Осадчий О.О., студент
Гвоздецька К.П., студентка
Харківський національний університет радіоелектроніки, м. Харків
Кафедра Електронних обчислювальних машин

ВАЖЛИВІСТЬ ВИКОРИСТАННЯ ПРИВАТНИХ МЕРЕЖ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ

В останнє десятиліття все більшої популярності на IT-ринку набувають хмарні технології. Розробка цих технологій зумовлена зростанням у геометричній прогресії потоків і обсягів інформації та потреби у її доступності для користувачів у будь-який момент [1]. Збільшення кількості хмарних обчислень детермінує, у свою чергу, розвиток хмарних платформ і сервісів для створення додатків, а також протоколів роботи в платформі.

При цьому актуальним є питання вибору ефективної хмарної платформи для обміну даними великого обсягу в контексті інтернету речей [2]. Під Інтернетом речей (Internet of Things, IoT) вітчизняні та зарубіжні науковці розуміють концепцію обчислювальної мережі, що складається із взаємозв’язаних фізичних пристроїв, що мають вбудовані сенсори і програмне забезпечення для обміну даними з іншими пристроями.

Існує можливість з'єднати всю IT–інфраструктуру, що стосується пристроїв IoT, в одну мережу — і ця приватна мережа дозволяє забезпечити безпечний зв'язок між розгорнутими пристроями IoT та інфраструктурою, яка контролює чи отримує з них дані [3].

Завдяки досягненням у криптографії, обчислювальних технологіях та поширеності Інтернету можна шифрувати трафік даних та тунелювати його через Інтернет на сервер, розташований у приватній мережі. Захищений тунель створює віртуальне посилання, яке поширює приватну мережу на загальнодоступну [4]. Цей вид мережі, який використовує загальнодоступні мережі для забезпечення підключення до приватної, називається віртуальною приватною мережею (VPN).

Використовуючи сервер доступу OpenVPN як рішення безпеки IoT, користувач може створити власну приватну мережу для IoT заради безпечного ведення та налагодження зв’язку з пристроями, а також для уникнення атак, що можуть загрожувати зміною даних або несанкціонованим стеженням через розумні пристрої. Втручання зловмисником у незахищену мережу Інтернету речей може загрожувати втратою цінної інформації.

VPN — це чудове рішення для захисту даних, що надсилаються та приймаються різними пристроями, які утворюють інтернет речей [5]. Застосувавши VPN у мережах Інтернету речей, є можливість зробити ці мережі набагато надійнішими та безпечнішими. Це можна зробити так, що лише авторизовані пристрої можуть стати частиною приватної мережі.

Література

1. T. Vitalii, B. Anna, H. Kateryna and D. Hrebeniuk, "Method of Building Dynamic Multi-Hop VPN Chains for Ensuring Security of Terminal Access Systems," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 613-618, doi: 10.1109/PICST51311.2020.9467953.

2. 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.

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

4. 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.

5. 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.