УДК 004.932:004.8

Шедловська Я. І., к.т.н. , доцент кафедри інформаційних технологій та комп'ютерної інженерії
Шедловський І. А., к.т.н. , доцент, доцент кафедри інформаційних технологій та комп'ютерної інженерії
Пономаренко А. Ю. , студент гр. 123м-22-1

(*Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна*)

РОЗРОБКА АЛГОРИТМУ БЕЗПЕЧНОГО ПІДКЛЮЧЕННЯ РОЗПОДІЛЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ ДО ІНТЕРНЕТУ

Корпоративні мережі містять цінні та конфіденційні дані компанії, такі як фінансова інформація, інтелектуальна власність, персональні дані співробітників та клієнтів. Виникає необхідність захисту цих даних від несанкціонованого доступу, витоків або пошкоджень[1]. Ось кілька ключових аспектів, які відіграють роль у захисті інформації в корпоративних мережах [2]:

- Використання фаєрволів та інших мережевих пристроїв безпеки допомагає контролювати трафік у мережі, фільтрувати потенційно шкідливі пакети даних та запобігати несанкціонованому доступу.
- Віртуальні персональні мережі (VPN): забезпечують шифроване з'єднання між віддаленими точками мережі, що захищає передану інформацію від перехоплення зловмисниками.
- Ідентифікація та автентифікація допомагають запобігти несанкціонованому доступу до корпоративних ресурсів.
- Шифрування даних на рівні файлів, дисків та в мережі забезпечує додатковий рівень захисту від витоків інформації .
- Регулярне оновлення програмного забезпечення та застосування патчів на всіх рівнях інфраструктури допомагає усунути вразливості, які можуть бути використані зловмисниками.
- Моніторинг і аудит: моніторинг дозволяє виявити аномальну поведінку в мережі, а системи аудиту фіксують дії користувачів для подальшого аналізу .

У роботі було розроблено корпоративну мережу підприємства середнього бізнесу, що має центральний офіс та кілька віддалених. Підприємству необхідно здійснювати обмін конфіденційною інформації між офісами. Обмін інформацією забезпечується відкритими каналами інтернету, тому виникає необхідність розробки алгоритму безпечного підключення розподіленої корпоративної мережі до інтернету [3].

На рис. 1 представлена високорівнева мережева діаграма, що демонструє різні типи бізнес-підключень, які можуть бути реалізовані з використанням архітектури що розробляється, яка включає в себе центральний офіс та два віддалені офісу . Мережа побудована за допомогою WAN-маршрутизаторів (Cisco 2811) і LAN-комутаторів (Cisco Catalyst 2960).

Перед підключенням локальної мережі офісу до Інтернету необхідно забезпечити внутрішню безпеку локальної мережі, тому було обрано наступну послідовність дій:

1. Забезпечення безпеки локальної мережі (розмежування доступу до мережевих пристроїв, налаштування віддаленого управління мережевими пристроями, налаштування контролю додавання нових пристроїв, конфігурація VLAN).

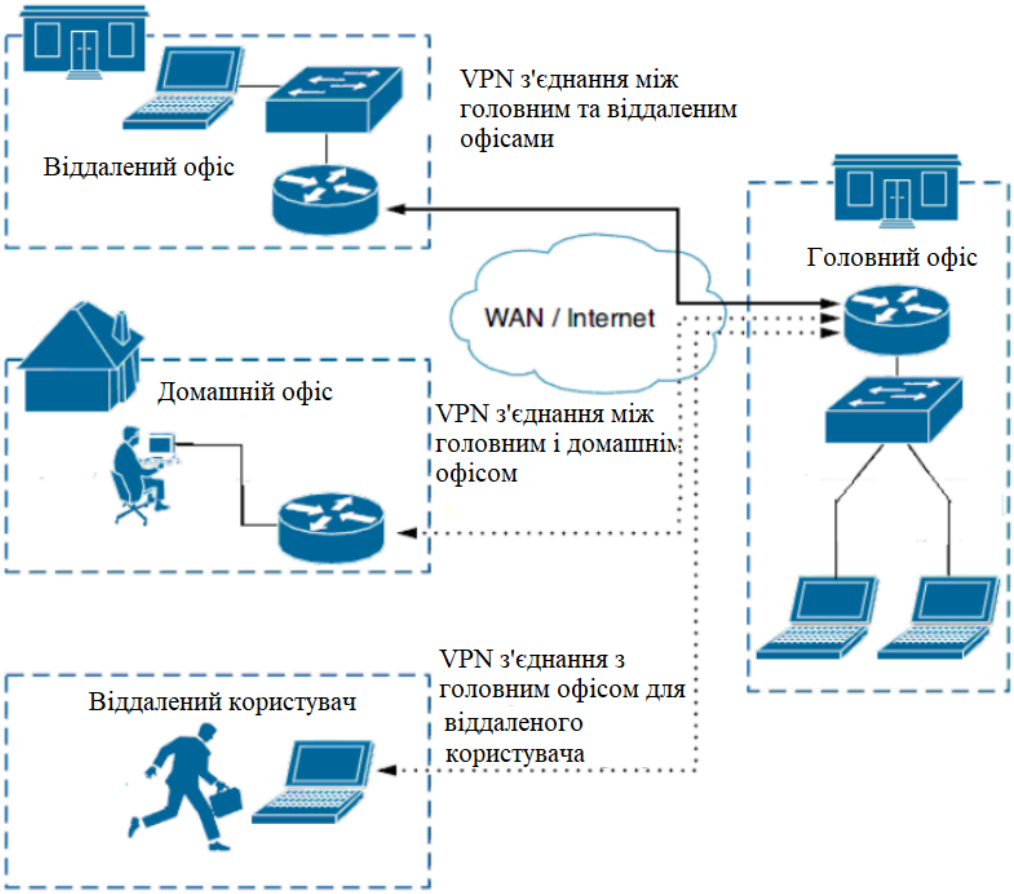

Рисунок 1 - Мережева діаграма підприємства

2. Організація безпечного підключення до мережі інтернет (налаштування віддзеркалення трафіку на центральному комутаторі, налаштування списків доступу до локальних та віддалених ресурсів, реалізація VPN з'єднання Standard Cisco IPSec між віддаленими офісами, налаштування PAT).

3. Перевірка функціонування та захищеності мережі.

В роботі було розроблено алгоритм безпечного підключення розподіленої корпоративної мережі до інтернету засобами обладнання компанії Cisco. Він включає етапи із забезпечення безпеки мережевого обладнання, внутрішніх ресурсів мережі компанії, організації безпечної взаємодії між віддаленими офісами та контроль доступу в мережі інтернет. Реалізація алгоритму була виконана в офіційній середовищі моделювання Cisco Packet Tracer

Список використаних джерел:

1. M. S. Deshmukh, A. S. Alvi “Detection and Prevention of Malicious Activities in Vulnerable Network Security Using Deep Learning” Proceedings of the 2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications - Lecture Notes in Networks and Systems pp. 319-326, 2022. 10.1007/978-981-16-6407-6_29

2. В. Л. Бурячок, Р. В. Киричок, П. М. Складанний ”Основи інформаційної та кібернетичної безпеки”. Навчальний посібник. / 2018. – 320 с.

3. Z. Zhang, X. Guo “Research on the Application of Network Security Technologies in the Network Security Operations and Maintenance Process”. Journal of Electronics and Information Science (2023) Vol. 8: 32-38. 10.23977/10.23977/jeis.2023.080406