Трокоз Є. М., ст. викладач,
Плитус Д. І., магістрант,
Державний університет «Житомирська політехніка»

СЦЕНАРІЇ ВИКОРИСТАННЯ VPN В КОРПОРАТИВНИХ МЕРЕЖАХ

Технологія VPN (віртуальні приватні мережі) є ключовим елементом сучасної корпоративної інфраструктури, забезпечуючи захищений доступ до ресурсів компанії через публічні мережі, такі як Інтернет. Вона дозволяє організаціям досягати високого рівня безпеки, гнучкості та економічної ефективності в управлінні мережами [1]. В даній роботі наведено способи та особливості використання VPN в різних сценаріях в корпоративній мережі (рис. 1).

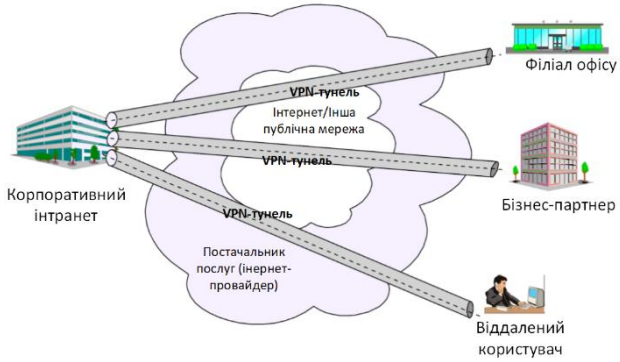

Рис. 1. Сценарії використання VPN в корпоративній мережі

З'єднання між віддаленими офісами. Одним із найпоширеніших сценаріїв є створення захищених з'єднань між головним офісом компанії та її філіями. VPN забезпечує надійне передавання даних через публічний Інтернет, що дозволяє уникнути використання дорогих виділених ліній.

На межі інтранетів обох офісів встановлюються брандмауери або маршрутизатори з функцією VPN для захисту корпоративного трафіку від потенційних загроз. Це дозволяє шифрувати всі передані дані, забезпечуючи конфіденційність інформації навіть при її передаванні через ненадійні та публічні мережі. Крім того, компанія може легко розширити власний інтранет, включивши до нього нові філії, створюючи тим самим масштабовану корпоративну мережу.

Мережа бізнес-партнерів і постачальників. Для взаємодії з бізнес-партнерами та постачальниками VPN пропонує можливість створення розширеної корпоративної мережі. Раніше для таких потреб компанії використовували орендовані лінії зв'язку, які є не лише дорогими, але й обмеженими географічно. Використання VPN дозволяє подолати ці обмеження, створюючи приватне зашифроване з'єднання через Інтернет.

Наприклад, виробник деталей може використовувати VPN для обміну конфіденційною інформацією з постачальниками, такою як дані про запаси чи графіки виробництва. У цьому випадку застосовуються механізми аутентифікації та шифрування, що гарантує захищеність інформації навіть за її передавання через публічні мережі.

Підключення віддалених працівників. VPN є незамінним інструментом для організації віддаленої роботи. Співробітники, які працюють поза межами офісу, можуть безпечно підключатися до корпоративного інтранету з будь-якої точки світу, використовуючи захищене VPN-з'єднання [2].

Наприклад, працівник, перебуваючи вдома або в дорозі, може отримати доступ до конфіденційних файлів чи серверів офісу. Це реалізується шляхом встановлення зашифрованого тунелю між пристроєм працівника та корпоративною мережею, забезпечуючи захист даних від несанкціонованого доступу.

Така технологія сприяє підвищенню мобільності співробітників і забезпечує стабільну роботу компанії навіть у випадку виникнення надзвичайних ситуація за яких неможливо фізично перебувати в офісі.

Отже, використання VPN в корпоративних мережах відкриває широкі можливості для забезпечення захищеної, гнучкої та масштабованої мережевої інфраструктури. Вона дозволяє компаніям інтегрувати філії, бізнес-партнерів і віддалених працівників у єдину мережу, мінімізуючи витрати та забезпечуючи високий рівень безпеки, що є вкрай важливим в умовах швидкого обміну даними та глобальної інтеграції.

Список використаних джерел

1. Eric F Crist. Mastering OpenVPN 1st Edition. – Birmingham: Packt Publishing, 2015. – 366 p.
2. What Are the Different Types of VPN? URL: https://www.paloaltonetworks.com/cyberpedia/types-of-vpn