УДК 004:7

***Сердійчук І.С., магістрант***
***Єфіменко А.А., к.т.н., доцент***
*Державний університет «Житомирська політехніка»*

## АРХІТЕКТУРНІ РІШЕННЯ ДЛЯ МОНІТОРИНГУ ТА РОЗПОДІЛУ РЕСУРСІВ ШЛЮЗІВ БЕЗПЕКИ ГЕТЕРОГЕННОЇ МЕРЕЖІ

Сучасний етап розвитку корпоративних мереж характеризується високим рівнем гетерогенності, об'єднуючи різноманітні класи пристроїв, операційні системи та канали зв'язку. У таких умовах шлюзи безпеки відіграють критичну роль, забезпечуючи автентифікацію, шифрування трафіку та фільтрацію загроз на межі корпоративного периметра. Постійне зростання обсягів переданих даних та збільшення кількості віддалених підключень призводять до значного підвищення вимог до продуктивності та надійності цих вузлів[1].

Аналіз існуючих інфраструктур показує, що традиційна монолітна архітектура шлюзів безпеки часто не здатна впоратися з непередбачуваними піковими навантаженнями. Виконання складних криптографічних операцій швидко виснажує обчислювальні ресурси маршрутизаторів. Наслідком цього стає збільшення кількості втрачених пакетів, зростання джитера та критичне уповільнення часу відгуку корпоративних сервісів. Крім того, у разі апаратного або програмного збою єдиного шлюзу виникає ризик повної зупинки бізнес-процесів підприємства через втрату захищеного зв'язку.

Метою дослідження є розробка архітектурних рішень для ефективного розподілу ресурсів та забезпечення відмовостійкості шлюзів безпеки у гетерогенному мережевому середовищі. Для вирішення визначеної проблеми пропонується впровадження кластерної архітектури з використанням технологій балансування навантаження та забезпечення високої доступності. Запропонована архітектура передбачає розгортання групи шлюзів, що працюють у режимі Active-Active для паралельного та рівномірного оброблення криптографічних потоків, або Active-Passive для миттєвого автоматичного перемикання у разі відмови основного вузла[3].

Ключовим компонентом розробленого рішення є інтеграція централізованої системи моніторингу. Вона має здійснювати безперервний збір телеметричних даних з кожного шлюзу, включаючи метрики завантаження CPU, використання пам'яті, поточної пропускної здатності та затримки пакетів. На основі цих показників алгоритми динамічного розподілу ресурсів здатні автоматично перенаправляти нові сесії на найменш завантажені вузли, уникаючи перевантаження окремих елементів мережі.

За результатами аналізу сформульовано такі рекомендації щодо розподілу ресурсів:

- впровадити відмовостійкі кластери шлюзів безпеки із підтримкою синхронізації станів сесій для усунення єдиної точки відмови[2];
- застосовувати адаптивні алгоритми балансування навантаження, які в реальному часі враховують поточний стан апаратних ресурсів кожного криптографічного шлюзу;
- інтегрувати централізовану систему моніторингу для безперервного аналізу телеметрії та автоматичного перенаправлення трафіку при виявленні перевантажень;
- забезпечити можливість горизонтального масштабування мережевого периметра за рахунок модульного додавання нових вузлів без зупинки роботи корпоративних сервісів.

Таким чином, результати аналітичного дослідження свідчать, що перехід до розподіленої кластерної архітектури з активним моніторингом дозволяє нівелювати ризики відмови мережевого периметра. Запропоноване рішення оптимізує використання апаратних ресурсів, зменшує час затримки при обробці трафіку та суттєво підвищує загальний рівень надійності захищених комунікацій. Перспективним напрямом подальших досліджень є розробка та застосування методів машинного навчання для предиктивного аналізу навантаження та превентивного розподілу ресурсів шлюзів безпеки.

**Список використаних джерел**

1. Convery S. Network Security Architectures. Indianapolis : Cisco Press, 2004. 792 p.

2. Kopparapu C. Load Balancing Servers, Firewalls, and Caches. New York : John Wiley & Sons, 2002. 224 p.

3. Bourke T. Server Load Balancing. Sebastopol : O'Reilly & Associates, 2001. 192 p.