УДК 004.056

РОЗРОБЛЕННЯ МОДЕЛІ ТЕХНІЧНОГО ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЇ

Орест Полотай, Дубик Анастасія-Оксана

кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів

кафедра безпеки інформаційних технологій Національного університету «Львівська політехніка», м.Львів

Описано важливість вивчення та поглиблення знань з розробки моделей технічного захисту мережевої інфраструктури організацій.

Ключові слова: захист мережі, Cisco Packet Tracer, моделі захисту

Describes the importance of studying and deepening knowledge on the development of models of technical protection of the network infrastructure of organizations.

Key words: network protection, Cisco Packet Tracer, protection models

У сучасному цифровому світі, де інформація є ключовим ресурсом, а технологічний прогрес зростає експоненційно, питання безпеки мережевої інфраструктури стає надзвичайно актуальним та невідкладним. Кіберзагрози, що небезпечно еволюціонують, стають викликом для надійності та конфіденційності інформації, яка обробляється в мережевих системах. Від традиційних атак до вдосконалених методів кіберзлочинців, мережеві інфраструктури стають об’єктом зростаючого інтересу та загроз.

Мережева інфраструктура – це сукупність різного устаткування, а також програмного забезпечення, яка формує особливе середовище для ефективного процесу обміну даними, а також для роботи бізнес-додатків.

За допомогою мережевої інфраструктури організації обмінюються даними та пов’язують всі робочі ІТ-елементи. Мережева інфраструктура може сильно відрізнятися з точки зору:

- розміру покривається території;
- кількості підключених користувачів;
- кількості та видів доступних послуг.

Мережева інфраструктура складається з:

- активного обладнання (комутатори, маршрутизатори й т.д.);
- пасивних пристроїв (кабелі, кабельні канали, монтажні шафи, комутаційні панелі, розетки інформаційного типу);
- периферійних комп’ютерів і обладнання (ксерокси, робочі станції, сервери, принтери та сканери);
- програмного забезпечення для управління та моніторингу мережевої інфраструктури.

Важливо вміти розробляти моделі технічного захисту мережевої інфраструктури організації. Вивчення сучасної техніки та методів захисту, спрямованих на запобігання та виявлення кібератак, забезпечуючи високий рівень безпеки, є дуже важливим для забезпечення неперервності бізнес-процесів та дотримання вимог конфіденційності.

У цьому контексті, потрібно розглядати важливі аспекти впровадження технічного захисту, включаючи аналіз поточних загроз, ідентифікацію слабких місць в мережевій інфраструктурі, розробку ефективних стратегій захисту, та впровадження сучасних технологій кібербезпеки. Метою таких вивчень є не лише надання вичерпного огляду сучасних викликів та загроз у сфері кібербезпеки, але і розробка конкретної моделі захисту, яка забезпечить ефективний контроль та реагування на потенційні атаки.

Вивчення цієї теми є ключовим елементом підготовки фахівців з інформаційної безпеки та технічних спеціалістів. Розуміння та вдосконалення заходів технічного захисту мережевої інфраструктури визначають успішність організацій у високотехнологічному середовищі. Під час вивчення цієї теми, важливо навчитися розкривати важливі аспекти та внесок власний внесок у сферу кібербезпеки, сприяючи створенню більш захищеної та надійної мережевої інфраструктури для організацій.

Безумовно, вивчення теми "Розроблення моделі технічного захисту мережевої інфраструктури організації" має величезну важливість у сучасних умовах технологічного розвитку та поширення кіберзагроз. Зростання обсягу цифрової інформації, яка зберігається та обробляється в мережевій інфраструктурі, підвищує загрози з боку кіберзлочинців, які можуть намагатися незаконно отримати доступ до цих даних. Зростання кількості та складності кібератак, включаючи вимагання викупу, розповсюдження вірусів та шкідливих програм, підкреслює необхідність розробки та вдосконалення технічних заходів безпеки. Захист важливих корпоративних даних та конфіденційної інформації є вирішальним для уникнення фінансових втрат, порушень законодавства про конфіденційність та збереження репутації організації. Вдосконалені технічні засоби захисту дозволяють підтримувати неперервність бізнесу, забезпечуючи стабільну роботу мережевої інфраструктури навіть під час потенційних кібератак або природних катастроф. Організації повинні відповідати регулятивним вимогам щодо захисту даних та конфіденційності, і технічний захист мережевої інфраструктури є ключовим елементом для виконання цих вимог. Захист мережевої інфраструктури є необхідним для безпечного впровадження нових технологій, таких як хмарні обчислення, Інтернет речей (IoT) та штучний інтелект, що вимагає вдосконаленої кібербезпеки.

Отже, вивчення та розробка моделі технічного захисту мережевої інфраструктури стає критичним етапом для забезпечення безпеки, стійкості та довіри в сучасних корпоративних та технологічних середовищах.

Література

1. Кухарська Н.П., Полотай О.І. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації. Information Technology and Security. July-December 2019. Vol. 7. Iss. 2 (13), pp. 126-136.

2. Полотай О, Бойко К. Програмно-технічний захист інформації за допомогою охоронної системи. Захист інформації вінформаційнокомунікаційних системах : зб. тез. ІІІ Всеукр. наук.-практ.конф. Молодих учених, студентів і курсантів. Львів, ЛДУ БЖД. – 2019. С.76-78.

3. Полотай О., Мороз Ю., Великий В. Методи технічного захисту інформації у сфері інформаційної безпеки. Інформаційна безпека інформаційні технології: Збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів. – Львів, 2020. – С. 40-41.