XLV INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE «KEY ASPECTS OF THE DEVELOPMENT OF SCIENTIFIC RESEARCH IN MODERN CONDITIONS»

Section name – Information Technology & Cybersecurity

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОГНОЗУВАННЯ ВИЯВЛЕННЯ АНОМАЛІЙ МЕРЕЖЕВОГО ТРАФІКУ

Рихва Володимир,
Аспірант кафедри кібербезпеки та інформаційних технологій
volodymyr.rykhva@hneu.net
Харківський національний економічний
університет імені Семена Кузнеця, Україна

У сучасному світі, де цифрові технології стали невід'ємною частиною нашого повсякденного життя, безпека мережевого трафіку набуває особливого значення. Поширення Інтернету речей (IoT), експоненційне зростання обсягів даних і зростаюча залежність від онлайн-сервісів вимагають розробки ефективних методів для захисту мережевих систем. Аномалії мережевого трафіку – це відхилення від нормальної поведінки мережі, які можуть виникати раптово та серйозно впливати на її функціонування. Варто зауважити, що не всі аномалії викликані шкідливою активністю, такою як DDoS-атаки, сканування портів або вірусні атаки. Часто вони можуть бути результатом зміни характеру використання програмного забезпечення користувачами або інших несанкціонованих змін.

Виявлення аномалій відіграє ключову роль у кібербезпеці. Цей процес полягає у виявленні даних, які відрізняються від звичайного або очікуваного поведінкового шаблону, наприклад, відхилень від звичайного розподілу ймовірностей, або незвичайних змін у формі та амплітуді сигналів у часових рядах.

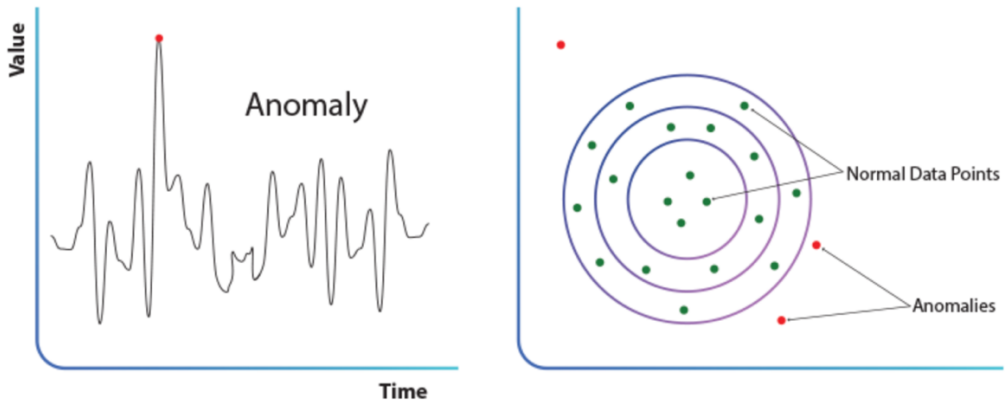

Рис.1. Приклади аномальної поведінки

Аномалії, що можуть виникнути у мережі можна поділити на дві основні категорії:

1. Аномалії, пов'язані з продуктивністю: включають проблеми, що впливають на швидкодію та ефективність мережі, такі як затримки, втрати пакетів або перевантаження каналів.

2. Аномалії, пов'язані з безпекою: включають несанкціоновані дії, які можуть загрожувати цілісності, конфіденційності або доступності інформації [1].

Для виявлення та попередження безпекових інцидентів використовується широкий спектр спеціалізованих систем і засобів, зокрема системи управління мережею, аналізатори мережевих протоколів, системи тестування навантаження, системи моніторингу мережі, міжмережеві екрани (firewall), антивірусне програмне забезпечення, системи виявлення та запобігання атак (Intrusion Detection and Prevention Systems, IDS/IPS), системи контролю цілісності, криптографічні засоби захисту тощо.

Однак традиційні методи виявлення аномалій у мережевому трафіку часто стикаються з проблемами масштабованості, високим рівнем помилкових спрацьовувань та недостатньою ефективністю у виявленні нових, невідомих загроз. З розвитком технологій машинного навчання та, зокрема, глибинного навчання (Deep Learning), з'явилися нові можливості для підвищення ефективності систем виявлення аномалій [2]. Глибинне навчання, як одна з галузей штучного інтелекту, дозволяє моделювати складні нелінійні залежності в даних, що робить його потужним інструментом для аналізу великого обсягу мережевого трафіку. Використання нейронних мереж глибокої архітектури дає змогу автоматично витягувати ознаки та виявляти приховані закономірності, які можуть бути недоступними для традиційних методів. Сучасні дослідження показують, що методи глибинного навчання мають значний потенціал у виявленні аномалій, забезпечуючи високу точність та швидкість обробки. Проте існують виклики, пов'язані з необхідністю великих обсягів даних для навчання, проблемами інтерпретованості моделей, а також адаптацією до постійно змінних умов мережі. У зв'язку з цим актуальним завданням є розробка та дослідження методів виявлення аномалій у мережевому трафіку на основі глибинного навчання, які б забезпечували високу ефективність, адаптивність та стійкість до різноманітних загроз.

На сьогоднішій день використання методів штучного інтелекту вже активно застосовується для виявлення мережевих загроз [3]. Рис.2 ілюструє розподіл алгоритмів і методів штучного інтелекту для виявлення кіберзагроз:

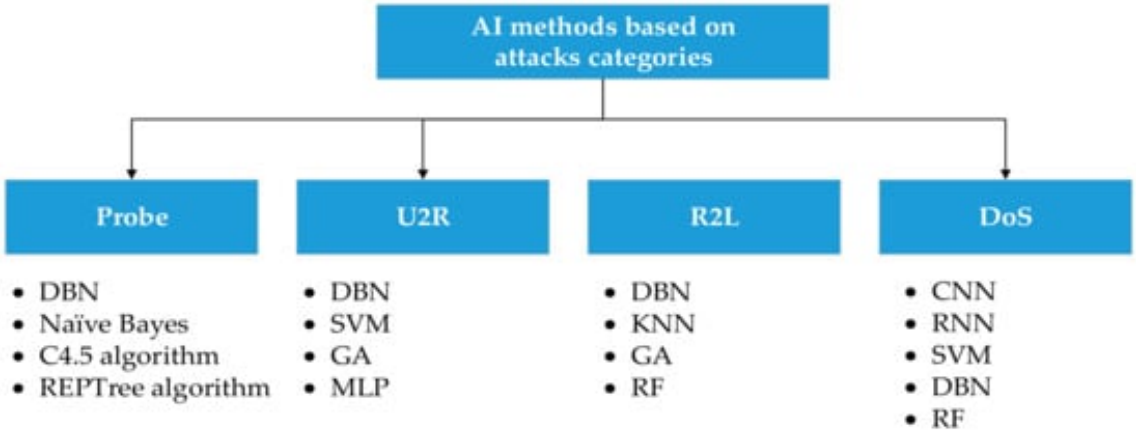

Рис.2. Ілюстрація методів штучного інтелекту на основі категорій атак

Прогнозування кібератак є однією з найперспективніших областей застосування ШІ та машинного навчання в кібербезпеці [4]. Здатність передбачати та запобігати атакам ще до їх виникнення має потенціал для значного підвищення безпеки мережі та системи. Це дає змогу своєчасно виявляти кібератаки та сповіщати про них ще до того, як вони відбудуться. На Рис.3 показано використання ШІ та машинного навчання для прогнозування кібератак.

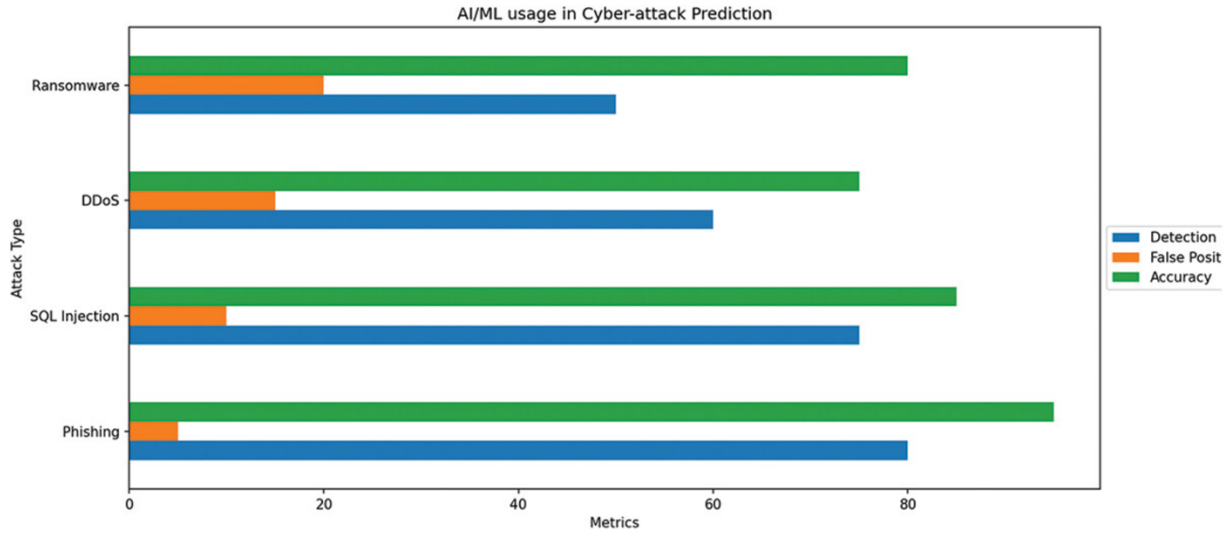

Рис. 3. Використання ШІ у прогнозуванні кібератак

Отже, виявлення аномалій у мережевому трафіку є важливим елементом забезпечення кібербезпеки, що дозволяє ефективно реагувати на нові та існуючі загрози. З розвитком методів глибинного навчання та машинного навчання з'являються нові можливості для покращення точності та адаптивності систем виявлення аномалій, що особливо важливо у контексті постійно зростаючої складності та обсягів мережевих даних. Використання штучного інтелекту для прогнозування кібератак має значний потенціал для підвищення безпеки мережевих систем та своєчасного запобігання інцидентам.

References

1. Столяр А. Л. Аналіз сучасних методів виявлення аномалій в комп'ютерних мережах. 2023, URL: https://doi.org/10.18372/2073-4751.74.17888.

2. Sunanda Gamage, Jagath Samarabandu. Deep learning methods in network intrusion detection: A survey and an objective comparison. 2020, URL: https://doi.org/10.1016/j.jnca.2020.102767

3. Mujaheed Abdullahi, Yahia Baashar, Hitham Alhussian. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. 2022, URL: https://doi.org/10.3390/electronics11020198

4. Nachaat Mohamed. Current trends in AI and ML for cybersecurity: A state-of-the-art survey". 2023, URL: https://doi.org/10.1080/23311916.2023.2272358