УДК 621.391

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОАКТИВНИХ РІШЕНЬ З ВІДМОВОСТІЙКОЇ МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНІЙ МЕРЕЖІ

О.В. Лемешко, А.О. Круглова
Харківський національний університет радіоелектроніки

А.В. Крепко
Харківський національний університет Повітряних Сил імені Івана Кожедуба

Abstract *– The work established that an essential solution for proactively ensuring fault tolerance of networks is the support of load balancing both at the transport network level and access level using FHRP. However, FHRP load balancing is based on manual settings, which impose high requirements on the network administrator's professional training and experience level. Therefore, the task of improving mathematical models and methods that make up the algorithmic basis of fault-tolerant routing protocols is urgent. At the same time, a mandatory requirement for these models and methods is to consider the border routers' reliability through which the load incoming from access networks is balanced. The work describes four mathematical solutions to the problem of proactive fault-tolerant routing. To ensure a high level of Quality of Service, all analyzed solutions support the requirements of the Traffic Engineering concept, and two take into account the reliability of border routers (RATE and ResMetrTE). On the network topology chosen for the study, the problem of proactive fault-tolerant routing was solved using the solutions described in work. The results of the calculations confirmed the sensitivity of the RATE and ResMetrTE routing solutions to the reliability of border routers. Within the considered example, it was established that taking into account the level of border routers' reliability when organizing load balancing between them using RATE or ResMetrTE solutions led to an increase in the upper bound of the network link utilization - from 15% to 27% on average. The work demonstrates that the implementation of analyzed load balancing solutions can be ensured using the GLBP protocol using the weighted balancing mode when the weight of each border router is determined not empirically but based on the results of calculations within the RATE or ResMetrTE solutions.*

Анотація *– У роботі встановлено, що важливим рішенням щодо проактивного забезпечення відмовостійкості мереж є підтримка балансування навантаження як на рівні транспортної мережі, так і на рівні доступу засобами FHRP. Проте балансування навантаження за допомогою FHRP базується на використанні ручних налаштувань, що накладає високі вимоги щодо рівня фахової підготовки та досвіду адміністратора мережі. Тому актуальною є задача щодо вдосконалення математичних моделей і методів, які складають алгоритмічну основу протоколів відмовостійкої маршрутизації. При цьому обов'язковою вимогою до цих моделей і методів є забезпечення врахування рівня надійності пригранічних маршрутизаторів, між якими балансується навантаження, що надходить від мереж доступу. У роботі описано чотири математичні рішення задачі проактивної відмовостійкої маршрутизації. З метою забезпечення високого рівня якості обслуговування всі аналізовані рішення підтримують вимоги концепції Traffic Engineering, а два з них враховують рівень надійності пригранічних маршрутизаторів (RATE та ResMetrTE). На обраній для дослідження мережній топології здійснено розв'язання задач проактивної відмовостійкої маршрутизації за допомогою описаних у роботі рішень. Результати розрахунків підтвердили чутливість маршрутних рішень RATE та ResMetrTE до рівня надійності пригранічних маршрутизаторів. У межах розглянутого прикладу встановлено, що врахування рівня надійності пригранічних маршрутизаторів при організації балансування навантаження між ними за допомогою рішень RATE або ResMetrTE призводило до деякого підвищення порогу завантаженості каналів зв'язку мережі – у середньому від 15% до 27%. У роботі продемонстровано, що впровадження аналізованих рішень щодо балансування навантаження може бути забезпечено за допомогою протоколу GLBP з використанням режиму зваженого балансування, коли вага кожного пригранічного маршрутизатора визначається не емпірично, а обґрунтовується за результатами розрахунків у межах рішень RATE або ResMetrTE.*

Вступ

Сучасні інфокомунікаційні мережі (ІКМ) є складними організаційно-технічними системами, які функціонують в умовах постійного впливу внутрішніх і зовнішніх впливів, що нерідко викликає відмову у наданні тих чи інших сервісів. До таких впли-

вів випадкового характеру можна віднести, наприклад, збої апаратного та програмного забезпечення мережного обладнання, його перевантаження, компрометацію або невмілу експлуатацію [1-3]. Тому більшість ІКМ мають у своєму арсеналі вбудований функціонал щодо забезпечення відмовостійкості шляхом проактивного та реактивного захисту (резервування) елементів мережі. Подібні рішення реалізуються практично на всіх рівнях еталонної моделі взаємодії відкритих систем (ЕМВВС), на мережному рівні ЕМВВС за підвищення відмовостійкості відповідають серед інших також протоколи маршрутизації [4, 5].

Проактивна відмовостійкість забезпечується засобами балансування навантаження на принципах Traffic Engineering (TE) та підтримки використання шляхів з різною маршрутною метрикою, як це реалізовано, наприклад, у протоколі EIGRP (Enhanced Interior Gateway Routing Protocol) [6-10]. Це дозволяє ефективно використовувати весь доступний мережний ресурс, тому при виході з ладу того чи іншого елемента мережі втрати будуть мінімальними. Реактивний захист зазвичай реалізується на підставі організації швидкої перемаршрутизації з резервуванням маршрутизаторів, каналів і шляхів ІКМ. Для захисту приграничних маршрутизаторів, які виконують для мереж доступу функцію шлюзу за замовчуванням, використовуються протоколи резервування першого переходу (First Hop Redundancy Protocols, FHRP) [11-15]. Деякі з них, як, наприклад, протокол GLBP (Gateway Load Balancing Protocol) також підтримує балансування навантаження, яке надходить від мереж доступу на приграничні маршрутизатори, що підвищує ефективність як проактивного, так і реактивного захисту шлюзу за замовчуванням та ІКМ загалом від імовірних відмов.

На даний час процес балансування навантаження як на рівні транспортної мережі, так і на рівні доступу до ІКМ все ще багато в чому залежить від адміністративного втручання у роботу маршрутизаторів. Навіть у найбільш просунутих у цьому відношенні протоколах EIGRP та GLBP ключові параметри, які впливають на порядок балансування навантаження, визначаються адміністратором мережі та налаштовуються вручну. Автоматично та за замовчуванням балансування навантаження реалізується в протоколі EIGRP лише за шляхами, які мають однакову мінімальну метрику, а у протоколі GLBP – з використанням досить примітивного алгоритму Round-Robin (RR). Тобто в обох випадках доступний мережний ресурс використовується рівномірно, без урахування різниці у продуктивності, надійності та безпечності шляхів і приграничних маршрутизаторів. Врахування диференціації у значеннях перелічених показників для різних маршрутних рішень вимагає високого рівня фахової підготовки та досвіду роботи адміністратора. Ручні налаштування, крім того, займають досить багато часу, особливо для масштабних мереж.

Таким чином, процес балансування навантаження з урахуванням різнотипності та різнорідності доступного мережного ресурсу доцільно також автоматизувати та реалізовувати за допомогою вдосконалених або нових протоколів відмовостійкої маршрутизації. Розв'язання цієї задачі пов'язано з використанням нових математичних моделей, методів та обчислювальних алгоритмів, які складають основу новітніх маршру-

тних протоколів [4, 5]. Тому метою даної роботи є дослідження на порівняльний аналіз проактивних рішень з відмовостійкої маршрутизації в ІКМ, які базуються на різних підходах щодо врахування рівня надійності мережного обладнання, наприклад, приграничних маршрутизаторів.

І. Потокова модель маршрутизації з балансуванням навантаження в інфокомунікаційній мережі

Нехай при описі порівнювальних маршрутних рішень використовуються позначення, що представлені у табл. 1. У процесі дослідження за основу була взята потокова модель маршрутизації з балансуванням навантаження на принципах Traffic Engineering [16]. В її межах ми припускаємо, що структуру мережі описує граф $G=(M,L)$ (табл. 1). Тоді K — це множина потоків, які циркулюють між мережами доступу за допомогою ресурсу транспортної мережі. З кожним k-м потоком пакетів ($k \in K$) пов'язані мережі доступу – джерело (V_s^k) та отримувач (V_d^k). Параметр λ^k характеризує середню інтенсивність (швидкість) пакетів k-го потоку на вході в ІКМ, яка вимірюється в пакетах за секунду (1/с).

На маршрутні змінні $x_{i,j}^k$ у разі використання одношляхової маршрутизації потоків в ІКМ накладаються такі обмеження:

$$x_{i,j}^k \in \{0;1\}, \tag{1}$$

а при реалізації багатошляхової маршрутизації:

$$0 \le x_{i,j}^k \le 1. \tag{2}$$

Якщо мережа доступу взаємодіє лише з одним із приграничних маршрутизаторів ІКМ, то на змінні доступу накладаються обмеження виду

$$y_{i,j}^k \in \{0;1\} \quad \text{та} \quad z_{j,i}^k \in \{0;1\}. \tag{3}$$

У випадку підтримки балансування навантаження на рівні доступу, як це реалізовано в протоколах VRRP, GLBP і CARP [11], на ці ж змінні накладаються умови, аналогічні до (2):

$$0 \le y_{i,j}^k \le 1 \ \text{та} \ \ 0 \le z_{i,j}^k \le 1. \tag{4}$$

Таблиця 1 – Використані позначення

Позначення	Опис
$G=(M,L)$	Граф мережі
$M=R\bigcup V$	Множина вершин графа G ($R\bigcap V=\varnothing$)
$R=\left\{R_i, i=\overline{1,m}\right\}$	Підмножина вершин, що моделюють маршрутизатори
$V=\left\{V_j, j=\overline{1,v}\right\}$	Підмножина вершин, що описують мережі доступу
$R^+\subset R$	Підмножина вершин, що моделюють прикордонні маршрутизатори ІКМ
$R^-\subset R$	Підмножина вершин, що моделюють транзитні маршрутизатори ІКМ
$R_j^+\subset R^+$	Підмножина вершин графа , що моделює ті прикордонні маршрутизатори, що утворюють віртуальний маршрутизатор для мережі доступу V_j
$L=E\bigcup W$	Множина дуг графа G ($E\bigcap W=\varnothing$)
$E=\left\{E_{i,j}, i,j=\overline{1,m}, i\neq j\right\}$	Множина дуг, що моделюють канали зв'язку ІКМ, які з'єднують маршрутизатори
$W^+=\left\{W_{i,j}^+, i=\overline{1,v}, j=\overline{1,m^+}\right\}$	Множина дуг, що описують лінії доступу, які з'єднують мережі доступу та прикордонні маршрутизатори
$W^-=\left\{W_{i,j}^-, i=\overline{1,m^+}, j=\overline{1,v}\right\}$	Множина дуг, що описують лінії доступу, які з'єднують прикордонні маршрутизатори ІКМ та мережі доступу
$\varphi_{i,j}$	Пропускна здатність каналу зв'язку, що моделюється дугою $E_{i,j}\in E$
K	Множина потоків пакетів, що циркулюють в ІКМ
K_i^+	Множина потоків, що надходять до ІКМ від мережі доступу V_i
K_i^-	Множина потоків, що виходять з ІКМ до мережі доступу V_i
V_s^k	Мережа доступу, яка є джерелом k-го потоку пакетів
V_d^k	Мережа доступу, яка є отримувачем пакетів k-го потоку
λ^k	Середня інтенсивність пакетів k-го потоку
$x_{i,j}^k$	Маршрутна змінна, яка характеризує частку k-го потоку в каналі зв'язку, представленого дугою $E_{i,j}$
$y_{i,j}^k$	Змінна доступу, яка визначає частку k-го потоку, що протікає в лінії доступу, представленій дугою $W_{i,j}^+$
$z_{j,i}^k$	Змінна доступу, яка характеризує частку k-го потоку, що протікає в лінії доступу, представленій дугою $W_{j,i}^-$
α	Верхній поріг завантаженості каналів зв'язку ІКМ

Для забезпечення збереження потоку на рівні доступу на відповідні керуючі змінні накладаються додаткові умови-обмеження:

$$\sum_{R_j \in R_p^+} y_{p,j}^k = 1,\ V_p = V_s^k; \tag{5}$$

$$\sum_{R_j \in R_h^+} z_{j,h}^k = 1,\ \ V_h = V_d^k. \tag{6}$$

Умови збереження потоку на рівні транспортної мережі мають наступний вигляд [4, 16]:

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^k = 0;\ \ k \in K,\ R_i \in R^-; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k = y_{p,i}^k;\ \ k \in K,\ R_i \in R^+,\ V_p = V_s^k; \\ \sum\limits_{j:E_{j,i}\in E} x_{j,i}^k = z_{i,h}^k;\ \ k \in K,\ R_i \in R^+,\ V_h = V_d^k. \end{cases} \tag{7}$$

Виконання умов (7) дозволяє забезпечити взаємозв'язок при розрахунку керуючих змінних різних типів, а відповідно і скоординувати процеси балансування навантаження на рівні доступу та ІКМ загалом. Для забезпечення балансування навантаження в ІКМ на принципах ТЕ в модель вводяться умови запобігання перевантаження такого виду [7]:

$$\sum_{k\in K} \lambda^k x_{i,j}^k \le \alpha \varphi_{i,j}, \tag{8}$$

де α – верхній поріг завантаженості каналів зв'язку ІКМ (табл. 1), який виступає такою додатковою керуючою змінною, на значення якої накладаються такі обмеження:

$$0 \le \alpha \le 1. \tag{9}$$

Тоді задачу балансування навантаження в ІКМ можна сформулювати в оптимізаційній формі. Критерієм оптимальності за аналогією до [7, 16] буде виступати умова

$$\min_{x,y,z,\alpha} \alpha, \tag{10}$$

а обмеженнями – умови (1)-(9).

II. Врахування надійності приграничних маршрутизаторів при балансуванні навантаження в інфокомунікаційній мережі

У загальному випадку в межах моделі (1)-(10) балансування навантаження, що надходить в ІКМ з мережі доступу V_p через приграничний маршрутизатор R_j, реалізується шляхом виконання умов:

$$\sum_{k\in K_p^+} \lambda^k y_{p,j}^k = m_{p,j}^+ \sum_{k\in K_p^+} \lambda^k , \tag{11}$$

де $m_{p,j}^+$ – метрики балансування, які визначають частку сумарного трафіку, що надходить в ІКМ від мережі доступу V_p через приграничний маршрутизатор R_j. Тобто при визначенні показників балансування має бути дотримана рівність

$$\sum_{R_j\in R_p^+} m_{p,j}^+ = 1 . \tag{12}$$

У разі рівномірного балансування навантаження (Round-Robin Load-Balancing) відповідна метрика балансування обернено пропорційна до кількості підключених до обраної мережі доступу приграничних маршрутизаторів:

$$m_{p,j}^+ = \frac{1}{\left|R_p^+\right|} . \tag{13}$$

Таким чином, метрики балансування для окремих приграничних маршрутизаторів, які створюють віртуальний шлюз за замовчуванням для мережі доступу V_p, будуть однаковими. Якщо мережа підтримує балансування не тільки на рівні окремих потоків (3), але й на рівні пакетів кожного потоку окремо (4), то для реалізації алгоритму RR необхідно забезпечити, щоб

$$y_{i,j}^k = \frac{1}{\left|R_i^+\right|} . \tag{14}$$

Крім того, протокол GLBP підтримує зважене балансування навантаження, яке в моделі (11) відповідає адміністративному встановленню метрик балансування. Це дослідження також пропонує впровадження зваженого балансування навантаження шляхом адаптації метрик балансування відповідно до рівня надійності приграничних маршрутизаторів.

Нехай коефіцієнт готовності A_i характеризує кожен приграничний маршрутизатор $R_i \in R^+$ відповідно до його рівня надійності. Значення коефіцієнту готовності маршрутизатора визначається як відношення часу, коли він знаходився у працездатному стані, до загального часу його роботи, тобто він приймає значення від нуля до одиниці. Таким чином, щоб реалізувати балансування навантаження з урахуванням надійності приграничних маршрутизаторів у системі (11), у роботах [17, 18] пропонується визначати метрики балансування за такою формулою:

$$m_{p,j}^{+} = \frac{A_j}{\sum\limits_{R_i \in R_p^+} A_i},\ R_j \in R_p^+ . \tag{15}$$

Таким чином, у разі балансування навантаження між інтерфейсами віртуального маршрутизатора більше пакетів буде відправлено на більш надійний мережний пристрій.

Рішення, представлене виразами (11)-(15), відноситься до приграничних маршрутизаторів, через які трафік надходить до ІКМ. Для випадку балансування навантаження на приграничному маршрутизаторі R_j, через який трафік виходить з ІКМ до мережі доступу V_p, застосовуються за аналогією з (11), (13) та (15) такі умови [17, 18]:

$$\sum_{k \in K_p^-} \lambda^k z_{j,p}^k = m_{j,p}^- \sum_{k \in K_p^-} \lambda^k , \tag{16}$$

при застосуванні алгоритму Round-Robin

$$m_{p,j}^- = \frac{1}{\left| R_p^- \right|}, \tag{17}$$

при врахуванні коефіцієнтів готовності

$$m_{j,p}^- = \frac{A_j}{\sum\limits_{R_i \in R_p^+} A_i},\ R_j \in R_p^+, \tag{18}$$

де $m_{j,p}^-$ – метрики балансування, які визначають частку сумарного трафіку, що виходить з ІКМ до мережі доступу V_p через приграничний маршрутизатор R_j.

Метрики балансування та коефіцієнти готовності пропонується врахувати у процесі проактивної відмовостійкої маршрутизації двома способами. Перший спосіб базується на тому, що критерій оптимальності маршрутних рішень (10) залишається незмінним, а на змінні доступу накладаються додаткові обмеження (11), (15), (16) та

(18). Це рішення запропоноване у роботі [18] та носить назву RATE (Resilience Aware TE). Другий спосіб стосується перегляду критерія оптимальності (10), який приймає таку форму

$$\min_{x,y,z,\alpha}\left(\sum_{k\in K}\sum_{V_p\in V}\sum_{R_i\in R_p^+}(1-A_i)y_{p,i}^k+\sum_{k\in K}\sum_{V_p\in V}\sum_{R_j\in R_p^-}(1-A_j)z_{j,p}^k+c_\alpha\alpha\right), \qquad (19)$$

де c_α – ваговий коефіцієнт, який регулює вплив на оптимальне рішення значення порогу α у порівнянні зі значеннями змінних доступу. При збільшенні вагового коефіцієнта c_α маршрутні рішення будуть наближатись за ефективністю балансування до рішень, які отримуються за допомогою критерія (10). Зменшення коефіцієнта c_α посилює вплив на балансування навантаження рівня надійності приграничних маршрутизаторів. Проактивне рішення щодо відмовостійкої маршрутизації, яке базується на моделі (1)-(9) та критерії оптимальності (19) буде мати назву ResMetrTE (Resilience Metrics TE).

Рішення RATE та ResMetrTE будуть порівнюватись з моделлю (1)-(10), яку скорочено позначимо через TE, а також з рішенням RRTE, при якому до моделі (1)-(10) додаються умови (11), (13), (16) та (17).

III. Дослідження процесів балансування навантаження в ІКМ

Мета проведеного дослідження полягала у тому, щоб встановити характер впливу на ефективність процесу балансування навантаження в ІКМ врахування рівня надійності приграничних маршрутизаторів у межах рішень RATE та ResMetrTE. Ефективність процесу балансування оцінювалась за верхнім порогом завантаженості каналів зв'язку ІКМ (α). За визначенням мінімальний рівень забезпечувала реалізація моделі TE (1)-(10), що максимально впливало на рівень якості обслуговування – на продуктивність, середні затримки, джитер і рівень втрат пакетів. Рішення RRTE моделювало роботу протоколу GLBP із налаштуваннями за замовчуванням щодо балансування навантаження.

За основу була взята структура ІКМ (рис. 1), яка складалась із дванадцяти маршрутизаторів ($R_1 \div R_{12}$), що були з'єднані між собою за допомогою сімнадцяти каналів зв'язку ($v=17$). У розривах каналів зв'язку (рис. 1) вказані їх пропускні здатності (1/с). Для прикладу в ІКМ передавався один потік пакетів між мережами доступу V_1 та V_2. Для мережі доступу V_1, яка виступала джерелом потоку пакетів, віртуальним маршрутизатором виступали інтерфейси приграничних маршрутизаторів R_1, R_4 та R_7. Для мережі-отримувача V_2 віртуальний маршрутизатор (шлюз за замовчуванням) створювали інтерфейси приграничних маршрутизаторів R_6, R_9 та R_{12}.

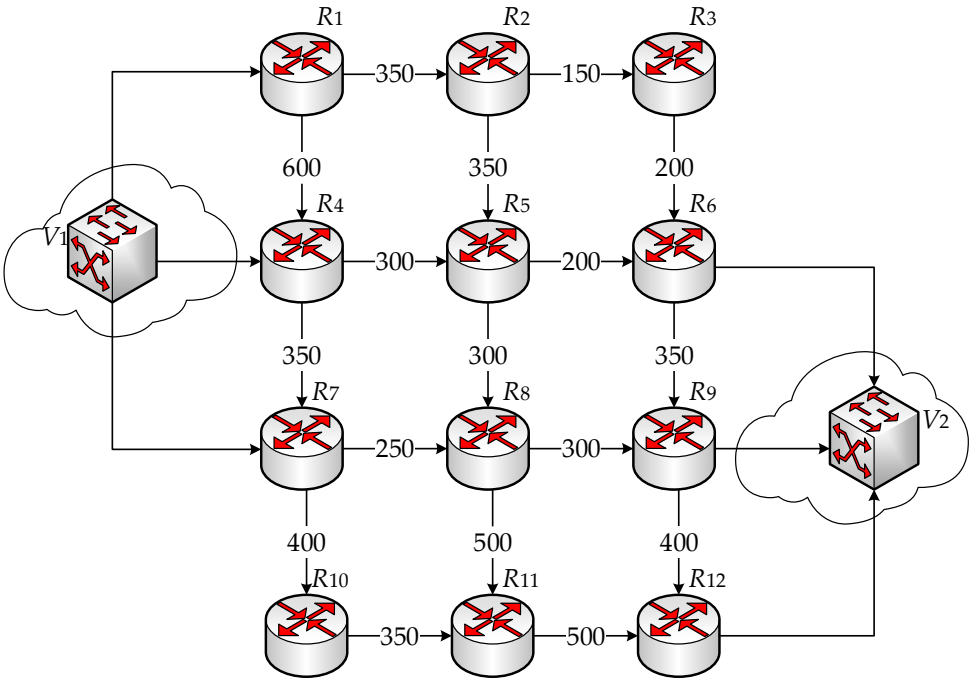


Рис. 1. Приклад структури ІКМ, яка досліджувалась

Моделювалось три варіанти щодо диференціації рівня надійності різних приграничних маршрутизаторів (табл. 2). У межах першого варіанту коефіцієнти готовності приграничних маршрутизаторів приймали значення від 0,9 до 1; в межах другого варіанту – від 0,6 до 1; в межах третього варіанту – від 0,4 до 1.

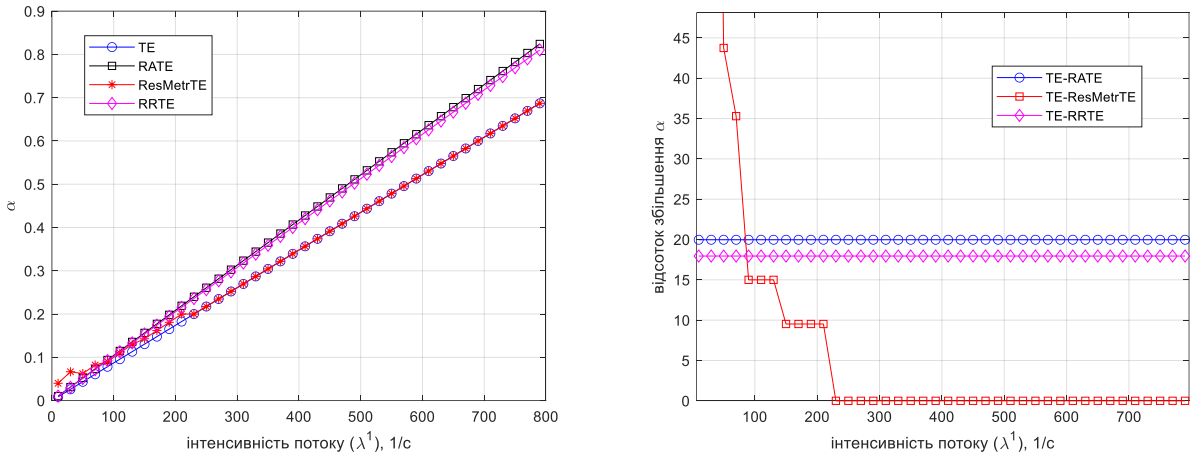
Таблиця 2. Варіанти комбінацій коефіцієнтів готовності приграничних маршрутизаторів ІКМ

Варіант / приграничні маршрутизатори	R_1	R_4	R_6	R_7	R_9	R_{12}
Варіант № 1	0,92	0,95	1	1	0,98	0,94
Варіант № 2	0,6	0,7	0,9	0,9	0,8	0,7
Варіант № 3	0,99	0,7	0,4	0,4	0,8	0,95

Зазначимо, що значення коефіцієнтів готовності маршрутизаторів та їх інтерфейсів визначаються не тільки номінальними характеристиками, які стосуються заявленої виробником експлуатаційної надійності пристрою, але й поточним його станом, пов'язаним, наприклад, з перевантаженням, збоями щодо електроживлення тощо, що також позначається на рівні відмов в обслуговуванні.

В процесі дослідження інтенсивність потоку між мережами доступу V_1 та V_2 змінювалась від 10 до 800 1/с з кроком 20 1/с. Тоді на рис. 2 представлені результати розрахунків щодо реалізації чотирьох порівнюваних рішень відмовостійкої маршрутизації та балансування навантаження для першого варіанта вихідних даних (табл. 2) при c_α=0,4. На рис. 2 а продемонстровано динаміку зміни верхнього порогу

завантаженості каналів зв'язку ІКМ залежно від значення інтенсивності потоку, який надходить від мереж доступу. На рис. 2 б показано, на скільки відсотків збільшиться значення порогу α при використанні рішень RATE, ResMetrTE та RRTE у порівнянні з рішенням TE.



а) б)

Рис. 2. Результати розрахунків щодо реалізації чотирьох порівнюваних рішень відмовостійкої маршрутизації та балансування навантаження для першого варіанта вихідних даних (табл. 2)

Як показали результати розрахунків (рис. 2), врахування рівня надійності приграничних маршрутизаторів у межах рішень RATE та ResMetrTE призводить до підвищення порогу завантаженості каналів зв'язку ІКМ, що є деякою платнею за підвищення відмовостійкості ІКМ. При цьому в межах рішення ResMetrTE врахування рівня надійності мережного обладнання забезпечувалось при досить невисокому навантаженні на ІКМ (до 200 1/с включно). Зі зростанням навантаження на ІКМ (рис. 2 б) рішення ResMetrTE та TE давали однаковий результат. Крім того, рішення RATE та RRTE забезпечували приблизно однаковий результат, оскільки для першого варіанту вихідних даних (табл. 2), коефіцієнти готовності приграничних маршрутизаторів приймали максимально високі значення, тобто їх значення майже співпадали. Це фактично призводило до того, що метрики балансування (13) та (15), (17) та (18) практично не відрізнялись між собою.

У табл. 3 наведені результати балансування навантаження в ІКМ для чотирьох порівнюваних рішень за умови, що інтенсивність потоку складала 200 1/с. Отримані результати демонструють чутливість маршрутних рішень RATE та ResMetrTE до рівня надійності приграничних маршрутизаторів (табл. 2).

На приграничні маршрутизатори, які мали високу надійність, надходило вище навантаження, а на менш надійні – відповідно нижче навантаження. При цьому у даному прикладі наглядно показано, що рішення RATE забезпечувало диференціацію в завантаженості приграничних маршрутизаторів відповідно до рівня диференціації їх коефіцієнтів готовності.

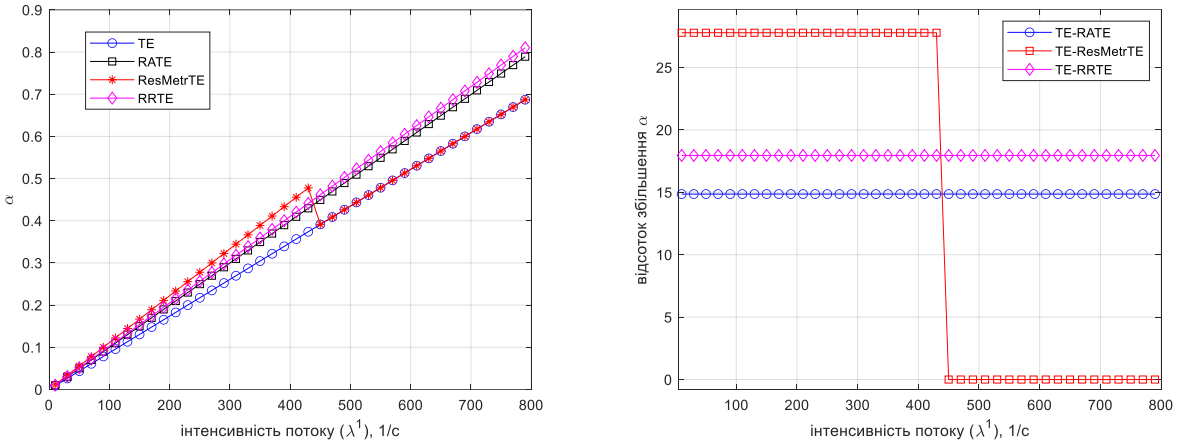
Таблиця 3. Результати балансування навантаження в ІКМ для чотирьох порівнюваних рішень за умови, що інтенсивність потоку складала 200 1/с

Зв'язки	$\varphi_{i,j}$	Інтенсивності потоку пакетів для різних рішень			
		TE	RATE	ResMetrTE	RRTE
$W_{1,1}^{+}$		60,87	64,11	28,57	66 ⅔
$W_{1,4}^{+}$		52,17	66,20	57,14	66 ⅔
$W_{1,7}^{+}$		86,96	69,69	114,29	66 ⅔
$E_{1,2}$	350	60,87	31,30	28,57	30,77
$E_{2,3}$	150	26,09	31,30	28,57	30,77
$E_{1,4}$	600	0	32,81	0	35,90
$E_{2,5}$	350	34,78	0	0	0
$E_{3,6}$	200	26,09	31,30	28,57	30,77
$E_{4,5}$	300	52,17	52,16	57,14	51,28
$E_{5,6}$	200	34,78	41,73	38,10	41,02
$E_{4,7}$	350	0	46,85	0	51,28
$E_{5,8}$	300	52,17	10,43	19,04	10,26
$E_{6,9}$	350	0	4,53	0	5,13
$E_{7,8}$	250	43,48	52,16	47,62	51,28
$E_{8,9}$	300	52,17	62,59	57,14	61,54
$E_{7,10}$	400	43,48	64,38	66,67	66 ⅔
$E_{8,11}$	500	43,48	0	9,52	0
$E_{9,12}$	400	0	0	0	0
$E_{10,11}$	350	43,48	64,38	66,67	66 ⅔
$E_{11,12}$	500	86,96	64,38	76,19	66 ⅔
$W_{6,2}^{-}$		60,87	68,50	66,67	66 ⅔
$W_{9,2}^{-}$		52,17	67,12	57,14	66 ⅔
$W_{12,2}^{-}$		86,96	64,38	76,19	66 ⅔

Рішення ResMetrTE забезпечувало пропорційний розподіл навантаження відповідно до ранжування маршрутизаторів за рівнем надійності. На перший за надійністю маршрутизатор R_7 надходило вдвічі вище навантаження аніж на наступний за надійністю маршрутизатор R_4. Так само на четвертий маршрутизатор надходило навантаження, яке було вдвічі вищим за навантаження, що надходило на найменш надійний маршрутизатор R_1. На вихідних маршрутизаторах R_6, R_9 та R_{12}

у межах рішення ResMetrTE порядок балансування не завжди залежав від рівня їх надійності, що пояснювалось впливом на оптимальність маршрутних рішень також порогу α у критерії (19). З подальшим збільшенням навантаження його вплив ставав визначальним, а рішення ResMetrTE зовсім втрачало чутливість до рівня надійності мережного обладнання. При зменшенні вагового коефіцієнта c_α вплив порогу α у критерії (19) стає слабкішим, а при c_α=0 у межах рішення ResMetrTE будуть використовуватись лише найбільш надійні маршрутизатори з тих, що утворюють віртуальний шлюз за замовчуванням для тієї чи іншої мережі доступу. Менш безпечні маршрутизатори почнуть використовуватись лише за умови перевантаження маршрутів, що починаються з найбільш надійного приграничного маршрутизатора.

На рис. 3 представлені результати розрахунків щодо реалізації чотирьох порівнюваних рішень відмовостійкої маршрутизації та балансування навантаження для другого варіанта вихідних даних (табл. 2) при c_α=15.



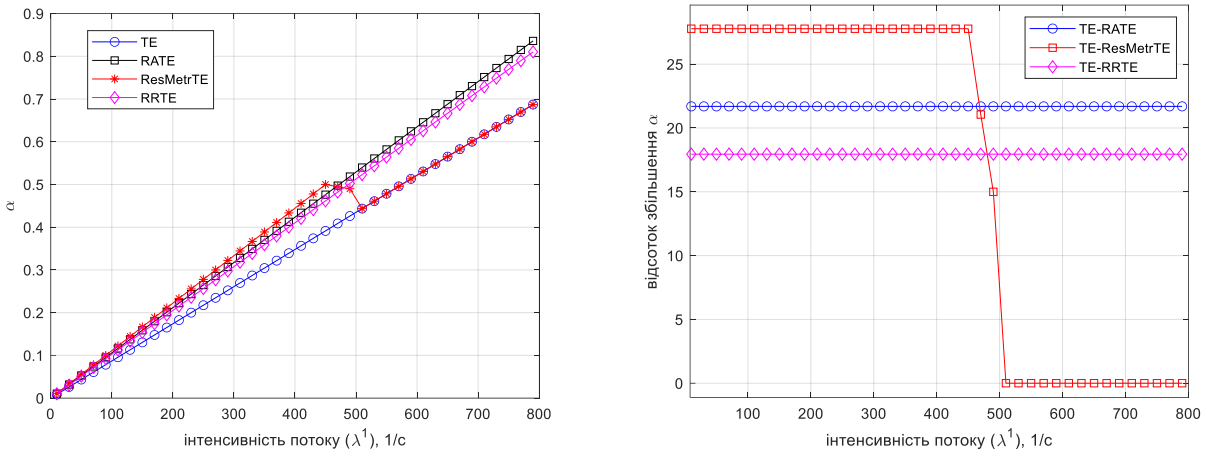
а) б)

Рис. 3. Результати розрахунків щодо реалізації чотирьох порівнюваних рішень відмовостійкої маршрутизації та балансування навантаження для другого варіанта вихідних даних (табл. 2)

Реалізація рішень RATE та ResMetrTE, направлених на врахування рівня надійності приграничних маршрутизаторів, призводила до підвищення порогу завантаженості каналів зв'язку ІКМ приблизно на 15% та 27,8%. В умовах навантаження на мережу в 450 1/с і вище рішення ResMetrTE за наведених вихідних даних втрачало свою чутливість до рівня надійності мережного обладнання.

На рис. 4 представлені результати розрахунків щодо реалізації чотирьох порівнюваних рішень відмовостійкої маршрутизації та балансування навантаження для третього варіанта вихідних даних (табл. 2) при c_α=15. Реалізація рішень RATE та ResMetrTE, направлених на врахування рівня надійності приграничних маршрутизаторів, призводила до підвищення порогу завантаженості каналів зв'язку ІКМ приблизно на 21,7% та 27,8%. В умовах, коли навантаження на мережу складало

вище 500 1/с рішення ResMetrTE за наведених вихідних даних також втрачало свою чутливість до рівня надійності мережного обладнання.



а) б)

Рис. 4. Результати розрахунків щодо реалізації чотирьох порівнюваних рішень відмовостійкої маршрутизації та балансування навантаження для третього варіанта вихідних даних (табл. 2)

III. Приклад впровадження отриманих маршрутних рішень за допомогою протоколу GLBP

Важливим моментом процесу дослідження є розробка пропозицій щодо практичної реалізації отриманих рішень у сучасних і перспективних ІКМ. У даній роботі пропонується з цією метою задіяти функціонал протоколу відмовостійкої маршрутизації GLBP, в якому керуючі параметри, що відповідають за балансування навантаження, будуть задаватись не емпіричним шляхом, а теоретично обґрунтовано, за результатами розрахунків у межах розглянутих і проаналізованих у попередніх розділах рішень.

Приклад подібних налаштувань буде продемонстровано на фрагменті мережної структури (рис. 5), яка створена у симуляторі GNS 3. Мережа включає в себе три приграничні маршрутизатори (R1÷R3), інтерфейси Fast Ethernet 0/0 яких утворюють віртуальний шлюз за замовчуванням для мережі доступу, яка містить сім комп'ютерів (PC1÷PC7). Віртуальний маршрутизатор, який виконує функції шлюзу за замовчуванням для цих семи комп'ютерів, створений у межах 192-ї GLBP групи, має IP-адресу 192.168.0.254/24. Трафік, який генерувався на PC1÷PC7, направлявся до PC8. IP-адреси комп'ютерів і реальних інтерфейсів маршрутизаторів вказано на рис. 5.

На рис. 6 продемонстровано приклад налаштування протоколу GLPB на маршрутизаторі R1 з використанням алгоритму Round-Robin для балансування навантаження. Подібні налаштування проводились і на маршрутизаторах R2 та R3.

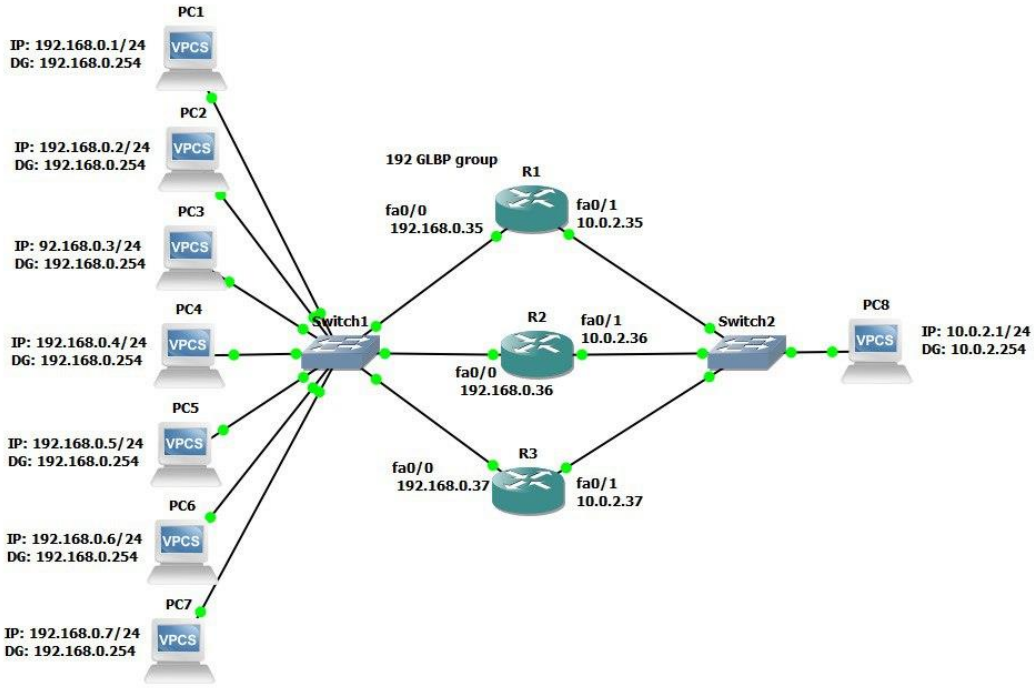


Рис. 5. Схема фрагменту мережної структури

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int fa 0/0
R1(config-if)#ip address 192.168.0.35 255.255.255.0
R1(config-if)#glbp 192 ip 192.168.0.254
R1(config-if)#glbp 192 load-balancing round-robin
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

Рис. 6. Приклад налаштування протоколу GLPB на маршрутизаторі R1 з використанням алгоритму Round-Robin для балансування навантаження

Для подальшої перевірки реалізованого порядку балансування навантаження було використано протокол ICMP, а саме повідомлення Echo Request. За допомогою команди `ping` з комп'ютерів PC1÷PC7 надсилалось по 5 пакетів на комп'ютер PC8 (рис. 7). Для підрахунку (реєстрації) пакетів ICMP, які надійшли на обраний інтерфейс маршрутизатора, було створено списки контролю доступу (Access Control List, ACL). Приклад налаштування ACL для маршрутизатора R1 показано на рис. 8. Такі ж налаштування проводились і на маршрутизаторах R2 та R3.

Після успішної передачі пакетів здійснювалась перевірка стану ACL на кожному з маршрутизаторів з метою визначення того, з якого саме комп'ютера надходили пакети. Так, наприклад, протокол GLBP при використанні алгоритму Round-Robin розподілив пакети, які надходили з різних комп'ютерів, таким чином, як показано на рис. 9 – 11. Тобто маршрутизатор R1 було обрано як шлюз для PC1, PC4 та PC7 (рис. 9),

маршрутизатор R2 цю функцію виконував для PC2 та PC5 (рис. 10), а маршрутизатор R3 – для PC3 та PC6 (рис. 11), що підтвердило правильність проведених налаштувань.

```
PC1> ping 10.0.2.1
84 bytes from 10.0.2.1 icmp_seq=1 ttl=63 time=30.208 ms
84 bytes from 10.0.2.1 icmp_seq=2 ttl=63 time=30.709 ms
84 bytes from 10.0.2.1 icmp_seq=3 ttl=63 time=30.202 ms
84 bytes from 10.0.2.1 icmp_seq=4 ttl=63 time=30.718 ms
84 bytes from 10.0.2.1 icmp_seq=5 ttl=63 time=31.134 ms
```

Рис. 7. Приклад генерування тестового набору пакетів за допомогою команди ping на PC1

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 111 permit icmp 192.168.0.1 0.0.0.0 10.0.2.0 0.0.0.255
R1(config)#access-list 111 permit icmp 192.168.0.2 0.0.0.0 10.0.2.0 0.0.0.255
R1(config)#access-list 111 permit icmp 192.168.0.3 0.0.0.0 10.0.2.0 0.0.0.255
R1(config)#access-list 111 permit icmp 192.168.0.4 0.0.0.0 10.0.2.0 0.0.0.255
R1(config)#access-list 111 permit icmp 192.168.0.5 0.0.0.0 10.0.2.0 0.0.0.255
R1(config)#access-list 111 permit icmp 192.168.0.6 0.0.0.0 10.0.2.0 0.0.0.255
R1(config)#access-list 111 permit icmp 192.168.0.7 0.0.0.0 10.0.2.0 0.0.0.255
R1(config)#access-list 111 permit ip any any
R1(config)#
R1(config)#int fa 0/0
R1(config-if)#ip access-group 111 in
R1(config-if)#exit
```

Рис. 8. Приклад налаштування ACL на маршрутизаторі R1

```
R1#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255 (5 matches)
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255 (5 matches)
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255 (5 matches)
    80 permit ip any any (246 matches)
```

Рис. 9. Приклад перевірки списків контролю доступу на маршрутизаторі R1 при використанні алгоритму Round-Robin

```
R2#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255 (5 matches)
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255 (5 matches)
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (246 matches)
```

Рис. 10. Приклад перевірки списків контролю доступу на маршрутизаторі R2 при використанні алгоритму Round-Robin

```
R3#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255 (5 matches)
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255 (5 matches)
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (246 matches)
```

Рис. 11. Приклад перевірки списків контролю доступу на маршрутизаторі R3 при використанні алгоритму Round-Robin

Для налаштування зваженого балансування в межах протоколу GLBP на кожному інтерфейсі маршрутизаторів, які створювали віртуальний шлюз за замовчуванням, встановлювались вагові коефіцієнти, що відповідали результатам розрахунків, наприклад, *для* рішення ResMetrTE. Тобто на маршрутизаторі R1 було налаштовано ваговий коефіцієнт 29 (рис. 12 а), на маршрутизаторі R2 – 57 (рис. 12 б), а на R3 – 114 (рис. 12 в).

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int fa 0/0
R1(config-if)#glbp 192 load-balancing weighted
R1(config-if)#glbp 192 weighting 29
R1(config-if)#exit
```

а)

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int fa 0/0
R2(config-if)#glbp 192 load-balancing weighted
R2(config-if)#glbp 192 weighting 57
R2(config-if)#exit
```

б)

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int fa 0/0
R3(config-if)#glbp 192 load-balancing weighted
R3(config-if)#glbp 192 weighting 114
R3(config-if)#exit
```

в)

Рис. 12. Приклад налаштування протоколу GLPB на маршрутизаторах R1÷R3 з використанням зваженого балансування навантаження

В результаті протокол GLBP при використанні зваженого балансування розподілив пакети, які надходили з різних комп'ютерів, таким чином, як показано на

рис. 13 – 15. Маршрутизатор R1 було обрано як шлюз для PC1 (рис. 13), маршрутизатор R2 цю функцію виконував для PC3 та PC6 (рис. 14), а маршрутизатор R3 – для PC2, PC4, PC5 та PC7 (рис. 15). Таким чином, за допомогою протоколу GLBP було реалізовано балансування навантаження за комп'ютерами (хостами) у пропорції 1:2:4, що приблизно відповідало наперед заданому порядку на рівні 29:57:114.

```
R1#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255 (5 matches)
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (126 matches)
```

Рис. 13. Приклад перевірки списків контролю доступу на маршрутизаторі R1 при використанні зваженого балансування

```
R2#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255 (5 matches)
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255 (5 matches)
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (129 matches)
```

Рис. 14. Приклад перевірки списків контролю доступу на маршрутизаторі R2 при використанні зваженого балансування

```
R3#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255 (5 matches)
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255 (5 matches)
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255 (5 matches)
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255 (5 matches)
    80 permit ip any any (132 matches)
```

Рис. 15. Приклад перевірки списків контролю доступу на маршрутизаторі R3 при використанні зваженого балансування

Висновки

Встановлено, що важливим рішенням щодо проактивного забезпечення відмовостійкості ІКМ є підтримка балансування навантаження як на рівні транспортної мережі, так і на рівні доступу засобами FHRP. На жаль, більшість налаштувань щодо балансування навантаження за допомогою FHRP базується на

використанні ручних втручаннях, що накладає високі вимоги щодо рівня фахової підготовки та досвіду адміністратора мережі. Тому актуальною представляється задача щодо вдосконалення математичних моделей і методів, які складають алгоритмічну основу протоколів відмовостійкої маршрутизації. При цьому обов'язковою вимогою до цих моделей і методів є забезпечення врахування рівня надійності приграничних маршрутизаторів, між якими балансується навантаження, що надходить від мереж доступу.

У роботі описано чотири математичні рішення задачі проактивної відмовостійкої маршрутизації. З метою забезпечення високого рівня якості обслуговування всі аналізовані рішення підтримують вимоги концепції Traffic Engineering, а два з них враховують у явному вигляді рівень надійності приграничних маршрутизаторів, який характеризується їх коефіцієнтами готовності. На обраній для дослідження мережній топології (рис. 1) здійснено розв'язання задач проактивної відмовостійкої маршрутизації за допомогою описаних у роботі рішень. Результати розрахунків підтвердили чутливість маршрутних рішень RATE та ResMetrTE до рівня надійності приграничних маршрутизаторів. Саме ці рішення забезпечували у більшості випадків такий порядок балансування навантаження, щоб на більш надійні приграничні маршрутизатори трафік надходив більш інтенсивно, і навпаки – менш надійні пристрої завантажувались менш інтенсивно. В межах розглянутого прикладу встановлено, що врахування рівня надійності приграничних маршрутизаторів при організації балансування навантаження між ними за допомогою рішень RATE або ResMetrTE призводило до деякого підвищення порогу завантаженості каналів зв'язку ІКМ – у середньому від 15% до 27%.

У роботі продемонстровано, що впровадження аналізованих рішень щодо балансування навантаження може бути забезпечено за допомогою протоколу GLBP з використанням режиму зваженого балансування (Load-Balancing Weighted) (рис. 12), коли вага кожного приграничного маршрутизатора визначається не емпірично, а обґрунтовується за результатами розрахунків у межах рішень RATE або ResMetrTE.

Перспективи подальших досліджень у цьому напрямку пов'язані із забезпеченням високої масштабованості маршрутних рішень шляхом переходу до ієрархічних методів маршрутизації [19]; із реалізацією схем захисту не тільки структурних елементів мережі (маршрутизаторів та каналів зв'язку), але й значень функціональних характеристик, пов'язаних з рівнем якості обслуговування [20] та мережної безпеки [21].

Список літератури

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

2. *Da Silva, A.S., Smith, P., Mauthe, A., Schaeffer-Filho, A.* (2015), "Resilience support in software-defined networking", Computer Networks, No. 92, P. 189–207. **DOI**: https://doi.org/10.1016/j.comnet.2015.09.012

3. *Tipper, D.* (2014), "Resilient network design: challenges and future directions", Telecommunication Systems, No. 56(1), P. 5–16. **DOI**: https://doi.org/10.1007/s11235-013-9815-x

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

5. *Лемешко, О.В., Єременко, О.С., Євдокименко, М.О., Шаповалова, А.С., Слейман, Б.* (2022), Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах: Монографія. Х.: ХНУРЕ, 198 с. **DOI**: https://doi.org/10.30837/978-966-659-378-1.

6. *Osborne, E. D., Simha, A.* (2003), Traffic engineering with MPLS, Cisco Press, 608 p.

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

8. *Lemeshko, O., Yeremenko, O.* (2017), "Enhanced method of fast re-routing with load balancing in software-defined networks", Journal of Electrical Engineering, No. 68(6), P. 444–454. **DOI**: https://doi.org/10.1515/jee-2017-0079.

9. *Lemeshko, O., Yeremenko, O., Yevdokymenko, M.* (2019), "MPLS Traffic Engineering Solution of Multipath Fast ReRoute with Local and Bandwidth Protection", Advances in Computer Science for Engineering and Education II, ICCSEEA 2019, Advances in Intelligent Systems and Computing, Springer, Cham, No. 938, P. 113–125. **DOI**: https://doi.org/10.1007/978-3-030-16621-2_11

10. *Lemeshko, O., Yeremenko, O., Hailan, A. M., Yevdokymenko, M., Shapovalova, A.* (2020), "Policing Based Traffic Engineering Fast ReRoute in SD-WAN Architectures: Approach Development and Investigation", Al-Bakry A. et al. (Eds.), New Trends in Information and Communications Technology Applications, NTICT 2020, Communications in Computer and Information Science, No. 1183, Springer, Cham, P. 29–43. **DOI**: https://doi.org/10.1007/978-3-030-55340-1_3.

11. First Hop Redundancy Protocols Configuration Guide. Cisco IOS Release 15.1 M&T (2018). Americas Headquarters Cisco Systems, Inc., 164 p.

12. *Chiesa, M., Kamisiński, A., Rak, J., Rétvári, G., Schmid, S.* (2021), "A Survey of Fast-Recovery Mechanisms in Packet-Switched Networks", IEEE Communications Surveys & Tutorials, No. 23(2), P. 1253–1301. **DOI**: https://doi.org/10.1109/COMST.2021.3063980.

13. *Elhourani, T., Gopalan, A. and Ramasubramanian, S.* (2016), "IP fast rerouting for multi-link failures", IEEE/ACM Transactions on Networking, No. 24(5), P. 3014–3025. **DOI**: https://doi.org/10.1109/TNET.2016.2516442.

14. *Malik, A., Aziz, B., Adda, M., Ke, C.H.* (2017), "Optimisation methods for fast restoration of software-defined networks", IEEE Access, No. 5, P. 16111–16123. **DOI**: https://doi.org/10.1109/ACCESS.2017.2736949.

15. *Lemeshko, O., Yeremenko, O., Tariki, N.* (2017), "Solution for the default gateway protection within fault-tolerant routing in an IP network", International journal of electrical and computer engineering systems, No. 8(1), P. 19-26. **DOI**: https://doi.org/10.32985/ijeces.8.1.3.

16. *Лемешко, О.В., Круглова, А.О., Журавльова, А.С., Лемешко, В.О.* (2020), "Вдосконалена модель балансування навантаження в інфокомунікаційній мережі", Проблеми телекомунікацій, No. 2(27). С. 56–67. URL: https://pt.nure.ua/wp-content/uploads/2021/11/202_lemeshko_balancing.pdf.

17. *Lemeshko, O., Yeremenko, O., Mersni, A., Yevdokymenko, M.* (2021), "Resilience Aware Traffic Engineering FHRP Solution (Invited Paper)", Proceedings of the 2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Kyiv, Ukraine, November 29 – December 3, P. 88–92. **DOI**: https://doi.org/10.1109/UkrMiCo52950.2021.9716677.

18. *Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Mersni, A., Lemeshko, V., Persikov, M.* (2023), "Resilience Improvement by Traffic Engineering Fault-Tolerant Routing in Programmable Networks", In: Ilchenko, M., Uryvsky, L., Globa, L. (eds) Progress in Advanced Information and Communication Technology and Systems, MCiT 2021, Lecture Notes in Networks and Systems, No. 548, Springer, Cham, P. 235–255. **DOI**: https://doi.org/10.1007/978-3-031-16368-5_12.

19. *Lemeshko, O., Nevzorova, O., Hailan, A. M.* (2018), "Hierarchical Method of Routing and Resource Allocation in DiffServ-TE Network", Proceedings of the 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 20-24 February, P. 1–5. **DOI**: https://doi.org/10.1109/TCSET.2018.8336366.

20. *Lemeshko, O., Yeremenko, O., Yevdokymenko, M.* (2018), "Tensor Model of Fault-Tolerant QoS Routing with Support of Bandwidth and Delay Protection", Proceedings of the 2018 IEEE 13th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), P. 135–138. **DOI**: https://doi.org/10.1109/STC-CSIT.2018.8526707.

21. *Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Shapovalova, A., Hailan, A. M., Mersni, A.* (2019), "Cyber Resilience Approach Based on Traffic Engineering Fast ReRoute with Policing", Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), P. 117–122. **DOI**: https://doi.org/10.1109/IDAACS.2019.8924294.