Proceedings of the XIV International Scientific and Technical Conference of Young Scientists and Students “Current Issues of Modern Technologies”, 11-12 December 2025, Ternopil, 302-304. PE Palianytsia V.A. [in Ukrainian].

2. Banakh, R., Nyemkova, E., Justice, C., Piskozub, A., & Lakh, Y. Data Mining Approach for Evil Twin Attack Identification in Wi-Fi Networks. Data, 2024, vol. 9(10), p. 119.

Налаштування безпечної мережевої інфраструктури для балансування навантаження та відмовостійкості

УДК 004.7:004.056

Вікторія Ваврічен[1], Тарас Лобур[2]

Тернопільський національний технічний університет імені Івана Пулюя, [1]viktoriavavrichen@gmail.com, [2]lobur_t@tntu.edu.ua

У сучасних комп’ютерних мережах важливим завданням є забезпечення стабільного й безпечного доступу до Інтернету та безперервної передачі даних. Для організацій, які використовують хмарні сервіси, відеозв’язок, віддалене адміністрування та інші онлайн-ресурси, навіть короткочасна втрата з’єднання може спричинити порушення робочих процесів. Тому актуальним завданням є використання кількох незалежних каналів зв’язку для балансування навантаження та автоматичного перемикання на резервний канал.

Під час дослідження було використано VMware Workstation, у якому створено віртуальне тестове середовище. VMware Workstation дозволяє використовувати віртуальні мережеві адаптери, комутатори та окремі віртуальні мережі, що є зручним для тестування мережевих сценаріїв, зокрема пропускної здатності, стабільності та безпеки з’єднання. Основним мережевим пристроєм виступив MikroTik RouterOS CHR.

У тестовому середовищі було змодельовано мережеву інфраструктуру з трьома незалежними каналами зв’язку, зокрема основний WAN-канал, Starlink та LTE як резервне підключення. На початковому етапі було виконано базове налаштування MikroTik RouterOS: призначено IP-адреси інтерфейсам, налаштовано шлюзи, DNS, локальну мережу та правила NAT [1]. NAT використовувались для забезпечення безпечного доступу внутрішньої мережі до зовнішніх ресурсів через кожен з каналів зв’язку. Наступним етапом було застосовано механізм Mangle з використанням алгоритму per-connection-classifier для реалізації балансування навантаження, що дало можливість розподілити трафік на три частини. Далі виконано маркування з’єднання і пакетів відповідно до таблиць маршрутизації, які забезпечують рівномірний розподіл трафіку між усіма трьома каналами, що забезпечує коректну маршрутизацію навіть у випадку відмови одного з них.

Після налаштування балансування навантаження та відмовостійкості на базі MikroTik RouterOS було проведено моніторинг мережевого трафіку. Для цього використовувалися такі інструменти, як Ping, Tracert, SpeedTest, а також Wireshark для глибшого аналізу пропускної здатності, стабільності та безпеки

з'єднання [2]. Було проаналізовано фактичне проходження трафіку через різні інтерфейси, що дозволило оцінити коректність маршрутів, в тому числі їх легітимність, NAT та Mangle-правил, балансування навантаження та відмовостійкості. Під час моніторингу також аналізувалися показники якості з'єднання: затримка, втрата пакетів, перевантаження каналів, помилки конфігурації та пропускна здатність, що дозволило оцінити, який канал працює стабільніше, як поводиться мережа під час навантаження та чи виникають затримки під час перемикання на резервний канал.

Результати тестування підтвердили відсутність втрат пакетів (0%) і стабільну відповідь від усіх трьох каналів зв'язку (рис.1), що свідчить про коректність реалізованих налаштувань інтерфейсів, відсутність втрати пакетів і зміни маршруту, правил Mangle та NAT для кожного активного підключення.

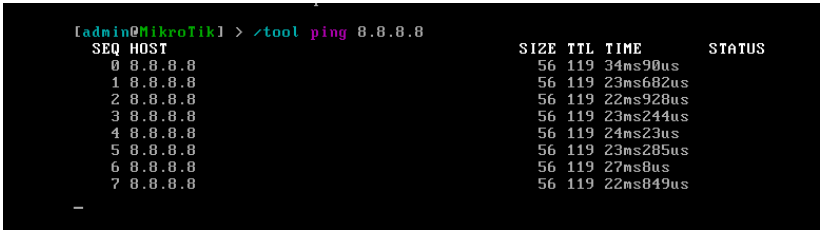

Рис.1. Результати тестування стабільності каналів зв'язку

Для тестування механізму відмовостійкості змодельовано сценарій, коли при відключенні одного з інтерфейсів трафік автоматично перенаправляється через інші канали зв'язку, що забезпечує безперервність з'єднання. У MikroTik RouterOS відмовостійкість використовується для резервування WAN-з'єднання та автоматичного перемикання на інший канал у разі відмови основного (рис.2).

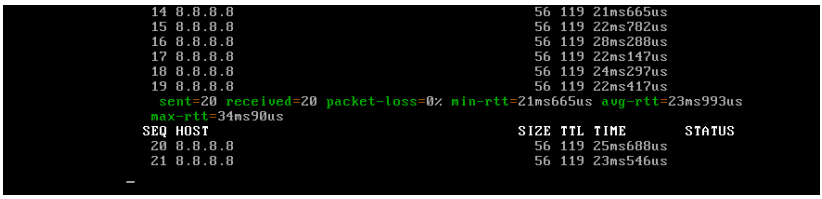

Рис.2. Результати тестування механізму відмовостійкості

Отже, у результаті роботи було налаштовано віртуальну мережеву інфраструктуру на базі MikroTik RouterOS з трьома незалежними каналами зв'язку, реалізовано балансування навантаження та механізм автоматичного перемикання на резервний канал. Результати тестування свідчать, що поєднання балансування навантаження і відмовостійкості дозволяє підвищити стабільність та безпеку мережевої інфраструктури. Балансування навантаження забезпечує ефективніше використання кількох каналів, а резервування дозволяє зберегти доступ до Інтернету у разі відмови одного з підключень. Проведено моніторинг

пропускної здатності, аналізу затримок, оцінено роботу каналів і виявлено особливості проходження пакетів у багатоканальній мережі.

1. O. Mishko, D. Matiuk, M. Derkach, Security of Remote IoT System Management by Integrating Firewall Configuration into Tunneled Traffic, Sci. J. TNTU, 115(3) (2024) 122–129.
2. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T. (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, 1-11.

Підготовка фахівців з кібербезпеки в умовах розвитку штучного інтелекту: необхідність посилення фізичного та радіотехнічного компонентів освіти

УДК 004.056:37.091.3

Сергій Семендяй

Національний університет "Чернігівська політехніка", serhii_semendiai@icloud.com

Сучасний розвиток технологій штучного інтелекту суттєво трансформує підходи до підготовки фахівців у сфері інформаційних технологій та кібербезпеки [1]. Значна частина завдань, пов'язаних із програмуванням, автоматизацією аналізу коду, генерацією конфігурацій та навіть пошуком вразливостей, дедалі активніше виконується із використанням інтелектуальних систем. Це призводить до зміни вимог до професійних компетентностей майбутніх фахівців. Водночас існує категорія знань та практичних навичок, які не можуть бути повністю замінені засобами штучного інтелекту, оскільки вони безпосередньо пов'язані з фізичними процесами поширення сигналів, особливостями роботи апаратури та реальними характеристиками середовищ передавання інформації.

Освітні програми спеціальності «Кібербезпека та захист інформації» традиційно містять дисципліни, пов'язані з технічним захистом інформації, безпекою бездротових і мобільних систем, виявленням технічних каналів витоку інформації та фізичними основами технічних засобів розвідки. Саме ці дисципліни формують у студентів розуміння того, що будь-яка інформаційна система функціонує не лише на програмному чи мережевому рівні, а й у реальному фізичному середовищі, де існують електромагнітні поля, паразитні випромінювання, наведення, побічні електромагнітні випромінювання та інші фактори, здатні створювати додаткові загрози безпеці інформації.

У сучасних умовах особливого значення набуває підготовка фахівців, які здатні працювати із вимірювальним обладнанням та спеціалізованими комплексами технічного контролю. Йдеться про використання аналізаторів спектру, SDR-платформ «HackRF» та Ettus Research USRP, нелінійних локаторів, детекторів поля, детекторів бездротових протоколів, а також спеціалізованих пошукових комплексів, зокрема типу «ANDRE» та «Delta». Ефективне використання таких засобів вимагає не лише теоретичних знань, а й