Бухарова Л.Д., студентка
Гвоздецька К.П., студентка
Харківський національний університет радіоелектроніки, м. Харків
Кафедра Електронних обчислювальних машин

ОГЛЯД НАЙПОПУЛЯРНІШИХ МЕТОДІВ ШИФРУВАННЯ

На сьогоднішній день на ринку існує значна кількість VPN-провайдерів, що надають величезну кількість різних типів шифрування. Шифрування – це процес кодування інформації, в результаті якого вона стає недоступною для третіх осіб [1].

Існують різні технології VPN з різним ступенем шифрування. Наприклад, протокол тунелювання «точка-точка» (PPTP) працює швидко, але набагато менш безпечний, ніж інші протоколи, такі як IPSec або OpenVPN, який використовує SSL / TLS (Secure Sockets Layer / Transport Layer Security). Крім того, при використанні VPN на основі TLS також важливі тип алгоритму шифрування і довжина ключа [2].

Хоча OpenVPN підтримує безліч комбінацій шифрів, протоколів обміну ключами і алгоритмів хешування, найбільш поширеною реалізацією, запропонованої постачальниками послуг VPN для з'єднань OpenVPN, є шифрування AES з обміном ключами RSA і сигнатурами SHA. Рекомендованими параметрами є шифрування AES256 з ключем RSA довжиною не менше 2048 біт і криптографічною хеш-функцією SHA-2 (SHA256) замість SHA-1.

Проте, розглянувши протокол OpenVPN можна сказати, що незважаючи на те, що він заснований на відкритих джерелах, він вважається одним з найбезпечніших протоколів VPN [3]. Він стабільний і надійний, легко конфігурується для роботи на будь-якому порту, підтримує апаратне прискорення для поліпшення швидкості, здатний перетинати міжмережеві екрани і трансляцію мережевих адрес (NAT) і використовує бібліотеки OpenSSL для шифрування.

У той же час, найменш захищений протокол VPN – це протокол PPTP. Він має слабке шифрування і відносно легко блокується провайдерами.

Так протоколи тунелювання VPN пропонують різні функції і рівні безпеки, і для кожного з них є переваги і недоліки [4, 5]. Існує п'ять основних протоколів тунелювання VPN: Протокол тунелювання захищених сокетів (SSTP), Протокол тунелювання «точка-точка» (PPTP), Протокол тунелювання другого рівня (L2TP), OpenVPN і Internet Key Exchange версії 2 (IKEv2).

Варто зазначити, що шифрування може впливати на швидкість з'єднання. Вибір технології VPN і методів шифрування повинен проводитися в кожному конкретному випадку, в залежності від того, які дані будуть передаватися.

Література

1. Коваленко А.А. Метод забезпечення живучості комп’ютерної мережі на основі VPN-тунелювання / А.А. Коваленко, Г.А. Кучук, В.М. Ткачов // Системи управління, навігації та зв’язку. Збірник наукових праць. – Полтава: ПНТУ, 2021. – Т. 1 (63). – С. 90-95. – doi:https://doi.org/10.26906/SUNZ.2021.1.090.

2. Ruban I.V., Churyumov G.I., Tokariev V.V., Tkachov V.M. Structural-functional reconfiguration of computer systems with reconstruct structure. Проблеми інформатики та моделювання: тези доповідей 19-ї міжн. наук.-техн. конф., м. Одеса, 11-16 вер. 2019р. Одеса, С.71 — 72.

3. Tkachov, V., Kovalenko, A., Kuchuk, H., & Ni, I. (2021). Метод забезпечення живучості високомобільної комп'ютерної мережі. Advanced Information Systems-Sučasnì ìnformacìjnì sistemi, 5(2), 159-165.

4. Tkachov V. Principles of Constructing an Overlay Network Based on Cellular Communication Systems for Secure Control of Intelligent Mobile Objects / Vitalii Tkachov, Andriy Kovalenko, Mykhailo Hunko and Kateryna Hvozdetska // Информационные технологии и безопасность. Материалы XIX Международной научно-практической конференции ИТБ-2020. – К.: ООО «Инжиниринг», 2020.

5. Kuchuk, N., Kovalenko, A., Tkachov, V., Rosinskiy, D., & Kuchuk, H. (2021). Predicting traffic anomalies in container virtualization. Computer And Information Systems And Technologies.