УДК 004.77
В. Поліщук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ НА ОСНОВІ АНАЛІЗУ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

UDC 004.77
V. Polishchuk

DEVELOPMENT OF AN ANOMALY-BASED INTRUSION DETECTION SYSTEM USING MACHINE LEARNING FOR NETWORK TRAFFIC ANALYSIS

Сучасні інформаційні системи стикаються з низкою проблем, серед яких зростання кількості кібератак, еволюція методів атак, а також недостатня адаптивність традиційних систем виявлення вторгнень (IDS). Традиційні IDS здебільшого базуються на сигнатурному або евристичному аналізі, що дозволяє ефективно виявляти лише добре відомі атаки. Їх основним недоліком є нездатність розпізнавати нові, невідомі загрози і частота хибнопозитивних (false positive) спрацьовувань, що ускладнює роботу аналітиків безпеки. Тому розробка системи виявлення вторгнень на основі аналізу аномалій у мережевому трафіку з використанням машинного навчання є надзвичайно актуальною. Такий підхід дозволяє забезпечити адаптацію до нових загроз та ефективне виявлення невідомих атак [1].

Використання машинного навчання для обробки мережевого трафіку дозволяє побудувати моделі, які навчаються розпізнавати відхилення від нормальної поведінки. Алгоритми, такі як кластеризація (наприклад, DBSCAN) чи метод опорних векторів (SVM), успішно застосовуються для аналізу великих обсягів мережевих даних [2].

Система виявлення вторгнень була реалізована з використанням TensorFlow, Snort та Python-бібліотеки Scikit-learn для обробки даних. Тестування системи виконано на основі набору даних CICIDS2017, який містить як звичайні сесії, так і сесії з атаками, які відображає відповідний мережевий трафік. Розроблена система дозволила ефективно виявляти аномалії у мережевому трафіку, зокрема атаки типу Brute Force, DoS та DDoS, з високою точністю, забезпечуючи адаптивний підхід до нових загроз.

Загалом, розвиток технологій обробки даних і штучного інтелекту відкриває нові можливості для галузі кібербезпеки та вирішення її основних завдань щодо захисту. Зокрема, автоматизація аналізу мережевого трафіку дозволяє значно скоротити час реакції на загрози, підвищуючи ефективність роботи IT-фахівців. Такі системи можуть працювати як у локальних мережах, так і в хмарних середовищах, що робить їх універсальними для різних типів організацій [3].

Завдяки використанню таких систем у корпоративних мережах різного масштабу можна підвищити загальний рівень безпеки, зменшити ризики витоку даних і забезпечити стабільну роботу інформаційних ресурсів. Інтеграція алгоритмів машинного навчання дозволяє адаптувати системи до нових загроз, виявляючи аномалії навіть у разі невідомих атак. Реалізація подібних рішень сприяє підвищенню ефективності моніторингу мереж і забезпечує довготривалий захист від новітніх кіберзагроз.

Література

1. Xie Y., Yu S. A deep learning approach to network intrusion detection // IEEE Transactions on Emerging Topics in Computing. 2015.
2. Kim D. Y., Kang H. Anomaly detection in network traffic using unsupervised deep learning methods // IEEE Access. 2020.
3. Sommer R., Paxson V. Outside the closed world: On using machine learning for network intrusion detection // IEEE Symposium on Security and Privacy. 2010.