УДК 621.391:004.056 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.024

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Лемешко В.О., Персіков М.А.
Науковий керівник – д.т.н., проф. Єременко О.С.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
e-mail: valentyn.lemeshko@nure.ua, mykhailo.persikov@nure.ua

This work is devoted to determining the features of implementing secure routing in information and communication systems. The importance of ensuring information security at all seven OSI model layers is noted. At the Network Layer, an increasingly important role in ensuring network security indicators will be assigned to routing protocols, which should adapt to the realities of today and, when forming routing metrics, take into account, along with the Quality of Service indicators, network security metrics. In addition, when configuring routers and routing protocols, it is also necessary to use existing tools to increase network security.

Забезпечення інформаційної безпеки – це складна та багатоаспектна проблема, яка для успішного рішення вимагає скоординованої роботи щодо використання наявних організаційних та технічних ресурсів на всіх етапах її проходження та обробки. Важливе місце у передачі інформації відводиться інформаційно-комунікаційним системам (ІКС), основою яких останнім часом є програмно-конфігуровані мережі (Software-defined Networking, SDN). Тому в SDN для забезпечення безпеки інформації намагаються задіяти функціонал всіх семи рівнів моделі OSI (Open Systems Interconnection) [1].

На мережному рівні все більша роль у забезпеченні показників мережної безпеки буде відводитись протоколам маршрутизації, які повинні адаптуватись до реалій сьогодення та при формуванні маршрутних метрик враховувати поруч з показниками якості обслуговування (Quality of service, QoS) додатково й мережні показники, які пов’язані з інформаційною безпекою – ймовірність компрометації маршрутизатора, каналу, маршруту, ризики інформаційної безпеки тощо [2, 3]. Прикладом подібного вдосконалення з адаптацією до стану мережі є пропрієтарний протокол EIGRP (Enhanced Interior Gateway Routing Protocol), запропонований компанією Cisco [2]. Саме цей протокол дозволяє формувати у реальному часі композитні метрики, які зважено враховують різноманітні мережні показники – від пропускної здатності інтерфейсів та їхньої завантаженості, до затримок та рівня втрат пакетів на цих інтерфейсах. Опосередковано при розрахунку маршрутної метрики також враховується й кількість хопів (переприйомів пакетів) вздовж маршруту. У оновленій версії протоколу

EIGRP з’явився шостий показник, який за необхідністю адміністратор може прив’язати до того чи іншого показника мережної безпеки. Варіюючи ваговими коефіцієнтами $k_1 \div k_6$ адміністратор зможе встановлювати ієрархію впливу QoS-показників та/або показників мережної безпеки на процес визначення оптимального маршруту.

Сформовані подібним чином маршрутні метрики можуть бути використані як в уже класичних алгоритмах розрахунку шляхів DUAL, Дійкстри та Беллмана-Форда, так і у більш перспективних потокових моделях та методах безпечної маршрутизації, в яких, крім мережних показників, додатково враховуються ще й характеристики мережного трафіка [2, 3]. Це є дуже важливим з погляду того, що вимоги до рівня конфіденційності різних повідомлень, пакетів чи потоків можуть суттєво відрізнятись.

З іншого боку, не варто забувати, що процес маршрутизації сам по собі є досить цікавим для зловмисників об’єктом для компрометації у результаті успішно організованих атак і вторгнень. На жаль, і маршрутизатори, як елемент апаратного забезпечення ІКС, і самі протоколи маршрутизації, як елемент програмного забезпечення ІКС, мають вразливості та відмінні від нуля ймовірності їхньої реалізації (використання) з боку зловмисників. Тому адміністратору мережі при налаштуванні маршрутизаторів та протоколів маршрутизації також не варто нехтувати використанням традиційних засобів підвищення рівня мережної безпеки – налаштування авторизованого доступу з використанням безпечних протоколів віддаленого налаштування пристроїв (наприклад, SSH), а також криптографічної автентифікації при передачі повідомлень щодо оновлень стану ІКС, використання надійних паролів і коректних політик фільтрації трафіка.

Список використаних джерел:

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

2. Лемешко О. В., Єременко О. С., Невзорова О. С. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість : моногр. Харків : ХНУРЕ, 2020. 308 с. DOI: https://doi.org/10.30837/978-966-659-282-1.

3. Лемешко О. В., Єременко О .С., Євдокименко М. О., Шаповалова А. С., Слейман Б. Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах : моногр. М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. Харків : ХНУРЕ, 2022. 198 с. DOI: https://doi.org/10.30837/978-966-659-378-1.