Шнипко Т. А., магістрантка
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОЇ БЕЗПЕКИ: КОМПЛЕКСНИЙ ПІДХІД ДО ЗАХИСТУ ІНФРАСТРУКТУРИ

Захист інформації в сучасних інфокомунікаційних мережах є одним із визначальних пріоритетів. Серед основних загроз слід виділити викрадення конфіденційної інформації, знищення даних, спотворення інформації та виведення з ладу комп'ютерних систем. Ефективна система безпеки повинна мати комплексний характер і забезпечувати захист від різноманітних загроз, включаючи контроль за діяльністю працівників, які мають доступ до внутрішніх ресурсів автоматизованої інформаційної системи.

Для досягнення цієї мети необхідно використовувати спеціалізовані апаратно-програмні засоби, які забезпечують високий рівень безпеки, здійснюють моніторинг комп'ютерної системи в режимі реального часу, захищають дані від зовнішніх і внутрішніх атак, а також своєчасно реагують на спроби несанкціонованого доступу.

У зв'язку з тим, що традиційні моделі безпеки комп'ютерних мереж поступово втрачають свою ефективність, виникає нагальна потреба у розробленні та впровадженні нових підходів для забезпечення захисту автоматизованих інформаційних систем від сучасних кіберзагроз.

Використання програмного середовища Cisco Packet Tracer дозволило моделювати можливі загрози та тестувати різні конфігурації захисту. У процесі дослідження особливу увагу було зосереджено на впровадженні пристроїв та архітектури безпеки, що забезпечують захист від сучасних кіберзагроз. Було проаналізовано кілька способів вдосконалення сегменту локальної мережі (LAN) за допомогою даного програмного забезпечення, а саме:

- сегментація мережі (поділ мережі на менші, ізольовані сегменти покращує безпеку та продуктивність);
- впровадження брандмауера (брандмауер – це ключовий елемент захисту мережі від зовнішніх загроз);
- використання систем IDS/IPS (системи виявлення та запобігання вторгненням (IDS/IPS) допомагають виявляти та блокувати шкідливу активність в мережі);
- налаштування VPN-з'єднань (віртуальні приватні мережі (VPN) забезпечують безпечне з'єднання між віддаленими користувачами та локальною мережею);
- застосування концепції Zero Trust (Zero Trust – це модель безпеки, яка передбачає, що жоден користувач або пристрій не є повністю довіреним, навіть якщо він знаходиться всередині мережі; Cisco Packet Tracer дозволяє моделювати Zero Trust архітектури для посилення безпеки та контролю доступу);
- моніторинг та аналіз трафіку (Cisco Packet Tracer надає інструменти для моніторингу та аналізу мережевого трафіку);
- автоматизація завдань (Cisco Packet Tracer підтримує scripting та автоматизацію завдань);
- використання хмарних сервісів (Cisco Packet Tracer інтегрується з хмарними сервісами, що дозволяє моделювати гібридні мережі та перевіряти їхню роботу);
- безперервне навчання та експерименти (Cisco Packet Tracer – це чудовий інструмент для навчання та експериментів, його можна використовувати для вивчення нових технологій та перевірки своїх знань).

Таким чином, вдосконалення сегмента LAN засобами Cisco Packet Tracer – це безперервний процес, який залежить від наших потреб та цілей. Комбінуючи різні методи та технології, можна створити безпечну та ефективну мережу, яка відповідає сучасним вимогам захисту інфраструктури.

Список використаних джерел:

1. S. Anitha, S. Kavitha, and P. Kavitha, "Machine Learning for Operating Systems Security," International Journal of Scientific & Engineering Research, vol. 13, no. 2, pp. 243-246, 2022.
2. Навчальний курс CSOv1-ZH-POL: Співробітник CyberOps. URL: www.netacad.com.
3. Навчальний курс Вивчення мережі за допомогою Cisco Packet Tracer URL.: www.netacad.com.
4. Що таке Zero Trust і навіщо він потрібен. URL: https://www.softwareone.com/uk-ua/blog/articles/2021/06/17/zero-trust-security.