

УДК 621.391

# ОГЛЯД ТЕОРЕТИЧНИХ РІШЕНЬ ЩОДО ВІДМОВИСТОЇКОЇ МАРШРУТИЗАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ



[О.С. ЄРЕМЕНКО](#), [М.О. ЄВДОКИМЕНКО](#)

Харківський національний  
університет радіоелектроніки

**Abstract** – In this article, the existing solutions in the field of fault-tolerant routing have been analyzed, which allowed formulating a list of key requirements that prospective solutions should meet, as well as mathematical models and methods on which they are based. These include flow-based traffic nature, which is a distinctive feature of most multimedia services and a compulsory moment when implementing bandwidth protection schemes and other network Quality of Service indicators; optimization problem statement: the focus on optimizing the use of available network resources; high scalability of solutions for fault-tolerant routing; support for basic protection schemes for network elements (node / communication link / path / bandwidth and QoS level for a set of indicators); coordinated solving of specific tasks for fault-tolerant routing, for example, default gateway protection, fast rerouting, etc.; extension of existing solutions to support load balancing associated with the implementation of a multipath routing strategy with appropriate support for protection schemes not single path, but a multipath, that is, the set of paths in which packets of the same flow are transmitted; acceptable computational complexity of routing solutions. The classification of perspective schemes of protection of the Quality of Service (QoS) level is developed, which is important to be implemented during the fault-tolerant routing of multimedia flows. Appropriate routing solutions should provide QoS protection at the same time for a variety of Network Performance (NP) or Quality of Experience (QoE) indicators, requiring the development of new or improved existing mathematical models and fault-tolerant routing methods in accordance with the requirements.

**Анотація** – В даній статті проведено аналіз відомих рішень в області відмовостійкої маршрутизації, що дозволив сформулювати перелік ключових вимог, яким повинні відповідати перспективні рішення, а також математичні моделі та методи, на яких вони ґрунтуються. Розроблено класифікацію перспективних схем захисту рівня якості обслуговування, які важливо реалізувати в ході відмовостійкої маршрутизації мультимедійних потоків. Відповідні маршрутні рішення мають забезпечувати захист QoS одночасно за множиною показників мережної продуктивності (NP) або за показниками якості обслуговування, що сприймається на рівні користувачів (QoE), що вимагає розробки нових або вдосконалення існуючих математичних моделей і методів відмовостійкої маршрутизації відповідно до наведених вимог.

**Аннотация** – В данной статье проведен анализ известных решений в области отказоустойчивой маршрутизации, позволивший сформулировать перечень ключевых требований, которым должны соответствовать перспективные решения, а также математические модели и методы, на которых они основаны. Разработана классификация перспективных схем защиты уровня качества обслуживания, которые важно реализовать в ходе отказоустойчивой маршрутизации мультимедийных потоков. Соответствующие маршрутные решения должны обеспечивать защиту QoS одновременно по множеству показателей сетевой производительности (NP) или по показателям качества обслуживания, воспринимаемого на уровне пользователей (QoE), что требует разработки новых или совершенствования существующих математических моделей и методов отказоустойчивой маршрутизации в соответствии с приведенными требованиями.

## Вступ

Незважаючи на постійно зростаючу надійність сучасного комунікаційного обладнання, проблема забезпечення заданого рівня відмовостійкості телекомунікаційних мереж також стоїть досить гостро. До основних глобальних причин відмов у телекомунікаційних мережах (ТКМ) відносять масштабні катастрофи, соціально-політичні та економічні чинники, вторинні відмови, людський фактор (помилки людини-оператора), загрози мережній безпеці, екологічні проблеми та ін. [1-10]. Крім того, серед основних технологічних факторів, що викликають відмови в обслуговуванні в мережі, виділяють відмови фізичного рівня, збої та переважанення мереж-

ного обладнання при його експлуатації, помилки при конфігурації та оновленні термінального та мережного програмного забезпечення [1-4]. У зв'язку з цим на сьогоднішній день надзвичайно актуальною є задача, пов'язана з побудовою так званих відмовостійких мереж (Resilient Networks), здатних забезпечити високий рівень якості обслуговування (Quality of Service, QoS) та відмовостійкості (Quality of Resilience, QoR) [1, 2].

Варто зазначити, що відмовостійкість мереж була визначена як окремий аспект забезпечення якості обслуговування, що зосереджує увагу на параметрах, пов'язаних із відмовостійкістю ТКМ. Надзвичайна важливість QoR обумовлена її значенням для функціонування мереж, а також впливає з широкого спектру технологій, що забезпечують диференційовану QoS кінцевим користувачам [1, 3].

До основних засобів забезпечення відмовостійкості ТКМ відносять:

- інженерні методики організації експлуатації, технічного обслуговування та ремонту телекомунікаційного обладнання;
- засоби діагностики (самодіагностики) та перевірки (оцінки) працездатності елементів мережі;
- протоколи моніторингу та збору інформації про стан мережі;
- засоби превентивного виявлення відмов елементів мережі та аналізу ймовірних несправностей;
- протоколи резервування (дуплікації) елементів мережі та її сегментів;
- протоколи маршрутизації;
- балансування навантаження;
- планування мережі з введенням структурної та функціональної надлишковості;
- методи реконфігурації мережі.

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

## **I. Аналіз моделей і методів відмовостійкої маршрутизації в телекомунікаційних мережах**

Як показав проведений аналіз, множину рішень щодо відмовостійкої маршрутизації умовно можна розділити на наступні класи: евристичні, графові та комбінаторні, потокові рішення, відмовостійка маршрутизація в SDN мережах, а також рішення на основі балансування навантаження відповідно до концепції Traffic Engineering (TE).

Серед *евристичних алгоритмів* відмовостійкої маршрутизації розглянемо найбільш вагомі, які були виділені в ході проведеного аналізу робіт [11-21]. Так у роботі [11] було запропоновано адаптивний евристичний алгоритм відмовостійкої маршрутизації на основі використання графу  $(n, k)$ -зірки, який має широкі властивості

щодо масштабованості. Автори реалізують ідею збирання інформації, яка використовується в процесі маршрутизації на графі  $n$ -зірки, для застосування на графі  $(n, k)$ -зірки  $(S_{n,k})$  (рис. 1).

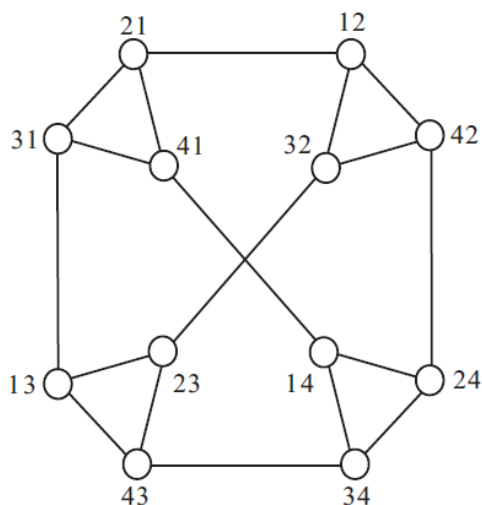


Рис. 1. Приклад графу  $(4, 2)$ -зірки  $(S_{4,2})$

При цьому кожен вузол  $S_{n,k}$  ідентифікується за допомогою перестановки  $k$ , вибраної з  $\{1, 2, \dots, n\}$ , де  $n$  та  $k$  (при  $1 \leq k \leq n-1$ ) є кількістю доступних для вибору та вибраних символів відповідно. Також авторами було запропоновано використання ймовірнісного вектору безпеки (Probabilistic Safety Vector, PSV) та розроблено алгоритм маршрутизації з метою визначення безвідмовного маршруту за допомогою PSV. При цьому ефективність маршрутизації PSV погіршується зі збільшенням відсотку вузлів, що відмовили, особливо при перевищенні порогу відмов вузлів у 25%. Для підвищення ефективності маршрутизації з більшим відсотком відмов вузлів також запропоновано адаптивний метод визначення порогу для PSV. При цьому ефективність маршрутизації оцінювалася за середньою довжиною шляхів. Маршрутизація PSV з динамічним порогом показала найкращу продуктивність при моделюванні у порівнянні з іншими методами. Також до переваг запропонованого методу можна віднести його прийнятну обчислювальну складність.

В роботі [12] авторами запропоновано евристичний алгоритм відмовостійкої маршрутизації в mesh-мережах на основі мурашиного алгоритму пошуку оптимального шляху, коли враховуються вузли, що відмовили. При цьому для розв'язання задачі відмовостійкої маршрутизації в запропонованому алгоритмі використовувався алгоритм оптимізації мурашиної колонії (Ant Colony Optimization, ACO) при застосуванні кольорових феромонних мурах для подолання проблеми відновлення функціонування мережних елементів. Запропоноване рішення порівнювалось з алгоритмом відмовостійкої маршрутизації в mesh-мережах з використанням збалансованого кільця. Результати моделювання показали, що запропонований алгоритм швидко реагував на відмови в мережі, щоб в кожний момент часу можна було вибрати оптимальний шлях від відправника до одержувача. Продуктивність алгоритму

було підвищено за допомогою оновлень мурах з метою інформування інших вузлів про виявлений найкоротший шлях.

У роботі [13] було запропоновано алгоритми відмовостійкої маршрутизації для ієрархічних дуальних мереж (Hierarchical Dual-Net, HDN) з обмеженою чи довільною кількістю вузлів, що відмовили. При цьому HDN побудовано на основі симетричного графа, який називається базовою мережею, як тривимірного тору та  $n$ -вимірного гіперкубу. Наведені алгоритми дозволяють знайти маршрут без відмов між відправником та одержувачем при відомій множині вузлів, що відмовили.

В статті [14] авторами розроблено механізм швидкої перемаршрутизації в IP-мережах із використанням кістякових дерев із коренем, які не перетинаються за дугами, що гарантує відновлення після 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), 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 у порівнянні з раніше відомими методами.

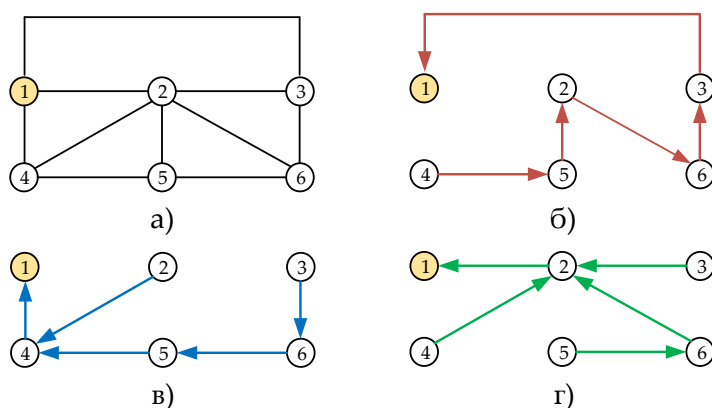


Рис. 2. Приклад дерев, які моделюють рішення задачі перемаршрутизації за шляхами, що не перетинаються за дугами: (а) мережа, (б) червоне дерево, (в) синє дерево і (г) зелене дерево

Відомо, що інколи при відмовостійкій маршрутизації виникає задача визначення шляху між двома вузлами в мережі, які повинні відвідувати 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, в статті [16] пропонується нова рекурсивна евристика для пошуку найкоротшого маршруту без циклів від вузла відправника до вузла одержувача, який відвідує певний набір транзитних вузлів у мережі. З метою забезпечення живучості до відмов вздовж шляху було запропоновано евристичний підхід, який модифікувався для того, щоб забезпечити захист розрахованого шляху за допомогою відповідного резервного шляху, який не перетинається з основним за вузлами. Працездатність запропонованої евристики при обчи-

сленні шляху із захистом і без нього оцінювалася порівняно із розв'язанням цієї задачі методами цілочисельного лінійного програмування (Integer Linear Programming, ILP). При цьому ILP рішення може не отримати шукане рішення протягом часу, що вимагається, особливо це стосується мереж великої розмірності, що виправдовує необхідність розробки евристичних алгоритмів.

Розглянемо ефективні *графові та комбінаторні рішення* щодо відмовостійкої маршрутизації, які представлені в роботах [22-27]. В роботі [22] 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 з сусідніх вузлів, щоб відправити повідомлення, беручи до уваги приблизні маршрутні ймовірності. Проведене авторами комп'ютерне моделювання підтвердило ефективність запропонованих алгоритмів.

Відомо, що вузли безпроводових сенсорних мереж (Wireless Sensor Networks, WSN) можуть швидко виходити з ладу, що призводить до відмов при маршрутизації та блокування зв'язку. В свою чергу в роботі [23] 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 випадковим чином розгортає деякі супер вузли (super nodes) з великим запасом енергії та потужною продуктивністю у WSN. Ці вузли несуть відповідальність за збір 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 у порівнянні з іншими алгоритмами відмовостійкої маршрутизації (Gossiping, DD, Low Energy Adaptive Clustering Hierarchy (LEACH)) навіть в умовах атак шкідливих вузлів у WSN.

У роботі [24] було запропоновано модель відмовостійкої маршрутизації на основі графа зірки з векторами безпеки (безвідмовності). При цьому використання вектору безпеки здатне забезпечувати ефективну відмовостійку маршрутизацію в ТКМ 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.

В роботах [25, 26] запропоновано моделі відмовостійкої маршрутизації на основі рівнів безпеки із застосуванням млинцевих графів та графів гіпер-зірка. Крім того, було проведено порівняння таких типів графів, як гіпер-зірка, зірка, гіперкуб та млинцевий граф щодо ефективності їх використання при відмовостійкій маршрутизації.

В роботі [27] досліджено можливості використання при підвищенні відмовостійкості ТКМ циркулянтних графів, які забезпечують високу гнучкість щодо кількості вузлів та зв'язності мережі (рис. 3). Було запропоновано архітектуру оптичної мережі на основі циркулянтного графу спільно з відмовостійкою маршрутизацією. Показано, що підвищення зв'язності мережі допомагає зменшити необхідну кількість довжин хвиль для одночасної взаємодії між усіма вузлами. Також у [27] було розроблено модель оцінки надійності з'єднання як при відмові вузлів, так і каналів зв'язку мережі. При цьому із застосуванням запропонованого алгоритму надійність зростала майже лінійно зі зростанням зв'язності мережі в логарифмічному масштабі.

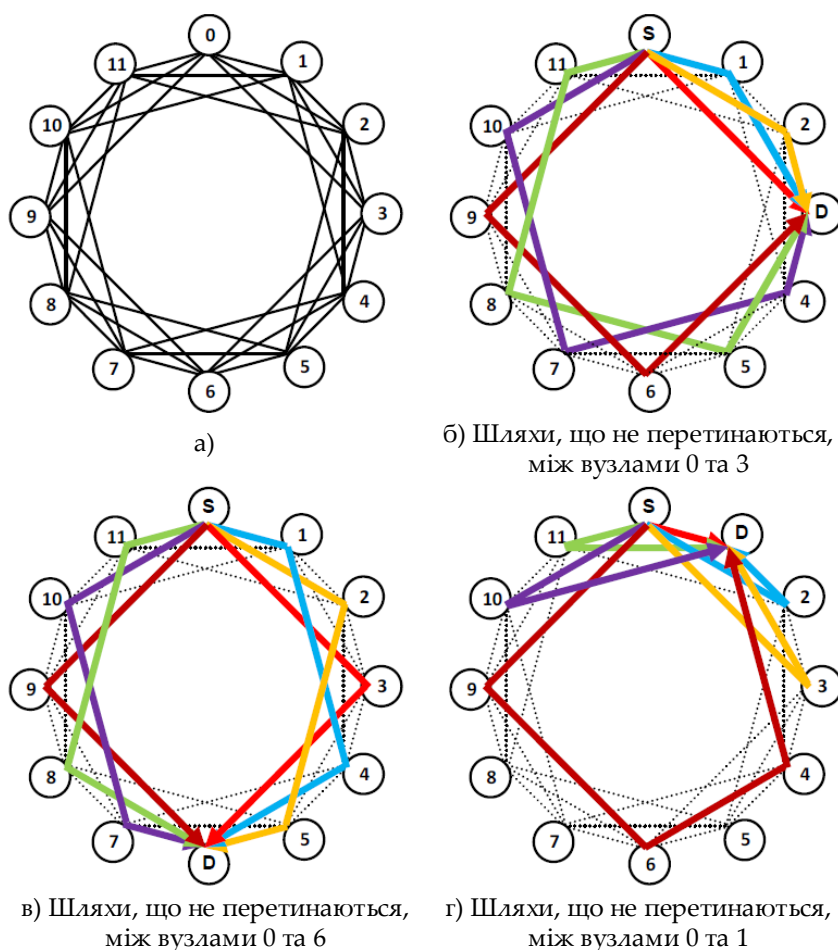


Рис. 3. Архітектура мережі на основі циркулянтного графу та приклади відмовостійкої маршрутизації за шляхами, що не перетинаються за вузлами

Проте найбільш перспективними та ефективними представляються саме *потоківі моделі та методи* відмовостійкої маршрутизації [2-4, 28-34], оскільки, вони враховують потоковий характер трафіку, що передається в сучасних телекомунікаційних мережах, а також, як правило, формулюються у вигляді оптимізаційних задач, орієн-

тованих на оптимізацію використання мережних ресурсів, допускаючи реалізацію схем захисту пропускну здатності мережі.

Відомо, що основні та резервні шляхи при швидкій 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. В статті [28] авторами запропоновано лінійну оптимізаційну модель для розрахунку шляхів як при реалізації одношляхової стратегії маршрутизації, так і при багатошляховій маршрутизації з метою забезпечення балансування навантаження. Отримані авторами результати щодо завантаженості каналів зв'язку при використанні запропонованої лінійної моделі при одношляховій та багатошляховій маршрутизації було порівняно з відповідними значеннями для шляхів, розрахованих згідно зі стандартними процедурами для IP-мереж, що дозволило визначити вигреш при використанні мережних ресурсів.

В свою чергу робота [29] присвячена вирішенню завдання мінімізації споживання енергії у відмовостійких ТКМ. При 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 при відсутності відмов, але використання мережного ресурсу здійснюється як основним, так і резервним шляхами. Отже, автори [29] пропонують механізм спільного захисту (*shared protection*), який не залежить від відмов, при MPLS маршрутизації, а сформульована задача носить назву *спільного захисту при удосконаленому трафік інжинірингу (Shared protection Smart Traffic Engineering, SSTE)*. При цьому задача SSTE є NP-складною, оскільки включає в себе задачу визначення дерев Штейнера як окремий випадок. Проте в роботі [29] авторами запропоновано формулювання цієї задачі за Бендерсом, яке є набагато ефективнішим з обчислювальної точки зору.

В роботі [30] було запропоновано алгоритми розрахунку шляхів при відмовостійкій 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, що 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 запропоновані підходи у великих мережах можуть не дозволити отримати розв'язання задачі відмовостійкої маршрутизації за заданий час. Тому для вирішення поставленої задачі авторами запропоновано евристику, яка здатна знайти рішення в більшості випадків. Крім того, розрахункові рішення мають прийнятну від-

носну похибку стосовно вартості отриманого шляху або пари шляхів, а процесорний час, який вимагає евристика, значно менше часу, який вимагає вирішувач ILP.

В роботі [31] представлено рішення щодо розподілу резервної пропускної здатності (*Spare Capacity Allocation, SCA*) при використанні спільного резервного захисту шляху при подвійних відмовах каналів зв'язку (*dual link failures*). Дана робота розширює застосування задачі SCA в IP mesh-мережах та WDM. Отже, в ході розв'язання 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 було розширено термінологію при захисті каналів 1+1 та 1:1 для захисту резервного шляху. Крім того, в роботі було показано, що удосконалений евристичний алгоритм успішної безвідмовної маршрутизації (*Successive Survivable Routing, SSR*) для випадку подвійних відмов добре масштабується в мережах з великою розмірністю.

Використання резервних (альтернативних) шляхів є загальною методикою забезпечення захисту при відмовах елементів ТКМ (вузлів / каналів зв'язку / шляхів тощо). Однак обчислення відповідних множин основних і резервних шляхів, що не перетинаються, вимагає значного часу, використовуючи доступні алгоритми (наприклад, підхід Бхандарі [32]). Це, в свою чергу, може значно вплинути на здатність мережі обслуговувати динамічні потоки (тобто ті, що характеризується відносно короткою тривалістю надання послуги). Щоб забезпечити вирішення цієї проблеми, в роботі [32] запропоновано підхід щодо попереднього обчислення множини шляхів, що не перетинаються, з метою отримання можливості обслуговування потоків одразу після їх надходження в мережу. Цей підхід базується на тому спостереженні, що задача обчислення множини шляхів, що не перетинаються за вузлами, еквівалентна задачі визначення «найдешевшого» циклу топології мережі, що проходить через вузли відправника та одержувача відповідного потоку. Зокрема, авторами запропоновано узагальнення цієї схеми, якщо припустити, що будь-яка пара шляхів, що не перетинаються за вузлами, може бути отримана шляхом об'єднання базових циклів, визначених для топології мережі (рис. 4).

Вводиться новий метод для розрахунку найдешевших циклів на основі так званих базових циклів, який, як підтверджено для реальних мережних топологій, зменшує до 70% часу, необхідного для встановлення шляхів, що не перетинаються за вузлами (у порівнянні з результатами, отриманими за схемою Бхандарі).

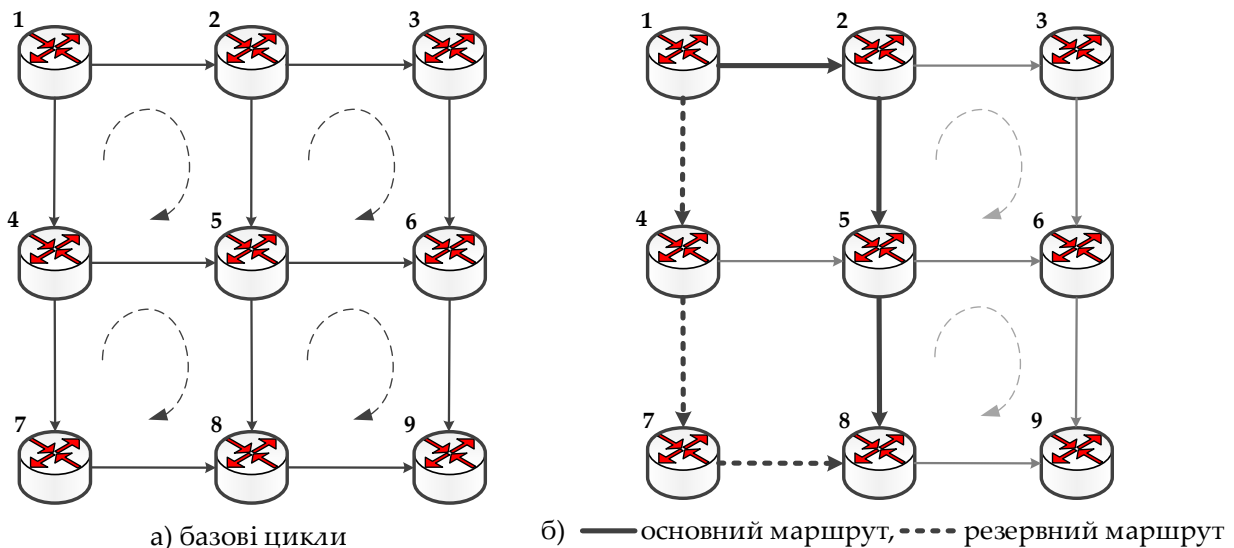


Рис. 4. Ілюстрація основної ідеї схеми попереднього розрахунку основного та резервного шляхів, що не перетинаються

Крім того, слід відмітити, що на сьогоднішній день телекомунікаційні мережі повинні 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 при проектуванні відмовостійких і високонадійних ТКМ. В статтях [33, 34] було 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)*, в топології мережі та відповідний захист і маршрутизацію з метою надавання диференційованих класів відмовостійкості з різним рівнем доступності. В роботі [33] було досліджено саму концепцію спайна на прикладі, що ілюструє потенційні переваги даного підходу. Також було показано, як структурні властивості топології мережі можуть бути використані для визначення евристики для вибору відповідного спайна та порівняння з випадком, коли всі мережні компоненти мають однакову доступність.

Концепція застосування спайнів показана на наступному прикладі. Нехай повнозв'язна мережа, яка представлена графом, показаним на рис. 5, включає в себе чотири вузла та шість каналів зв'язку. При цьому для кожного  $l$ -го каналу зв'язку відома його метрика доступності  $a_l$ , яка змінюється в межах від 0 до 1 [33]. В даному прикладі обрано спайн, до складу якого входять канали зв'язку  $1 \rightarrow 2$ ,  $1 \rightarrow 3$  та  $1 \rightarrow 4$ , що мають вищі значення метрики доступності  $a_1$ ,  $a_5$  та  $a_4$  відповідно.

Таким чином, доступність основного маршруту (*working path, WP*) для потоку, що передається, визначається згідно з виразом [33]:

$$A^{WP} = \prod_{l \in WP} a_l. \quad (1)$$

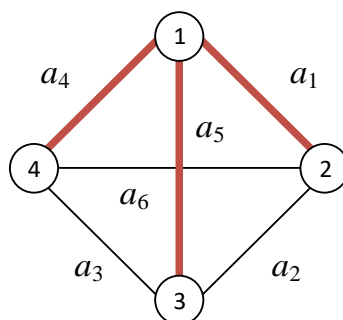


Рис. 5. Приклад мережі з повнозв'язною топологією та обраного спайна на ній

Аналогічно формулі (1) визначається доступність резервного маршруту  $A^{BP}$  (*backup path, BP*). Тоді як доступність мережі для потоку, що передається, можна отримати таким чином [33]:

$$A = 1 - (1 - A^{WP})(1 - A^{BP}). \quad (2)$$

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

Далі задача ефективного забезпечення високого рівня міжкінцевої доступності при передачі потоків між вузлами ТКМ формулювалась у вигляді оптимізаційної при використанні різних критеріїв оптимальності:

- максимізація суми доступності основних шляхів для всіх потоків, що еквівалентно максимізації середньої вартості доступності основних шляхів для всіх потоків;
- максимізація мінімуму доступності основних шляхів для всіх потоків.

У дослідженнях останніх років велика увага приділяється концепції надання диференційованих класів відмовостійких послуг через мережі зв'язку. В ряді рішень автори намагалися вирішити ці завдання шляхом створення різних категорій послуг із різними схемами захисту. Проте більшість з них орієнтовані на застосування в однорангових мережах та не мають узгодженої міжрівневої координації при багаторівневих (ієрархічних) сценаріях. Крім того, існує зростаюча потреба у наданні послуг з високими вимогами до відмовостійкості у мережах майбутнього. Це, однак, має бути зроблено економічно ефективним способом і без надмірної складності. В статті [34] запропоновано вдосконалення попереднього підходу на основі спайнів, який дозволяє спростити розробку необхідного механізму та забезпечує як високу відмовостійкість, так і її диференціацію. Отже, запропонований підхід використовує ідею концепції спайну щодо введення підмереж на фізичному рівні з відносно високою доступністю каналів зв'язку та вузлів [33]. Це створює основу для диференціації відмовостійкості між різними класами потоків. Потім міжрівневе відображення та маршрутизація з урахуванням спайну виконуються таким чином, щоб інформація щодо здатності диференціювання передавалася на верхній рівень. Тут також пропонувалося два оптимі-

заційних формулювання задачі маршрутизації та відображення, а також оцінено їх ефективність при багаторівневому сценарії.

Серед досліджень щодо відмовостійкості в SDN мережах можна виділити роботи [3, 10, 35-37]. Так, наприклад, в [35] запропоновано алгоритм локальної швидкої перемаршрутизації (*Local Fast Reroute, LFR*) з агрегацією потоків в програмно-конфігурованих мережах SDN. В алгоритмі LFR в разі виявлення відмови каналу зв'язку всі потоки трафіка, вражені відмовою, агрегуються у так званій «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. Проведені чисельні результати довели, що LFR забезпечує швидке відновлення, мінімізуючи загальну кількість потоків у SDN.

Зростаюча складність сучасних мережних додатків та величезний попит на інтернет-ресурси вимагають від інфраструктур ТКМ здатності адаптуватися до вимог високого ступеню робастності та надійності. Як було сказано вище, в SDN мережах надзвичайно актуальним є саме завдання підвищення відмовостійкості та своєчасне оновлення інформації про стан мережі, яким присвячено дослідження [36]. В ньому визначені нові алгоритми, які спрямовані на покращення пошуку резервних шляхів у мережах великої розмірності при одиночних відмовах каналів зв'язку з мінімальними часовими витратами на оновлення інформації про стан мережі. Нове рішення спрямоване на підвищення ефективності та зменшення операцій по обробці 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), як правило, призводить до підвищення обчислювальної складності та зниження масштабованості протокольних рішень. Відомо, що ефективність протокового рішення багато в чому визначається адекватністю та якістю покладеної в його основу математичної моделі розрахунку. Як показав проведений аналіз [38], порядок FRR і TE визначається в ході розв'язання оптимізаційних задач різного рівня складності. При цьому реалізація схеми захисту пропускної здатності мережі, як правило, призводить до нелінійного формулювання оптимізаційної задачі та відповідного зростання обчислювальної складності одержуваних рішень.

## **II. Перспективи розвитку методів відмовостійкої маршрутизації в напрямку реалізації схем захисту рівня якості обслуговування в ТКМ**

Варто відзначити, що при відмовостійкій маршрутизації в сучасних мультисервісних ТКМ вже недостатньо забезпечити реалізацію схем захисту каналу/вузла/шляху. Необхідно, щоб вздовж і основного, і резервного маршрутів виконувались вимоги щодо рівня якості обслуговування. Варто зазначити, що при обслуговуванні пакетів більшої частини сучасних додатків вже необхідно забезпечити QoS за *множиною* показників – показниками пропускної здатності, часовими показниками, а також показниками на-

дійності. Так, наприклад, потоки пакетів мультимедійних додатків однаково чутливі і до пропускної здатності, що виділяється, і до рівня затримок пакетів тощо (табл. 1). Тому і при розв'язанні задач відмовостійкої маршрутизації треба забезпечувати захист не одного, а множини показників якості обслуговування як вздовж основного, так і резервного маршрутів.

Таблиця 1. Чутливість трафіка різних додатків до значень QoS-показників

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

Грунтуючись на результатах проведеного аналізу існуючих і перспективних рішень щодо відмовостійкої маршрутизації проведена класифікація перспективних схем захисту рівня якості обслуговування в телекомунікаційних мережах (табл. 2). Так до першого типу QoS<sup>1</sup>-FRR відносяться рішення щодо швидкої перемаршрутизації із захистом одного показника мережної продуктивності (Network Performance, NP), наприклад, пропускної здатності [1-4, 10, 28, 33, 34, 39-46], так як саме пропускна здатність є ключовим і одним з найважливіших показників якості обслуговування. Досить ефективні рішення щодо відмовостійкої маршрутизації із захистом каналу/вузла/шляху та пропускної здатності мережі запропоновані в роботах [40-46], які охоплюють варіанти реалізації як одношляхової, так і багатошляхової стратегій маршрутизації.

Таблиця 2. Схеми захисту рівня якості обслуговування в телекомунікаційних мережах

Тип схеми	Показники мережної продуктивності (Network Performance)			Quality of Experience, QoE	
	Пропускна здатність	Середня затримка	Ймовірність втрат пакетів	R	MMq
QoS <sup>1</sup> -FRR	✓	✗	✗	✗	✗
QoS <sup>2</sup> -FRR	✓	✓	✗	✗	✗
	✓	✗	✓	✗	✗
QoS <sup>3</sup> -FRR	✓	✓	✓	✗	✗
QoE-FRR	✗	✗	✗	✓	✗
	✗	✗	✗	✗	✓

В [39] було розроблено механізм швидкої перемаршрутизації, адаптований до використання в програмно-конфігурованих мережах з централізованою архітектурою. При цьому контролер, що розраховує основні та резервні маршрути, використовує сценарій ефективного спільного резервування пропускну здатності для резервних шляхів. Таким чином, запропоноване рішення щодо резервування та спільного використання пропускну здатності сприяє більш ефективному використанню наявного мережного ресурсу.

В роботах [40, 41] в рамках рішень щодо швидкої перемаршрутизації також запропоновано схему захисту пропускну здатності при розрахунку резервних маршрутів, тоді як умови захисту каналу та вузла при реалізації багатошляхової маршрутизації представлено в лінійній формі. До того ж, введення системи критеріїв оптимальності рішень з встановленням ієрархії співвідношень вагових коефіцієнтів у відповідних цільових функціях дозволило підвищити продуктивність ТКМ та масштабованість рішень щодо швидкої перемаршрутизації, а також знизити їх обчислювальну складність.

Дворівневий метод швидкої перемаршрутизації з балансуванням навантаження в програмно-конфігурованих мережах, який також включає захист рівня якості обслуговування за єдиним показником пропускну здатності, запропоновано в [42]. Метод визначається введенням відповідно до принципу прогнозування взаємодій дворівневої ієрархії розрахунків маршрутних змінних, що відповідають за формування основних і резервних шляхів з реалізацією схем захисту каналу, вузла, шляху та їх пропускну здатності і забезпеченням збалансованої завантаженості каналів зв'язку мережі потоками, що передаються як за основними, так і за резервними маршрутами, що відповідає вимогам концепції Traffic Engineering. Також ефективне рішення, засноване на концепції TE, було отримано в [43], яке представляє собою узгоджене рішення завдань щодо балансування навантаження і швидкої перемаршрутизації із захистом каналу, вузла та пропускну здатності в ході розв'язання задачі лінійного програмування.

В роботі [44] представлено комплексний метод ієрархічно-координаційної міждоменої швидкої перемаршрутизації при забезпеченні захисту приграничних маршрутизаторів ядра мережі на підставі розрахунку основних та резервних міждомених шляхів як при реалізації одношляхової, так і для багатошляхової маршрутизації, заснований на декомпозиційному представленні потокової моделі маршрутизації та використанні принципу цільової координації. Цей метод дозволяє підвищити масштабованість та відмовостійкість маршрутних рішень. В роботі [45] запропоновано систему поточкових моделей відмовостійкої маршрутизації з захистом шлюзу за замовчуванням при реалізації функцій відмовостійкості шляхом введення додаткових керуючих змінних, відповідальних за вибір основного та резервного шлюзів за замовчуванням з балансуванням навантаження між ними, а також забезпеченням погодженого розв'язання задач щодо захисту шлюзу за замовчуванням і швидкої перемаршрутизації в транспортній мережі.

Наступний за складністю тип схем захисту рівня якості обслуговування в ТКМ – це QoS–FRR, який передбачає захист рівня якості обслуговування за двома показни-

ками мережної продуктивності. Так, в роботі [46] запропоновано математичну модель відмовостійкої QoS-маршрутизації в мультисервісній ТКМ, за допомогою якої забезпечується реалізація схеми захисту рівня якості обслуговування за показниками пропускної здатності та середньої міжкінцевої затримки пакетів. Шукані умови захисту рівня якості обслуговування вдалось отримати на підставі тензорного опису процесу відмовостійкої маршрутизації. У роботі [47] запропоноване рішення відповідно до схеми QoS<sup>2</sup>-FRR, яке представлено нелінійною потоковою моделлю швидкої перемаршрутизації із захистом таких двох показників мережної продуктивності, як пропускна здатність та ймовірність втрат пакетів. Ця модель на рівні умов збереження потоку вже враховує обмеженість буфера черг на інтерфейсах маршрутизаторів ТКМ, що дозволило контролювати ймовірне перевантаження мережного ресурсу.

Перспективним напрямом розвитку рішень щодо відмовостійкої маршрутизації є підтримка третього типу схем QoS<sup>3</sup>-FRR, коли реалізується захист рівня якості обслуговування за розширеною множиною показників – за трьома показниками мережної продуктивності, наприклад, пропускною здатністю, середньою міжкінцевою затримкою та ймовірністю втрат пакетів. Крім того, особливим типом рішень вбачається швидка перемаршрутизація потоків пакетів з підтримкою рівня якості обслуговування, що сприймається на рівні користувача (Quality of Experience, QoE). Відповідно до стандартів ITU-T, при обслуговуванні мультимедійних потоків важливо забезпечити реалізацію схеми QoE-FRR, наприклад, за показником рейтингу якості (Rating, R) – при передачі голосового трафіка (VoIP) [48] або показником мультимедійної якості (Multimedia Quality, MMq) [49] – при передачі трафіка відео-телефонії.

## Висновки

Аналіз відомих рішень в області відмовостійкої маршрутизації дозволив сформулювати перелік ключових вимог, яким повинні відповідати перспективні рішення в цій області і, перш за все, математичні моделі та методи, на яких вони ґрунтуються:

- врахування потокового характеру трафіку, що є відмінною рисою більшості мультимедійних послуг і обов'язковим моментом при реалізації схем захисту пропускної здатності та інших показників якості обслуговування 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 та рівня QoS за множиною показників);
- узгоджене вирішення окремих завдань відмовостійкої маршрутизації, наприклад, захист шляху за замовчуванням, швидка перемаршрутизація тощо;
- розширення можливостей існуючих 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, по яких передаються пакети одного і того ж потоку;

– прийнятна обчислювальна складність рішень маршрутизації.

Проведена класифікація перспективних схем захисту рівня якості обслуговування (табл. 2), які важливо реалізувати в ході відмовостійкої маршрутизації переважно мультимедійних потоків. Перспективні маршрутні рішення мають забезпечувати захист QoS одночасно за множиною показників мережної продуктивності (NP) або за показниками якості обслуговування, що сприймається на рівні користувачів (QoE). Все це вимагає розробки нових або вдосконалення існуючих математичних моделей і методів відмовостійкої маршрутизації відповідно до наведених вимог.

### Список літератури:

1. 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.
2. 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.
3. Rak J. Resilient Routing in Communication Networks (Computer Communications and Networks), 1st edition. – Springer, 2015. – 181 p.
4. 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.
5. 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).
6. 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.
7. 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.
8. 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.
9. 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.
10. 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>.

11. *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.
12. *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.
13. *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.
14. *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.
15. *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.
16. *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.
17. *Antonakopoulos S., Bejerano Y., Koppol P.* Full protection made easy: The DisPath IP fast re-route scheme // *IEEE/ACM Transactions on Networking*. – 2015. – Vol.23, No.4. – P. 1229-1242. – DOI: 10.1109/TNET.2014.2369855.
18. *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.
19. *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.
20. *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.
21. *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.
22. *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).
23. *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.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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>.

30. 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>.

31. 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.

32. 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>.

33. 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.

34. 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.

35. 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.

36. 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.

37. Rzym G., Wajda K., Chotda 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>.
38. 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.
39. Hasan H., Cosmas J., Zaharis Z., Lazaridis P., Khwandah S. Development of FRR mechanism by adopting SDN notion // *Software, Telecommunications and Computer Networks (SoftCOM): Proceedings of the 24th International Conference*. Split, Croatia, 22-24 September, 2016. – IEEE, 2016. – P. 1-7. – DOI: 10.1109/SOFTCOM.2016.7772133.
40. 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, Issue6. – P. 477–490. – DOI: 10.1615/TelecomRadEng.v76.i6.30.
41. 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.
42. 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.
43. 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.
44. Lemeshko O., Yeremenko O., Nevzorova O. Hierarchical Method of Inter-Area Fast Rerouting // *Transport and Telecommunication Journal*. – 2017. – Vol.18, Issue 2. – P.155–167. – DOI: 10.1515/ttj-2017-0015.
45. 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. – Volume 8, Number 1. – P. 19–26.
46. Єременко О.С. Тензорна модель відмовостійкої маршрутизації з підтримкою якості обслуговування в мультисервісній телекомунікаційній мережі [Електронний ресурс] / О.С. Єременко // *Проблеми телекомунікацій*. – 2017. – № 2 (21). – С. 16 - 31. – Режим доступу до журн.: [http://pt.journal.kh.ua/2017/2/1/172\\_yeremenko\\_qosfr.pdf](http://pt.journal.kh.ua/2017/2/1/172_yeremenko_qosfr.pdf).
47. Лемешко О.В., Євдокименко М.О., Єременко О.С. Поточкова модель швидкої перемаршрутизації із захистом рівня обслуговування за показниками пропускної здатності та ймовірності втрат // *Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах: Матеріали VII-ої міжнародної науково-практичної конференції (м. Чернівці, 8-10 листопада 2018 р.)*. – Чернівці: «Місто», 2018. – С. 18-20.
48. ITU-T. The e-model, a computational model for use in transmission planning // *ITU-T Recommendation G. 107*. – 2015. – 24 p.
49. ITU T. Opinion model for video-telephony applications // *ITU-T Recommendation P. 1070*. – 2018. – 25 p.