

*Потьомкіна К.О., студентка*

*Гвоздецька К.П., студентка*

*Харківський національний університет радіоелектроніки, м. Харків*

*Кафедра Електронних обчислювальних машин*

## **ПЕРЕВАГИ VPN МЕРЕЖ ДЛЯ ОСОБИСТОГО ВИКОРИСТАННЯ**

VPN–з'єднання встановлює безпечне з'єднання між користувачем й Інтернетом. Через VPN весь трафік даних спрямовується через зашифрований віртуальний тунель. Це маскує особисту IP-адресу користувача, коли він користується Інтернетом, роблячи його місце розташування невидимим для всіх. Існує багато різних типів VPN, але є лише три основні:

- перший тип — це SSL VPN. Не завжди співробітники компанії мають доступ до корпоративного ноутбука, який вони використовують для роботи з дому . У таких випадках часто вдаються до використання особистих пристроїв (ПК, ноутбука, планшета, мобільного телефону). У цьому випадку компанії вдаються до використання SSL–VPN, яке зазвичай реалізується через відповідний апаратний блок. Необхідною умовою зазвичай є браузер з підтримкою HTML–5, який використовується для виклику сторінки входу в систему. Браузери з підтримкою HTML-5 доступні практично для будь-якої операційної системи. Доступ захищений ім'ям користувача і паролем.

- другий тип — міжсайтовий VPN. Цей тип , ще називають VPN типу "мережа до мережі" — це приватна мережа, призначена для приховування приватних інтрамереж і наданням користувачам безпечних мереж доступу до ресурсів один одного. VPN типу "мережа до мережі" корисний, якщо є кілька філій у компанії, кожне з яких має власну локальну мережу (LAN), підключену до WAN (глобальної мережі). VPN–з'єднання типу "мережа до мережі" також корисні, якщо є дві окремі інтрамережі , між якими можна відправляти файли без явного доступу користувачів з однієї локальної мережі до іншої.

- третій тип — VPN-клієнт – сервер. Підключення через VPN-клієнт можна уявити, як підключення домашнього комп'ютера до офісу за допомогою подовжувального кабелю. Співробітники можуть підключатися до корпоративної мережі з домашнього офісу через захищене з'єднання і працювати ніби з офісу. Це більш поширена форма VPN, яка особливо корисна для провайдерів незахищених загальнодоступних WLAN. Він запобігає доступу третіх осіб до мережевого з'єднання і його компрометацію, а також шифрує дані на всьому шляху до провайдера. Отже, підсумовуючи всі факти, можна зробити висновок, що таким чином, знаючи типи чинних VPN мереж, можна з легкістю обрати те, що потрібно користувачеві виходячи з ситуації.

#### Література

1. Tkachov, V., Kovalenko, A., Kuchuk, H., & Ni, I. (2021). Метод забезпечення живучості високомобільної комп'ютерної мережі. *Advanced Information Systems-Sučasni informacijni 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 Hvozdet'ska // 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.