Пекарєв М. Д., магістрант
Головня О. С., к.пед.н., доцент
Державний університет «Житомирська політехніка»

ТЕХНОЛОГІЇ ТА ПРОТОКОЛИ ЗАХИСТУ МЕРЕЖІ

У контексті зростання кіберзагроз і збільшення обсягу мережевого трафіку питання захисту корпоративних мереж залишається одним із пріоритетних завдань у сфері інформаційної безпеки. Розвиток технологій захисту мереж орієнтований на досягнення трьох основних цілей: забезпечення конфіденційності, цілісності та доступності даних[1]. Метою даного дослідження є розгляд ключових технологій та протоколів, що застосовуються для захисту мережевих систем.

Однією з базових технологій є шифрування, яке забезпечує конфіденційність переданих даних шляхом їхнього перетворення у вигляд, незрозумілий без відповідного ключа дешифрування. Зокрема, протоколи SSL/TLS застосовуються для захисту веб-комунікацій і є стандартом для безпечного з'єднання в Інтернеті (HTTPS). З технічної точки зору, ці протоколи реалізують гібридну криптографічну систему: для встановлення з'єднання використовується асиметричне шифрування, після чого обмінюється симетричний ключ, що забезпечує швидке шифрування трафіку. Ефективність алгоритмів, таких як AES (Advanced Encryption Standard), підтверджена численними дослідженнями: навіть за наявності сучасних обчислювальних потужностей для зламування AES-256 знадобилися б трильйони років [2].

Протокол IPsec (Internet Protocol Security), що функціонує на мережевому рівні, забезпечує не лише шифрування, а й автентифікацію даних. У його транспортному режимі шифрується тільки корисне навантаження пакета, що робить його ефективним для корпоративних мереж із високими вимогами до продуктивності. Тунельний режим, навпаки, шифрує весь пакет, включно із заголовками, що ідеально підходить для створення віртуальних приватних мереж (VPN).

Віртуальні приватні мережі залишаються ключовою технологією для захисту віддаленого доступу до корпоративних ресурсів. Зокрема, протокол IKEv2/IPsec широко використовується завдяки підтримці мобільності та безперервності з'єднання, що особливо важливо для сучасних гібридних робочих моделей. Порівняно з іншими протоколами VPN, такими як L2TP чи PPTP, IKEv2/IPsec забезпечує кращу стійкість до атак типу "людина посередині" та вищу швидкість передачі даних завдяки оптимізації механізмів шифрування.

Системи виявлення та запобігання вторгненням (IDS/IPS) доповнюють традиційні методи захисту, використовуючи алгоритми машинного навчання для аналізу трафіку в реальному часі. Наприклад, сучасні IPS-системи здатні ідентифікувати атаки типу DoS/DDoS на основі аномалій у поведінці трафіку, що значно знижує ризики порушення доступності послуг.

Автентифікація є ключовим компонентом контролю доступу до мережі. Використання двофакторної автентифікації (2FA) стало стандартом у корпоративному середовищі. У межах технологій автентифікації перспективним напрямом є застосування біометричних методів, зокрема, автентифікація на основі розпізнавання відбитків пальців чи обличчя, які інтегруються з мобільними пристроями через протоколи FIDO2.

Розробка та впровадження комплексних рішень безпеки, що поєднують міжмережеві екрани, системи IDS/IPS та шифрувальні протоколи, дозволяє створити багаторівневий захист. Дослідження показують, що інтеграція таких рішень з інструментами моніторингу та аналізу (наприклад, SIEM-системами) підвищує ефективність виявлення атак до 93%.

Таким чином, сучасні технології та протоколи захисту мережі забезпечують високу стійкість до широкого спектра загроз. Однак їхня ефективність безпосередньо залежить від рівня впровадження, постійного моніторингу та своєчасного оновлення безпекових рішень, що залишається одним із основних викликів для IT-фахівців.

Список використаних джерел

1. Основи інформаційної безпеки Лужецький В.А., Кожухівський А.Д., Войтович О.П. – Друковане джерело
2. Інформаційна безпека Кавун С.В., Носов В.В., Манжай О.В. – URL:http://repository.hneu.edu.ua/bitstream/123456789/3105/1/Навчальний%20посібник.%20Інформаційна%20безпека.%20Ч.%202%20Кавун%20С.В..pdf
3. Протоколи формування захищених каналів – URL: https://ssbb.ua/poshuk-i-vyyavlennya-proslyshky/poshuk-zakladnykh-ustrojstv/protokoly-formirovaniya-zashishennykh-kanalov-na-kanalnom-urovne/