.

Секція: **Математика та статистика**

УДК 519.85

Бутрин М. − ст. гр. КН-321
Відокремлений структурний підрозділ «Тернопільський фаховий коледж ТНТУ імені Івана Пулюя»

МАТЕМАТИЧНІ МЕТОДИ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРЗАХИСТІ ТА УПРАВЛІННІ РОЯМИ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Науковий керівник: к.пед.н. Фігурська Л. В

Butryn M.
Separate Structural Subdivision «Ternopil Professional College of Ternopil Ivan Puluj National Technical University»

MATHEMATICAL METHODS OF ARTIFICIAL INTELLIGENCE SYSTEMS IN CYBERSECURITY AND SWARM CONTROL OF UNMANNED AERIAL VEHICLES

Supervisor**:** PhD in Pedagogy, Liubov Fihurska

Ключові слова: штучний інтелект, кіберзахист, рої дронів
Keywords: artificial intelligence, cyber defense, drone swarms

Постановка проблеми. Останні роки наочно показали, що число автоматизованих кібератак на державну інфраструктуру після 2022 року, за різними підрахунками, зросло в десять разів. Паралельно безпілотні апарати з другорядного розвідувального засобу перетворились на повноцінний бойовий інструмент, що виконує ударні, розвідувальні і логістичні функції. Це вимагає застосування штучного інтелекту як технології, що дозволяє реагувати на події швидше, ніж це фізично здатна робити людина.

Класичні IDS/IPS-системи захищають мережу за принципом «впізнай знайомого ворога» − вони порівнюють трафік із базою відомих сигнатур атак. Метод добре себе виправдовує проти задокументованих загроз, але пасує перед zero-day-вразливостями та поліморфним шкідливим програмним забезпеченням.

Машинне навчання підходить до задачі з протилежного боку: замість каталогу відомих атак воно будує ймовірнісну модель нормальної поведінки мережі, де кожен стан системи описується вектором параметрів $X = (x_1, \dots x_n)$. Відхилення визначається як подія з малою ймовірністю $P(x) < \varepsilon$, що дозволяє виявляти навіть раніше невідомі атаки.

Нейронні мережі і алгоритми reinforcement learning формалізують процес реагування як задачу оптимізації в межах марковського процесу прийняття рішень, де максимізується функція очікуваної винагороди $Q(s,a) = E|\sum_{t=0}^{\infty} \gamma^t R_t|$,

де s -- поточний стан системи (наприклад: мережа під атакою, нормальний режим, перевантаження),
a -- дія (ізолювати вузол, змінити маршрут, заблокувати трафік)
Rt-- винагорода в момент часу t (наприклад: +1 − атака зупинена, −1 -- система зламана, −0,2 -- зайва ізоляція),
γ ***(0 < γ < 1)*** -- коефіцієнт «важливості майбутнього» (близько до 1 − думаємо наперед, близько до 0 − реагуємо миттєво)
E -- математичне сподівання (усереднення, бо результат не завжди однаковий).

Ця функція показує, наскільки вигідно виконати дію *a* у стані *s*, з урахуванням усіх майбутніх наслідків.

Адаптивне навчання є ключовою відмінністю ШІ-захисту від статичних систем. Поведінка мережі описується як випадковий процес, де кожен стан задається вектором параметрів *X(t)*, а його розподіл ймовірностей *P(X)* постійно оновлюється на основі нових спостережень. Зокрема, оновлення моделі може бути представлене у байєсівській формі:

$$P(X \mid D) = \frac{P(D \mid X)\,P(X)}{P(D)}$$

де D -- нові дані про мережеву активність. Це означає, що кожна нова атака змінює апріорні оцінки і підвищує точність подальшого виявлення.

У поєднанні з концепцією Moving Target Defense (MTD), де стан системи змінюється у часі *S(t),* захист набуває динамічного характеру.

Концепція роєвого застосування дронів передбачає децентралізовану систему агентів A_i, де глобальна поведінка виникає з локальних взаємодій $f(Ai, Aj)$. Кожен апарат приймає рішення на основі локального стану $s_i(t)$, а ключові задачі системи зводяться до мінімізації ймовірності зіткнень *P(collision),* оптимального розподілу ресурсів $min\sum cijxij$ та підтримання зв'язності графа *G(t).*

Захист каналів управління реалізується через багаторівневу модель стійкості: криптографію AES (зниження *P(decrypt)*), частотне стрибкоподібне перемикання FHSS (підвищення ентропії *H(X))* та інерціальну навігацію як резерв при деградації каналу C(t). ШІ виконує функцію керування u(t), забезпечуючи адаптивне перемикання каналів у реальному часі. Наступальні кібероперації формалізуються як задача оптимізації у просторі вразливостей Ω:

$$arg(max\, I(\omega)),$$

що описує вибір найефективнішого вектора впливу на цифрову інфраструктуру противника.

Висновки. Штучний інтелект у кіберзахисті та управлінні роями БпЛА забезпечує швидке й адаптивне реагування на загрози, а його ефективність безпосередньо ґрунтується на математичних методах -- теорії ймовірностей, оптимізації, динамічних систем і теорії інформації. Саме ці підходи дозволяють формалізувати процеси виявлення атак, прийняття рішень і координації автономних систем в умовах невизначеності та активної протидії.

Список використаних джерел:

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016. 800 p.
2. Bonabeau E., Dorigo M., Theraulaz G. Swarm Intelligence: From Natural to Artificial Systems. Oxford University Press, 1999. 320 p.
3. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // IEEE Symposium on Security and Privacy. 2010. P. 305-316.
4. Яковів І. Б. Перспективи застосування роїв БПЛА в сучасних збройних конфліктах // Науковий вісник НУОУ. 2023. № 4. С. 45–52.