УДК 004.7

ВИКОРИСТАННЯ VPN ЯК ЗАСОБУ ЗАХИСТУ ДАНИХ У ПУБЛІЧНИХ МЕРЕЖАХ

С. Царенко, група КН-23
Науковий керівник: ***В. Резніченко,*** викладач
Центральноукраїнський національний технічний університет

У сучасному світі питання інформаційної безпеки набуває надзвичайної важливості через швидкий розвиток інформаційних технологій і глобалізацію Інтернету. Відкриті публічні мережі, зокрема Wi-Fi точки доступу в кафе, аеропортах та інших громадських місцях, створюють значні ризики для безпеки персональних і конфіденційних даних користувачів. За даними досліджень, близько 80% кібератак здійснюється через незашифровані мережі або слабке їх шифрування [1]. Внаслідок цього, інформація, що передається без належного захисту, може бути перехоплена зловмисниками.

Одним з основних інструментів для захисту даних у таких умовах є віртуальні приватні мережі (VPN). VPN (Virtual Private Network) – це технологія, яка дозволяє створити зашифрований тунель між кінцевим пристроєм і сервером, що перешкоджає перехопленню або зміні даних при їх передачі через публічні мережі. Найважливішим елементом роботи VPN є шифрування [6]. За допомогою VPN користувач може захистити себе від атак типу Man-in-the-Middle, DNS-спуфінгу та підслуховування трафіку [2]. Важливим аспектом є також захист приватності користувача, зокрема маскування реальної IP-адреси, що дозволяє уникнути відстеження онлайн-діяльності.

Актуальність дослідження VPN у публічних мережах також підтверджується зростаючим використанням VPN-сервісів серед користувачів Інтернету. За даними статистики, близько 30% користувачів Інтернету в усьому світі активно використовують VPN для захисту своїх даних, особливо при підключенні до відкритих Wi-Fi точок доступу [3]. Зокрема, у країнах з високим рівнем інтернет-цензури VPN стає важливим інструментом для обходу блокувань і доступу до обмеженого контенту [4].

Віртуальні приватні мережі використовують різні протоколи для забезпечення безпеки та шифрування даних при їх передачі через Інтернет:

1. PPTP (Point-to-Point Tunneling Protocol)

PPTP є одним із найстаріших протоколів для створення VPN-з’єднань. Він широко підтримується на різних платформах, включаючи Windows, Linux і macOS [5].

2. L2TP/IPsec (Layer 2 Tunneling Protocol with Internet Protocol Security)

L2TP є удосконаленим протоколом PPTP, який забезпечує більший рівень безпеки завдяки використанню IPsec для шифрування даних. Водночас, L2TP/IPsec має високі вимоги до ресурсів і може бути повільним при використанні в мережах з обмеженою пропускною здатністю [5].

3. OpenVPN

OpenVPN є одним з найбільш популярних протоколів через свою гнучкість, відкритість і високий рівень безпеки. Він використовує SSL/TLS для шифрування трафіку, що дозволяє забезпечити високий рівень конфіденційності та аутентифікації [5].

4. IKEv2/IPsec (Internet Key Exchange version 2)

IKEv2 – це один з найновіших і найбільш швидких протоколів для VPN. Він підтримує мобільні з'єднання і забезпечує високу стабільність при зміні мережі або при втраті з’єднання [5].

5. WireGuard

WireGuard – це сучасний і високопродуктивний протокол VPN, який швидко став популярним завдяки простоті налаштування та високій швидкості роботи. WireGuard використовує нові криптографічні алгоритми, що дозволяють йому працювати швидше і забезпечувати кращий рівень безпеки при меншій витраті ресурсів [5].

Таблиця 1. Порівняння параметрів VPN протоколів

Протокол	Рівень безпеки	Швидкість з'єднання	Сумісність	Простота налаштування	Стійкість до атак
PPTP	низький	висока	висока	дуже проста	низька
L2TP/IPsec	високий	середня	висока	середня	висока
OpenVPN	дуже високий	середня	висока	відносно складна	дуже висока
IKEv2/IPsec	високий	висока	висока	легка	висока
WireGuard	високий	дуже висока	середня	легка	висока

Типовими загрозами, з якими стикаються користувачі є: Sniffing (перехоплення трафіку), Man-in-the-Middle (MitM), DNS Spoofing, IP-трекінг [2].

Таблиця 2. Загрози в публічних мережах і способи захисту за допомогою VPN

Загроза	Характеристика	Захист VPN
Sniffing	Хакери можуть бачити незашифровані пакети, що проходять через Wi-Fi	Шифрує увесь трафік, роблячи його нечитаємим
Man-in-the-Middle	Зловмисник перехоплює трафік між користувачем і сервером	Створює захищений тунель, виключаючи втручання
DNS Spoofing	Підміна DNS-запитів, що веде на фейкові сайти	Примусово використовує надійні DNS через VPN
IP-трекінг	Відстеження дій користувача за його IP-адресою	Маскує справжній IP користувача

Таким чином, дослідження можливостей, переваг, обмежень та практичного застосування VPN є актуальним з точки зору забезпечення інформаційної безпеки особистості, а також може мати практичне значення для широкого кола користувачів, які щоденно працюють у відкритих мережах.

Список літератури

1. У 2024 році кількість кібератак на Україну зросла на 70%. Інститут масової інформації. URL: https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zrosla-na-70-i65931 (дата звернення: 14.05.2025).
2. 10 поширених типів кібератак та методів захисту. ТОВ "Зе Кернел". URL: https://thekernel.ua/10-poshyrenykh-typiv-kiberatak/ (дата звернення: 14.05.2025).
3. Захист VPN: Все, що потрібно знати. URL: https://7vpn.com/ua/blog/zahyst-vpn-vse-shho-potribno-znaty/ (дата звернення: 14.05.2025).
4. Що таке VPN і як його використовувати в Україні: Повне керівництво 2025. Захищена сторінка. URL: https://www.site2b.ua/ua/web-blog-ua/shho-take-vpn-i-yak-jogo-vikoristovuvati-v-ukraini.html (дата звернення: 14.05.2025).
5. Як обрати найкращий протокол VPN у 2025 - Surfshark. Surfshark. URL: https://surfshark.com/uk/blog/vpn-protocols (дата звернення: 14.05.2025).
6. VPN та його вплив на кібербезпеку: повний посібник для бізнесу та приватних користувачів. URL: https://itorakul.com.ua/vpn/ (дата звернення: 14.05.2025).