УДК 004.7

Макаревич С.О., здобувач
Дячук О.Ю., ст. викладач
Колощук М.С., ст. викладач
Державний університет «Житомирська політехніка»

ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОЇ МАРШРУТИЗАЦІЇ В OSPF-МЕРЕЖАХ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ VPN

На сучасному етапі розвитку телекомунікаційних систем забезпечення безпеки мережевої інфраструктури є одним із ключових завдань функціонування організацій. Протоколи динамічної маршрутизації, зокрема OSPF (Open Shortest Path First), широко застосовуються для побудови масштабованих і відмовостійких мереж. Водночас базова специфікація OSPF не передбачає повноцінних механізмів шифрування переданих даних, що створює потенційні загрози порушення конфіденційності та цілісності інформації [4].

Метою роботи є підвищення рівня безпеки OSPF-мереж шляхом інтеграції VPN-технологій для захисту маршрутної інформації.

Наукова новизна полягає у запропонованому підході до інтеграції протоколу OSPF із VPN-тунелями для забезпечення захисту службового маршрутизаційного трафіку.

До основних загроз, пов'язаних із використанням OSPF, належать атаки підміни маршрутів (route spoofing), що призводять до перенаправлення трафіку через несанкціоновані вузли, атаки типу «людина посередині» (Man-in-the-Middle), які дозволяють перехоплювати та змінювати передані дані, а також replay-атаки, що передбачають повторне використання перехоплених пакетів. Окрім цього, атаки типу відмови в обслуговуванні (DoS) можуть реалізовуватися шляхом перевантаження мережі надлишковими LSA-повідомленнями, що призводить до деградації продуктивності мережевих пристроїв.

Для підвищення рівня захисту мережевої взаємодії доцільним є використання технологій віртуальних приватних мереж (VPN), які забезпечують створення захищених тунелів передачі даних у недовіреному середовищі. VPN реалізує механізми шифрування, автентифікації та контролю цілісності інформації, що дозволяє ефективно захищати як користувацький, так і службовий трафік.

Серед протоколів, що застосовуються у VPN-рішеннях, особливе місце займає IPsec (Internet Protocol Security), який забезпечує захист IP-трафіку на мережевому рівні шляхом шифрування та автентифікації пакетів [5, 6]. Використання IPsec дозволяє гарантувати

конфіденційність маршрутних оновлень OSPF та запобігти несанкціонованому втручанню в процес маршрутизації.

Методами дослідження є аналіз наукових джерел і стандартів, а також моделювання мережевої взаємодії у середовищі GNS3 із використанням маршрутизаторів Cisco та протоколу OSPF у поєднанні з VPN-технологіями.

У межах дослідження розглянуто архітектуру мережі, що включає взаємодію між кількома маршрутизаторами в ізольованому середовищі, у якій протокол OSPF функціонує всередині захищених VPN-тунелів. Такий підхід дозволяє ізолювати маршрутний трафік від зовнішнього середовища, забезпечити шифрування службових повідомлень та обмежити доступ до мережі лише автентифікованим пристроям.

У результаті моделювання встановлено, що використання VPN-технологій, зокрема IPsec, дозволяє:

- забезпечити шифрування маршрутних оновлень OSPF;
- знизити ризик реалізації атак типу Man-in-the-Middle та replay-атак;
- обмежити доступ до маршрутизаційної інформації лише автентифікованим вузлам;
- підвищити загальну стійкість мережі до атак на рівні маршрутизації.

Таким чином, інтеграція протоколу OSPF із VPN-технологіями є ефективним підходом до підвищення безпеки мереж. Запропонований підхід дозволяє забезпечити захист маршрутної інформації, зменшити ризики кіберзагроз та підвищити надійність функціонування мережевої інфраструктури, що підтверджує доцільність його застосування в сучасних умовах.

Список використаних джерел

1. Cisco Systems. Dynamic Routing Protocols: OSPF, EIGRP, RIPv2, IS-IS, BGP. URL: https://community.cisco.com/t5/networking-knowledge-base/dynamic-routing-protocols-ospf-eigrp-ripv2-is-is-bgp/ta-p/4511577

2. Shapira T., Shavitt Y. A Deep Learning Approach for IP Hijack Detection Based on ASN Embedding // NetAI, 2020. URL: https://dl.acm.org/doi/10.1145/3405671.3405819

3. Murphy S. Security Issues in OSPF Routing Protocol // RFC 6860, 2013. URL: https://datatracker.ietf.org/doc/html/rfc6860

4. RFC 2328. OSPF Version 2 Specification. URL: https://datatracker.ietf.org/doc/html/rfc2328

5. RFC 4301. Security Architecture for the Internet Protocol. URL: https://datatracker.ietf.org/doc/html/rfc4301

6. RFC 2401. Security Architecture for the Internet Protocol (IPsec). URL: https://datatracker.ietf.org/doc/html/rfc2401