КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.914
УДК 004.738.5:004.056

Чакрян Вадим Хазарович
к.т.н., старший викладач кафедри інфокомунікаційної інженерії імені В.В. Поповського
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID: 0000-0003-4827-9779
vadym.chakrian@nure.ua

Андрушко Дмитро Володимирович
к.т.н., старший викладач кафедри інфокомунікаційної інженерії імені В.В. Поповського
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID: 0009-0004-0749-9729
dmytro.andrushko@nure.ua

Снігуров Аркадій Владиславович
к.т.н., доцент, декан факультету інфокомунікацій
(за сумісництвом доцент кафедри інфокомунікаційної інженерії імені В.В. Поповського)
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID: 0000-0003-1355-7978
arkadii.snihurov@nure.ua

Пшеничних Сергій Васильович
к.т.н., ст. науковий співробітник, доцент кафедри інфокомунікаційної інженерії ім. В.В. Поповського
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID: 0000-0003-0533-2306
serhii.pshenychnykh@nure.ua

АНАЛІЗ МЕТОДІВ РОЗРАХУНКУ МЕТРИКИ ПРОТОКОЛУ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ OSPF З УРАХУВАННЯМ ПАРАМЕТРУ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. У статті розглянуто проблему удосконалення метрик протоколу динамічної маршрутизації OSPF шляхом урахування ризику інформаційної безпеки. Стандартна метрика OSPF орієнтована лише на пропускну здатність каналів і не враховує можливі загрози, що може призвести до компрометації конфіденційності, цілісності чи доступності даних у телекомунікаційних мережах. На основі аналізу сучасних досліджень, присвячених захисту маршрутизації, зокрема з використанням механізмів довіри, криптографії та алгоритмів машинного навчання, визначено доцільність доповнення класичних підходів показниками ризику. У роботі запропоновано три варіанти модифікованих метрик, які дозволяють враховувати рівень ризику вузлів і каналів зв'язку під час вибору маршруту. Для перевірки їх ефективності виконано моделювання на прикладі мережевої топології з чотирма маршрутизаторами, де досліджено зміни оптимальних шляхів за умов різних значень ризику. Результати показали, що один із запропонованих методів забезпечує найкращий баланс між пропускною здатністю та рівнем безпеки, тоді як інші або надмірно чутливі до ризику, або вимагають додаткового налаштування параметрів для практичного застосування. Отримані висновки підтверджують доцільність включення показника ризику інформаційної безпеки у процес маршрутизації, що дозволяє підвищити стійкість мереж до кібератак та покращити надійність функціонування інфраструктури. Подальші дослідження планується спрямувати на розширення експериментальної бази для різних типів мережевих топологій та на розробку методів оптимального налаштування параметрів, що впливають на вагу ризику у метриках.

Ключові слова: OSPF; маршрутизація; метрика; інформаційна безпека; ризик; кібербезпека; телекомунікаційні мережі.

ВСТУП

Протокол динамічної маршрутизації Open Shortest Path First (OSPF) використовується у сучасних IPv4 [**Помилка! Джерело посилання не знайдено.**] та IPv6 [**Помилка! Джерело посилання не знайдено.**] мережах для вибору автоматичного вибору шляху передачі потоку пакетів. Він є одним із найбільш розповсюджених протоколів маршрутизації у сучасних мережах, що забезпечує швидку конвергенцію та ефективне керування трафіком у великих інфраструктурах [**Помилка! Джерело посилання не знайдено.**]. Порівняльні дослідження показують, що хоча інші протоколи, зокрема Enhanced Interior Gateway Routing Protocol (EIGRP), можуть демонструвати швидше відновлення після відмов, саме OSPF забезпечує вищу масштабованість і стійкість у середовищі IPv6 [**Помилка! Джерело посилання не знайдено.**]. Водночас класичні метрики OSPF, побудовані переважно на пропускній здатності каналів, не враховують безпекові аспекти, що може призводити до додаткових ризиків при маршрутизації трафіку [**Помилка! Джерело посилання не знайдено.**]. У цій роботі пропонується розглянути методи розрахунку метрики протоколу OSPF на основі базових параметрів та з урахуванням показнику ризику інформаційної безпеки.

Постановка проблеми. Базова метрика протоколу OSPF не враховує ризики інформаційної безпеки при виборі маршруту передачі потоку пакетів в телекомунікаційній мережі. При цьому, в мережі може існувати більше одного маршруту передачі, а проміжні вузли, які здійснюють маршрутизацію можуть мати різний рівень захищеності від кібератак і мати різну ймовірність бути активно атакованими. Врахування ризику інформаційної безпеки в процесі вибору маршруту передачі потоку пакетів дозволяє вибирати маршрут не тільки на основі параметрів якості передачі, а й враховувати потенційні ризики порушення конфіденційності, цілісності, та доступності інформації.

Аналіз останніх досліджень і публікацій. У статті [**Помилка! Джерело посилання не знайдено.**] розглянуто методи протидії DDoS-атакам у безпроводових сітчастих мережах із використанням OSPF, де запропоновано багатошляхову маршрутизацію, аутентифікацію та криптографічні механізми. Робота підкреслює необхідність доповнення базових механізмів протоколу додатковими засобами захисту, що може стати основою для врахування безпекових параметрів у процесі маршрутизації.

У низці досліджень [**Помилка! Джерело посилання не знайдено.**]–[**Помилка! Джерело посилання не знайдено.**] запропоновано алгоритми побудови маршрутів з урахуванням довіри до вузлів. У статті [**Помилка! Джерело посилання не знайдено.**] описано підхід, що дозволяє уникати недовірених маршрутизаторів, у роботі [**Помилка! Джерело посилання не знайдено.**] наведено метод мінімізації кількості таких вузлів, якщо їх виключення неможливе, а у статті [**Помилка! Джерело посилання не знайдено.**] показано вдосконалений варіант, який забезпечує формування маршрутів виключно через довірені вузли або, за їх відсутності, через маршрути з мінімальною кількістю недовірених. Такі підходи демонструють, що модифікація алгоритму Дейкстри, на якому базується OSPF, може враховувати фактори безпеки під час вибору маршруту.

У роботі [**Помилка! Джерело посилання не знайдено.**] досліджено ефективність різних функцій вартості у OSPF (ступінчастих, лінійних та експоненційних), що дало змогу оцінити їх потенціал для підвищення захищеності маршрутизації за рахунок адаптації метрик до динамічних умов мережі. У статті [**Помилка! Джерело посилання не знайдено.**] розглянуто можливості застосування алгоритмів машинного навчання для класифікації мережних пристроїв за рівнем безпеки, що створює основу для інтеграції

цих даних у процес формування маршрутів. У публікації [**Помилка! Джерело посилання не знайдено.**] узагальнено досвід використання машинного навчання у програмно-конфігурованих мережах, де підкреслено його значення для оптимізації маршрутизації та врахування ризиків.

У дослідженнях [**Помилка! Джерело посилання не знайдено.**], [**Помилка! Джерело посилання не знайдено.**] запропоновано моделі маршрутизації, у яких базові метрики OSPF були доповнені показниками ризику інформаційної безпеки. Показано, що використання таких удосконалених моделей дозволяє формувати маршрути за критерієм «якість–безпека», знижуючи ймовірність компрометації даних і підвищуючи відмовостійкість мереж.

Сучасні дослідження акцентують увагу на різних аспектах удосконалення OSPF — від включення довіри до вузлів та адаптивних функцій вартості до інтеграції алгоритмів машинного навчання й показників ризику інформаційної безпеки.

Мета статті. Проаналізувати підходи до врахування ризику інформаційної безпеки у базовій формулі розрахунку метрики протоколу OSPF при розв’язанні задачі однокритеріальної оптимізації вибору маршруту передачі потоку пакетів в умовах одношляхової маршрутизації в телекомунікаційній мережі.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

В даній роботі розглядається лише модель одношляхової маршрутизації, в якій вирішується задача вибору єдиного оптимального маршруту передачі потоку пакетів (ПП) [**Помилка! Джерело посилання не знайдено.**].

Опишемо структуру телекомунікаційної мережі (ТКМ) за допомогою зваженого орієнтованого графа G=(V,E), де множина вершин V моделює множину вузлів ТКМ, а множина дуг E описує множину каналів зв’язку між ними. Кожній дузі $(i,j)\in E$ відповідає пропускна здатність КЗ $\mu_{i,j}$. Кожному k-му потоку пакетів з множини K відповідає ряд параметрів: λ_k, s_k, r_k — інтенсивність k-го потоку пакетів, вузол-відправник та вузол-отримувач відповідно. Управляючою змінною служить $X^k_{i,j}$, яка характеризує долю інтенсивності k-го потоку пакетів, що передається в каналі зв’язку $(i,j)\in E$.

З метою недопущення перевантажень мережевих вузлів і мережі в цілому необхідно забезпечити виконання умов збереження потоку:

$$\left.\begin{array}{l}\sum_{j:(i,j)\in E} X^k_{i,j} - \sum_{j:(j,i)\in E} X^k_{j,i} = 0, k\in K, i\neq s_k, r_k,\\ \sum_{j:(i,j)\in E} X^k_{i,j} - \sum_{j:(j,i)\in E} X^k_{j,i} = 1, k\in K, i=s_k,\\ \sum_{j:(i,j)\in E} X^k_{i,j} - \sum_{j:(j,i)\in E} X^k_{j,i} = -1, k\in K, i=r_k.\end{array}\right\}, \quad (1)$$

Умова запобігання перевантаження каналів формалізується наступним чином:

$$\sum_{k\in K} \lambda_k \cdot X^k_{i,j} \le \mu_{i,j} \cdot \alpha, (i,j)\in E, \quad (2)$$

де α — верхній поріг використання каналу зв’язку ТКМ.

Відповідно до фізики розв’язуваної задачі при моделюванні одношляхової маршрутизації на змінні $X^k_{i,j}$ накладається наступне обмеження:

$$X^k_{i,j}\in\{0,1\}. \quad (3)$$

В ході оптимізації процесу маршрутизації необхідно мінімізувати цільову функцію, представлену в лінійній формі виду:

$$\min \sum_{(i,j)} M_{i,j} \cdot X_{i,j}, \quad (4)$$

де каналу зв'язку присвоюється метрика $M_{i,j}$.

Завдання одношляхової маршрутизації сформулюються як оптимізаційна задача з критерієм (4) і обмеженнями (1)–(3). Вирішення даної задачі формалізується як задача булевого програмування, або лінійного-програмування відповідно.

Для розрахунку базової метрики протоколу OSPF використаємо наступну формулу:

$$M_{p_{i,j}} = \sum_{k \in p_{i,j}} LC_k, \quad (5)$$

де $M_{p_{i,j}}$ — метрика протоколу OSPF для шляху p при передачі ПП між вузлами i,j; LC_k — вартість каналів зв'язку k, що входять в шлях $p_{i,j}$.

Вартість каналів зв'язку розраховується за наступною формулою:

$$LC_k = \left\lfloor \frac{B_{ref}}{\mu_k} \right\rfloor, \quad (6)$$

де B_{ref} — параметр, що встановлюється адміністратором ТКМ, при цьому стандартно $B_{ref}=10^8$ біт/с; μ_k — параметр реальної пропускної здатності каналів зв'язку (біт/с).

У наведеному способі протокол динамічної маршрутизації OSPF ніяк не враховує ризики інформаційної безпеки при виборі маршруту передачі трафіку.

Удосконалення метрики розрахунку метрики OSPF з урахуванням вимог інформаційної безпеки.

В даній роботі не проводиться аналіз того, як оцінювати ризик інформаційної безпеки. При цьому, якщо ризик розраховується кількісними методами, то він визначається величиною завданих збитків з певною ймовірністю. Для спрощення, щоб оперувати нормалізованим значенням приймемо $R_{p_{i,j}} \in [0;1]$, де $R_{p_{i,j}}$ це ризик інформаційної безпеки шляху p при передачі потоку пакетів між вузлами i,j.

Введемо декілька обмежень. Так як зростання ризику інформаційної безпеки повинно зменшувати ймовірність передачі потоку пакетів по вибраному маршруту, необхідно щоб зростала величина метрики цього маршруту, тобто $M_{p_{i,j}} \uparrow$ при $R_{p_{i,j}} \uparrow$. Варто зазначити, що максимальна метрика шляху для протоколу OSPF це 2^{24}-1, тобто 16777215 — досягнення цього значення вказує на недоступну мережу в мережевих топологіях. В нашому випадку не можна допускати, щоб при врахуванні параметрів ризику інформаційної безпеки в метриці OSPF досягалась ця величина, що визначає ще одне обмеження $M_{max} \leq 16777214$. Також, метрика шляху не повинна бути меншою чи дорівнювати нулю, *тобто* $0 < M_{p_{i,j}} \leq M_{max}$.

З урахуванням вищенаведених обмежень, розглянемо декілька варіацій удосконаленої формули розрахунку метрики протоколу OSPF. Згідно (5), так як метрика маршруту складається з суми метрик каналів зв'язку, які в нього входять, то для удосконалення будемо використовувати метод розрахунку вартості каналів зв'язку (6):

$$LC_k = \left\lfloor \left(\frac{B_{ref}}{\mu_k} \right)^{R_k} \right\rfloor, \quad (7)$$

$$LC_k = \left\lfloor \frac{B_{ref}}{\mu_k^{(1-R_k)}} \right\rfloor, \quad (8)$$

$$LC_k = \left\lfloor \frac{B_{ref}}{\mu_k} \cdot C^{R_k} \right\rfloor, \quad (9)$$

де R_k — це ризик каналу зв'язку k, який розраховується як просте математичне середнє ризиків вузлів, які входять в канал зв'язку k; C — це коефіцієнт, який може задаватись адміністратором ТКМ, щоб визначати ступінь впливу ризику інформаційної

безпеки на метрику, при цьому C≥1, а також його величину потрібно підбирати таким чином, щоб виконувалась нерівність $M_{p_{i,j}} \leq M_{max}$.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Розглянемо використання удосконалених формул метрик на прикладі. Для цього розглянемо наступну топологію ТКМ на рис. 1 нижче.

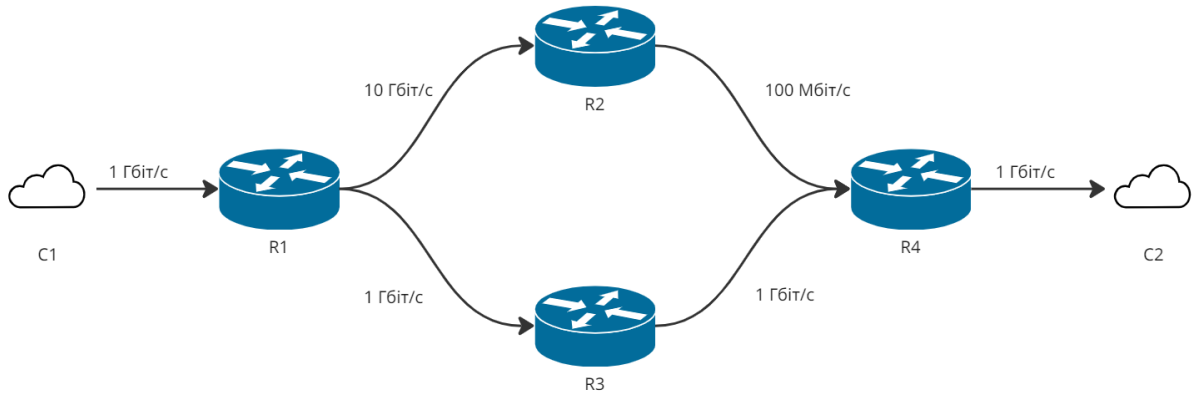

Рис. 1. Топологія ТКМ

У топології на рис. 1 наведені наступні елементи: R1, R2, R3, та R4 — є маршрутизаторами, C1 — відправник потоку пакетів, C2 — виступає приймачем потоку пакетів, а також для кожного каналу зв'язку наведена його пропускна здатність.

Згідно з методом розрахунку метрик маршрутів протоколу OSPF, якщо в даній топології залишити стандартний $B_{ref}=10^8$, *то вартості усіх каналів зв'язку будуть однакові* $LC_k=1$, а значить, що метрики шляхів будуть теж однакові $M_{R1\to R2\to R4\to C2}=M_{R1\to R3\to R4\to C2}=3$. Для того, щоб виправити це приймемо $B_{ref}=\mu_{max}$, *де* μ_{max} *— це найбільша пропускна здатність в заданій зоні роботи протоколу OSPF. Тоді:* $B_{ref}=10^{10}$, $LC_{R1\to R2}=1$, $LC_{R2\to R4}=100$, $LC_{R1\to R3}=LC_{R3\to R4}=LC_{R4\to C2}=10$. Перерахуємо метрики маршрутів: $M_{R1\to R2\to R4\to C2}=111$, $M_{R1\to R3\to R4\to C2}=30$.

Для експерименту, введемо наступні параметри: ризик на маршрутизаторах R1 та R4 завжди дорівнює нулю, коефіцієнт C=256. *Змоделюємо ситуацію, коли ризик на R2 зменшується з кроком 0,1 від 1 до 0, а на R3 навпаки збільшується з кроком 0,1 від 0 до 1. Приймемо, що кожен крок відбувається в момент часу* t_x. *Наведемо значення зміни ризику на маршрутизаторах у табл. 1 нижче.*

Таблиця 1

Зміни параметри ризику в часі

	R_{R1}	R_{R2}	R_{R3}	R_{R4}
t_1	0	1	0.00	0
t_2	0	0.9	0.10	0
t_3	0	0.8	0.20	0
t_4	0	0.7	0.30	0
t_5	0	0.6	0.40	0
t_6	0	0.5	0.50	0

t_7	0	0.4	0.60	0
t_8	0	0.3	0.70	0
t_9	0	0.2	0.80	0
t_{10}	0	0.1	0.90	0
t_{11}	0	0	1.00	0

Нижче наведені графіки (рис. 2, рис. 3, рис. 4) розрахунку метрик маршрутів в залежності від ризику за формулами (7)–(9) відповідно.

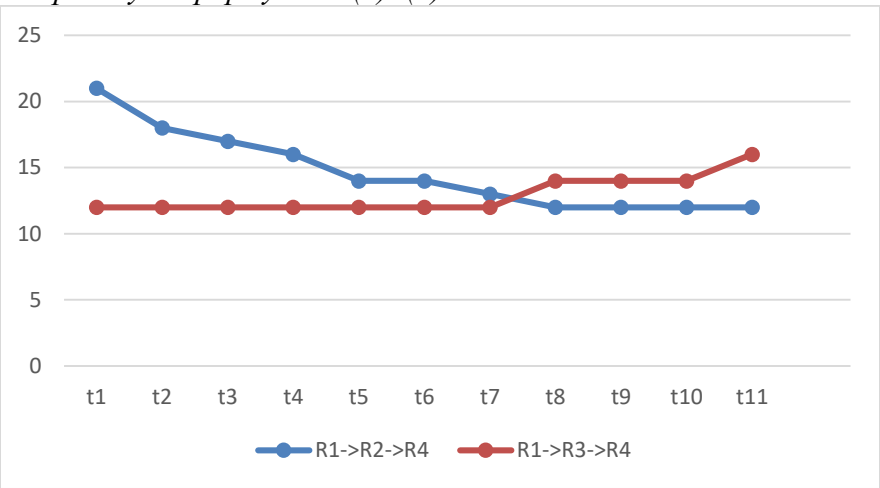

Рис. 2. Графік залежності метрик маршрутів від ризиків інформаційної безпеки на маршрутизаторах R2 та R3 за формулою (7)

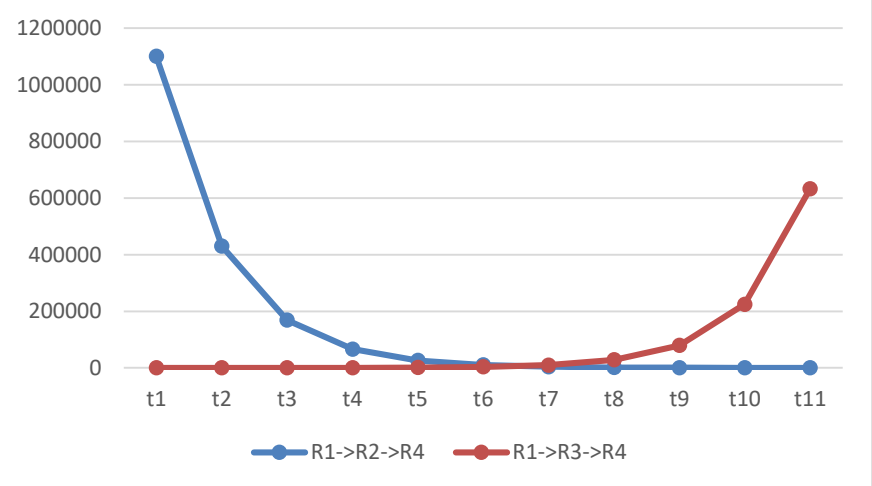

Рис. 3. Графік залежності метрик маршрутів від ризиків інформаційної безпеки на маршрутизаторах R2 та R3 за формулою (8)

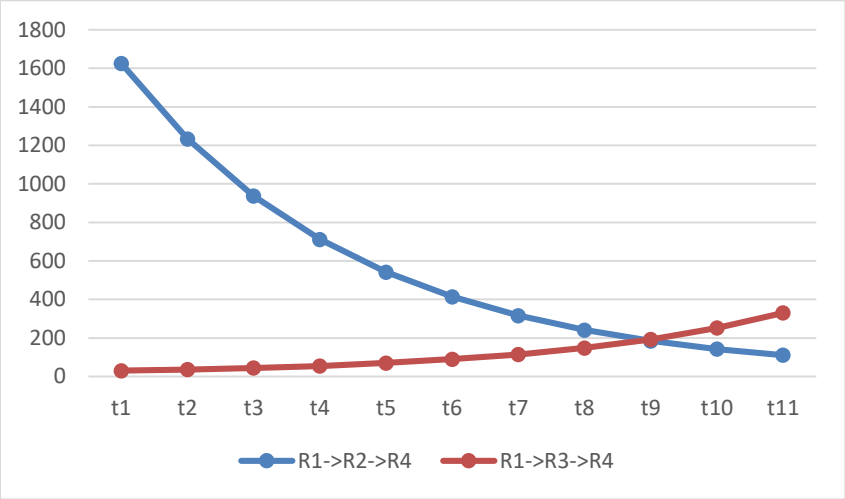

Рис. 4. Графік залежності метрик маршрутів від ризиків інформаційної безпеки на маршрутизаторах R2 та R3 за формулою (9)

Вищенаведені графіки демонструють, що відбувається перемаршрутизація потоку пакетів за новим маршрутом, коли $M_{R1\to R2\to R4}<M_{R1\to R3\to R4}$. Це відбувається у момент t_8 на графіку на рис. 2, у t_7 на рис. 3, і t_9 на рис. 4.

Як бачимо з графіку на рис. 3, метрика приймає значення більше 1000000. При $B_{ref}\gg\mu_k$ і при $R_k\to1$, а також із зростанням кількості маршрутизаторів в ТКМ, значно зростає ймовірність досягти M_{max}. Використання формули (8) має багато обмежень в реальних мережах і не є оптимальним.

При використанні формули (9) перемаршрутизація в заданих умовах відбувається в момент t_9, тобто пізніше, ніж при використанні формули (7). При цьому $M_{R1\to R2\to R4}$ зростала у майже 15 разів, порівняно з метрикою, яка розраховується за стандартною формулою без урахування ризику інформаційної безпеки. У великих топологіях ТКМ і при $B_{ref}\gg\mu_k$ та $R_k\to1$, значно зростає ймовірність досягти M_{max}. Тому, в даному випадку дуже важливо вірно підібрати значення коефіцієнту С. Обмеженням для коефіцієнту може виступати наступне:

$$C_{max}\leq\frac{M_{max}}{M_{max_{area}}}, \tag{10}$$

де $M_{max_{area}}$ — максимальна метрика будь-якого маршруту в заданій ТКМ.

Якщо С буде замалим, тоді ризик інформаційної безпеки може не мати достатньо впливу на метрику, щоб відбувалась перемаршрутизація по більш безпечним маршрутам. Коректний вибір значення коефіцієнту С потребує додаткових досліджень, які будуть проведені в майбутньому.

В заданих умовах найбільш підходящою формулою розрахунку метрики з урахуванням параметру ризику інформаційної безпеки є формула (7). Але її обмеження полягає в тому, що в умовах коли $B_{ref}\leq\mu_k$, вартості каналів LC_k будуть дорівнювати 1, і тоді показник ризику інформаційної безпеки буде мати обмежений або відсутній вплив на розрахунок метрик маршрутів. Також потребується окреме дослідження цієї формули в ТКМ, в яких присутні канали зв'язку з великою пропускною здатністю і з дуже малою пропускною здатністю, наприклад, з різницею між ними у 10000 разів (10 Гбіт/с і 1,544 Мбіт/с).

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Протокол OSPF залишається одним з найпоширеніших серед протоколів внутрішньої динамічної маршрутизації. При цьому стандартна метрика протоколу OSPF, на основні якої вибирається оптимальний маршрут передачі потоку пакетів в мережі не враховує ризики інформаційної безпеки, що може призвести до порушення конфіденційності, цілісності, або доступності даних в заданій ТКМ. Цю задачу можна вирішувати різними методами та підходами, що було продемонстровано під час аналізу сучасних досліджень на цю тему.

В даній роботі було запропоновано проаналізувати удосконалені методи розрахунку метрики протоколу OSPF, які враховують ризик інформаційної безпеки вузлів-маршрутизаторів та дозволяють вибирати оптимальний маршрут на основі базових параметрів метрики і параметру ризику. При цьому, в даній роботи, розглядалась лише модель одношляхової маршрутизації потоку пакетів.

В ході проведення дослідження були отримані наступні результати:

- запропоновано три удосконалені метода врахування показнику ризику у формулі розрахунку метрики протоколу OSPF;
- проведено моделювання процесу вибору оптимального маршруту передачі потоку пакетів в заданій ТКМ при використанні запропонованих удосконалених методів розрахунку метрик маршрутів;
- було виявлено, що для заданих умов, згідно з накладеними обмеженнями, найкращим методом виявився розрахунок метрики за формулою (7);
- при цьому, було встановлено, що кожен з методів має свої недоліки і потребує більш детального аналізу та додаткових експериментів з моделюванням вибору оптимального маршруту передачі потоку пакетів в різних ТКМ з різними початковими мовами.

В якості подальших напрямків дослідження пропонується вибрати наступні:

- провести більше експериментів з моделювання вибору оптимального маршруту передачі потоку пакетів в різних ТКМ з різними початковими параметрами для методі розрахунку метрики на основі формули (7), щоб визначити потенційні додаткові обмеження використання цього методу окрім тих, які були описані в даній роботі;
- в методі розрахунку метрики за формулою (9) провести дослідження по вибору оптимальної величини коефіцієнту C.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Moy, J. (1998). *OSPF Version 2* (RFC 2328). Internet Engineering Task Force. https://doi.org/10.17487/RFC2328
2. Coltun, R., Ferguson, D., & Moy, J. (2008). *OSPF for IPv6* (RFC 5340). Internet Engineering Task Force. https://doi.org/10.17487/RFC5340
3. Åkerberg, L., & Johansson Baurne, V. (2024). *Practical analysis and simulation of OSPF protocol vulnerabilities* (Master's thesis). KTH Royal Institute of Technology.
4. Shahid, K., Ahmad, S. N., & Rizvi, S. T. H. (2024). Optimizing network performance: A comparative analysis of EIGRP, OSPF, and BGP in IPv6-based load-sharing and link-failover systems. *Future Internet, 16*(9), 339. https://doi.org/10.3390/fi1609033
5. Thaenchaikun, C., & Kanjanasit, K. (2025). A comparative study of OSPF metrics in routing algorithms for dynamic path selection in network security. *ASEAN Journal of Science and Technology Report, 28*(2), e256556. https://doi.org/10.55164/ajstr.v28i2.25655

6. Hassan, A., Sharma, R., & Singh, G. (2019). Preventing and isolating distributed denial of service (DDoS) attack in wireless mesh networks (WMNs). *International Journal of Innovative Technology and Exploring Engineering*, *8*(9S), 447–452. https://doi.org/10.35940/ijitee.I1071.0789S1
7. Obelovska, K., Snaichuk, Y., Selecky, J., Liskevych, R., & Valkova, T. (2023). An approach toward packet routing in the OSPF-based network with a distrustful router. *WSEAS Transactions on Information Science and Applications, 20*(45), 432–441. https://doi.org/10.37394/23209.2023.20.45
8. Obelovska, K., Tkachuk, O., & Snaichuk, Y. (2024). Minimizing the number of distrustful nodes on the path of IP packet transmission. *Computation*, *12*(5), 91. https://doi.org/10.3390/computation12050091
9. Obelovska, K., Snaichuk, Y., Liskevych, O., Mitoulis, S.-A., & Liskevych, R. (2025). Mitigation of risks associated with distrustful routers in OSPF networks – An enhanced method. *Computers, 14*(2), 43. https://doi.org/10.3390/computers14020043
10. Yeremenko, O. S., & Pliekhova, H. A. (2022). Doslidzhennia modelei bezpechnoi marshrutyzatsii na osnovi bazovykh metryk urazlyvostei u merezhakh SDN [Research of secure routing models based on basic vulnerability metrics in SDN networks]. *Problemy Telekomunikatsii*, *2*(31), 34–41. http://pt.nure.ua/3
11. Maiba, M. A., & Yeremenko, O. S. (2023). Rozviazannia zadachi klasyfikatsii merezhnykh prystroiv na osnovi parametriv bezpeky za dopomohoiu mashynnoho navchannia [Solving the problem of classifying network devices based on security parameters using machine learning]. *Problemy Telekomunikatsii*, *2*(33), 44–50. http://pt.nure.ua/3
12. Amin, R., Rojas, E., Aqdus, A., Ramzan, S., Casillas-Perez, D., & Arco, J. M. (2021). A survey on machine learning techniques for routing optimization in SDN. *IEEE Access, 9*, 104582–104604. https://doi.org/10.1109/ACCESS.2021.309909
13. Chakryan, V. Kh. (2017). *Modeli ta metody marshrutyzatsii trafiku v telekomunikatsiinykh merezhakh z urakhuvanniam vymoh informatsiinoi bezpeky* [Models and methods of traffic routing in telecommunication networks considering information security requirements] (PhD dissertation). Kharkiv National University of Radio Electronics.
14. Lemeshko, O. V., Yeremenko, O. S., & Yevdokymenko, M. O. (2021). Fault-tolerant multicast routing in an infocommunication network with path and bandwidth protection. *Problems of Telecommunication, 1*(28), 36–43. http://pt.nure.ua/28

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Chakrian Vadym Khazarovych
PhD (Eng.), Senior Lecturer of the Department of Infocommunication Engineering named after V.V. Popovskyi
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID ID: 0000-0003-4827-9779
vadym.chakrian@nure.ua

Andrushko Dmytro Volodymyrovych
PhD (Eng.), Senior Lecturer of the Department of Infocommunication Engineering named after V.V. Popovskyi
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID ID: 0009-0004-0749-9729
dmytro.andrushko@nure.ua

Snihurov Arkadii Vladyslavovych
PhD (Eng.), Associate Professor, Dean of the Faculty of Infocommunications (part-time Associate Professor of the Department of Infocommunication Engineering named after V.V. Popovskyi)
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID ID: 0000-0003-1355-7978
arkadii.snihurov@nure.ua

Pshenychnykh Serhii Vasylovych
Ph.D. (Engineering), Senior Researcher,
Associate Professor of the V.V. Popovskyy Department of Infocommunication Engineering
Kharkiv National University of Radio Electronics. Ukraine, Kharkiv, Ukraine
ORCID ID: 0000-0003-0533-2306
serhii.pshenychnykh@nure.ua

ANALYSIS OF METHODS FOR CALCULATING THE OSPF DYNAMIC ROUTING PROTOCOL METRIC CONSIDERING INFORMATION SECURITY RISK

Abstract. This paper addresses the problem of improving the metrics of the OSPF dynamic routing protocol by incorporating information security risk. The standard OSPF metric is based solely on channel bandwidth and does not account for potential threats, which may compromise the confidentiality, integrity, or availability of data in telecommunication networks. Based on the analysis of recent research focused on secure routing, such as the use of trust mechanisms, cryptographic techniques, and machine learning algorithms, the feasibility of enhancing traditional approaches with risk indicators is substantiated. The study proposes three modified metric variants that integrate node and link risk levels into the routing decision process. To evaluate their effectiveness, a simulation was performed on a network topology with four routers, analyzing how optimal paths change under varying risk conditions. The results demonstrate that one of the proposed methods ensures the best balance between bandwidth efficiency and security, while others are either overly sensitive to risk or require careful parameter adjustment to be practical. The findings confirm the importance of including information security risk in the routing process, which significantly strengthens network resilience against cyberattacks and improves overall infrastructure reliability. Future work will focus on expanding the experimental base with diverse topologies and traffic parameters, as well as developing methods for optimal parameter tuning to balance the influence of risk in OSPF metrics.

Keywords: OSPF; routing; metric; information security; risk; cybersecurity; telecommunication networks.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Moy, J. (1998). *OSPF Version 2* (RFC 2328). Internet Engineering Task Force. https://doi.org/10.17487/RFC2328
2. Coltun, R., Ferguson, D., & Moy, J. (2008). *OSPF for IPv6* (RFC 5340). Internet Engineering Task Force. https://doi.org/10.17487/RFC5340

3. Åkerberg, L., & Johansson Baurne, V. (2024). *Practical analysis and simulation of OSPF protocol vulnerabilities* (Master's thesis). KTH Royal Institute of Technology.
4. Shahid, K., Ahmad, S. N., & Rizvi, S. T. H. (2024). Optimizing network performance: A comparative analysis of EIGRP, OSPF, and BGP in IPv6-based load-sharing and link-failover systems. *Future Internet, 16*(9), 339. https://doi.org/10.3390/fi1609033
5. Thaenchaikun, C., & Kanjanasit, K. (2025). A comparative study of OSPF metrics in routing algorithms for dynamic path selection in network security. *ASEAN Journal of Science and Technology Report, 28*(2), e256556. https://doi.org/10.55164/ajstr.v28i2.25655
6. Hassan, A., Sharma, R., & Singh, G. (2019). Preventing and isolating distributed denial of service (DDoS) attack in wireless mesh networks (WMNs). *International Journal of Innovative Technology and Exploring Engineering, 8*(9S), 447–452. https://doi.org/10.35940/ijitee.I1071.0789S1
7. Obelovska, K., Snaichuk, Y., Selecky, J., Liskevych, R., & Valkova, T. (2023). An approach toward packet routing in the OSPF-based network with a distrustful router. *WSEAS Transactions on Information Science and Applications, 20*(45), 432–441. https://doi.org/10.37394/23209.2023.20.45
8. Obelovska, K., Tkachuk, O., & Snaichuk, Y. (2024). Minimizing the number of distrustful nodes on the path of IP packet transmission. *Computation, 12*(5), 91. https://doi.org/10.3390/computation12050091
9. Obelovska, K., Snaichuk, Y., Liskevych, O., Mitoulis, S.-A., & Liskevych, R. (2025). Mitigation of risks associated with distrustful routers in OSPF networks – An enhanced method. *Computers, 14*(2), 43. https://doi.org/10.3390/computers14020043
10. Yeremenko, O. S., & Pliekhova, H. A. (2022). Doslidzhennia modelei bezpechnoi marshrutyzatsii na osnovi bazovykh metryk urazlyvostei u merezhakh SDN [Research of secure routing models based on basic vulnerability metrics in SDN networks]. *Problemy Telekomunikatsii, 2*(31), 34–41. http://pt.nure.ua/3
11. Maiba, M. A., & Yeremenko, O. S. (2023). Rozviazannia zadachi klasyfikatsii merezhnykh prystroiv na osnovi parametriv bezpeky za dopomohoiu mashynnoho navchannia [Solving the problem of classifying network devices based on security parameters using machine learning]. *Problemy Telekomunikatsii, 2*(33), 44–50. http://pt.nure.ua/3
12. Amin, R., Rojas, E., Aqdus, A., Ramzan, S., Casillas-Perez, D., & Arco, J. M. (2021). A survey on machine learning techniques for routing optimization in SDN. *IEEE Access, 9*, 104582–104604. https://doi.org/10.1109/ACCESS.2021.309909
13. Chakryan, V. Kh. (2017). *Modeli ta metody marshrutyzatsii trafiku v telekomunikatsiinykh merezhakh z urakhuvanniam vymoh informatsiinoi bezpeky* [Models and methods of traffic routing in telecommunication networks considering information security requirements] (PhD dissertation). Kharkiv National University of Radio Electronics.
14. Lemeshko, O. V., Yeremenko, O. S., & Yevdokymenko, M. O. (2021). Fault-tolerant multicast routing in an infocommunication network with path and bandwidth protection. *Problems of Telecommunication, 1*(28), 36–43. http://pt.nure.ua/28