УДК 004:7

Сердійчук І.С., магістрант
Бродський Ю.Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

ШЛЯХИ УДОСКОНАЛЕННЯ ЗАХИСТУ ГЕТЕРОГЕННОЇ МЕРЕЖІ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ КОМПЛЕКСУ VPN-ТЕХНОЛОГІЙ

Стабільність та безпека функціонування корпоративних мереж є ключовою умовою безперервності бізнес-процесів сучасних організацій. Стрімка цифровізація призвела до трансформації класичних локальних мереж у складні гетерогенні системи, які об'єднують різнорідні компоненти: серверні кластери, стаціонарні робочі станції, мобільні пристрої співробітників та датчики інтернету речей. Кожен із цих елементів має відмінні обчислювальні можливості та працює під управлінням різних операційних систем, що створює нові виклики для систем захисту інформації.

Основним механізмом забезпечення конфіденційності даних при передачі через відкриті канали зв'язку залишаються технології віртуальних приватних мереж (VPN). Проте аналіз сучасних підходів до їх впровадження виявляє суттєву проблему: застосування уніфікованих стандартів тунелювання для всіх учасників мережі є неефективним. «Важкі» протоколи створюють критичне навантаження на мережу, що призводить до значних затримок у передачі даних. Водночас, спрощені рішення, орієнтовані на швидкість, можуть не забезпечувати достатнього рівня криптографічної стійкості для захисту конфіденційної корпоративної інформації.

Метою роботи є підвищення рівня захищеності та продуктивності гетерогенної мережі шляхом розробки методу адаптивного використання VPN-технологій. В рамках дослідження проведено порівняльний аналіз провідних протоколів. Встановлено, що новітні протоколи, такі як WireGuard, демонструють значно менші затримки завдяки оптимізованій кодовій базі, тоді як класичний IPSec забезпечує кращу сумісність із наявним мережевим обладнанням. Теоретична значущість дослідження полягає в обґрунтуванні гібридної моделі, де вибір технології захисту відбувається динамічно, виходячи з параметрів кінцевого вузла.

За результатами аналізу сформульовано рекомендації щодо удосконалення захисту гетерогенної мережі:

- впровадити класифікацію мережевих вузлів за рівнем обчислювальної потужності та вимогами до безпеки;

- застосовувати адаптивний підхід до вибору протоколу: використовувати WireGuard або оптимізований IKEv2 для мобільних пристроїв для зменшення затримок, та OpenVPN/IPSec з посиленими алгоритмами шифрування для зв’язку між філіями;
- розробити модель загроз, специфічну для гетерогенного середовища, враховуючи вразливості кінцевих точок з обмеженими ресурсами;
- використовувати засоби автоматизованого керування конфігураціями для динамічного перемикання параметрів тунелювання.

Окрему увагу в процесі реалізації цих рекомендацій слід приділити питанням відмовостійкості та балансуванню навантаження. Оскільки запропонований гібридний підхід передбачає одночасне функціонування кількох шлюзів або різних конфігурацій на одному пристрої, критично важливо забезпечити постійний моніторинг ресурсів маршрутизатора.

Таким чином, результати аналітичного дослідження свідчать, що відмова від монолітної архітектури VPN на користь адаптивної моделі дозволяє досягти синергетичного ефекту. Комбінований підхід забезпечує зниження навантаження на клієнтські пристрої та на саму мережу, що прямо корелює з підвищенням загальної продуктивності праці співробітників за рахунок зменшення часу відгуку інформаційних систем. При цьому рівень захищеності мережевого периметра залишається високим, оскільки інші алгоритми не застосовуються для передачі критично важливих даних. Перспективним напрямом подальших досліджень є розробка алгоритмів автоматичного перемикання протоколів тунелювання в реальному часі на основі поточного стану каналу зв'язку.

Список використаних джерел:

1. Оліфер В. Г., Оліфер Н. А. Комп'ютерні мережі. Принципи, технології, протоколи. Київ : Каравела, 2020. 992 с.

2. Столлінгс В. Криптографія та мережева безпека: принципи та практика. Москва : Вільямс, 2018. 750 с.

3. Goralski W. The Illustrated Network: How TCP/IP Works in a Modern Network. Morgan Kaufmann, 2017. 866 p.