE. Новизна рішень полягає, по-перше, у декомпозиційному поданні потокової моделі маршрутизації з балансуванням навантаження за принципами Traffic Engineering; по-друге, у модифікації маршрутних метрик та умов балансування навантаження пропорційної віддаленості каналів зв'язку за кількістю переприйомів від маршрутизаторів відправника та отримувача, що дозволило підвищити масштабованість маршрутних рішень: знизити обсяг службового навантаження, що циркулює в мережі, а також час розв'язання маршрутних задач загалом. Це досягалося, по-перше, за рахунок зменшення розміру маршрутних задач пропорційно кількості приграничних маршрутизаторів та кількості потоків пакетів; по-друге, на підставі підвищення збіжності методів до оптимальних рішень у середньому від 1,5–2 до 3,5–5, а в деяких випадках і до 8 разів залежно від розміру та зв'язності мережі, а також її завантаженості.

12. Уперше представлено математичну модель і метод ієрархічно-координаційної міждоменної маршрутизації в програмно-конфігурованій мережі, що складається з множини послідовно з'єднаних доменів. Новизна моделі полягає в тому, що на основі її декомпозиційного представлення щодо кожного окремого домену, по-перше, набули нової форми умови збереження потоку для доменів різних типів: відправників, отримувачів пакетів та транзитних доменів; по-друге, вдалося коректно сформулювати умови міждоменної взаємодії, виконання яких гарантувало зв'язність міждоменних шляхів. Новизна методу міждоменної маршрутизації полягає у використанні принципу цільової координації, що дозволило реалізувати ієрархічно-координаційну міждоменну маршрутизацію, наблизивши якість розподіленої маршрутизації за доменами до результатів централізованої маршрутизації, але суттєво знизивши водночас розмірність маршрутної задачі, що в підсумку сприяє підвищенню масштабованості рішень щодо міждоменної маршрутизації.

13. Уперше запропоновано трирівневий метод ієрархічно-координаційної маршрутизації в інфокомунікаційній мережі SDN/MPLS. Новизна методу полягає у введенні трирівневої ієрархії розрахунку маршрутних змінних з послідовною координацією отриманих рішень: нульовий та перший рівні відповідали за організацію та координацію внутрішньодоменної маршрутизації,

а задача другого рівня – реалізація та координація міждоменної взаємодії. Це дозволило підвищити масштабованість рішень задачі міждоменної маршрутизації в мережі SDN/MPLS.

14. Удосконалено метод ієрархічно-координаційної міждоменної швидкої перемаршрутизації, оснований на декомпозиційному представленні потокової моделі маршрутизації та використанні принципу цільової координації. Новизною методу є забезпечення захисту приграничних маршрутизаторів ядра мережі на підставі розрахунку основних та резервних міждоменних шляхів як у процесі реалізації одношляхової, так і багатшляхової маршрутизації, що дозволило підвищити масштабованість і відмовостійкість маршрутних рішень.

Наукове видання

**ЛЕМЕШКО** Олександр Віталійович  
**ЄРЕМЕНКО** Олександра Сергіївна  
**НЕВЗОРОВА** Олена Сергіївна

**ПОТОКОВІ МОДЕЛІ ТА МЕТОДИ МАРШРУТИЗАЦІЇ  
В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ:  
ВІДМОВОСТІЙКІСТЬ, БЕЗПЕКА, МАСШТАБОВАНІСТЬ**

**Монографія**

Відповідальний випусковий О.В. Лемешко  
Редактор Л.В. Кузьміна  
Комп'ютерна верстка Л.Ю. Светайло

Підп. до друку 14.02.20. Формат 60x84 1/16. Умов. друк. арк. 18,1.  
Тираж 100 прим. Ціна договірна.

Віддруковано в типографії ФОП Андреев К.В.  
61157, Харків, вул. Богомольця, 9, кв. 50.  
Свідоцтво про державну реєстрацію №24800170000045020 від 30.05.2003 р.  
er.zakaz@gmail.com; тел. 063-993-62-73



**ЛЕМЕШКО Олександр Віталійович** – завідувач кафедри інфокомунікаційної інженерії імені В.В. Поповського Харківського національного університету радіоелектроніки, доктор технічних наук, професор.

Член IEEE, ACM.

Має понад 300 публікацій.

Напрями наукової діяльності: управління трафіком, оптимізація та якість обслуговування в інфокомунікаціях, безпроводові мережі, ієрархічна та відмовостійка маршрутизація, мережна безпека.

*oleksandr.lemeshko@nure.ua*



**ЄРЕМЕНКО Олександра Сергіївна** – професор кафедри інфокомунікаційної інженерії імені В.В. Поповського Харківського національного університету радіоелектроніки, доктор технічних наук, доцент, старший науковий співробітник.

Член IEEE (Senior Member), ACM.

Має понад 160 публікацій.

Напрями наукової діяльності: управління трафіком в інфокомунікаційних мережах, якість обслуговування, відмовостійка та безпечна маршрутизація.

*oleksandra.yeremenko@nure.ua*



**НЕВЗОРОВА Олена Сергіївна** – асистент кафедри інфокомунікаційної інженерії імені В.В. Поповського Харківського національного університету радіоелектроніки, кандидат технічних наук.

Член IEEE.

Має понад 40 публікацій.

Напрями наукової діяльності: оптимізація ієрархічних систем, маршрутизація, якість обслуговування.

*olena.nevzorova@nure.ua*

