УДК 004.056
Л. Гнатківський; А. Турчманович; Н. Загородна, к. т. н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ ПІДХОДІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

UDC 004.056
L. Hnatkivskyi; A. Turchmanovych; N. Zagorodna, PhD., Assoc. Prof.

RESEARCH OF APPROACHES TO IMPROVE EFFICIENCY OF INTRUSION DETECTION SYSTEMS

Сучасна мережева безпека базується на багаторівневому підході, що включає різноманітні технологічні рішення. Міжмережеві екрани (firewalls) контролюють потоки трафіку на основі встановлених правил, системи виявлення (IDS) та запобігання вторгненням (IPS) аналізують мережеву активність на предмет шкідливої поведінки, а SIEM-платформи агрегують та аналізують інформацію про події безпеки з усіх джерел.

У цій екосистемі IDS відіграють особливу роль інтелектуального аналітичного інструменту. На відміну від активних систем блокування, IDS функціонує в пасивному режимі моніторингу, аналізуючи копію мережевого трафіку без втручання в його потік, що дає можливість ідентифікувати потенційні загрози безпеці, виявляти складні багатоетапні атаки та несанкціоновані спроби доступу до корпоративних ресурсів. Однак стрімка еволюція методів кібератак, зростання обсягів мережевого трафіку та поява нових технологій вимагають постійного вдосконалення можливостей IDS для підтримання їхньої ефективності. Більшість джерел за способом виявлення атак поділяють IDS на такі, що працюють:

- на основі сигнатур (Signature-Based) та порівнюють мережеву активність з базою відомих патернів атак;
- на основі аномалій (Anomaly-Based) та класифікують мережеву активність на нормальну та аномальну на основі правил або евристик, здатні виявляти раніше невідомі загрози;
- на основі специфікації (Specification-Based) та відстежують процеси та порівнюють фактичні дані з очікуваною поведінкою програм;
- гібридні (Hybrid) поєднують різні методи, щоб забезпечити більш точне та ефективне виявлення атак.

Основними шляхами підвищення ефективності роботи IDS вважають впровадження методів штучного інтелекту, використання методів нечіткої логіки, розробку механізмів безперервного навчання та використання алгоритмів машинного навчання для аналізу контексту подій, що значно знижує кількість false positives.

Література

1. Rajasekaran, K. (2020). Classification and Importance of Intrusion Detection System. International Journal of Computer Science and Information Security,. 10. 44.
2. Alrayes, Fatma & Zakariah, Mohammed & Alzaylaee, Mohammed & Amin, Syed & Khan, Zafar Iqbal. (2025). Optimizing Intrusion Detection System (IDS) with Hybrid Random Forest and CNN-LSTM Models for Improved Accuracy and Efficiency. 10.21203/rs.3.rs-6766340/v1.