УДК 004.056
Гуменюк В. Р., Муж В. В., к.ю.н., доцент кафедри кібербезпеки.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В IPS ТА IDS СИСТЕМАХ

Humeniuk V. R., Muzh V. V., Cand. Sc. (Law), Associate Professor of the Department of Cybersecurity.

USING ARTIFICIAL INTELLIGENCE IN IPS AND IDS SYSTEMS

В сучасному світі кібербезпеки, системи виявлення та запобігання вторгненням (IPS/IDS) відіграють ключову роль у захисті організацій від широкого спектру кіберзагроз. Однак, зі зростанням складності та хитромудрості кібератак, традиційні IPS/IDS системи стикаються з рядом викликів, що обмежують їхню ефективність. Серед цих викликів:

1. Невідповідність до нових загроз**:** Традиційні IPS/IDS системи часто базуються на відомих сигнатурах атак, що робить їх менш ефективними проти нових чи модифікованих загроз, які не відповідають існуючим сигнатурам.
2. Високий рівень помилкових позитивних сповіщень: Системи, що базуються на сигнатурах, схильні до великої кількості помилкових сповіщень, що може призводити до "втоми" аналітиків безпеки та ігнорування справжніх загроз.
3. Обмежена масштабованість та гнучкість: Традиційні системи вимагають постійного оновлення сигнатур та правил, що може бути трудомістким та не завжди встигає за швидкістю розвитку загроз.

Впровадження AI і ML у IPS/IDS може допомогти подолати ці виклики. Штучний інтелект може вчитися з даних про вже відомі атаки, підлаштовуючись під нові методи ведення кібервійни. Це забезпечує глибший аналіз поведінкових патернів, дозволяючи виявити загрози, які не можуть бути визначені традиційними методами. Застосування ML може значно зменшити кількість помилкових позитивних сповіщень, підвищуючи точність системи і зменшуючи навантаження на аналітиків. Також, AI та ML можуть забезпечити більшу гнучкість та масштабованість систем безпеки, адаптуючись до змін у кіберзагрозах в реальному часі. Основною мотивацією дослідження є покращення ефективності IPS/IDS систем шляхом інтеграції AI та ML, що дозволить організаціям ефективніше виявляти та реагувати на кіберзагрози, забезпечуючи більш високий рівень безпеки.

Основна мета цього дослідження покликана вивчити, як AI і ML можуть бути інтегровані в існуючі IPS/IDS системи, з метою підвищення їхньої ефективності у виявленні, запобіганні, реагуванні та відновленні після інцидентів безпеки. Також вивчаються методи адаптації цих систем до постійно змінюваних загроз. У роботі розглядаються наступні дослідницькі запитання:

1. Які AI/ML технології та алгоритми можна використовувати в IPS/IDS системах, та які їхні переваги та недоліки?
2. Як можна інтегрувати AI/ML у існуючі системи безпеки, зокрема в IPS/IDS?
3. Як впровадження AI/ML впливає на ефективність систем IPS/IDS у боротьбі з кіберзагрозами?

Література

1. Intrusion Detection System using AI and Machine Learning Algorithm (2017). [online] irjet.net. Available at: https://www.irjet.net/archives/V4/i12/IRJET-V4I12314.pdf.