Автор:
Андрій КРАВЧЕНКО
студент 41КНз групи
Науковий керівник:
Кандидат педагогічних наук, доцент, доцент кафедри компютерної та програмної інженерії
Олена СНІГУР

# ПРОЄКТУВАННЯ БЕЗПЕЧНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ З ВІДДАЛЕНИМ ДОСТУПОМ НА ОСНОВІ VPN-СЕРВІСУ WIREGUARD

**Анотація:** У тезах розглянуто питання організації захищеного віддаленого доступу до корпоративної мережі підприємства. Проаналізовано сучасні технології VPN, обґрунтовано вибір протоколу WireGuard як оптимального рішення за критеріями швидкодії та безпеки. Описано етапи проєктування мережевої інфраструктури, налаштування політик безпеки та результати тестування ефективності розгорнутої системи.

**Ключові слова:** корпоративна мережа, VPN, WireGuard, віддалений доступ, інформаційна безпека, тунелювання, шифрування, мережева архітектура.

**Вступ:** Сучасні умови ведення бізнесу вимагають від організацій забезпечення надійного та безпечного доступу співробітників до корпоративних ресурсів з будь-якої точки світу. Зростання популярності дистанційної роботи актуалізує проблему захисту передачі даних через публічні мережі. Традиційні рішення, такі як OpenVPN або IPsec, часто є складними в налаштуванні та мають надлишковий код, що може впливати на продуктивність та безпеку. Тому метою роботи стало проєктування та побудова корпоративної мережі на основі новітнього протоколу WireGuard, який забезпечує високу швидкість з'єднання та сучасні стандарти криптографії при мінімальних витратах системних ресурсів.

У ході дослідження було проведено порівняльний аналіз існуючих VPN-технологій. Встановлено, що WireGuard має значні переваги перед аналогами завдяки компактній кодовій базі (менше 4000 рядків коду), використанню сучасних криптографічних примітивів (Curve25519, ChaCha20, Poly1305) та механізму Cryptokey Routing. Це дозволяє значно зменшити поверхню атаки та спростити аудит безпеки системи.

Практична частина роботи полягає у розробці структури корпоративної мережі з урахуванням вимог до відмовостійкості та конфіденційності. Було розгорнуто VPN-сервер на базі ОС Linux та налаштовано клієнтські підключення для різних платформ. Особливу увагу приділено налаштуванню політик безпеки та контролю доступу (ACL) для розмежування прав користувачів всередині тунелю. Реалізована схема дозволяє співробітникам безпечно підключатися до внутрішніх серверів компанії, використовуючи публічні канали зв'язку, при цьому трафік надійно шифрується.

Ефективність запропонованого рішення перевірено шляхом навантажувального тестування. Результати показали, що мережа на базі WireGuard демонструє меншу затримку (latency) та вищу пропускну здатність порівняно з OpenVPN, а також швидше відновлює з'єднання при зміні IP-адреси клієнта (роумінг). Стабільність роботи підтверджено під час імітації пікових навантажень.

**Висновок:** У результаті виконання роботи спроєктовано та побудовано захищену

корпоративну мережу з використанням технології WireGuard. Розроблене рішення забезпечує конфіденційність, цілісність та доступність даних, відповідає сучасним вимогам кібербезпеки та є легко масштабованим. Практичне впровадження такої системи дозволяє підприємству мінімізувати ризики витоку інформації при організації віддаленої роботи персоналу.

**Список використаних джерел:**


1. Donenfeld J. A. WireGuard: Next Generation Kernel Network Tunnel. *NDSS Symposium*. 2017.
2. Оліфер В. Г., Оліфер Н. А. Комп'ютерні мережі. Принципи, технології, протоколи: підручник. — К.: Каравела, 2020.
3. WireGuard: fast, modern, secure VPN Tunnel. URL: https://www.wireguard.com (дата звернення: 25.04.2025).
4. Брюс Шнайєр. Прикладна криптографія. Протоколи, алгоритми, вихідні тексти на мові С. — 2-ге вид. — 2018.