УДК 004.85

Палагін В.В., д.т.н., професор
Івченко О.В., к.т.н., доцент
Палагіна О.А., к.т.н., доцент
Воробкало О.К., магістрант
Черкаський державний технологічний університет

МЕТОДИ AI/ML ДЛЯ АНАЛІЗУ ТА НЕЙТРАЛІЗАЦІЇ КІБЕРАТАК НА VLAN

Сучасна концепція побудови корпоративних та промислових мереж, включаючи інфраструктури 5G, базується на технології VLAN (IEEE 802.1Q) як фундаментальному інструменті логічної сегментації трафіку [1]. Однак, незважаючи на широке розповсюдження, сегментація на другому рівні моделі OSI (Layer 2) не є самодостатнім засобом захисту. Зростаюча складність мережевих ландшафтів та поява нових векторів атак на протоколи канального рівня роблять проблему безпеки VLAN критично важливою. Особливої гостроти це питання набуває в умовах динамічних середовищ, де традиційні статичні засоби захисту не встигають адаптуватися до мінливих сценаріїв вторгнень.

Основними деструктивними впливами на віртуальні мережі є атаки, спрямовані на обхід логічної ізоляції. Серед них ключовими є [2]:

- *VLAN Hopping (Double Tagging)* - використання зловмисником подвійного тегування 802.1Q для надсилання пакетів у суміжний VLAN в обхід маршрутизатора;
- *Switch Spoofing* - імітація зловмисником поведінки комутатора за допомогою протоколу DTP (Dynamic Trunking Protocol) для встановлення магістрального з'єднання (trunk) та отримання доступу до всіх VLAN мережі;
- *MAC-flooding (CAM-table overflow)* - генерація великої кількості фіктивних MAC-адрес для переповнення таблиці комутації, що змушує комутатор працювати у режимі концентратора (hub), транслюючи трафік на всі порти.

Класичні підходи до захисту VLAN базуються на «жорсткій» детермінованій логіці: відключення невикористовуваних портів, вимкнення DTP, використання Port Security або статична фільтрація подвійних тегів. Хоча ці методи забезпечують високу швидкість обробки (low latency) та відсутність помилкових спрацьовувань для відомих сигнатур, вони мають суттєві недоліки, зокрема:

- *негнучкість* - нездатність виявити атаки, параметри яких хоча б мінімально відрізняються від встановлених правил;
- *складність масштабування* - необхідність ручного переписування конфігурацій при кожній зміні архітектури мережі;

- *вразливість до динамічних атак* - детермінована логіка безсила проти інтелектуальних методів обходу, які імітують легітимну поведінку.

Застосування методів машинного навчання (AI/ML) для захисту VLAN дозволяє перейти від статичного аналізу окремих кадрів до комплексного моніторингу динаміки мережевого трафіку. Метод базується на вилученні статистичних ознак (features) з потоку даних, таких як ентропія MAC-адрес, частота появи тегів 802.1Q, часові інтервали між пакетами та специфічні прапорці протоколів канального рівня. Використання алгоритмів класифікації дає змогу виявляти складні закономірності, які не охоплюються жорсткою логікою. Це вирішує проблему «негнучкості» класичних методів: система стає здатною ідентифікувати атаку навіть за умови мінімальної модифікації її параметрів зловмисником, що значно знижує рівень помилкових пропусків (False Negatives) у порівнянні з детермінованими фільтрами.

Технічна реалізація пропонується у вигляді інтелектуального модуля аналізу, який інтегрується у дзеркальний порт комутатора (SPAN/RSPAN) або працює на рівні програмно-конфігурованих мереж (SDN). Процес включає етап попередньої обробки трафіку та агрегування потоку Ethernet-кадрів у вектори ознак. Підготовлена ML-модель аналізує ці вектори в режимі реального часу, порівнюючи поточну активність із профілем легітимної поведінки мережі. Такий підхід забезпечує адаптивність захисту, коли система самостійно корегує межі спрацювання при зміні архітектури мережі, усуваючи необхідність постійного ручного переписування конфігурацій та правил доступу.

Таким чином, застосування запропонованого підходу на основі AI/ML дозволяє трансформувати захист VLAN із пасивного набору статичних правил у динамічну адаптивну систему, здатну виявляти аномалії на випередження, що забезпечує високий рівень безпеки складних мережевих інфраструктур завдяки автоматизації аналізу трафіку та мінімізації впливу людського фактора.

Список використаних джерел

1. IEEE Std 802.1Q-2018. IEEE Standard for Local and Metropolitan Area Networks — Virtual LANs. — New York : IEEE, 2018. — 1992 p.

2. Nurfaishal M. D., Akbar Y. Analisis Efektivitas Keamanan Jaringan Layer 2: Port Security, VLAN Hopping, DHCP Snooping. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*. 2024. Vol. 5, no. 3. P. 3278–3290. DOI: 10.35870/jimik.v5i3.975.