УДК 004.8:004.056.5

Андрій ПРИЛОЖЕНКО, Олексій СТОПАКЕВИЧ

Національний університет «Одеська політехніка»

ШТУЧНИЙ ІНТЕЛЕКТ У СИСТЕМАХ КІБЕРБЕЗПЕКИ

Вступ. Сучасний ландшафт кіберзагроз характеризується безпрецедентним зростанням складності, швидкості та обсягів атак. Традиційні методи захисту, такі як антивіруси на основі сигнатур, міжмережеві екрани з фіксованими правилами та прості системи виявлення вторгнень (Intrusion Detection System), дедалі частіше виявляються неефективними проти новітніх загроз, зокрема атак нульового дня, поліморфного шкідливого програмного забезпечення та складних цільових атак (Advanced Persistent Threat). Ці атаки часто маскуються під легітимний трафік, що робить їх виявлення майже неможливим для статичних систем захисту.

Мета: Метою дослідження є аналіз можливостей та методів застосування технологій штучного інтелекту (ШІ), зокрема машинного (Machine Learning) та глибокого (Deep Learning) навчання, для побудови адаптивних та проактивних систем кібербезпеки, здатних ідентифікувати та реагувати на складні кіберзагрози в режимі реального часу.

1.Недоліки традиційних систем кіберзахисту

Традиційні системи, такі як Signature-based IDS/IPS, покладаються на заздалегідь відому базу даних сигнатур (зразків) відомих загроз. Розглянемо основні недоліки цього підходу.

1. Реактивність. Система може виявити лише ті загрози, які вже були ідентифіковані, проаналізовані, і для яких була створена сигнатура. Це залишає організації вразливими до атак нульового дня.

2. Обсяг сигнатур. Бази даних сигнатур розростаються до величезних розмірів, що вимагає значних обчислювальних ресурсів для сканування трафіку та файлів.

3. Маскування. Зловмисники активно використовують техніки обфускації та поліморфізму, щоб змінити «вигляд» шкідливого коду, роблячи його нерозпізнаваним для сигнатурних сканерів. Статичні правила міжмережевих екранів також не здатні аналізувати поведінковий контекст дій користувача або мережевого потоку, що дозволяє атакам розвиватися всередині периметра мережі після початкового проникнення. Виникає гостра потреба в переході від реактивного до проактивного, предиктивного захисту, який можуть забезпечити інструменти ШІ [1], [2].

2.Два підходи машинного навчання для виявлення аномалій.

Ключовою перевагою штучного інтелекту в кібербезпеці є його здатність навчатися та адаптуватися. Замість пошуку відомих «поганих» зразків, системи на основі ШІ вивчають «нормальну» поведінку мережі, користувачів, програм та пристроїв. Будь-яке відхилення від цієї встановленої базової лінії (baseline) розглядається як потенційна аномалія або загроза. Для цього використовуються переважно два такі підходи машинного навчання.

1. Навчання з учителем (Supervised Learning). Моделі (наприклад, Support Vector Machines, Random Forests, нейронні мережі) навчаються на величезних, заздалегідь розмічених наборах даних, що містять приклади як легітимного, так і шкідливого трафіку чи файлів. Цей підхід ефективний для класифікації спаму, фішингових листів та відомих типів шкідливого ПЗ.

2. Навчання без учителя (Unsupervised Learning). Цей підхід є критично важливим для виявлення атак нульового дня. Моделі (наприклад, кластеризація, K-Means, Density-Based Spatial Clustering of Applications with Noise) аналізують нерозмічені дані, самостійно знаходячи в них приховані патерни та структури. Система будує профіль нормальної активності і сигналізує про будь-які викиди (outliers), які не відповідають цьому профілю. Наприклад, якщо обліковий запис користувача, який зазвичай працює з 9:00 до 18:00 з однієї IP-адреси, раптово починає масове завантаження даних о 3:00 ночі з іншої країни – це явна аномалія, яку ШІ негайно зафіксує [1], [2].

3. Глибоке навчання та автоматизоване реагування

Розглянемо більш просунуті методи, зокрема глибоке навчання (Deep Learning). Моделі DL, такі як рекурентні нейронні мережі (РНМ) та їх різновиди (Long Short-Term Memory, Gated Recurrent Unit), особливо ефективні для аналізу послідовних даних, якими є мережеві пакети або лог-файли. Вони здатні розуміти контекст і виявляти складні, розтягнуті в часі атаки, які складаються з багатьох, на перший погляд, не пов'язаних між собою подій. Однак, виявлення загрози – це лише частина завдання. Сучасні системи кібербезпеки інтегрують ШІ в платформи класу SOAR (Security Orchestration, Automation and Response)[3].

SOAR використовує ШІ для автоматизації рутинних завдань аналітиків безпеки. Коли ML-модель виявляє аномалію, SOAR-платформа матиме такі можливості.

1. Збагатити дані. Автоматично зібрати додаткову інформацію про підозрілу IP-адресу, хеш файлу чи домен з відкритих джерел (Threat Intelligence).

2. Оцінити ризик. Присвоїти інциденту пріоритет на основі контексту (наприклад, чи стосується це критичного сервера).

3. Виконати реагування. Автоматично виконати заздалегідь визначений сценарій (playbook), наприклад, заблокувати IP-адресу на міжмережевому екрані, ізолювати інфікований пристрій від мережі або призупинити дію скомпрометованого облікового запису. Це дозволяє реагувати на загрози за мілісекунди, замість годин чи днів, які потрібні людині-аналітику. Порівняльний аналіз основних алгоритмів ML, що застосовуються в кібербезпеці, наведено в таблиці 1 [4].

Разом з тим, впровадження ШІ створює і нові виклики. По-перше, це так звані «змагальні атаки» (adversarial attacks), коли зловмисники цілеспрямовано "обманюють" ML-модель, подаючи їй на вхід згенеровані дані, що призводять до хибної класифікації[5]. Наприклад, незначна зміна кількох пікселів у зображенні може змусити нейронну мережу "не побачити" загрозу. По-друге, ШІ-моделі вимагають величезних обсягів якісних даних для навчання, що може бути проблемою для багатьох організацій.

Таблиця 1 – Порівняння алгоритмів ШІ для завдань кібербезпеки

Алгоритм	Тип навчання	Основне завдання	Переваги	Недоліки
Random Forest	З учителем	Класифікація (спам, шкідливе ПЗ)	Висока точність, стійкість до перенавчання	"Чорна скринька", важко інтерпретувати
K-Means	Без учителя	Виявлення аномалій (поведінка)	Простота, швидкість на великих даних	Потрібно знати кількість кластерів (k)
DBSCAN	Без учителя	Виявлення аномалій (викиди)	Не вимагає знання 'k', знаходить кластери довільної форми	Чутливий до параметрів, повільний
LSTM (RNN)	З учителем/без учителя	Аналіз послідовностей (мережеві пакети, лог-файли)	Розуміння контексту, виявлення APT	Висока обчислювальна складність

Висновок. Отже, штучний інтелект фундаментально змінює парадигму кібербезпеки, переміщуючи фокус з реактивного захисту на основі сигнатур до проактивного виявлення загроз на основі аналізу поведінки та аномалій. Методи машинного та глибокого навчання дозволяють ідентифікувати складні та раніше невідомі атаки. Інтеграція ШІ з платформами SOAR забезпечує автоматизоване реагування, що критично важливо в умовах зростаючої швидкості кібератак. Попри виклики, пов'язані зі змагальними атаками та потребою у великих даних, ШІ є сьогодні найперспективнішим інструментом для побудови стійких та адаптивних систем захисту інформації в майбутньому.

Перелік використаних джерел.

1. Buczak, A. L., & Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security. IEEE Communications Surveys & Tutorials. 2021. Vol. 18, No. 2. P. 1153–1176.

2. Xin, Y., et al. Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access. 2022. Vol. 6. P. 35365–35381.

3. Gartner Magic Quadrant for Security Orchestration, Automation and Response (SOAR) Platforms. (2024). [Електронний ресурс]. Режим доступу: https://www.gartner.com/en/research

4. Goodfellow, I., Bengio, Y., Courville, A.Deep Learning. MIT Press, 2022. 800 p.

5. Корченко О.Г., Іванченко Є.В. Аналіз ризиків в системах кіберзахисту на основі нечіткої логіки та нейронних мереж. Київ: Видавництво "Політехніка", 2023. 240 с.