Дмитрієв О.Г., магістрант
Державний університет «Житомирська політехніка»

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ ОБЛАДНАННЯ MIKROTIK ТА CISCO У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ

У сучасних умовах зростання кількості та складності кіберзагроз захист корпоративних мереж стає критичним завданням для будь-якої організації. Вибір обладнання для побудови мережевої інфраструктури впливає на рівень безпеки, продуктивності та загальні витрати на утримання мережі. Одними з найпоширеніших рішень у сфері мережевої безпеки є обладнання MikroTik та Cisco, які пропонують різні підходи до забезпечення захисту мереж. Ефективність використання цих рішень залежить від технічних можливостей, алгоритмів захисту та рівня стійкості до атак.

Метою дослідження є проведення порівняльного аналізу ефективності обладнання MikroTik та Cisco у забезпеченні безпеки корпоративних мереж. Дослідження охоплює аналіз алгоритмів захисту, продуктивності, масштабованості та вартості рішень MikroTik та Cisco у контексті забезпечення мережевої безпеки. Важливим аспектом є визначення переваг і недоліків кожного типу обладнання для формування оптимальної стратегії побудови захищеної мережі.

MikroTik забезпечує високу гнучкість і доступність для малого та середнього бізнесу. Невисока вартість, простота налаштування та широкий функціонал роблять це обладнання привабливим для використання у мережах невеликого масштабу. MikroTik пропонує вбудовані функції захисту, включаючи фільтрацію трафіку на рівні маршрутизації, міжмережеві екрани, захист від атак шляхом відключення невикористовуваних портів, а також шифрування трафіку за допомогою AES-256 [1]. VPN-рішення на базі MikroTik забезпечують безпечний віддалений доступ до мережі, що підвищує загальний рівень захисту. Однак, обладнання MikroTik має певні обмеження щодо масштабованості та продуктивності в умовах високого навантаження [2].

Cisco орієнтоване на забезпечення безпеки великих корпоративних мереж і надає більш складні та функціонально насичені рішення. Обладнання Cisco включає брандмауери нового покоління (NGFW) із глибокою інспекцією трафіку, VPN-рішення з використанням IPsec та SSL, інтеграцію з системами виявлення та запобігання атак (IDS/IPS), а також автоматизоване моніторинг трафіку з виявленням аномалій [3]. Високий рівень безпеки забезпечується за рахунок застосування складних алгоритмів шифрування та механізмів адаптивного реагування на інциденти безпеки. Основними перевагами Cisco є висока продуктивність, надійність і масштабованість, що робить це обладнання ідеальним для ядра мережі [4].

Інтеграція обладнання MikroTik та Cisco дозволяє створити ефективну багаторівневу систему захисту корпоративної мережі. MikroTik можна використовувати для управління доступом і фільтрації трафіку на периферійному рівні, тоді як Cisco ефективно забезпечує захист на рівні ядра мережі та обробку великого обсягу трафіку [5]. Такий підхід дозволяє оптимізувати витрати та досягти високого рівня безпеки за рахунок використання переваг обох платформ. Наприклад, використання MikroTik для побудови VPN-з'єднань і фільтрації трафіку в поєднанні з можливостями Cisco щодо централізованого управління безпекою забезпечує комплексний захист від зовнішніх і внутрішніх загроз [3].

У ході дослідження встановлено, що MikroTik забезпечує гнучкість, простоту налаштування та низьку вартість, що робить його ефективним рішенням для малих і середніх підприємств. Cisco надає більш складні та інноваційні рішення, орієнтовані на великі компанії з високими вимогами до безпеки та продуктивності [4]. Поєднання MikroTik і Cisco дозволяє створити масштабовану та захищену мережеву інфраструктуру, що відповідає вимогам сучасної кібербезпеки.

Висновки дослідження свідчать про те, що комбіноване використання обладнання MikroTik і Cisco дозволяє досягти оптимального балансу між гнучкістю, продуктивністю та рівнем безпеки. Рекомендується використовувати MikroTik для фільтрації трафіку та управління доступом на периферійному рівні, тоді як Cisco доцільно впроваджувати на рівні ядра мережі для забезпечення масштабованості та високого рівня захисту [5]. Такий підхід дозволяє створити ефективну та стійку до загроз корпоративну мережу з урахуванням особливостей функціонування обладнання MikroTik та Cisco.

Список використаних джерел:

1. MikroTik Wiki. Офіційна документація MikroTik. URL: https://wiki.mikrotik.com
2. Cisco. "Security solutions for small and medium businesses." Cisco.com, 2023. URL: https://www.cisco.com
3. Kent K., Souppaya M. NIST Special Publication 800-92, "Guide to Computer Security Log Management", 2006.
4. Ponemon Institute LLC. Exabeam SIEM Productivity Study, 2019.

Schneider M., Davies A., Ahlm E. Critical Capabilities for Security Information and Event Management, 2024.