УДК 621.391

ПОТОКОВА МОДЕЛЬ МАРШРУТИЗАЦІЇ З БАЛАНСУВАННЯМ НАВАНТАЖЕННЯ НА ПРИНЦИПАХ TRAFFIC ENGINEERING З ВРАХУВАННЯМ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

М.О. ЄВДОКИМЕНКО, М.М. ШАПОВАЛ
Харківський національний університет радіоелектроніки

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

Abstract *– A practical approach to load balancing in a telecommunication network (TCN) is implementing Traffic Engineering (TE) technology principles to reduce link utilization and improve QoS level. In order to adapt TE solutions with network security requirements, this paper proposes a mathematical model for secure routing, which belongs to the class of flow-based optimization solutions. The model is based on the conditions of multi-flow routing implementation, flow conservation, and TCN link overload prevention. Due to this, the problem of secure routing is formulated in an optimization form. The model's novelty is the modified conditions of load balancing in TCN. Along with the indicators of link capacity with the help of weighting coefficients, the network security (NS) indicators of TCN elements are also taken into account. The network security (NS) indicators in the TCN modeling process include information security risks of routers and communication links, losses from breach of confidentiality and integrity of information, probability of existing vulnerabilities exploitation, etc. The study confirmed the effectiveness of the proposed solution. On the test TCN topology, it is demonstrated that the use of a secure routing model allows to calculate the routes and provide such an order of load balancing, which compromises meeting the requirements of both QoS and NS. In the routing process, information security risk reduction in packet transmission by about 11.3% was accompanied by an increase (on average by 26%) in the upper bound of the network link utilization.*

Анотація *– Ефективним підходом до балансування навантаження в телекомунікаційній мережі (ТКМ) є реалізація принципів технології Traffic Engineering (ТЕ) з метою зниження завантаженості каналів зв'язку та покращення рівня QoS. Для адаптації ТЕ-рішень до вимог мережної безпеки у даній роботі запропоновану математичну модель безпечної маршрутизації, яка відноситься до класу потокових оптимізаційних рішень. Модель базується на умовах реалізації багатошляхової маршрутизації, збереження потоку та запобігання перевантаженню каналів зв'язку ТКМ. Завдяки цьому задача безпечної маршрутизації сформульована в оптимізаційній формі. Новизною моделі є модифіковані умови балансування навантаження в ТКМ, в межах яких поруч з показниками пропускної здатності каналів за допомогою вагових коефіцієнтів враховуються також і показники мережної безпеки (Network Security, NS) елементів ТКМ. До складу врахованих у процесі моделювання ТКМ показників мережної безпеки варто віднести ризики інформаційної безпеки маршрутизаторів і каналів зв'язку, збитки від порушення конфіденційності та цілісності інформації, ймовірності використання наявних вразливостей тощо. Проведене дослідження підтвердило ефективність запропонованого рішення. На тестовій топології ТКМ продемонстровано, що використання моделі безпечної маршрутизації дозволяє розраховувати маршрути та забезпечити такий порядок балансування навантаження, який є компромісом у виконанні вимог як щодо QoS, так і NS. У процесі маршрутизації зменшення ризику інформаційної безпеки при передачі пакетів приблизно на 11,3% супроводжувалось підвищенням (у середньому на 26%) верхнього порогу завантаженості каналів зв'язку.*

Вступ

Основними вимогами, які висуваються до сучасних телекомунікаційних систем і мереж, традиційно є забезпечення заданого рівня якості обслуговування та мережної

безпеки. Ці задачі мають розв'язуватися комплексно, пов'язано одна з одною, на основі оптимального використання доступного мережного ресурсу. Проте сучасні мережні технології та протоколи не відповідають даним вимогам, орієнтуючись на покращення окремо показників або якості обслуговування (Quality of Service, QoS), або мережної безпеки (Network Security, NS) [1-4].

Розповсюдженим підходом до розв'язання задач безпечної та QoS-маршрутизації є використання маршрутних метрик, що мають бути безпосередньо пов'язаними з показниками QoS і NS [5-10]. Метричний підхід показує досить високу ефективність в умовах забезпечення QoS або NS за одним попередньо обраним основним показником ефективності ТКМ, наприклад, кількістю переприйомів, середньою затримкою або ймовірністю компрометації пакетів [7, 8]. У статті [10] запропоновано маршрутне рішення з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей.

Проте практика вимагає комплексних рішень в області QoS і NS, що призводить до необхідності використання композитних метрик, які є функцією зважених за певним законом множини показників якості обслуговування та мережної безпеки [9]. Варто зазначити, що ТКМ – це складна технічна система, основними факторами складності якої є динамічність стану та мультисервісний характер функціонування. Для такої системи досить важко визначити, наприклад, експертним шляхом співвідношення між показниками QoS і NS при формуванні композитних маршрутних метрик для різних типів трафіка. Проведений аналіз показав [11-15], що заслуговує уваги подальший розвиток підходу, що базується на реалізації принципів Traffic Engineering (TE) для забезпечення балансування навантаження з метою підвищення рівня QoS з урахуванням не тільки пропускної здатності каналів зв'язку, але й їх показників мережної безпеки. У роботі [11] таким показником виступає ймовірність компрометації каналів зв'язку.

У даній роботі пропонується використати під час організації балансування навантаження в ТКМ принципи, що закладено в технологію Traffic Engineering, а також показники ризику інформаційної безпеки та базові метрики критичності вразливостей [10], що дозволить більш повно та системно врахувати аспекти забезпечення як якості обслуговування, так і мережної безпеки. Це обумовлено тим, що балансування навантаження призводить до мінімізації завантаженості каналів зв'язку, яка позитивно впливає на такі QoS-показники, як продуктивність, середня затримка, джитер та ймовірність втрат пакетів. З іншого боку, показники ризику інформаційної безпеки та метрики критичності вразливостей [10] враховують цілу множину аспектів та параметрів, пов'язаних з NS: ризик інформаційної безпеки в каналах зв'язку ТКМ; збитки від порушення конфіденційності та цілісності інформації, доступності мережного ресурсу у випадку використання наявних вразливостей; показники складності їх використання на вузлах мережі та отримання доступу до мережних елементів та мережі загалом внаслідок використання зазначених вразливостей.

I. Базова математична модель маршрутизації з балансуванням навантаження в телекомунікаційній мережі

Припустимо, що топологія телекомунікаційної мережі представляється у вигляді орієнтованого графа $G=(R,\ E)$, у якому $R=\left\{R_i\ ;\ \ i=\overline{1,m}\right\}$ – множина вершин, що описують маршрутизатори ТКМ, $E=\left\{E_{i,j};\ \ i,j=\overline{1,m},\ \ i\neq j\right\}$ – множина дуг, що моделюють канали зв'язку (КЗ). Кожній дузі $E_{i,j}\in E$ можна поставити у відповідність ряд функціональних параметрів, які характеризують її показники QoS і NS. Так, наприклад, позначимо через $\varphi_{i,j}$ пропускну здатність каналу $E_{i,j}\in E$, яка буде вимірюватись в пакетах за секунду (пак/с).

З погляду на те, що ТКМ є мультисервісною, то нехай у мережі одночасно циркулює множина потоків пакетів K. При цьому вважатимемо, що для кожного k-го потоку відомі такі його характеристики: λ^k – середня інтенсивність (пакетна швидкість) потоку (пак/с); s_k і d_k – маршрутизатор-відправник і маршрутизатор -отримувач відповідно. Визначення порядку маршрутизації та балансування навантаження в ТКМ буде здійснюватися у процесі розрахунку множини маршрутних змінних $x_{i,j}^k$, кожна з яких характеризує долю k-го потоку пакетів, що протікає в каналі зв'язку (КЗ) між маршрутизаторами R_i та R_j. На ці змінні накладаються умови виду [11-16]

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

Граничні значення маршрутних змінних відповідають випадку реалізації в ТКМ одношляхової маршрутизації. Проміжні значення (від нуля до одиниці) характерні для багатошляхової маршрутизації в ТКМ. Множина шляхів, що розраховані та будуть використовуватись в процесі маршрутизації того чи іншого потоку, надалі буде називатися мультишляхом.

У межах потокових моделей маршрутизації на маршрутні змінні (1) також накладаються умови збереження потоку на маршрутизаторах ТКМ [11-16]:

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k-\sum\limits_{j:E_{j,i}\in E} x_{j,i}^k=1,\ \ k\in K,\ \ R_i=s_k;\\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k-\sum\limits_{j:E_{j,i}\in E} x_{j,i}^k=0\ ,\ \ k\in K,\ \ R_i\neq s_k,d_k;\\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k-\sum\limits_{j:E_{j,i}\in E} x_{j,i}^k=-1,\ \ k\in K,\ \ R_i=d_k. \end{cases} \tag{2}$$

Тоді середню інтенсивність *k*-го потоку пакетів у каналі $E_{i,j}\in E$ (пак/с) можна розрахувати за формулою:

$$\lambda_{i,j}^{k} = \lambda^{k} x_{i,j}^{k}.$$

Характерною рисою потокових моделей ТЕ-маршрутизації є така специфічна форма умов запобігання перевантаження каналів зв'язку та балансування навантаження в ТКМ [11-16]:

$$\sum_{k \in K} \lambda^{k} x_{i,j}^{k} \le \alpha \varphi_{i,j}, \; E_{i,j} \in E \tag{3}$$

та критерію оптимальності маршрутних рішень

$$\alpha \to \min, \tag{4}$$

де

$$0 \le \alpha \le 1 \tag{5}$$

– верхній поріг завантаженості каналів зв'язку ТКМ, який також виступає додатковою керуючою змінною.

Відповідно до моделі (1)–(5) коефіцієнти використання (завантаженості) окремих каналів зв'язку $E_{i,j} \in E$ визначаються за формулою

$$\alpha_{i,j} = \frac{\sum_{k \in K} \lambda^{k} x_{i,j}^{k}}{\varphi_{i,j}}. \tag{6}$$

Таким чином, у межах класичної потокової моделі ТЕ-маршрутизації [16] розрахунок маршрутних змінних відбувається у процесі розв'язання оптимізаційної задачі лінійного програмування з критерієм (3) за наявності обмежень (1)-(3) та (5).

II. Модифікація базової моделі маршрутизації для врахування базових метрик критичності вразливостей

Позначимо через $\mathbf{R}^{i}$ та $\mathbf{R}^{i,j}$ значення показників ризику інформаційної безпеки відповідно маршрутизатора $R_i \in R$ та каналу зв'язку $E_{i,j} \in E$. У роботі [10] пропонується рівень мережної безпеки каналу зв'язку $E_{i,j} \in E$ оцінювати через показник ризику інформаційної безпеки маршрутизатора $R_i \in R$, тобто маршрутизатора, з якого цей канал виходить:

$$\mathbf{R}^{i,j} = \mathbf{R}^{i}. \tag{7}$$

Ризик інформаційної безпеки довільного маршрутизатора R_i залежить від ступеня використання зловмисником наявних на ньому вразливостей [10, 17, 18]:

$$\mathbf{R}^i = \sum_{U_i^q \in U_i^*} BS_i^q \cdot P_i^q , \tag{8}$$

де $U = \left\{ U_i^q ; q = \overline{1,Q}, i = \overline{1,m} \right\}$ – множина вразливостей, що виявлені на вузлах (маршрутизаторах) ТКМ, U_i^q – q-та вразливість на маршрутизаторі R_i; $U_i^* \subset U$ – множина вразливостей на маршрутизаторі R_i; BS_i^q – показник критичності q-ї вразливості на R_i, що розраховується за допомогою базових метрик системи оцінки вразливостей, які представлені в рекомендації NIST CVSS v3 [17], та характеризує умовні збитки від використання зловмисником вразливості U_i^q; P_i^q – ймовірність використання q-ї вразливості зловмисником на маршрутизаторі R_i.

Для забезпечення високого рівня мережної безпеки засобами маршрутизації пропонується модифікувати модель (1)-(6) шляхом перегляду умов запобігання перевантаження каналів зв'язку та балансування навантаження в ТКМ (3) на принципах, що викладені у роботі [11]:

$$\sum_{k \in K} \lambda^k x_{i,j}^k \le \alpha v_{i,j} \varphi_{i,j} , \tag{9}$$

де вагові коефіцієнти $v_{i,j}$ мають відповідати, наприклад, таким умовам

$$v_{i,j} = 1 - \frac{\mathbf{R}^{i,j} - \min(\mathbf{R})}{\max(\mathbf{R})} , \tag{10}$$

де $\mathbf{R} = \left\{ \mathbf{R}^{i,j} \right\}$ – множина показників ризику інформаційної безпеки каналів зв'язку ТКМ, а $\min(\mathbf{R})$ та $\max(\mathbf{R})$ – відповідно мінімальне та максимальне значення цих показників.

Таким чином, каналу зв'язку з мінімальним ризиком інформаційної безпеки буде відповідати $v_{i,j} = 1$, тобто у процесі балансування навантаження буде враховуватись весь об'єм пропускної здатності даного КЗ. Зі зростанням рівня вразливості КЗ відповідний йому коефіцієнт $v_{i,j}$ буде зменшуватись, наближаючись до нуля. Тим самим буде знижуватись об'єм пропускної здатності каналу, доступний для передачі пакетів. Тобто, чим більш уразливим є канал зв'язку, тим менше він буде залучатись до маршрутизації мережного трафіку. За аналогією з результатами роботи [11] функція $v_{i,j}(\mathbf{R}^{i,j})$ буде називатись моделлю блокування каналів зв'язку в процесі безпечного балансування навантаження в ТКМ.

III. Дослідження процесів безпечної маршрутизації з балансуванням навантаження на принципах Traffic Engineering з урахуванням ризиків інформаційної безпеки

Дослідження запропонованої потокової моделі безпечної маршрутизації з балансуванням навантаження (1)-(10) проводилось на топології телекомунікаційної мережі, представленої на рис. 1. Основу мережі складали чотири маршрутизатори. Пакети одного тестового потоку передавались від першого маршрутизатора до четвертого. У розривах каналів зв'язку ТКМ наведено їхню пропускну здатність (рис. 1).

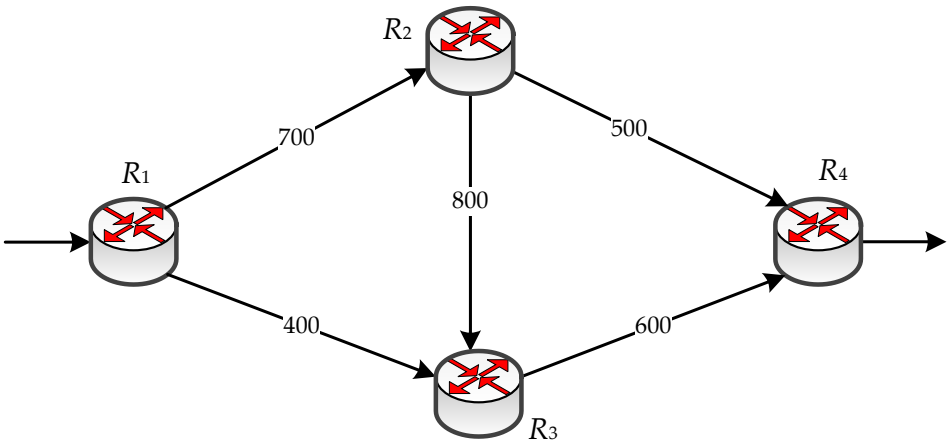

Рис. 1. Досліджуваний фрагмент структури ТКМ

Параметри мережної безпеки маршрутизаторів $R_1 \div R_4$ представлені в табл. 1. У ній наведено характерні для обраних типів маршрутизаторів основні (по три на кожного) вразливості, рівні їх критичності, базові оцінки та ймовірності використання.

Таблиця 1. Параметри мережної безпеки обраних для дослідження маршрутизаторів

Вузол ТКМ	Маршрутизатор	BS_i^q	P_i^q	Опис вразливості згідно [17]	Рівень критичності вразливості
R_1	Cisco RV325 Dual Gigabit WAN VPN Routers	8,1	0,1	CVE-2019-1828	Високий
		7,2	0,2	CVE-2021-1323	Високий
		8,8	0,15	CVE-2019-1724	Високий
R_2	Cisco RV042	7,2	0,25	CVE-2021-1325	Високий
		7,2	0,1	CVE-2021-1348	Високий
		7,2	0,05	CVE-2021-1337	Високий
R_3	Cisco Small Business RV160W	7,5	0,15	CVE-2021-1297	Високий
		9,8	0,2	CVE-2021-1602	Критичний
		9,8	0,25	CVE-2021-1295	Критичний
R_4	Cisco RV260W	7,4	0,05	CVE-2021-1308	Високий
		9,8	0,1	CVE-2021-1472	Критичний
		8,8	0,07	CVE-2021-1309	Високий

У процесі проведеного дослідження аналізувалися та порівнювались завантаженість мережі та рівень її інформаційної безпеки для двох моделей маршрутизації:

- модель 1 – класична модель ТЕ-маршрутизації (1)-(6);
- модель 2 – запропонована модель безпечної маршрутизації (1), (2), (4)-(10).

Рівень мережної безпеки отриманого маршрутного рішення оцінювався за допомогою показника ризику інформаційної безпеки пакетів k-го потоку, що передавались від маршрутизатора відправника до маршрутизатора отримувача, тобто «з кінця в кінець»:

$$\mathbf{R}_{E2E}^{k} = \sum_{s \in S^k} \frac{\lambda_s^k}{\lambda^k} \mathbf{R}_s^{path}, \tag{10}$$

де s^k – множина шляхів (маршрутів), що використовуються для передачі пакетів k-го потоку між заданою парою маршрутизаторів у ТКМ; λ_s^k – інтенсивність k-го потоку пакетів, що передаються s-м шляхом у ТКМ; $\mathbf{R}_s^{path}$ – ризик інформаційної безпеки s-го шляху в ТКМ, значення якого визначалось відповідно до формули

$$\mathbf{R}_s^{path} = \sum_{E_{i,j} \in Path_s} \mathbf{R}^{i,j}, \tag{11}$$

в якій $Path_s = \left\{E_{i,j}\right\}$ – множина каналів зв'язку мережі, що утворюють в ній s-й шлях між парою маршрутизаторів відправник-отримувач.

Данні, які наведені в табл. 1, були використані для розрахунку ризиків інформаційної безпеки маршрутизаторів, каналів зв'язку (7), шляхів (11) і вагових коефіцієнтів $v_{i,j}$ (9). Результати розрахунків при $\lambda^1 = 700$ пак/с представлені в табл. 2 та 3.

Таблиця 2. Показники мережної безпеки каналів зв'язку ТКМ

Канали зв'язку	$\mathbf{R}^{i,j}$	$v_{i,j}$	Модель 1		Модель 2	
			$\lambda_{i,j}^1$, пак/с	$\alpha_{i,j}$	$\lambda_{i,j}^1$, пак/с	$\alpha_{i,j}$
$E_{1,2}$	3,57	0,8753	445,4545	0,6364	430,9309	0,6156
$E_{1,3}$	3,57	0,8753	254,5455	0,6364	269,0691	0,6727
$E_{2,3}$	2,88	1	127,2727	0,1591	0	0
$E_{2,4}$	2,88	1	318,1818	0,6364	430,9309	0,8619
$E_{3,4}$	5,535	0,5203	381,8182	0,6364	269,0691	0,4484

Таблиця 3. Показники ризику інформаційної безпеки та завантаженості маршрутів

Маршрут	$\mathbf{R}_s^{path}$	Модель 1	Модель 2
		λ_s^1/λ^1	
$R_1 \to R_2 \to R_4$	6,45	0,4545	0,6156
$R_1 \to R_3 \to R_4$	9,105	0,3636	0,3844
$R_1 \to R_2 \to R_3 \to R_4$	11,985	0,1818	0

На рис. 2 та 3 показано результати розв'язання задачі маршрутизації з використанням моделі 1 та 2 відповідно. В розривах каналів зв'язку вказана наступна інформація (згори донизу): інтенсивність потоку, пропускна здатність.

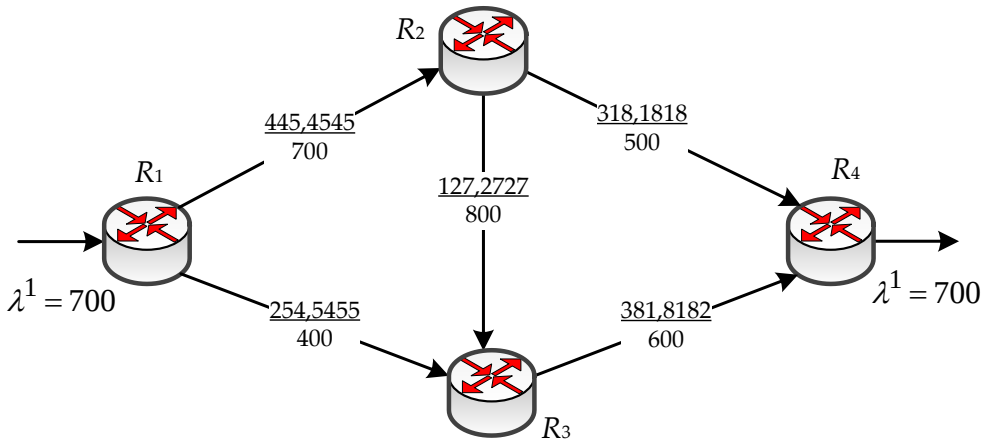

Рис. 2. Результат розв'язання задачі маршрутизації з використанням моделі 1

В табл. 4 наведено показники ефективності, за якими оцінювалась робота моделей маршрутизації 1 і 2. Це, перш за все, стосується показників щодо рівня QoS і NS: верхнього порогу завантаженості каналів зв'язку (4) та ризику інформаційної безпеки пакетів (10).

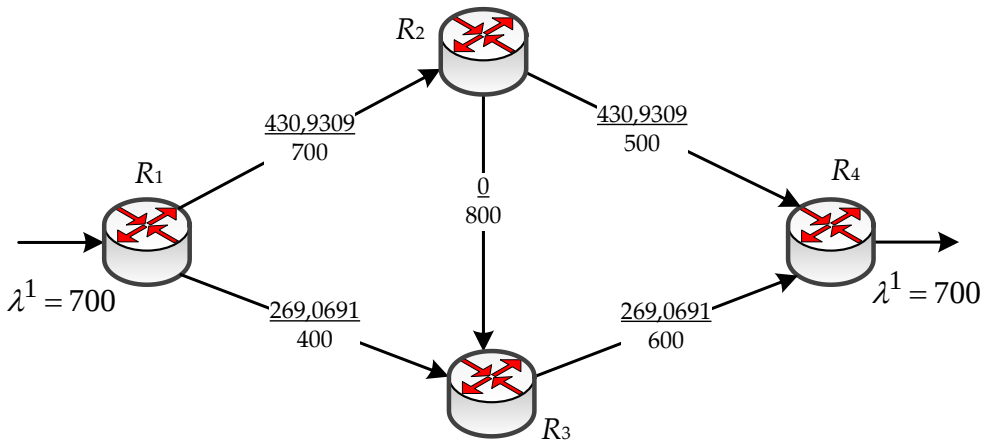

Рис. 3. Результат розв'язання задачі маршрутизації з використанням моделі 2

Таблиця 4. Показники ефективності маршрутних рішень

Тип моделі маршрутизації	α	$\mathbf{R}_{E2E}^{k}$
Модель 1	0,6364	8,4218
Модель 2	0,8619	7,4705

Результати проведеного дослідження, які наведено в табл. 2 – 4, а також на рис. 2 і 3, показали, що запропонована модель безпечної маршрутизації (1), (2), (4)-(10) при балансуванні навантаження враховує ризики інформаційної безпеки елементів ТКМ. Це призводить до менш інтенсивного завантаження небезпечних каналів зв'язку, наприклад, каналу $E_{3,4}$ і навпаки. Як показано в табл. 4, використання запропонованої моделі безпечної маршрутизації (1), (2), (4)-(10) призводить до зниження ризику інформаційної безпеки при передачі пакетів приблизно на 11,3%, що було забезпечено шляхом деякого підвищення (на 26%) верхнього порогу завантаженості каналів зв'язку.

Висновки

Забезпечення високого рівня якості обслуговування та мережної безпеки в сучасних ТКМ є актуальною науковою та прикладною задачею, розв'язання якої потребує реалізації системного підходу та комплексних рішень. Важливим засобом мережного рівня моделі взаємодії відкритих систем є протоколи маршрутизації, на які багато в чому покладаються функції щодо балансування навантаження в ТКМ. Водночас ефективним підходом до балансування навантаження в телекомунікаційній мережі є реалізація принципів технології Traffic Engineering з метою зниження завантаженості каналів зв'язку та покращення рівня QoS. Для адаптації ТЕ-рішень до вимог мережної безпеки у даній роботі запропоновано модель безпечної маршрутизації, що відноситься до класу потокових оптимізаційних рішень. Модель базується на умовах реалізації багатошляхової маршрутизації (1), збереження потоку (2) та запобігання перевантаженню каналів зв'язку ТКМ (9). Завдяки цьому задачу безпечної маршрутизації сформульовано в оптимізаційній формі з критерієм оптимальності (4) та системою обмежень (1), (2), (4), (9), що накладаються на керуючі, перш за все, маршрутні змінні.

Запропонована модель безпечної маршрутизації розвиває підходи, викладені у статтях [10, 11]. Новизною моделі є модифіковані умови балансування навантаження в ТКМ (9), в межах яких поруч з показниками пропускної здатності каналів за допомогою вагових коефіцієнтів (10) враховуються також і показники мережної безпеки елементів мережі. До складу врахованих у процесі моделювання ТКМ показників мережної безпеки варто віднести ризики інформаційної безпеки маршрутизаторів і каналів зв'язку, збитки від порушення конфіденційності та цілісності інформації, ймовірності використання наявних вразливостей тощо.

Проведене дослідження підтвердило ефективність запропонованого рішення. На тестовій топології ТКМ продемонстровано, що використання моделі безпечної марш-

рутизації (1), (2), (4)-(10) дозволяє розрахувати маршрути та забезпечити такий порядок балансування навантаження, який є компромісом у виконанні вимог як щодо QoS, так і NS. Зменшення у процесі маршрутизації ризику інформаційної безпеки при передачі пакетів приблизно на 11,3% супроводжувалось підвищенням (у середньому на 26%) верхнього порогу завантаженості каналів зв'язку.

Запропонована математична модель безпечної маршрутизація з балансуванням навантаження на принципах Traffic Engineering з урахуванням базових метрик критичності вразливостей може стати основою перспективного протоколу маршрутизації, шляхом налаштування якого можна адаптивно реалізовувати вимоги користувачів до ТКМ, а саме якості обслуговування та мережної безпеки.

Список літератури

1. *Chapman, C.* (2016), Network Performance and Security (Testing and Analyzing Using Open Source and Low-Cost Tools), 1st edition, Syngress, 380 p.

2. *Edgar, T., Manz, D.* (2017), Research Methods for Cyber Security, 1st edition. Syngress, 2017, 428 p.

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

4. *Linkov, I., Kott, A.* (2019), "Fundamental Concepts of Cyber Resilience: Introduction and Overview", In: Kott A., Linkov I. (eds) Cyber Resilience of Systems and Networks. Risk, Systems and Decisions, Springer, Cham., P. 1-25. **DOI**: https://doi.org/10.1007/978-3-319-77492-3_1

5. *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.

6. *Schudel, G., Smith, D. J.* (2008), Router Security Strategies Securing IP Network Traffic Planes, Cisco Press, 673 p.

7. *Lemeshko, O., Papan, J., Yeremenko, O., Yevdokymenko, M., Segec, P.* (2021), "Research and Development of Delay-Sensitive Routing Tensor Model in IoT Core Networks", Sensors, No. 21(11): 3934, P. 1-23. **DOI**: https://doi.org/10.3390/s21113934

8. *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), Lviv, Ukraine, 11-14 Sept., P. 135-138. **DOI**: https://doi.org/10.1109/STC-CSIT.2018.8526707

9. *Snihurov, A., Chakrian, V.* (2015), "Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters", Scholars Journal of Engineering and Technology, No. 3(8), P. 707-714.

10. *Євдокименко, М. О., Шаповалова, А. С., Шаповал, М. М.* (2020), "Потокова модель маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей", Проблеми телекомунікацій, No. 1(26), С. 48-62. Режим доступу: http://pt.nure.ua/wp-content/uploads/2021/03/201_yevdokimenko_security.pdf

11. *Lemeshko, O., Shapovalova, A., Al- Dulaimi, A.M.K., Yeremenko, O., Yevdokymenko, M.* (2020), "Flow-Based Routing Model With Load Balancing Under Network Security Parameters", Information and Telecommunication Sciences, No. 2, P. 44-50.

12. *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", In: 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

13. *Лемешко, О. В., Шаповалова, А. С., Єременко, О. С., Євдокименко, М. О., Хайлан, А. М.* (2019), "Математична модель швидкої перемаршрутизації з балансуванням навантаження та диференційованого обмеження трафіка в мережах SD-WAN", Системи управління, навігації та зв'язку, No. 4(56), С. 63-71. **DOI**: https://doi.org/10.26906/SUNZ.2019.4.063

14. *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 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, 18-21 September, P. 117-122. **DOI**: https://doi.org/10.1109/IDAACS.2019.8924294

15. *Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Shapovalova, A., Ilyashenko, A., Sleiman, B.* (2019), "Traffic Engineering Fast ReRoute Model with Support of Policing", Proceedings of the 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), Lviv, Ukraine, 2-6 July, P. 842-845. **DOI**: https://doi.org/10.1109/UKRCON.2019.8880006

16. *Lee, Y., Seok, Y., Choi, Y., Kim, C.* (2002), "A constrained multipath traffic engineering scheme for MPLS networks", Proceedings of the IEEE International Conference on Communications. Conference Proceedings. ICC 2002, No. 4, New York, NY, USA, 28 April-2 May, P. 2431-2436. **DOI**: https://doi.org/10.1109/ICC.2002.997280

17. *Scarfone, K., Scarfone, K., Mell, P.* (2012), "NIST Special Publication 800-94 Revision 1 (Draft) Guide to intrusion detection and prevention systems (IDPS)", National Institute of Standards and Technology, available at: http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf

18. *Peltier, T. R.* (2005), Information security risk analysis, CRC press, 344 p.