Трокоз Є.М., ст. викладач
Коржовський В.В., магістрант
Державний університет «Житомирська політехніка»

ПРОЄКТ ПІДСИСТЕМИ ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ, ПОБУДОВАНОЇ НА БАЗІ ТЕХНОЛОГІЙ ETHERNET ТА WI-FI

Потреба в надійному захисті локальних мереж організацій зростає разом із поширенням кібератак та інформаційних загроз. Технології Ethernet та WiFi є основними засобами підключення до мережі, проте кожна з них має свої слабкі місця, які можуть бути використані зловмисниками для несанкціонованого доступу до інформації [1]. Відповідно, розробка підсистеми захисту локальної мережі є важливим завданням для забезпечення конфіденційності, цілісності та доступності даних [2]. Основні компоненти підсистеми захисту Система автентифікації та авторизації:

1. Впровадження двофакторної автентифікації для підвищення рівня безпеки.
2. Використання сертифікатів і ключів для захисту облікових даних користувачів [3].
3. Контроль прав доступу на основі ролей (RBAC).

Шифрування даних:

1. Використання WPA3 для захисту Wi-Fi мережі, що забезпечує сучасніші методи шифрування [4].
2. Застосування IPsec для шифрування трафіку в Ethernet мережах, що захищає дані на рівні мережевого протоколу [5].
3. Захист даних у стані спокою (at rest) та під час передачі (in transit).

Інтрузія-виявлення та попередження систем (IDS/IPS):

1. Інсталяція систем виявлення вторгнень для моніторингу мережевого трафіку в режимі реального часу.
2. Впровадження систем попередження вторгнень для автоматичного реагування на виявлені загрози.
3. Аналітика та кореляція даних для виявлення складних атак.

Віртуальні приватні мережі (VPN):

1. Використання VPN для захисту віддалених підключень до локальної мережі організації.
2. Застосування протоколів шифрування, таких як OpenVPN або IPsec, для забезпечення захищеного тунелю [1].
3. Управління доступом до VPN з метою запобігання несанкціонованим підключенням.

Захист фізичних компонентів мережі:

1. Встановлення апаратних засобів безпеки для контролю доступу до мережевих пристроїв.
2. Використання замків, сейфів та інших фізичних бар'єрів для захисту від крадіжки чи пошкодження обладнання.
3. Організація регулярних аудитів безпеки для оцінки стану захисту фізичних компонентів.

Розробка та впровадження підсистеми

При розробці підсистеми захисту локальної мережі враховуються кілька ключових аспектів:

1. Вибір апаратного та програмного забезпечення: вибір відповідних засобів для забезпечення автентифікації, шифрування та виявлення вторгнень [2].
2. Навчання персоналу: розробка та проведення навчальних програм для співробітників щодо безпечного користування мережевими ресурсами.
3. Регулярні перевірки та оновлення: постійний моніторинг та оновлення підсистеми для захисту від нових загроз.
4. Інтеграція з існуючими системами: забезпечення сумісності та ефективної роботи з уже існуючими мережевими рішеннями в організації.

Висновки. Імплементація комплексної підсистеми захисту локальної мережі, побудованої на базі технологій Ethernet та Wi-Fi, дозволяє значно підвищити рівень інформаційної безпеки в організації. Забезпечення цілісності, конфіденційності та доступності даних є ключовими елементами ефективної системи захисту [3]. Використання сучасних технологій та методів забезпечення безпеки дозволяє мінімізувати ризики та захистити організацію від можливих кібератак [4].

Список використаної літератури

1. Коваль В. А. Технології захисту локальних мереж. Вісник Харківського національного університету «ХПІ». Серія «Інформатика та управління», 2018, № 3, с. 45–52.
2. Литвиненко П. С. Сучасні методи криптографічного захисту. Вісник Львівського національного університету. Серія «Прикладна математика», 2019, № 1, с. 121–130.
3. Петренко І. М. Захист бездротових мереж Wi-Fi: проблеми та рішення. Журнал «Інформаційні технології та безпека», Одеса: ОНПУ, 2021, Т. 20, № 2, с. 75–85.
4. Бойко О. Ф. Основи інформаційної безпеки. Науковий журнал «Інформаційна безпека», Київ: Видавничий дім, 2015, Т. 11, № 4, с. 60–67.
5. Сидоренко Ю. А. Системи виявлення та запобігання вторгнень у локальних мережах. Журнал «Комп'ютерні технології та безпека», Дніпро: ДНУ, 2020, Т. 22, № 1, с. 32–41.