УДК 004.056.55
Ю. Олійник; О. Оробчук, Ph.D
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN

UDC 004.056.55
Y. Oliynyk.; O. Orobchuk, Ph.D

METHODS OF PROTECTING INFORMATION AND TELECOMMUNICATION SYSTEMS AND NETWORKS FROM UNAUTHORIZED ACCESS USING VPN TECHNOLOGY

У сучасному цифровому світі питання захисту інформації стає дедалі важливішим. Інформаційно-телекомунікаційні системи є вразливими до кіберзагроз, що можуть спричиняти витік даних чи несанкціонований доступ. Одним із ефективних рішень є використання VPN, який створює захищені з'єднання навіть через публічні мережі. Це дозволяє забезпечити конфіденційність та цілісність даних, що передаються, знижуючи ризики для користувачів.

Розвиток кібератак, таких як «людина посередині» (MITM), вимагає застосування складних технологій безпеки. VPN забезпечує шифрування даних і мінімізує ризик їх перехоплення, що є важливим як для корпоративних систем, так і для приватних осіб. Це підвищує загальний рівень довіри до мережевих комунікацій.

У роботі проведено дослідження ефективності VPN-протоколів, таких як OpenVPN та WireGuard. Аналіз включав тестування продуктивності під час різного навантаження та вивчення стійкості до кібератак. Такий підхід дозволив визначити оптимальні технічні параметри для захисту мережевих ресурсів. Додатково, було розглянуто вплив різних конфігурацій на швидкість з'єднання та загальну безпеку системи.

WireGuard показав вищу продуктивність, тоді як OpenVPN забезпечив більшу гнучкість налаштувань. Надійність шифрування залежить від довжини ключів і обраних алгоритмів. Розроблено рекомендації для налаштування VPN-систем у контексті запобігання типових уразливостей. Важливо також враховувати специфічні потреби організації для оптимізації безпеки та ефективності мережі.

VPN є ключовим інструментом для захисту інформаційно-телекомунікаційних систем. Однак для максимального ефекту потрібно інтегрувати VPN у загальну стратегію кібербезпеки, забезпечуючи регулярні оновлення та оптимізацію налаштувань. Це включає впровадження додаткових заходів безпеки, таких як двофакторна автентифікація та моніторинг мережевої активності.

Література

1. RFC 7296 – Internet Key Exchange Protocol Version 2 (IKEv2).
2. Jason A. Donenfeld. WireGuard Cryptokey Routing Protocol.
3. OpenVPN Community. OpenVPN Protocol Documentation.