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

РОЗГЛЯД VPN ТА АНОНІМАЙЗЕРІВ В ЯКОСТІ ЗАСОБІВ БЕЗПЕЧНОГО ВИКОРИСТАННЯ НЕЗАХИЩЕНИХ МЕРЕЖ

Сучасний розвиток інформаційних технологій і, зокрема, мережі Internet, призводить до необхідності захисту інформації, переданої в рамках розподіленої корпоративної мережі, що використовує мережі відкритого доступу [1]. Однак Інтернет є незахищеною мережею, тому доводиться винаходити засоби захисту конфіденційних даних, переданих по незахищеній мережі.

Існує декілька засобів, один з яких це анонімайзери або проксі-сервера, вони приховують дані про комп'ютер або користувача в локальній мережі від віддаленого сервера. Розглянувши принцип роботи проксі-серверів, можемо сказати, що анонимайзер завжди розриває прямий ланцюг зв'язку і стає посередником між веб-браузером і потрібним веб-сервером [2].

У сфері кібербезпеки анонімізуючий проксі-сервер – це інструмент, який можна використовувати для того, щоб зробити онлайн-діяльність невідстежуваною або анонімною. Ці проксі, по суті, діють як посередницькі "шлюзи" між користувачем Інтернету та їхнім місцем призначення, як і VPN.

Проте VPN – це технологія, яка об'єднує довірені мережі, вузли і користувачів через відкриті мережі, яким немає довіри. Технологія, яка набуває все більшого поширення серед не тільки технічних фахівців, а й серед звичайних користувачів, яким також потрібно захищати свою інформацію (наприклад, користувачі Internet-банків або Internet-порталів) [3].

На відміну від анонімайзерів, VPN шифрують онлайн-трафік. Анонімайзер, в свою чергу, тільки маскує вашу IP-адресу, він не може захистити вас від відстеження вашим постачальником послуг Інтернету або іншими третіми сторонами.

Проксі-севери працюють на рівні додатків, тоді як VPN працюють на рівні операційної системи. Іншими словами, VPN може охоплювати весь Інтернет-трафік, що надходить з комп’ютера користувача, тоді як проксі-сервер покриває лише трафік, що надходить із певного браузера чи програми. Користувачі VPN можуть використовувати техніку, яка називається розділеним тунелюванням, щоб вибрати, який трафік буде маршрутизуватися через їх VPN [4,5].

Так будь-який інструмент, який перенаправляє веб-трафік клієнта для захисту його конфіденційності, швидше за все, вплине на швидкість Інтернету. Однак, оскільки VPN також шифрують дані клієнта, вони можуть бути повільнішими за анонімайзери. Компроміс полягає в тому, що VPN часто пропонують більш надійну безпеку та конфіденційність, ніж анонімайзери.

Література

1. 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.

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

3. 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.

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. V. Tkachov, M. Bondarenko, O. Ulyanov and O. Reznichenko, "Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory," 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), 2019, pp. 161-165, doi: 10.1109/ATIT49449.2019.9030494.