УДК 621.391

ПОТОКОВА МОДЕЛЬ МАРШРУТИЗАЦІЇ З УРАХУВАННЯМ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА ДОПОМОГОЮ БАЗОВИХ МЕТРИК КРИТИЧНОСТІ ВРАЗЛИВОСТЕЙ

М.О. Євдокименко, А.С. Шаповалова, М.М. Шаповал
Харківський національний університет радіоелектроніки

Abstract *– The paper proposes an improved flow-based routing model taking into account information security risks using basic vulnerability criticality metrics. The model is based on the conditions for the implementation of single- and multipath routing, flow conservation, and prevention of overload of communication links of the telecommunications network (TCN). Within the proposed model, the problem of secure routing is formulated in an optimization form. The novelty of the developed model is that expressions are used to calculate routing metrics, which characterize the risk of information security in communication links of the TCN and in accordance with the NIST recommendations, take into account damages from the violation of confidentiality and integrity of information, availability of network resources in case of use of existing vulnerabilities; indicators of the complexity of exploiting vulnerabilities at network nodes and gaining access to network elements and the network as a whole due to the use of these vulnerabilities. As shown by the results of the study, the use of the proposed model of secure routing allows ensuring the calculation and use of routes with minimal risk of information security, thereby ensuring the maximum level of network security for packets transmitted in the TCN. The proposed approach to the formation of routing metrics can also be used to ensure comprehensive consideration in the process of solving routing problems of both network security indicators and quality of service indicators. The prospects for the development of the obtained solutions include the synthesis of models and methods of secure routing by which it would be possible to provide (guarantee) a given level of network security based on the calculation and use of appropriate routes in TCN.*

Анотація *– В роботі запропонована вдосконалена потокова модель маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. Основу моделі складають умови реалізації одно- та багатошляхової маршрутизації, збереження потоку та запобігання перевантаженню каналів зв'язку телекомунікаційної мережі (ТКМ). В межах запропонованої моделі задача безпечної маршрутизації сформульована в оптимізаційній формі. Новизна розробленої моделі полягає в тому, що для розрахунку маршрутних метрик використовуються вирази, які характеризують ризик інформаційної безпеки в каналах зв'язку ТКМ та відповідно до рекомендацій NIST враховують збитки від порушення конфіденційності та цілісності інформації, доступності мережного ресурсу у випадку використання наявних вразливостей; показники складності використання вразливостей на вузлах мережі та отримання доступу до мережних елементів та мережі загалом внаслідок використання зазначених уразливостей. Як показали результати проведеного дослідження, використання запропонованої моделі безпечної маршрутизації дозволяє розрахувати та використати маршрути із мінімальним ризиком інформаційної безпеки, тим самим забезпечивши максимальний рівень мережної безпеки пакетам, які передаються в ТКМ. Запропонований підхід до формування маршрутних метрик може бути використаний також при забезпеченні комплексного врахування в процесі розв'язання задач маршрутизації як показників мережної безпеки, так і показників якості обслуговування. До перспектив розвитку отриманих рішень варто віднести синтез моделей і методів безпечної маршрутизації, за допомогою яких би вдалося гарантувати заданий рівень мережної безпеки на підставі розрахунку та використання відповідних маршрутів у ТКМ.*

Вступ

На сьогоднішній день гарантування кіберстійкості та безпеки телекомунікаційних мереж, особливо в умовах інтенсивної цифрової трансформації, є важливим та актуальним питанням. Наразі існуючі телекомунікаційні мережі (ТКМ), на жаль, не відпові-

дають вимогам сучасності та постійно зростаючим потребам користувачів інфокомунікаційних послуг і сервісів. Для вирішення цього важливого завдання необхідно, щоб сучасні ТКМ забезпечували та підтримували прийнятний рівень обслуговування в умовах атак зловмисників, компрометації мережних елементів, відмов різного походження, перевантаженням мережі, а також адаптивно реагували на всі перелічені інциденти при обмеженні їх негативних наслідків на функціонування мережі із забезпеченням захисту критично важливих елементів мережі та її ресурсів (каналів, вузлів, маршрутів). Так, на теперішній час на кожному рівні моделі OSI (Open Systems Interconnection) існує безліч методів, використання яких дозволяє підвищити безпеку ТКМ як на кожному рівні окремо, так і мережі загалом. Особливої уваги при цьому заслуговують методи забезпечення захисту ТКМ, що використовуються на мережному рівні, такі як аналізатори трафіку, VPN (Virtual Private Network), брандмауери, системи виявлення та протидії атакам тощо, серед яких слід відокремити використання протоколів безпечної маршрутизації (ПБМ). Завдяки ПБМ можливо не тільки підвищити безпеку в ТКМ, але й забезпечити кіберстійкість мережі [1, 2].

I. Огляд протоколів безпечної маршрутизації в ТКМ

Загалом головною ідеєю, покладеною в основу протоколів безпечної маршрутизації, є підвищення безпеки та кіберстійкості ТКМ. Всі ПБМ можна розподілити на проактивні та реактивні [3-11]. Проактивні ПБМ базуються на попередній оцінці ризиків інформаційної безпеки та використанні при передачі пакетів найбезпечніших мережних елементів. Так, протокол SEAD (Secure Efficient Ad hoc Distance-Vector) [4] ґрунтується на принципах роботи проактивного дистанційно-векторного протоколу DSDV (Destination Sequenced Distance Vector) [5]. Особливістю протоколу є нестандартний механізм аутентифікації записів оновлень в таблицях маршрутизації, заснований на хеш ланцюжках та дереві Меркла [6], із присвоєнням вищих порядкових номерів, перехоплення яких не дозволяє порушнику згенерувати оновлення з більш високим порядковим номером. Розвитком ПБМ SEAD є протокол SDSDV (Secure DSDV), який не передбачає побудову дерева Меркла, а оновлення таблиць маршрутизації проводиться на основі додаткових полів AL (Alteration Field) та AC (Accumulation Field), які використовуються для захисту від зниження значення метрики та підвищення порядкових номерів, що присвоюються з кожним оновленням [7].

Реактивні ПБМ, на відміну від проактивних, базуються на розрахунку маршруту за вимогою [8-13]. Одним з прикладів таких протоколів є протокол реактивної маршрутизації на основі довіри TSDRP (Trust Based Secure on Demand Routing Protocol), використання якого гарантує, що дані не будуть передаватися через зловмисні вузли [9]. Іншим представником реактивного протоколу є протокол для надійної доставки даних SPREAD (Security Protocol for REliable dAta Delivery) [10], який дозволяє забезпечити захист даних за рахунок зниження ймовірності втрати секретного повідомлення в умовах передачі по незахищеній ТКМ. Також відомим ПБМ є протокол SAR (Security-Aware Ad-hoc Routing) [11], що забезпечує високий ступінь безпеки ТКМ за

рахунок присвоювання кожному вузлу визначеного рівня безпеки, що є головною метрикою маршруту. Для підвищення відмово- та кіберстійкості на теперішній час все частіше використовують протоколи швидкої перемаршрутизації [12, 13], які мають здебільшого реактивний характер та орієнтовані на захист таких мережних елементів, як вузол, канал зв'язку, маршрут тощо. Проте, не дивлячись на більш високу ефективність з боку підвищення безпеки ТКМ, порівняно з проактивними ПБМ, реактивні протоколи програють за показниками якості обслуговування в ТКМ, а, перш за все, за показником середньої затримки в мережі. Це пов'язано з тим, що спочатку необхідно оцінити стан безпеки мережі та її елементів на основі аналізу параметрів безпеки, а потім вже розрахувати маршрут за потребою, використовуючи дані параметри.

Базуючись на проведеному аналізі ПБМ, слід зазначити, що всі вони є вдосконаленням традиційних протоколів маршрутизації (RIP, EIGRP, OSPF) [14-16] з використанням метрик безпеки. Подальше вдосконалення протоколів і моделей безпечної маршрутизації для усунення недоліків існуючих рішень повинно відповідати наступним вимогам:

- урахування особливостей структурної та функціональної побудови ТКМ;
- підтримка потокового характеру різноманітних типів трафіку;
- урахування параметрів безпеки як окремих елементів, так і мережі загалом;
- урахування ризиків інформаційної безпеки, що ґрунтуються на наявних і виявлених уразливостях на елементах мережі;
- підтримка рекомендованих показників якості обслуговування;
- прийнятна обчислювальна складність та масштабованість кінцевих рішень, які підлягатимуть подальшій протокольній реалізації.

Тому в даній роботі вирішується актуальне завдання, що полягає в удосконаленні потокової моделі маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. Удосконалення моделі полягатиме у введенні як маршрутних метрик вагових коефіцієнтів, що характеризуватимуть ризики, які створюються наявними на вузлах ТКМ уразливостями та кількісно відображатимуть умовну вартість використання каналів зв'язку. Використання даних вагових коефіцієнтів у рамках потокової моделі маршрутизації дозволить здійснювати передачу потоків пакетів за найбільш безпечними маршрутами в ТКМ.

II. Базова потокова модель маршрутизації в телекомунікаційній мережі

Нехай структура мережі описується графом $G = (R, E)$, у якому $R = \left\{ R_i ;\ i = \overline{1, m} \right\}$ – це множина вершин, що моделюють маршрутизатори, а $E = \left\{ E_{i,j};\ \ i, j = \overline{1, m},\ i \neq j \right\}$ – множина дуг, що представляють канали зв'язку (КЗ) в ТКМ. Тоді кожній дузі $E_{i,j} \in E$ ставиться у відповідність її пропускна здатність $\varphi_{i,j}$, (1/с). Нехай у ТКМ циркулює множина потоків пакетів K, які генеруються відповідними

мережними додатками. Для кожного k-го потоку відомі такі вихідні дані: λ^k – середня інтенсивність потоку трафіка, яка вимірюється в пакетах за секунду (1/с); s_k і d_k – вузол-відправник і вузол-отримувач пакетів k-го потоку відповідно.

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

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

або

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

Уведення умов (1) відповідає за реалізацію в ТКМ одношляхової стратегії маршрутизації. У випадку виконання умови (2) буде підтримуватися багатошляхова маршрутизація, не забороняючи одночасно використання й одношляхових рішень, за якої змінні $x_{i,j}^k$ можуть приймати крайні зі своїх можливих значень – нуль або одиницю (1). Множина застосованих шляхів надалі буде називатися мультишляхом.

Крім того, під час розрахунку маршрутних змінних мають виконуватися умови збереження потоку на маршрутизаторах мережі [17, 18]:

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^k = 1, \ k \in K, \ R_i = s_k; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^k = 0, \ k \in K, \ R_i \ne s_k, d_k; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^k = -1, \ k \in K, \ R_i = d_k. \end{cases} \tag{3}$$

У разі виконання умов (3) гарантується відсутність втрат пакетів на кожному маршрутизаторі та в мережі загалом, а також забезпечується зв'язність розрахованих маршрутів між відправником та отримувачем пакетів k-го потоку.

Для запобігання перевантаження каналів зв'язку ТКМ необхідно забезпечити виконання таких умов [18]:

$$\sum_{k\in K} \lambda^k x_{i,j}^k \le \varphi_{i,j}, \ E_{i,j} \in E, \tag{4}$$

кількість яких відповідає числу каналів зв'язку в мережі.

Для розрахунку оптимальних шляхів в ТКМ використаємо, наприклад, наступний лінійний критерій оптимальності [18]:

$$\sum_{k\in K}\sum_{E_{i,j}\in E} w_{i,j}x_{i,j}^{k} \Rightarrow \min, \tag{5}$$

де вагові коефіцієнти $w_{i,j}$ – це, фактично, маршрутні метрики, які мають враховувати основні характеристики безпеки КЗ.

III. Методика розрахунку метрик маршрутизації на основі оцінки ризику інформаційної безпеки каналів зв'язку

Оцінка вразливостей ТКМ є досить складним завданням з огляду на гетерогенність мережного обладнання та його програмного забезпечення. Найчастіше для цього використовується спеціалізоване апаратне або програмне забезпечення (наприклад, GFI LanGuard, Nessus, XSpider тощо), яке сканує мережу на предмет виявлення «слабких» місць у системі безпеки та попереджає про зони ризику в ТКМ [19-21]. Такі програми дозволяють оцінити мережну безпеку за допомогою активного та пасивного аналізу. Під активним аналізом (наприклад, тестування на проникнення) розуміється імітація атак зловмисника, яка перевіряє наявність уразливостей у мережі [22]. Пасивний аналіз полягає в пошуках уразливостей за непрямими ознаками без підтвердження їх наявності, наприклад, наявність відритих портів, зміст заголовків пакетів тощо [23-25]. Водночас в деяких дослідженнях вже пропонуються для більш точної оцінки безпеки мережі використовувати вищезазначені аналізи поетапно [26, 27]. Так, на першому етапі пропонується використовувати пасивний аналіз, як більш швидкий, але менш точний; а на другому етапі – після усунення виявлених вразливостей в результаті пасивного аналізу використовувати активний аналіз, який потребує більше часу, але є більш точним.

Додатково для оцінки безпеки та ризиків у ТКМ можуть використовуватися різноманітні організаційні стандарти та рекомендації щодо функціонування брандмауерів та їх політик безпеки, а також методи штучного інтелекту тощо [28, 29]. Це підтверджується наявністю багатьох досліджень вітчизняних та іноземних науковців, що відображається в міжнародних стандартах і рекомендаціях [30-33], таких як ISO 17799 (BS7799), ISO 15408, COBIT, COSO.

Ще одним з напрямків оцінки рівня захищеності мережі загалом є підходи, засновані на побудові уявлення можливих дій порушників у вигляді дерев або графів атак і подальшої перевірки властивостей цього дерева (графа) на основі використання різних методів, наприклад, методів верифікації на моделі (model checking), а також обчислення різноманітних метрик захищеності щодо виявлення аномалій за різними сценаріями [34-37].

Одним з ефективних засобів забезпечення захисту ТКМ є попередня оцінка ризику інформаційної безпеки, який може розраховуватись за допомогою використання зазначених у рекомендації NIST CVSS v3 [38] метрик критичності вразливостей: базових, часових і метрик навколишнього середовища.

В межах запропонованого рішення для розрахунку вагових коефіцієнтів $w_{i,j}$ обрано базові метрики, які, на відміну від часових метрик та метрик навколишнього середовища, характеризують незмінні за часом наявні вразливості на елементах мережі та дозволяють оцінити ризик інформаційної безпеки ТКМ взагалі, а не для окремих випадків компрометації мережних елементів.

Введемо наступні позначення:

$U = \left\{ U_i^q ; q = \overline{1,Q}, i = \overline{1,m} \right\}$ – множина вразливостей, які виявлені на вузлах (маршрутизаторах) ТКМ, де U_i^q – q-та вразливість на i-му вузлі ТКМ;

$U_i^* \subset U$ – множина вразливостей на i-му вузлі ТКМ;

BS_i^q – показник критичності q-ї вразливості на i-му вузлі ТКМ, що розраховується за допомогою базових метрик системи оцінки вразливостей, які представлені в рекомендації NIST CVSS v3 [38], та характеризує умовні збитки від використання зловмисником вразливості U_i^q;

P_i^q – ймовірність використання q-ї вразливості зловмисником на i-му вузлі мережі, що за фізичним змістом є ймовірністю компрометації.

Згідно з [38] для розрахунку ризику інформаційної безпеки від використання наявних уразливостей на i-му вузлі ТКМ використано наступний вираз:

$$R^i = \sum_{U_i^q \in U_i^*} BS_i^q \cdot P_i^q . \tag{6}$$

Згідно з рекомендацією NIST збитки відносно базових метрик уразливостей на вузлах мережі [38] розраховуються як

$$BS_i^q = (0,6 \cdot Imp_i^q + 0,4 \cdot Ex_i^q - 1,5) \cdot f(Imp_i^q), \tag{7}$$

де Imp_i^q – потенційний збиток від використання q-ї вразливості на i-му вузлі мережі; Ex_i^q – складність використання q-ї вразливості на i-му вузлі ТКМ; а $f(Imp_i^q)$ – функція від потенційного збитку в разі використання q-ї вразливості на i-му вузлі мережі.

Так, потенційний збиток від використання вразливості розраховується як [38]

$$Imp_i^q = 10,41\left[1 - (1 - Conf_i^q) \cdot (1 - Int_i^q) \cdot (1 - Av_i^q)\right], \tag{8}$$

де $Conf_i^q$ – збитки від порушення конфіденційності; Int_i^q – збитки від порушення цілісності; Av_i^q – збитки від порушення доступності у випадку використання q-ї вразливості на i-му вузлі ТКМ. Дані три метрики базової групи $Conf_i^q$, Int_i^q та Av_i^q визначають можливі наслідки використання зловмисником q-ї вразливості на i-му вузлі мережі. У кожній з цих метрик збитки від використання вразливості можуть бути *відсутніми*, тоді їх числове значення дорівнюватиме 0, *частковими* із значенням 0,275 або бути *повними* із значенням 0,66 [38].

Складність використання вразливості розраховується за допомогою наступного виразу:

$$Ex_i^q = 20 \cdot Ac_i^q \cdot Au_i^q \cdot AcV_i^q, \tag{9}$$

де Ac_i^q – показник системи оцінки вразливості, що характеризує складність отримання доступу (вектор доступу); Au_i^q – показник системи оцінки вразливості, що відповідає за вимоги до автентифікації; AcV_i^q – показник системи оцінки вразливості, який відображає спосіб використання q-ї вразливості на i-му вузлі ТКМ, що за фізичним змістом характеризується «віддаленістю» зловмисника, тобто кількістю пристроїв та/або обмежень доступу, через які зловмисник може досягнути i-го вузла ТКМ для здійснення атаки.

Функція від потенційного збитку $f(Imp_i^q)$ згідно з [38] приймає значення 0 у разі відсутності збитку, тобто $Imp_i^q = 0$. У даному дослідженні розглядатиметься випадок, коли потенційний збиток наявний ($Imp \neq 0$). Тобто у подальших розрахунках використаємо $f(Imp_i^q) = 1{,}176$ [38].

Зазначені показники є базовими метриками [38, 39], які характеризують загальну складність реалізації атаки при використанні тієї чи іншої вразливості на i-му вузлі мережі (табл. 1).

Тоді для кількісної оцінки найгіршого сценарію ризику інформаційної безпеки при компрометації каналу зв'язку $E_{i,j} \in E$, що виходять з i-го вузла, використаємо наступний вираз експоненціального характеру [40]:

$$R_{i,j} = w_{i,j} \cdot \ln \sum_{U_i^q \in U_i^*} e^{BS_i^q}, \tag{10}$$

де $w_{i,j}$ – вагові коефіцієнти (вага компрометації), які використовуються для оцінки ризику, створюваного використанням уразливостей на i-му вузлі ТКМ. Фактично коефіцієнти $w_{i,j}$ кількісно характеризують потенційний збиток при використанні наявних на i-му вузлі ТКМ уразливостей.

Таблиця 1. Значення показників для розрахунку базових метрик уразливостей [39]

Значення	Опис	Числова характеристика
Вектор доступу Ac_i^q		
Потрібен локальний доступ (Л)	Зловмисникові потрібен безпосередній фізичний доступ до об'єкту, на якому розташована вразливість	0,395
Можливий доступ з суміжної мережі (СмМ)	Зловмисникові потрібен доступ у межах однієї локальної мережі (одного широкомовного домену) до вразливого об'єкту	0,646
Можливий доступ з будь-якої мережі (М)	Зловмисник може використовувати вразливість віддалено з будь-якої ділянки мережі, в тому числі через Інтернет	1,0
Вимоги до автентифікації Au_i^q		
Множинна (М)	Зловмисник повинен зробити більше однієї процедури автентифікації для експлуатації вразливості вузла	0,45
Одинична (О)	Зловмиснику досить один раз автентифікуватися для експлуатації вразливості вузла	0,56
Відсутня (В)	Зловмисникові не потрібно проходити процедуру автентифікації для експлуатації вразливості вузла	0,704
Складність доступу до вузла AcV_i^q		
Складна (Ск)	Існує ряд жорстких обмежень доступу до вузла. Наприклад, експлуатація вразливості вузла можлива тільки в дуже короткий проміжок часу або вимагає застосування соціальної інженерії, при якій зловмисника може бути опізнано	0,35
Середня (Ср)	Існують деякі обмеження доступу до вузла. Наприклад, підключення до вразливого пристрою можливо тільки з певних вузлів або вразливий пристрій повинен функціонувати з нестандартними налаштуваннями	0,61
Легка (Л)	Немає особливих умов доступу до вразливості вузла. Наприклад, коли система доступна багатьом користувачам одночасно або коли вразлива конфігурація працює на множині вузлів мережі	0,71
Збиток конфіденційності $Conf_i^q$		
Відсутній (В)	Можливість порушення конфіденційності інформації відсутня	0,0
Частковий (Ч)	Існує значне, однак, обмежене розголошення конфіденційної інформації	0,275
Повний (П)	Існує повне розкриття конфіденційної інформації	0,66
Збиток цілісності Int_i^q		
Відсутній (В)	Можливість порушення цілісності інформації відсутня	0,0
Частковий (Ч)	Існує можливість часткової модифікації даних або системних файлів	0,275
Повний (П)	Існує можливість модифікації будь-яких даних вузла	0,66
Збиток доступності Av_i^q		
Відсутній (В)	Можливість порушення доступності ресурсу відсутня	0,0
Частковий (Ч)	Існує можливість зниження продуктивності або виведення з ладу деяких функцій вузла	0,275
Повний (П)	Існує можливість повного виведення вузла з ладу	0,66

Зазначимо, що у випадку, коли компрометація каналу зв'язку $E_{i,j} \in E$ відбувається тільки через використання вразливостей на i-му вузлі, то ризики інформаційної безпеки вузла та каналу зв'язку тотожно рівні, тобто

$$\sum_{U_i^q \in U_i^*} BS_i^q \cdot P_i^q = w_{i,j} \cdot \ln \sum_{U_i^q \in U_i^*} e^{BS_i^q}. \quad (11)$$

Розрахунок вагових коефіцієнтів $w_{i,j}$ грунтується на припущенні, що компрометація каналу зв'язку $E_{i,j} \in E$ відбуватиметься внаслідок компрометації i-го вузла ТКМ, тобто через використання наявних вразливостей на цьому вузлі. В даному випадку імовірність компрометації i-го вузла залежить від наявності та використання вразливостей на ньому та розраховується як ризик інформаційної безпеки.

Виходячи з (6)-(11), значення кожного з вагових коефіцієнтів (метрик маршрутизації) $w_{i,j}$ у виразі (5) можна розрахувати за допомогою наступного виразу:

$$w_{i,j} = \frac{\sum_{U_i^q \in U_i^*} BS_i^q \cdot P_i^q}{\ln \sum_{U_i^q \in U_i^*} e^{BS_i^q}}. \quad (12)$$

IV. Дослідження запропонованої потокової моделі безпечної маршрутизації з урахуванням ризиків інформаційної безпеки

Проведено дослідження запропонованої потокової моделі безпечної маршрутизації з метою підтвердження її працездатності, адекватності та ефективності отриманих результатів розрахунку. В межах розрахункового прикладу обрано структуру телекомунікаційної мережі, яка показана на рис. 1.

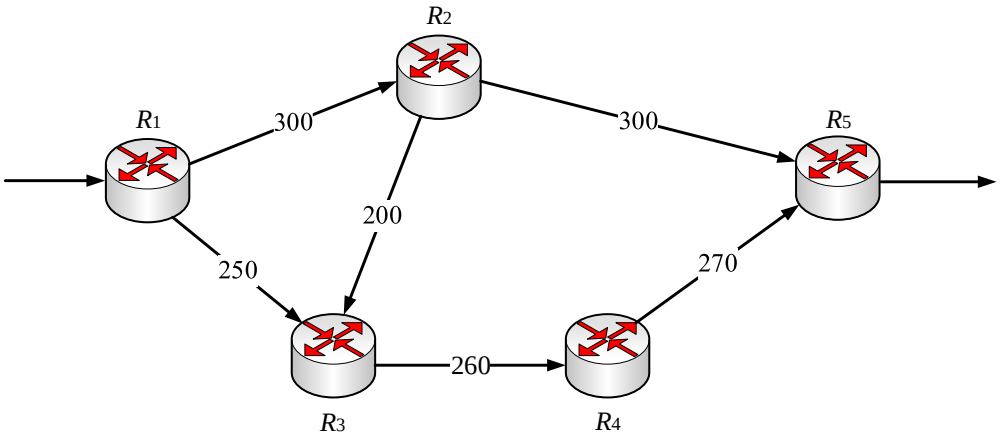

Рис. 1. Досліджуваний фрагмент структури ТКМ

Мережа складається з п'яти вузлів (маршрутизаторів). У процесі дослідження генерувався один потік потоків, тобто $k=1$, коли вузлом-джерелом пакетів виступав маршрутизатор R_1, а вузлом-отримувачем – маршрутизатор R_5. Інтенсивність потоку пакетів змінювалась від 0 до 400 1/с. У розривах каналів зв'язку (рис. 1) показана їх пропускна здатність (1/с). Для розрахунку вагових коефіцієнтів $w_{i,j}$ ($E_{i,j} \in E$) використовувався вираз (12) спільно з виразами (6)-(11). При цьому показник критичності q-ї вразливості на i-му вузлі ТКМ BS_i^q, що залежав від базових метрик системи оцінки вразливостей (табл. 1), визначався для різних маршрутизаторів із відповідною ймовірністю використання цієї q-ї вразливості зловмисником на i-му вузлі мережі P_i^q, як показано у табл. 2.

Таблиця 2. Характеристики вразливостей мережного обладнання для дослідження

Вузол ТКМ	Маршрутизатор	Базова оцінка BS_i^q	Ймовірність використання вразливості P_i^q	Опис вразливості згідно зі спеціалізованою базою даних	Рівень критичності вразливості
R_1	Cisco RV042	7,2	0,1	CVE-2020-3294	Високий
R_2	Cisco Small Business RV160W	9,8	0,6	CVE-2021-1289	Критичний
R_3	NETGEAR R7450 1.2.0.62_1.0.1	6,5	0,2	CVE-2020-35839	Середній
R_4	Xiaomi RM1800	7,5	0,3	CVE-2020-14098	Високий
R_5	Cisco RV260	9,8	0,6	CVE-2021-1292	Критичний

Для подальшої оцінки ефективності маршрутних рішень, отриманих за допомогою запропонованої моделі (1)-(5), (12), проведено їх порівняльний аналіз із рішеннями, які відповідали використанню у виразі (5) метрик протоколу EIGRP, а саме $w_{i,j}=10^7/\varphi_{i,j}$. Для зручності позначимо запропоновану модель – «*модель* 1», а модель з EIGRP-метрикою – «*модель* 2». Результати розв'язання задачі маршрутизації з використанням розробленої *моделі* 1 і *моделі* 2 представлено у табл. 3 та на рис. 2 та 3.

Таблиця 3. Результати аналізу *моделі* 1 та *моделі* 2 при інтенсивності потоку пакетів $\lambda^1=400$ 1/с

Канали зв'язку	Пропускна здатність КЗ, $\varphi_{i,j}$, 1/с	*Модель* 1		*Модель* 2
		Інтенсивність потоку, 1/с	Вагові коефіцієнти $w_{i,j}$	Інтенсивність потоку, 1/с
$E_{1,2}$	300	150	0,1	300
$E_{1,3}$	250	250	0,1	100
$E_{2,3}$	200	0	0,59	0
$E_{2,5}$	300	150	0,59	300
$E_{3,4}$	260	250	0,19	100
$E_{4,5}$	270	250	0,29	100

На цих рисунках у розривах каналів зв'язку вказані (згори донизу) їхні пропускні здатності (1/с), інтенсивність потоку, що протікає в каналі зв'язку (1/с), та для *моделі* 1 додатково вказані вагові коефіцієнти $w_{i,j}$ для кожного каналу зв'язку $E_{i,j} \in E$.

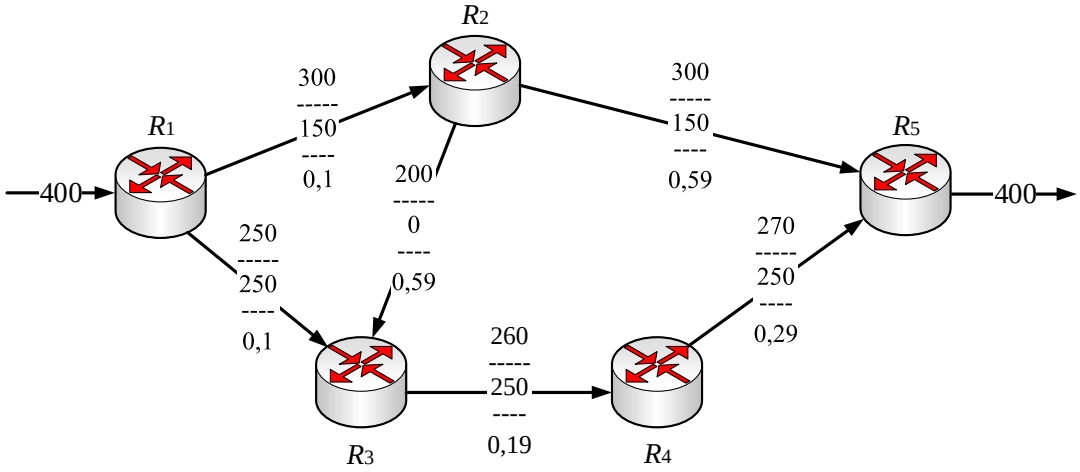

Рис. 2. Результат розв'язання задачі маршрутизації з використанням *моделі* 1

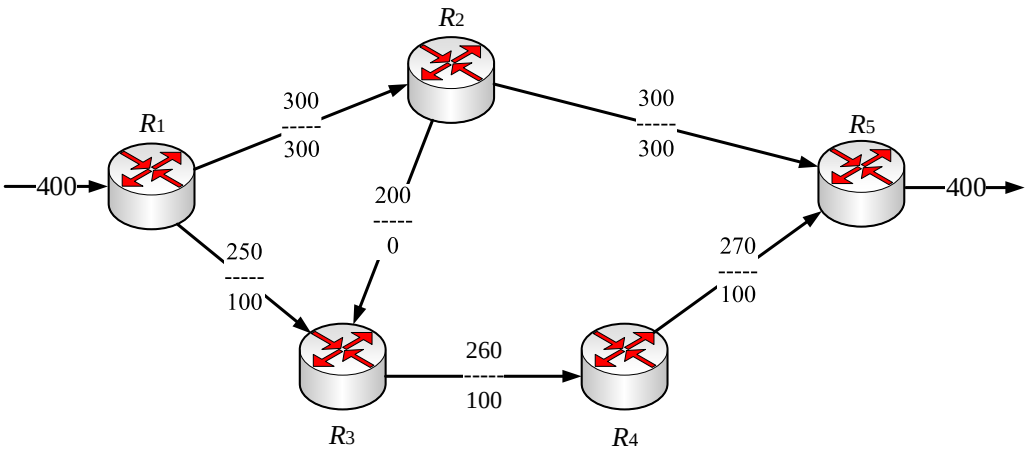

Рис. 3. Результат розв'язання задачі маршрутизації з використанням *моделі* 2

Як показано на рис. 1, у результаті розв'язання маршрутної задачі за допомогою запропонованої моделі (*модель* 1) потік пакетів з інтенсивністю 250 1/с передавався маршрутом $R_1 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$, який містив найменш уразливі канали зв'язку. При перевантаженні цього маршруту решта потоку (150 1/с) передавалася вже по наступному за вразливістю шляху $R_1 \rightarrow R_2 \rightarrow R_5$. На відміну від *моделі* 1, під час використання *моделі* 2 спочатку (до 300 1/с) завантажувався найкращий з погляду пропускної здатності та кількості переприйомів (хопів), але найбільш уразливий шлях $R_1 \rightarrow R_2 \rightarrow R_5$. Решта потоку (100 1/с) передавалася маршрутом $R_1 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$.

Загалом, порядок використання шляхів у ТКМ для різних інтенсивностей потоку пакетів під час реалізації моделей 1 та 2 представлені в табл. 4.

Таблиця 4. Порядок використання шляхів у ТКМ для різних інтенсивностей потоку пакетів

Інтенсивність потоку пакетів, λ^1 1/с	*Модель* 1	*Модель* 2
	Використані шляхи	
$\lambda^1 \in (0;250]$.	$R_1 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$	$R_1 \rightarrow R_2 \rightarrow R_5$
$\lambda^1 \in (250;300]$.	$R_1 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$	$R_1 \rightarrow R_2 \rightarrow R_5$
	$R_1 \rightarrow R_2 \rightarrow R_5$	
$\lambda^1 \in (300;400]$.	$R_1 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$	$R_1 \rightarrow R_2 \rightarrow R_5$
	$R_1 \rightarrow R_2 \rightarrow R_5$	$R_1 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$

Висновки

В роботі запропоновано вдосконалену потокову модель маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей (1)-(12). Основу моделі складають умови реалізації одно- та багатошляхової маршрутизації (1), (2), збереження потоку (3) та запобігання перевантаженню каналів зв'язку ТКМ (4). В межах запропонованої моделі задача безпечної маршрутизації сформульована в оптимізаційній формі з критерієм оптимальності (5). Новизна розробленої моделі полягає в тому, що для розрахунку маршрутних метрик використовуються вирази (12), які характеризують ризик інформаційної безпеки в каналах зв'язку ТКМ та відповідно до рекомендацій NIST враховують збитки від порушення конфіденційності та цілісності інформації, доступності мережного ресурсу у випадку використання наявних уразливостей; показники складності використання вразливостей на вузлах мережі та отримання доступу до мережних елементів та мережі загалом внаслідок використання зазначених уразливостей.

Як показали результати проведеного дослідження (табл. 3), використання запропонованої моделі безпечної маршрутизації дозволяє розрахувати та використати маршрути з мінімальним ризиком інформаційної безпеки, тим самим забезпечивши максимальний рівень мережної безпеки пакетам, які передаються в ТКМ. Запропонований підхід до формування маршрутних метрик може бути застосований також під час забезпечення комплексного врахування в процесі розв'язання задач маршрутизації як показників мережної безпеки, так і показників якості обслуговування. До перспектив розвитку отриманих рішень варто віднести синтез моделей і методів безпечної маршрутизації, за допомогою яких би вдалося гарантувати заданий рівень мережної безпеки на підставі розрахунку та використання відповідних маршрутів у ТКМ.

Список літератури

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

2. *Kenyon, T.* (2002), Data Networks: Routing, Security, and Performance Optimization, Digital Press, 1st edition, 806 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. *Govindasamy, J., Punniakody, S.* (2017), "A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack", Electrical Systems and Information Technology, No. l 5(3), P. 735-744. **DOI**: https://doi.org/10.1016/j.jesit.2017.02.002

5. *Wadhwani, G. K., Khatri, S. K., Muttoo, S. K.* (2018), "Critical Evaluation of Secure Routing Protocols for MANET", International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, P. 202-206, **DOI:** https://doi.org/10.1109/ICACCCN.2018.8748725

6. *Merkle, R. C. (*1987), "A digital signature based on a conventional encryption function", Pomerance C. (eds) Advances in Cryptology — CRYPTO '87, CRYPTO 1987, Lecture Notes in Computer Science, No. 293, Springer, Berlin, Heidelberg, P. 369–378. **DOI***:* https://doi.org/10.1007/3-540-48184-2_32

7. *Shashikala, R., Kavitha, C.* (2014), "Secured data integrity routing for Wireless Sensor Networks", International Conference on Advances in Electronics Computers and Communications, Bangalore, India, P. 1-6, **DOI:** https://doi.org/10.1109/ICAECC.2014.7002419.

8. *Khan, S., Khan, S., Loo J.* (2012), "Cross layer secure and resource-aware on-demand routing protocol for hybrid wireless mesh networks", Wireless Personal Communications, No. 62, P. 201-214. **DOI**: https://doi.org/10.1007/s11277-010-0048-y

9. *Aggarwal, A., Gandhi, S., Chaubey, N.* (2014), "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs", 2014 Fourth International Conference on Advanced Computing & Communication Technologies, Rohtak, India, P. 432-438. **DOI**: https://doi.org/10.1109/ACCT.2014.95

10. *Lou, W., Liu, W., Fang, Y.* (2004), "SPREAD: enhancing data confidentiality in mobile ad hoc networks," *IEEE INFOCOM 2004*, Hong Kong, China, No. 4, P. 2404-2413, **DOI:** https://doi.org/10.1109/INFCOM.2004.1354662

11. *Gu, Q.* (2011), "Secure Routing Protocols", van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security, Springer, Boston, MA, **DOI:** https://doi.org/10.1007/978-1-4419-5906-5_641

12. *Lemeshko, O., Yeremenko, O., Sleiman, B., Yevdokymenko, M.* (2020), "Fast ReRoute Model with Realization of Path and Bandwidth Protection Scheme in SDN", Advances in Electrical and Electronic Engineering, No. 18(1), P. 23–30. **DOI**: https://doi.org/10.15598/aeee.v18i1.3548

13. *Lemeshko, O., Yevdokymenko, M., Yeremenko, O.* (2020), "Fast ReRoute Tensor Model with Quality of Service Protection Under Multiple Parameters", Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, *Springer, Cham*, No. 48., P. 489–512, **DOI:** https://doi.org/10.1007/978-3-030-43070-2_22

14. *Diwan, D., Narang, V. K., Singh A. K.* (2017), "Security Mechanism in RIPv2, EIGRP and OSPF for Campus Network", Computer Science Trends and Technology (IJCST), No. 5(2), P. 399-404.

15. *Snihurov, A., Chakrian, V.* (2015), "Improvement of EIGRP Protocol Routing Algorithm Based on Information Security Metrics", Second International IEEE Conference on Problems of Infocommunications. Science and Technology (PIC S&T-2015), Kharkiv, P. 263-265, **DOI:** https://doi.org/10.1109/INFOCOMMST.2015.7357331

16. *Bhatia, M., Hartman, S., Zhang, D.* (2015), "Security Extension for OSPFv2 When Using Manual Key Management", RFC 7474, available at: https:// tools.ietf.org/html/rfc7474.

17. *Лемешко, А. В., Вавенко, Т. В.* (2011), "Анализ решений задач однопутевой и многопутевой маршрутизации многопотокового трафика в телекоммуникационных сетях", Системи обробки інформації, No. 8, С. 224-228.

18. *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.

19. *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

20. *Pattanavichai, S.* (2017), "Comparison for network security scanner tools between GFI LanGuard and Microsoft Baseline Security Analyzer (MBSA)", *15th International Conference on ICT and Knowledge Engineering (ICT&KE)*, Bangkok, P. 1-7, **DOI:** https://doi.org/10.1109/ICTKE.2017.8259628

21. *Chimmanee, S., Veeraprasit, T., Srisa-An, C.* (2014), "A Performance Evaluation of Vulnerability Detection: NetClarity Audito Nessus and Retina", International Journal of Computer Science and Network Security, No. 14(3), P. 34-40.

22. *Denis, M., Zena, C. , Hayajneh T.* (2016), "Penetration testing: Concepts, attack methods, and defense strategies", 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, P. 1-6. **DOI:** https://doi.org/10.1109/LISAT.2016.7494156

23. *Mallouli, W., Bessayah, F., Cavalli, A., Benameur, A.* (2008), "Security Rules Specification and Analysis Based on Passive Testing", IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference, *New* Orleans, LA, USA, P. 1-6. **DOI:** https://doi.org/10.1109/GLOCOM.2008.ECP.400

24. *Liu, D.* (2020), "Research on Data Security Analysis and Label Recognition Technology Based on Big Data Business Scenario", IEEE 10th International Conference on Electronics Information and Emergency Communication (ICEIEC), Beijing, China, P. 344-347. **DOI:** https://doi.org/10.1109/ICEIEC49280.2020.9152308

25. *Streilein, W., Kratkiewicz, K., Sikorski, M., Piwowarski, K., Webster, S.* (2007), "PANEMOTO: Network Visualization of Security Situational Awareness Through Passive Analysis", IEEE SMC Information Assurance and Security Workshop, West Point, NY, USA, P. 284-290, **DOI**: https://doi.org/10.1109/IAW.2007.381945

26. *Masys, A.* (2013), "Networks and network analysis for defence and security,"2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2013), Niagara Falls, ON, Canada, P 1479-1480. **DOI:** https://doi.org/10.1145/2492517.2492602

27. *Sinchana, K., Sinchana, C., Gururaj, H. L., Sunil Kumar, B. R.* (2019), "Performance Evaluation and Analysis of various Network Security tools," 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, P. 644-650, **DOI:** https://doi.org/10.1109/ICCES45898.2019.9002531

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

29. *Arteaga, J. H., Hancharou, F., Thams F., Chatzivasileiadis, S.* (2019), "Deep Learning for Power System Security Assessment", 2019 IEEE Milan PowerTech, Milan, Italy, P. 1-6. **DOI:** https://doi.org/10.1109/PTC.2019.8810906

30. ISO/IEC 17799:2005 (2005), "Information technology, Security techniques, Code of practice for information security management", available at: https://www.iso.org/standard/39612.html

31. ISO/IEC 15408-1:2009 (2009), "Information technology, Security techniques ,Evaluation criteria for IT security, Part 1: Introduction and general model", available at: https://www.iso.org/standard/50341.html

32. COBIT FRAMEWORK: INTRODUCTION & METHODOLOGY (2019), ISACA, available at: https://community.mis.temple.edu/mis5203sec001sp2019/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf

33. COSO (2017), "Enterprise Risk Management Integrating with Strategy and Performance", available at: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

34. *Paramasivan, B., Prakash, M. J. V., Kaliappan M.* (2015), "Development of a secure routing protocol using game theory model in mobile ad hoc networks", Journal of Communications and Networks, No. 17(1), P. 75-83. **DOI**: https://doi.org/10.1109/JCN.2015.000012

35. *Chandra, Y., Mishra, P.K., Arya, C. P.* (2016), "Attack graphs for defending cyber assets," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, P. 648-653.

36. *Buzhinsky, I., Vyatkin, V.* (2017), "Testing automation systems by means of model checking," 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, P. 1-7. **DOI:** https://doi.org/10.1109/ETFA.2017.8247579

37. *Wankhede, S. B.* (2019), "Anomaly Detection using Machine Learning Techniques", 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), Bombay, India, P. 1-3. **DOI**: https://doi.org/10.1109/I2CT45611.2019.9033532

38. Common Vulnerability Scoring System v3.1: Specification Document, Forum of Incident Response and Security Teams (2019), available at: https://www.first.org/cvss/specification-document

39. Common Vulnerability Scoring System v3.1: Examples, Forum of Incident Response and Security Teams (2019), available at: https://www.first.org/cvss/examples

40. *Abedin, M., Nessa, S., Al-Shaer, E., Khan, L.* (2006), "Vulnerability analysis For evaluating quality of protection of security policies", Proceedings of the 2nd ACM workshop on Quality of protection (QoP'06), P. 49-52. **DOI:** https://doi.org/10.1145/1179494.1179505

41. *Поповский, В. В., Лемешко, О. В., Мельникова, Л. И., Андрушко, Д. В.* (2005), "Обзор и сравнительный анализ основных моделей и алгоритмов многопутевой маршрутизации в мультисервисных телекоммуникационных сетях", Прикладная радиоэлектроника, No. 4(4), С. 372-382.