УДК 621.391

ДОСЛІДЖЕННЯ МОДЕЛЕЙ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ НА ОСНОВІ БАЗОВИХ МЕТРИК УРАЗЛИВОСТЕЙ У МЕРЕЖАХ SDN

О.С. ЄРЕМЕНКО
Харківський національний університет радіоелектроніки

Г.А. ПЛЄХОВА
Харківський національний автомобільно-дорожній університет

Abstract *– The article presents and investigates flow-based models of secure routing under base score metrics of vulnerability criticality in Software-Defined Networks (SDN). The analysis of the routing means functionality against possible attacks confirmed the perspective of their application, taking into account the base score metrics of vulnerability criticality to increase the level of network security of the SDN data plane. It is proposed to improve the existing secure routing model taking into account the base score metrics of vulnerability criticality by modifying the routing metrics so that the resulting model acquires the properties of secure QoS routing. In the improved model, the optimal route was chosen considering base score metrics of vulnerability criticality and the bandwidth of the communication links that make up this route. In addition, the quadratic optimality criterion is used in the model for the balanced distribution of flows transmitted in the data plane of the software-defined network into sub-flows taking into account the multipath routing strategy. The comparative analysis of the existing secure routing model, the QoS-routing model with metrics similar to the OSPF protocol, and the improved secure-QoS-routing model taking into account the base score metrics of vulnerability criticality proved the adequacy and efficiency of the model proposed in work. The comparison of models was based on calculating the compromise probability of the transmitted packet flow.*

Анотація *– У роботі представлено та досліджено потокові моделі безпечної маршрутизації на основі базових метрик уразливостей у програмно-конфігурованих мережах (Software-Defined Network, SDN). Проведений аналіз функціональних можливостей засобів маршрутизації щодо протидії ймовірним атакам підтвердив перспективність їхнього використання з урахуванням базових метрик критичності вразливостей для підвищення рівня мережної безпеки площини даних SDN. Запропоновано удосконалення існуючої моделі безпечної маршрутизації з урахуванням базових метрик критичності вразливостей шляхом модифікації маршрутних метрик таким чином, щоб отримувана модель набула властивостей безпечної QoS-маршрутизації. В удосконаленій моделі оптимальний маршрут обирався з урахуванням і базових метрик критичності вразливостей, і пропускної здатності каналів зв'язку, що складають цей маршрут. Крім того, в моделі задіяно квадратичний критерій оптимальності з метою збалансованого розподілу потоків, що передаються в площині даних програмно-конфігурованої мережі, на підпотоки з урахуванням стратегії багатошляхової маршрутизації. Проведений порівняльний аналіз існуючої моделі безпечної маршрутизації, моделі QoS-маршрутизації з метрикою протоколу OSPF та удосконаленої моделі безпечної QoS-маршрутизації з урахуванням базових метрик критичності вразливостей довів адекватність і працездатність запропонованої в роботі моделі. Порівняння моделей відбувалось на основі обчислення ймовірності компрометації пакетів потоку, що передавався.*

Вступ

Наразі розгортання таких мережних архітектур, як програмно-конфігуровані мережі (Software-Defined Networking, SDN), стикається з новими загрозами кібербезпеці, які вимагають розробку та дослідження нових спеціалізованих рішень щодо підвищення рівня мережної безпеки [1-4]. Незважаючи на високу відкритість і можливості програмованості, архітектура SDN замінює традиційну, проте збільшує кількість потенційних мережних атак, що призводить до нових проблем безпеки.

Зростаючий інтерес до розгортання SDN різних типів дозволяє виявляти їхні недоліки в процесі боротьби із загрозами кібербезпеці [4, 5]. Очевидно, що питання безпеки тісно пов'язані з характеристиками самих SDN мереж. Водночас серед об'єктів атак можуть бути пристрої різних рівнів SDN. Отже, відповідно до багаторівневої архітектури SDN загрози безпеці можна класифікувати на рівнях передачі даних, управління та застосунків. Зі свого боку площина даних складається з комутаторів та інших мережних пристроїв і головним чином відповідає за обробку даних, їх пересилання, відкидання, а також збір статистики. Функціонування площини даних відбувається на основі правил потоків, що надаються контролером мережі. Тоді як основними причинами проблем безпеки є власне архітектура SDN, зовнішні шкідливі атаки, недостатність контролю доступу та засобів шифрування.

Наразі важливе місце у комплексі засобів підвищення мережної безпеки, зокрема SDN, відводиться протоколам маршрутизації, які потребують системної та скоординованої взаємодії одночасно множини мережних елементів, SDN-комутаторів і контролерів мережі, під час формування (розрахунку) шляхів і правил потоків, вздовж яких має забезпечуватися необхідний рівень безпеки за обраними показниками та критеріями [5].

Проведений аналіз вразливостей площини даних SDN [4-6] і функціональних можливостей засобів маршрутизації щодо протидії можливим атакам [7-14] показав перспективність використання засобів безпечної маршрутизації на основі базових метрик критичності вразливостей для підвищення рівня мережної безпеки площини даних SDN. Аналіз стандарту CVSS щодо кількісного розрахунку рівня вразливості мережного обладнання довів доцільність його використання під час розробки та дослідження перспективних підходів до безпечної маршрутизації у площині даних програмно-конфігурованих мереж [15-19].

Отже, стаття присвячена актуальній науково-прикладній задачі, пов'язаній з удосконаленням потенційних рішень щодо підвищення рівня мережної безпеки у площині даних SDN засобами маршрутизації. В роботі досліджено низку моделей безпечної маршрутизації з урахуванням базових метрик критичності вразливостей. Було удосконалено існуючу модель [7], відповідно до чого сформульовано в оптимізаційній формі потокову модель безпечної QoS-маршрутизації.

I. Засоби безпечної маршрутизації для підвищення рівня мережної безпеки площини даних SDN

За вимогами стандартів ITU забезпечення інформаційної безпеки комунікаційних мереж здійснюється в межах трьох рівнів: безпеки інфраструктури, безпеки сервісів і безпеки застосунків [8]. У цьому випадку ефективність роботи верхніх двох рівнів, а саме сервісів і застосунків, визначається ефективністю функціонування засобів рівня безпеки інфраструктури. Водночас основним завданням рівня безпеки інфраструктури є забезпечення безпеки на рівні мережних пристроїв (наприклад, SDN-комутаторів), каналів зв'язку та маршрутів загалом, які складаються з цих елементів

мережі [8]. У напрямку безпечної маршрутизації проведено значну кількість теоретичних досліджень, починаючи від найпростіших емпіричних варіантів рішень до системних оптимізаційних підходів [7-14, 20, 21].

Так, у роботі [7] розроблено та досліджено модель безпечної маршрутизації з балансуванням навантаження в мережах на основі SD-WAN. Технологічне завдання безпечної маршрутизації з балансуванням навантаження було сформульовано у формі оптимізаційної задачі з квадратичним критерієм оптимальності. Така форма критерію дозволяє збалансувати частки потоків, що передаються в мережі, а комбінована маршрутна метрика враховує продуктивність і безпеку мережі. Запропонований підхід сприяє більш ефективному використанню наявних мережних ресурсів, враховуючи ймовірність компрометації каналів зв'язку під час прийняття маршрутних рішень.

Зі свого боку проактивні та реактивні методі безпечної маршрутизації конфіденційних повідомлень шляхами, що перетинаються, розроблені в [8], можуть рекомендуватися до використання як основа нових мережних протоколів безпечної маршрутизації та безпечної швидкої перемаршрутизації для багатошляхової передачі із заданими вимогами щодо граничної ймовірності компрометації в мережі.

У роботах [11, 12] пропонується під час вибору маршруту в мережі враховувати ризики інформаційної безпеки шляхом формування відповідних маршрутних метрик, коли в них спільно з показниками якості обслуговування враховується показник ризику інформаційної безпеки елементів мережі.

Тоді як у роботах [13, 14] пропонуються потокові моделі маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. У моделі [13] для розрахунку маршрутних метрик використовуються вирази, які характеризують ризик інформаційної безпеки в каналах зв'язку мережі 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 і мережі загалом внаслідок використання зазначених уразливостей. Запропонований авторами підхід до формування маршрутних метрик може бути використаний під час комплексного врахування в процесі розв'язання задач маршрутизації показників мережної безпеки.

Проведений аналіз функціональних можливостей засобів маршрутизації щодо протидії можливим атакам підтверджує перспективність використання засобів безпечної маршрутизації на основі базових метрик критичності вразливостей для підвищення рівня мережної безпеки площини даних SDN.

II. Потокова модель маршрутизації в програмно-конфігурованій телекомунікаційній мережі

Для подальшого дослідження використаємо базову потокову модель маршрутизації в телекомунікаційній мережі, запропоновану в [13, 20]. Основні характеристики цієї моделі наступні:

– $G=(R,E)$ – граф, що описує структуру мережі;

– $R=\left\{R_i; i=\overline{1,m}\right\}$ – множина вершин, що моделюють маршрутизатори;

– $E=\left\{E_{i,j}; i,j=\overline{1,m}; i\neq j\right\}$ – множина дуг, що представляють канали зв'язку мережі;

– $\varphi_{i,j}$ – пропускна здатність каналу зв'язку, що описується дугою $E_{i,j}\in E$ і вимірюється у пакетах за секунду (пак/с).

Припустимо, що у мережі циркулює множина потоків пакетів *K*, які генеруються відповідними мережними додатками. *Для* кожного *k*-го потоку відомі такі вихідні дані:

– λ^k – середня інтенсивність потоку трафіку (пак/с);

– s_k і d_k – вузол-відправник і вузол-отримувач пакетів *k*-го потоку відповідно.

Далі порядок маршрутизації в мережі (площині даних SDN) визначають маршрутні змінні $x_{i,j}^k$, кожна з яких характеризує долю (частину) *k*-го потоку, що протікає в каналі зв'язку між *i*-м та *j*-м вузлами комунікаційної мережі**.** Відповідно до фізичного змісту введених маршрутних змінних та залежно від реалізованої стратегії маршрутизації на них накладаються умови вигляду [7]:

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

Умови (1) відповідають реалізації багатошляхової стратегії маршрутизації в мережі. Множину застосованих шляхів надалі називатимемо мультишляхом.

Крім того, під час розрахунку маршрутних змінних $x_{i,j}^k$ мають виконуватися умови збереження потоку на маршрутизаторах мережі (вузлі-відправнику, вузлі-отримувачу та транзитних вузлах) [13, 20]:

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

У разі виконання умов (2) 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 [13, 20].

Для запобігання перевантаження каналів зв'язку мережі необхідно забезпечити виконання наступних умов [13, 20]:

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

кількість яких відповідає числу каналів зв'язку в мережі.

Далі використаємо наступний *лінійний* критерій оптимальності *для* розрахунку шляхів у мережі [13]:

$$J_1 = \sum_{k\in K} \sum_{E_{i,j}\in E} w_{i,j} x_{i,j}^k \Rightarrow \min, \tag{4}$$

де вагові коефіцієнти $w_{i,j}$ – маршрутні метрики, які мають урахувати основні характеристики безпеки каналів зв'язку, що обчислюються відповідно до методики, заснованої на використанні базових метрик уразливостей CVSS v3.0 і запропонованої в роботах [13, 20].

Нехай *модель 1* буде представлена виразами (1)-(3) і маршрутні метрики $w_{i,j}$ у критерії (4) визначаються відповідно до методики [13, 20]. Тоді як *модель 2* також заснована на базовій моделі (1)-(3), але в критерії оптимальності (5) використовуватимуться вагові коефіцієнти, аналогічні метриці маршрутного протоколу OSPF, тобто $f_{i,j}^{OSPF} = 10^8 / \varphi_{i,j}$:

$$J_2 = \sum_{k\in K} \sum_{E_{i,j}\in E} f_{i,j}^{OSPF} x_{i,j}^k \Rightarrow \min. \tag{5}$$

Таким чином, *модель 1* представляє собою модель безпечної маршрутизації, заснованої на урахуванні базових метрик критичності вразливостей. Відповідно *модель 2* є найпростішим прикладом QoS-маршрутизації, оскільки має на меті вибір найкращого шляху або мультишляху, який містить найбільш продуктивні канали зв'язку.

Далі ці моделі маршрутизації порівнювались між собою.

III. Удосконалення моделі безпечної маршрутизації з урахуванням базових метрик критичності вразливостей

Нехай *модель 3* включає в себе умови та обмеження (1)-(3), які є базовими *для* багатошляхової моделі маршрутизації. Відповідно *до* результатів, отриманих в роботі [20], модифікуємо маршрутні метрики таким чином, щоб отримувана модель набула властивостей безпечної QoS-маршрутизації. Тобто в *моделі 3* оптимальний маршрут

повинен обиратися з урахуванням і базових метрик критичності вразливостей, і пропускної здатності каналів зв'язку, що складають цей маршрут.

Отже, у межах позначень моделі (1)-(3) компоненти комбінованої метрики виглядатимуть наступним чином. Компонент комбінованої маршрутної метрики $f_{i,j}^{комб} = f_{i,j}^{OSPF} + f_{i,j}^{SEC}$ [7], що відповідає за продуктивність безпечного мультишляху, має наступний вид:

$$f_{i,j}^{OSPF} = \frac{w^{OSPF}}{\varphi_{i,j}}, \tag{6}$$

де $w^{OSPF} = 10^8$.

Тоді як компонент метрики, заснований на параметрі мережної безпеки, а саме базових метриках критичності вразливостей каналу зв'язку, модифікується як

$$f_{i,j}^{SEC} = w^{SEC} \cdot w_{i,j}, \tag{7}$$

де $w^{SEC} = \frac{w^{OSPF}}{R} = \frac{10^8}{R}$, а $w_{i,j}$ визначається відповідно до методики на основі базових метрик уразливостей CVSS v3.0, запропонованої в [13, 20].

Як і раніше у [7], R є співвідношенням між ваговими коефіцієнтами метрик продуктивності та мережної безпеки:

$$R = \frac{w^{OSPF}}{w^{SEC}}. \tag{8}$$

Для реалізації балансування навантаження в моделі 3 в процесі багатошляхової маршрутизації використовуватиметься критерій оптимальності квадратичної форми [20]:

$$J_3 = \min_x \sum_{k \in K} \sum_{E_{i,j} \in E} \left(f_{i,j}^{OSPF} + f_{i,j}^{SEC} \right) \cdot x_{i,j}^2 \Rightarrow \min. \tag{9}$$

IV. Дослідження та аналіз потокових моделей безпечної маршрутизації з урахуванням базових метрик критичності вразливостей

Проведемо дослідження та порівняльний аналіз розглянутих моделей, а також для модифікованої потокової моделі безпечної QoS-маршрутизації доведемо її працездатність, адекватність та ефективність застосування у межах розрахункових прикладів.

Отже, для прикладу обрано структуру комунікаційної мережі, що представляє площину даних SDN мережі, зображену на рис. 1. Мережа складається з п'яти вузлів

(маршрутизаторів) та семи каналів зв'язку. Під час дослідження генерувався лише один потік потоків, тобто $k=1$. Вузлом-джерелом пакетів обрано маршрутизатор R_1, а вузлом-отримувачем – маршрутизатор R_5.

Інтенсивність потоку пакетів у межах досліджень змінювалася від 0 до 270 пак/с. У розривах каналів зв'язку (рис. 1) показана їхня пропускна здатність (пак/с).

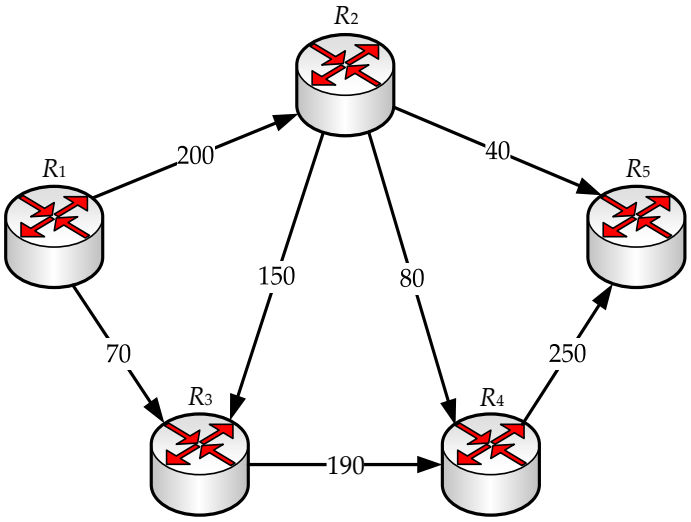

Рис. 1. Досліджуваний фрагмент структури мережі

Відповідно до вихідної структури шуканий вектор маршрутних змінних $\vec{x}$ та вектор комбінованих метрик у межах розглянутої *моделі 3* мають наступний вигляд:

$$\vec{x}=\begin{bmatrix} x_{1,2} \\ x_{1,3} \\ x_{2,3} \\ x_{2,4} \\ x_{2,5} \\ x_{3,4} \\ x_{4,5} \end{bmatrix}, \quad \vec{f}^{комб}=\begin{bmatrix} f_{1,2}^{комб} \\ f_{1,3}^{комб} \\ f_{2,3}^{комб} \\ f_{2,4}^{комб} \\ f_{2,5}^{комб} \\ f_{3,4}^{комб} \\ f_{4,5}^{комб} \end{bmatrix}.$$

Умови збереження потоку (2) для досліджуваної структури мережі мають такий вигляд:

$$\begin{cases} x_{1,2}+x_{1,3}=1; \\ -x_{1,2}+x_{2,3}+x_{2,4}+x_{2,5}=0; \\ -x_{1,3}-x_{2,3}+x_{3,4}=0; \\ -x_{2,4}-x_{3,4}+x_{4,5}=0; \\ -x_{2,5}-x_{4,5}=-1. \end{cases}$$

У досліджуваній структурі мережі можна виділити чотири окремі шляхи, які складатимуть мультишлях під час розв'язання задачі багатошляхової маршрутизації:

– шлях 1: $R_1 \rightarrow R_2 \rightarrow R_5$;

– шлях 2: $R_1 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$;

– шлях 3: $R_1 \rightarrow R_2 \rightarrow R_4 \rightarrow R_5$;

– шлях 4: $R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$.

Для розрахунку вагових коефіцієнтів $w_{i,j}$, що використовуються як маршрутні метрики у *моделі 1* та як компонент композитної маршрутної метрики у *моделі 3*, застосовано методику, запропоновану в [13, 19]. Отже, показник критичності вразливості на вузлі мережі, що залежить від базових метрик системи оцінки вразливостей, визначається відповідною ймовірністю використання вразливості на вузлі (табл. 1) [13].

Так, у табл. 1 кожному вузлу (маршрутизатору) відповідав спеціальний опис наявної вразливості згідно з базою даних загальновідомих уразливостей інформаційної безпеки CVE [13].

Використане мережне обладнання показано у табл. 1.

Таблиця 1. Характеристики вразливостей мережного обладнання для дослідження [20]

Вузол	Маршрутизатор	Імовірність використання вразливості	Опис вразливості відповідно до спеціалізованої бази даних
R_1	Cisco RV042	0,1	CVE-2020-3294
R_2	Cisco Small Business RV160W	0,6	CVE-2021-1289
R_3	NETGEAR R7450 1.2.0.62_1.0.1	0,2	CVE-2020-35839
R_4	Xiaomi RM1800	0,3	CVE-2020-14098
R_5	Cisco RV260	0,6	CVE-2021-1292

V. Дослідження моделі безпечної QoS-маршрутизації з урахуванням базових метрик критичності вразливостей

Проведемо числове дослідження моделі безпечної QoS-маршрутизації з урахуванням ризиків інформаційної безпеки, а саме *моделі 3*, яка представлена умовами та обмеженнями (1)-(3), (6)-(8) і квадратичним критерієм оптимальності (9).

Нехай потік інтенсивністю $\lambda^1 = 100$ пак/с передається між першим і п'ятим вузлами. Тоді як співвідношення між ваговими коефіцієнтами метрик продуктивності та мережної безпеки (8) змінювалось від 1 до 1000. Результати відповідних розрахунків показано в табл. 2 та проілюстровано на рис. 2.

Для розв'язання сформульованої оптимізаційної задачі використовувалась програма, написана мовою Python із застосуванням Python GEKKO Optimization Suite та NumPy.

Таблиця 2. Розподіл потоку $\lambda^1 = 100$ пак/с за умови використання моделі безпечної QoS-маршрутизації (*модель 3*)

R	1	50	100	200	300	400	500	600	1000
Шлях 1	40	32,9	30,3	28,4	27,6	27,2	27	26,7	26,4
Шлях 2	45,9	36,4	34,4	33	32,5	32,2	32	31,9	31,6
Шлях 3	14,1	22,7	24,7	26,1	26,6	26,9	27	27,2	27,4
Шлях 4	0	8	10,6	12,5	13,3	13,7	14	14,2	14,6

Відповідно до отриманих результатів лише за умови $R = 1$ вихідний потік розподілявся за трьома шляхами. У разі збільшення значення співвідношення R використовувались усі чотири шляхи для формування мультишляху для передачі вихідного потоку інтенсивністю $\lambda^1 = 100$ пак/с .

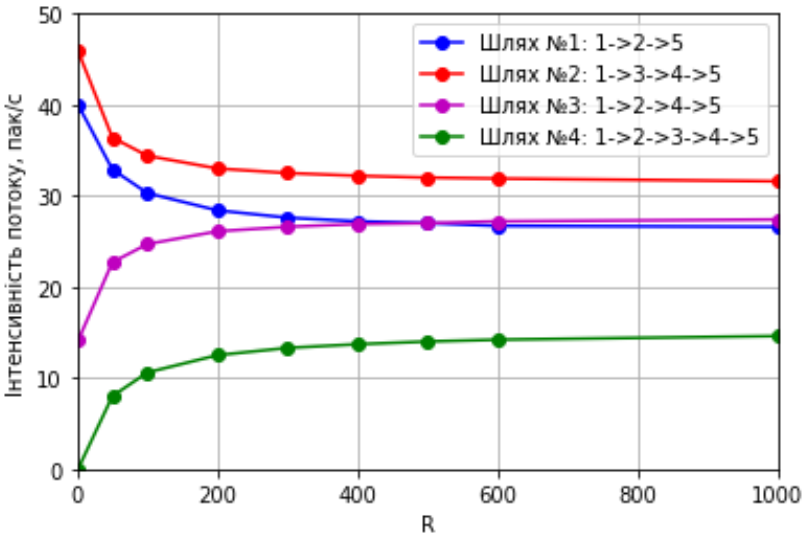

Рис. 2. Розподіл потоку за шляхами з використанням *моделі 3* ($\lambda^1 = 100$ пак/с, $R = 1 \div 1000$)

Враховуючи імовірності використання вразливості вузлів, які визначають й рівень вразливості каналів зв'язку, що виходять з нього, знайдемо відповідні ймовірності компрометації шляхів за методикою, вказаною в [8, 20].

Також, використовуючи імовірнісний підхід щодо оцінювання рівня мережної безпеки, запропонований в [20], отримаємо значення імовірності компрометації пакетів *k*-го потоку вздовж множини використаних шляхів:

$$p_{E2E}^{k} = \sum_{s \in S^k} \frac{\lambda_s^k}{\lambda^k} p_s , \tag{10}$$

де S^k – множина шляхів, що використовуються для передачі пакетів k-го потоку між заданою парою маршрутизаторів мережі;

λ_s^k – інтенсивність *k*-го потоку пакетів, що передаються *s*-м шляхом мережі;

p_s – імовірність компрометації *s*-го шляху, що визначається відповідно до формули

$$p_s = 1 - \prod_{E_{i,j} \in Path_s} (1 - p_{i,j}) , \tag{11}$$

у якій $Path_s = \{E_{i,j}\}$ – множина каналів зв'язку мережі, які утворюють *s*-й шлях.

Враховуючи відомі імовірності використання вразливостей обраного мережного обладнання – маршрутизаторів (табл. 1), отримаємо значення імовірностей компрометації каналів зв'язку досліджуваної мережі (рис. 3), оскільки рівень імовірності використання вразливості вузла визначає й рівень вразливості каналів зв'язку, що виходять з нього. На рис. 3 у розривах каналів показано дріб, у якому чисельник показує пропускну здатність, а знаменник – імовірність компрометації каналу зв'язку.

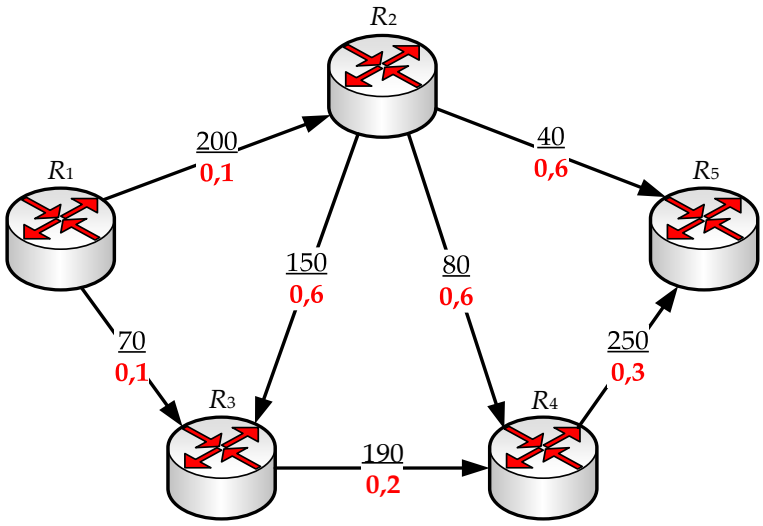

Рис. 3. Імовірності компрометації каналів зв'язку досліджуваного фрагмента структури мережі

Отже, відповідно до виразу (11) для наведеного прикладу розраховано імовірності компрометації шляхів (табл. 3). Водночас імовірність компрометації пакетів потоку, що передається, вздовж множини використаних шляхів згідно з (10) дорівнює $p^1_{E2E} = 0,63$.

Враховуючи все вищезазначене, найменш завантаженим завжди залишався шлях 4. Навіть за умови однакового рівня імовірності використання вразливості другого вузла, який визначає й рівень вразливості каналів зв'язку, що виходять з нього ($E_{2,3}$, $E_{2,4}$, $E_{2,5}$), і того, що канал $E_{2,4}$ має меншу пропускну здатність ніж $E_{2,3}$, більш завантаженим буде завжди шлях 3, оскільки імовірність компрометації шляху 3 менша за імовірність компрометації шляху 4 (табл. 3).

Таблиця 3. Імовірності компрометації шляхів

Характеристика шляхів, що складають мультишлях		Імовірність компрометації шляху
Шлях 1	$R_1 \rightarrow R_2 \rightarrow R_5$	0,64
Шлях 2	$R_1 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$	0,496
Шлях 3	$R_1 \rightarrow R_2 \rightarrow R_4 \rightarrow R_5$	0,748
Шлях 4	$R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$	0,798

Далі у табл. 4 та на рис. 4 показано поведінку *моделі 3* для випадку, коли інтенсивність потоку $\lambda^1 = 100$ пак/с, а співвідношення між ваговими коефіцієнтами метрик продуктивності та мережної безпеки було $R = 100$. Числові розрахунки показали зменшення частки потоку в каналі $E_{2,3}$, якщо зростає ймовірність його компрометації.

Таблиця 4. Розподіл потоку при безпечній QoS-маршрутизації за *моделлю 3*

($\lambda^1 = 100$ пак/с, $R = 100$, $p_{2,3} = 0,1 \div 0,8$)

$p_{2,3}$	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8
Шлях 1	29,8	29,9	30	30,1	30,2	30,3	30,4	30,4
Шлях 2	33	33,4	33,7	34	34,2	34,5	34,7	34,9
Шлях 3	23,7	24	24,2	24,4	24,6	24,7	24,9	25
Шлях 4	13,5	12,7	12,1	11,5	11	10,5	10	9,7

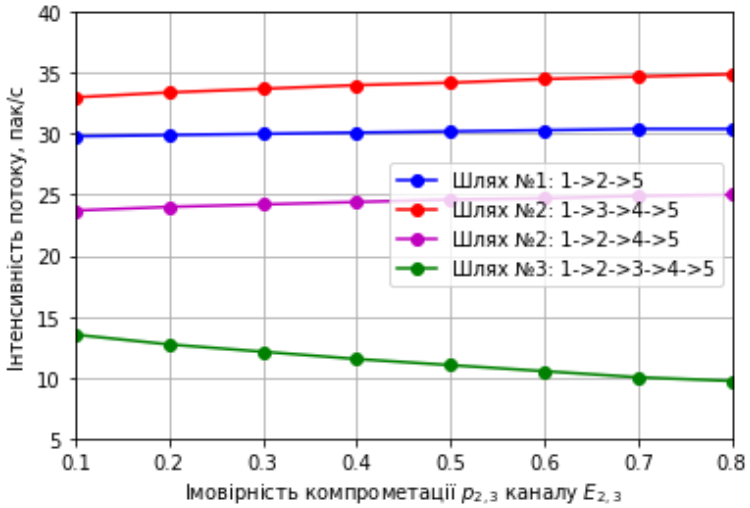

Рис. 4. *Динаміка розподілу потоку при безпечній* QoS-*маршрутизації за моделлю 3* ($\lambda^1 = 100$ пак/с, $R = 100$, $p_{2,3} = 0,1 \div 0,8$)

VI. Порівняльний аналіз моделей безпечної маршрутизації

Далі в табл. 5, 6 та на рис. 5, 6 і 7 наведено результати розв'язання задачі маршрутизації з використанням трьох моделей:

– *модель 1*, вирази (1)-(4);

– *модель 2*, вирази (1)-(3), (5);

– *модель 3*, вирази (1)-(3), (6)-(9).

На цих рисунках у розривах каналів зв'язку вказані (згори донизу) їхні пропускні здатності (пак/с), інтенсивність потоку, що протікає в каналі зв'язку (пак/с), а також *для моделі 1* і *моделі 3* додатково зазначені відповідні вагові коефіцієнти рівня мережної безпеки (імовірності компрометації) *для* кожного каналу зв'язку $E_{i,j} \in E$.

Як показано на рис. 5, унаслідок розв'язання задачі безпечної маршрутизації за допомогою *моделі 1* потік пакетів інтенсивністю $\lambda^1 = 200$ пак/с передавався за всіма чотирма маршрутами (табл. 5 і 6).

На відміну від *моделі 1* і *моделі 3*, під час використання *моделі* 2 потік пакетів інтенсивністю $\lambda^1 = 200$ пак/с передавався *лише* двома маршрутами, найкращими з погляду пропускної здатності (рис. 6, табл. 5 і 6), а саме:

– шлях 3: $R_1 \rightarrow R_2 \rightarrow R_4 \rightarrow R_5$;

– шлях 4: $R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$.

Тоді як рис. 7 демонструє результат розв'язання задачі безпечної QoS- маршрутизації під час використання *моделі 3* із запропонованою модифікацією (комбінованою маршрутною метрикою). Так само передавався потік пакетів інтенсивністю $\lambda^1 = 200$ пак/с, $R = 100$ за всіма чотирма маршрутами у межах досліджуваної структури мережі.

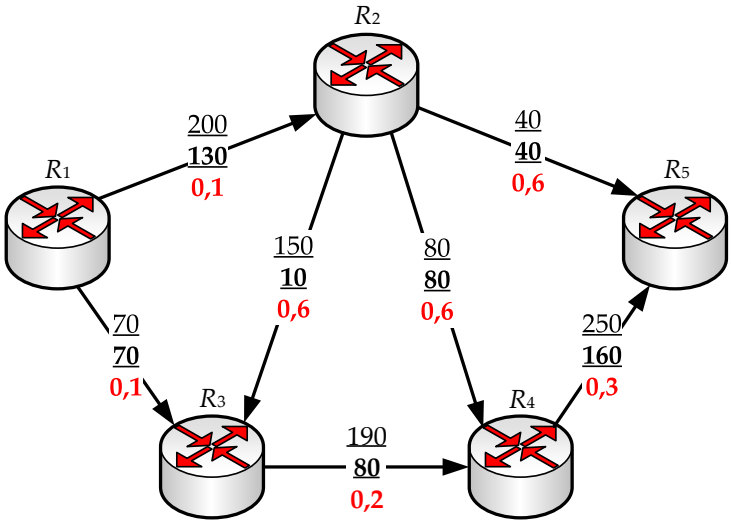

Рис. 5. Результат розв'язання задачі безпечної маршрутизації з використанням *моделі 1*

Таблиця 5. Результати порівняльного аналізу *моделі 1*, *моделі 2* та *моделі 3* ($R = 100$) за умови $\lambda^1 = 200$ пак/с

Канали зв'язку	Пропускна здатність каналу, $\varphi_{i,j}$, пак/с	*Модель 1*		*Модель 2*	*Модель 3*
		Інтенсивність потоку, пак/с	Вагові коефіцієнти $w_{i,j}$	Інтенсивність потоку, пак/с	Інтенсивність потоку, пак/с
$E_{1,2}$	200	130	0,1	200	130
$E_{1,3}$	70	70	0,1	0	70
$E_{2,3}$	150	10	0,6	150	30
$E_{2,4}$	80	80	0,6	50	60
$E_{2,5}$	40	40	0,6	0	40
$E_{3,4}$	190	80	0,2	150	100
$E_{4,5}$	250	160	0,3	200	160

Таблиця 6. Результати порівняльного аналізу розподілу потоку в межах мультишляху під час використання *Моделі 1*, *Моделі 2* та *Моделі* 3 ($R = 100$) за умови $\lambda^1 = 200$ пак/с

№ шляху	Імовірність компрометації шляху	*Модель 1*	*Модель 2*	*Модель 3*
		Інтенсивність потоку, пак/с	Інтенсивність потоку, пак/с	Інтенсивність потоку, пак/с
1	0,64	40	–	40
2	0,496	70	–	70
3	0,748	80	50	60
4	0,798	10	150	30

Проте під час порівняння результатів розподілу потоку, що передається, із застосуванням *моделі 1* і *моделі 3* необхідно звернути увагу, яким чином підпотоки балансуються за каналами $E_{2,3}$ та $E_{2,4}$, що є складовими четвертого та третього шляхів відповідно (табл. 5). Імовірності компрометації пакетів потоку, що передається вздовж множини використаних шляхів, із застосуванням *моделі 1* і *моделі 3* майже однакові (табл. 7). Проте, очевидно, що розподіл підпотоків у випадку *моделі 3* є більш збалансованим (табл. 7, рис. 7). Отже, канальний ресурс найбільш продуктивного четвертого шляху використовується ефективніше. Зі свого боку табл. 7 демонструє результати розрахунку імовірностей компрометації пакетів потоку, що передається вздовж множини використаних шляхів, у разі застосування усіх розглянутих моделей.

Таким чином, *модель 1* і *модель 3* проявляють однакові ймовірності компрометації пакетів потоку, що передається. Тоді як *модель 2*, яка використовує лише два шляхи у розрахованому мультишляху, не зважаючи на те, що вони є найбільш продуктивними, у межах таких самих вихідних даних (структурі мережі та обраних пристроях) має найгіршу ймовірність компрометації пакетів потоку, що передається.

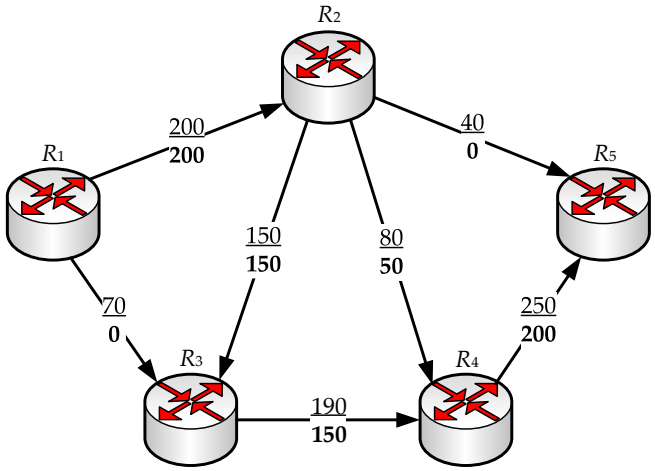

Рис. 6. Результат розв'язання задачі QoS-маршрутизації з використанням *моделі 2*

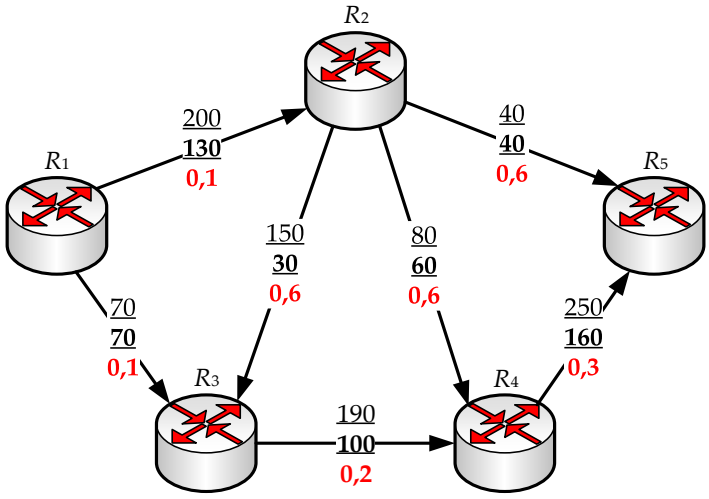

Рис. 7. Результат розв'язання задачі безпечної QoS-маршрутизації з використанням *моделі 3*

Таблиця 7. Порівняння імовірності компрометації пакетів потоку, що передається, вздовж множини використаних шляхів

Модель	Маршрути	p_{E2E}^{1}
модель 1	$R_1 \rightarrow R_2 \rightarrow R_5$ $R_1 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$ $R_1 \rightarrow R_2 \rightarrow R_4 \rightarrow R_5$ $R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$	0,641
модель 2	$R_1 \rightarrow R_2 \rightarrow R_4 \rightarrow R_5$ $R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$	0,786
модель 3	$R_1 \rightarrow R_2 \rightarrow R_5$ $R_1 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$ $R_1 \rightarrow R_2 \rightarrow R_4 \rightarrow R_5$ $R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$	0,646

Висновки

Проведений аналіз вразливостей площини даних SDN і функціональних можливостей засобів маршрутизації щодо протидії можливим атакам показав перспективність використання засобів безпечної маршрутизації на основі базових метрик критичності вразливостей для підвищення рівня мережної безпеки площини даних SDN. Зі свого боку аналіз стандарту CVSS щодо кількісного розрахунку рівня вразливості мережного обладнання довів доцільність його використання під час розробки та дослідження перспективних підходів до безпечної маршрутизації у площині даних програмно-конфігурованих мереж.

У роботі було запропоновано удосконалення існуючої моделі безпечної маршрутизації з урахуванням базових метрик критичності вразливостей. Отже, було модифіковано маршрутні метрики таким чином, щоб отримувана модель набула властивостей безпечної QoS-маршрутизації. Тобто в удосконаленій моделі оптимальний маршрут обирався з урахуванням і базових метрик критичності вразливостей, і пропускної здатності каналів зв'язку, що складають цей маршрут. Крім того, в моделі задіяно квадратичний критерій оптимальності (9) з метою збалансованого розподілу потоків, що передаються в площині даних програмно-конфігурованої мережі, на підпотоки з урахуванням обраної стратегії багатошляхової маршрутизації.

Проведений порівняльний аналіз існуючої моделі безпечної маршрутизації, моделі QoS-маршрутизації з метрикою за аналогією з протоколом OSPF та удосконаленої моделі безпечної QoS-маршрутизації з урахуванням базових метрик критичності вразливостей, довів адекватність і працездатність запропонованої в роботі моделі.

Список літератури

1. *Sabella, A., Irons-Mclean, R., Yannuzzi, M.* (2018), Orchestrating and Automating Security for the Internet of Things: Delivering Advanced Security Capabilities from Edge to Cloud for IoT. Cisco Press, 1008 p.

2. *Kurose, J.F., Ross, K.* (2020), Computer Networking. 8th Edition. Pearson, 775 p.

3. *Плєхова, Г.А.* (2022), "Аналіз засобів маршрутизації щодо підвищення рівня мережної безпеки у програмно-конфігурованих мережах", Проблеми електромагнітної сумісності перспективних безпроводових мереж зв'язку (EMC-2022): матеріали Восьмої Міжнародної науково-технічної конференції, Харків, ХНУРЕ, С. 41–42.

4. *Hoang, D.B., Farahmandian, S.* (2017), "Security of Software-Defined Infrastructures with SDN, NFV, and Cloud Computing Technologies", In Zhu, S., Scott-Hayward, S., Jacquin, L., Hill, R. (eds) Guide to Security in SDN and NFV, Computer Communications and Networks, Springer, Cham, P. 3–32. **DOI**: https://doi.org/10.1007/978-3-319-64653-4_1

5. *Liu, Y., Zhao, B., Zhao, P., Fan, P., Liu, H.* (2019), "A survey: Typical security issues of software-defined networking", China Communications, No. 16(7). P. 13–31. **DOI**: https://doi.org/10.23919/JCC.2019.07.002

6. *Sagare, A.A., Khondoker, R.* (2018), "Security Analysis of SDN Routing Applications", In Khondoker, R. (eds) SDN and NFV Security, Lecture Notes in Networks and Systems, No. 30, Springer, Cham, P. 1–17. **DOI**: https://doi.org/10.1007/978-3-319-71761-6_1

7. *Yeremenko, O., Persikov, M., Lemeshko, V., Altaki, B.* (2021), "Research and development of the secure routing flow-based model with load balancing", Проблеми телекомунікацій, No. 2(29), С. 3–14. **URL**: https://pt.nure.ua/wp-content/uploads/2021/12/212_yeremenko_secure.pdf

8. *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

9. *Lou, W., Kwon, Y.* (2006), "H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks", IEEE Transactions on Vehicular Technology, No. 55(4), P. 1320–1330. **DOI**: https://doi.org/10.1109/TVT.2006.877707

10. *Lou, W., Liu, W., Fang, Y.* (2004), "SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks", INFOCOM 2004: Proceedings of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, Hong Kong, China, 7–11 March, IEEE, P. 2404–2413. **DOI**: https://doi.org/10.1109/INFCOM.2004.1354662

11. *Снегуров, А.В., Чакрян, В.Х.* (2012), "Метод формирования метрик маршрутизации, основанный на рисках информационной безопасности", Системи управління, навігації та зв'язку, No. 4(24), С. 105–110.

12. *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), С. 707–714.

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

14. *Yevdokymenko, M., Yeremenko, O., Shapovalova, A., Shapoval, M., Porokhniak, V., Rogovaya, N.* (2021), "Investigation of the Secure Paths Set Calculation Approach Based on Vulnerability Assessment", Workshop Proceedings of the MoMLeT+DS 2021: 3rd International Workshop on

Modern Machine Learning Technologies and Data Science, June 5, Lviv-Shatsk, Ukraine, P. 207–217. **URL**: http://ceur-ws.org/Vol-2917/paper19.pdf

15. *Stallings, W.* (2018), Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley Professional, 800 p.

16. CVSS v3.1 Examples. FIRST – Forum of Incident Response and Security Teams. **URL**: https://www.first.org/cvss/examples

17. NIST National Vulnerability Database. NVD - Home. **URL**: https://nvd.nist.gov

18. CVSS v3.1 Specification Document. FIRST – Forum of Incident Response and Security Teams. **URL**: https://www.first.org/cvss/v3.1/specification-document

19. CVSS v3.0 User Guide. FIRST – Forum of Incident Response and Security Teams. **URL**: https://www.first.org/cvss/v3.0/user-guide

20. *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, Харків: ХНУРЕ, 198 с. **DOI**: https://doi.org/10.30837/978-966-659-378-1

21. *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), P. 49–52. **DOI**: https://doi.org/10.1145/1179494.1179505