УДК 004.056:621.391

АДАПТИВНА МАРШРУТИЗАЦІЯ В SD-WAN З ВРАХУВАННЯМ ПОКАЗНИКІВ МЕРЕЖНОЇ БЕЗПЕКИ

Порохняк В. Ю., Момот В. С.
e-mail: volodymyr.porokhniak@nure.ua, vladyslav.momot1@nure.ua
Науковий керівник – д.т.н., проф. Лемешко О. В.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського
м. Харків, Україна

This paper proposes an adaptive secure routing method in SD-WAN based on continuous vulnerability analysis of edge devices. The SDN controller uses information from public vulnerability intelligence sources (such as NVD, CVE, or similar databases) and CVSS metrics to dynamically redistribute traffic across edge devices while considering channel capacity limitations. The approach was tested in Mininet emulation on a topology with eight edge devices. The results demonstrate effective traffic redistribution and a significant reduction of the integral network security risk index while preserving overall network throughput.

У сучасних територіально-розподілених мережах передавання даних маршрутизація здебільшого здійснюється за допомогою розподілених протоколів, таких як BGP, OSPF або EIGRP. У такій архітектурі кожен маршрутизатор приймає рішення щодо вибору маршруту на основі локальної інформації про стан мережі. Подібний підхід має певні обмеження, зокрема відсутність централізованого контролю топології мережі та складність реалізації комплексних політик керування трафіком і безпекою.

Технологія Software-Defined Wide Area Network (SD-WAN) дозволяє реалізувати централізоване управління мережею за допомогою SDN-контролера, який має глобальне уявлення про топологію мережі та стан каналів зв’язку [1]. Це створює можливість застосування адаптивних алгоритмів маршрутизації, у яких під час вибору маршрутів можуть враховуватися не лише параметри якості обслуговування, але й показники інформаційної безпеки мережевих вузлів.

Підходи до врахування рівня безпеки мережевих вузлів під час балансування навантаження досліджено у роботі [2], де розглянуто систему рішень на основі моделей Security-Aware Traffic Engineering (SATE) та Security Metrics Traffic Engineering (SecMetrTE). У зазначеній роботі проведено порівняльний аналіз цих моделей, які дозволяють виконувати балансування навантаження між мережевими вузлами з урахуванням рівня їх інформаційної безпеки.

У даній роботі розглядається застосування подібного підходу в архітектурі SD-WAN, де функції прийняття рішень щодо маршрутизації реалізуються централізованим SDN-контролером. Контролер формує політики маршрутизації на основі глобальної інформації про стан мережі та

параметри каналів зв’язку. Оцінювання рівня безпеки вузлів виконується із використанням даних про відомі вразливості, отриманих з відкритих баз даних. Кількісна характеристика рівня ризику визначається за допомогою метрик Common Vulnerability Scoring System (CVSS), що дозволяють оцінити критичність вразливостей та їх вплив на безпеку мережевих вузлів [3].

Запропонований підхід передбачає адаптивний перерозподіл трафіку між доступними маршрутами залежно від рівня безпеки вузлів. На відміну від бінарних механізмів, за яких вузли з виявленими вразливостями повністю виключаються з маршрутизації, використовується більш гнучкий підхід. Вузли з підвищеним рівнем вразливості не блокуються повністю, але використовуються менш інтенсивно під час передавання трафіку. Це дозволяє зменшити навантаження на потенційно небезпечні вузли, зберігаючи при цьому стабільність функціонування мережі.

Дослідження ефективності запропонованого підходу проведено шляхом моделювання у середовищі Mininet з використанням програмного комутатора Open vSwitch. У межах експерименту було сформовано тестову топологію мережі, що включає вузли доступу та транзитні вузли, з’єднані каналами різної пропускної здатності. Аналіз поведінки алгоритму виконувався для декількох експериментальних сценаріїв, у яких використовувалася однакова топологія мережі та однаковий обсяг вхідного трафіку, але змінювався розподіл значень CVSS між мережевими вузлами. Результати експериментального дослідження наведено на рисунку 1.

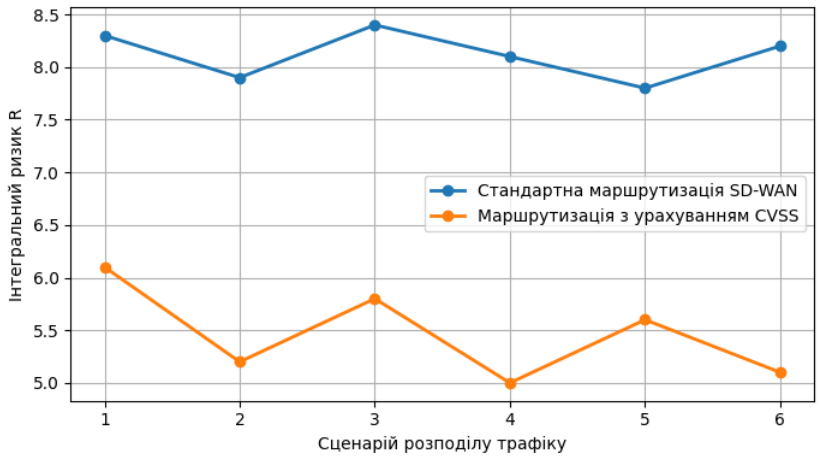

Рисунок 1 — Порівняння інтегрального ризику інформаційної безпеки мережі при стандартній маршрутизації та при використанні адаптивного підходу.

Для кількісного оцінювання рівня інформаційної безпеки мережі використовувався інтегральний показник ризику, який враховує частку трафіку, що проходить через кожний вузол мережі, а також значення метрики CVSS для відповідного вузла. Як показано на рисунку 1, застосування адаптивної маршрутизації дозволяє зменшити інтегральний ризик

інформаційної безпеки мережі приблизно на 28 % без зменшення загального обсягу переданого трафіку.

Таким чином, запропонований підхід дозволяє враховувати рівень безпеки мережевих вузлів під час маршрутизації трафіку в архітектурі SD-WAN. Інтеграція метрик вразливостей у процес керування маршрутизацією забезпечує зниження ризиків інформаційної безпеки без погіршення продуктивності мережі. Отримані результати підтверджують доцільність використання безпеково-орієнтованих механізмів керування трафіком у програмно-керованих мережах.

Список використаних джерел:

1. Ouamri M. A., Alharbi T., Singh D., Sylia Z. A comprehensive survey on software-defined wide area network (SD-WAN): principles, opportunities and future challenges. The Journal of Supercomputing. 2025. Vol. 81, Article 291.

2. Lemeshko O., Yeremenko O., Yevdokymenko M., Porokhniak V., Harkusha S., Harkusha O. System of Routing Solutions Based on Security-Aware Traffic Engineering Models. Advancements in Cybersecurity: Next-Generation Systems and Applications. CRC Press. 2025. pp. 253–271. DOI: https://doi.org/10.1201/9781003546153-11

3. Common Vulnerability Scoring System v3.1: Specification Document. FIRST : вебсайт. URL: https://www.first.org/cvss/v3.1/specification-document (дата звернення: 05.03.2026).