УДК 004.056.5:004.852

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ МАШИННОГО НАВЧАННЯ В КІБЕРБЕЗПЕЦІ: ОГЛЯД ІННОВАЦІЙ

Фролов Д.І., Дягілєва М.С.
e-mail: denys.frolov@nure.ua, e-mail: mila.diahilieva@nure.ua
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського
м. Харків, Україна

To develop machine learning (ML) technologies, bionic and evolutionary approaches are used. ML is effectively applied for the recognition and classification of malicious software. Since 2021, there has been a significant increase in the number of published patents, indicating a growing trend of integrating artificial intelligence into cybersecurity. Related research has great scientific and commercial potential, particularly for solving tasks related to process automation and increasing system adaptability.

В Україні вже більше десяти років фактично триває кібервійна та четвертий рік - повномасштабна. В поточному контексті, кількість кібератак, як складова військових активностей проти України, спрямована насамперед на критичну інфраструктуру країни.

Сучасні дослідження у галузі штучного інтелекту зосереджені на вдосконаленні методів представлення знань, моделювання міркувань, комунікації між людиною та системою, а також на розробці алгоритмів для навчання інтелектуальних систем. Одними з основних підходів в цьому процесі є біонічний та еволюційний підходи [1]. Машинне навчання (а також, глибинне навчання, як перспективна підгалузь машинного навчання) побудоване на зазначених підходах. Так, машинне навчання використовує нейронні мережі, які імітують структуру та функції людського мозку (біонічний підхід), а також, включає створення моделей, які здатні до самонавчання та адаптації (еволюційний підхід). Зазначені риси роблять його ефективним інструментом для вирішення таких складних завдань як розпізнавання та класифікація шкідливого програмного забезпечення (в тому числі, загроз нульового дня).

В зв’язку з цим, тематика дослідження застосування технологій машинного навчання (та, особливо, рішень, побудованих на новітніх архітектурах глибинного навчання та комп’ютерного зору) в кібербезпеці є особливо актуальною.

В рамках концептуального підходу до розпізнавання та класифікації зловмисного програмного забезпечення [2] було представлено такі перспективні нейромережеві архітектури, як, згорткова нейронна мережа (CNN), трансформер Swin v.1, гібридна згорткова нейронна мережа CoAtNet, а також, трансформер Swin v.2. Разом з цим, практичне

застосування моделей глибинного навчання в кібербезпеці, не обмежується тільки ними.

Розглянемо стан інновацій в цій галузі, використовуючи патентний пошук по базі даних WIPO PATENTSCOPE [3], яка належить Всесвітній організації інтелектуальної власності.

Станом на початок 2025 року, за ключовими словами “machine learning for cybersecurity” було знайдено 193 патенти. Найбільший підклас (за міжнародною патентною класифікацією [4]) за кількістю опублікованих патентів: G06F (комп'ютерні системи, що базуються на певних моделях обчислювання) (133 патенти або 69%). До основних заявників (з кількістю патентів 5-9) відносяться наступні компанії: Flexxon PTE. (9 патентів), Proofpoint (9), Qomplx Inc. (9), Microsoft Tech Licensing LLC (8), Google LLC (7), Ironnet Cybersecurity Inc (7), Bank Of America Co. (5), Bluest Mettle Solutions Private Ltd. (5), Chitkara University (5), Dapper Labs Inc. (5). Основним ринком виступають США. Динаміка публікацій представлена на рисунку 1.

Рисунок 1 – Динаміка опублікованих патентних заявок щодо машинного навчання для кібербезпеки та тренд (логаріфмічний) на 2025р.

Результати структурованого пошуку за ключовими словами “cybersecurity” та “machine learning” - 77 патентів. Лідером за кількість патентних заявок також виступають США. Серед основних заявників (2-5 патентів) також представлені всесвітньо відомі компанії, що працюють в сфері цифрових рішень для кібербезпеки (Google, Honeywell, IronNet Cybersecurity, Fireeye). Разом з цим, в переліку є більш нішеві компанії, такі як Dapper Labs (розробка ігор, blockchain, NFT) та DomainTools (Інтернет розвідка, дослідження доменів). Щодо років активності з публікації патентів щодо використання машинного навчання для забезпечення кібербезпеки, так само простежується тренд – починаючи з 2021 року кількість опублікованих патентів зросла приблизно в три рази (приблизно 15 патентів на рік) та підтримується на такому рівні, в середньому, протягом чотирьох років (2021-2024 роки). Три основні підкласи, в яких були опубліковані патенти в сфері рішень машинного навчання для кібербезпеки: G06F та G06N (по 55 патентів в кожному), H04L (48 патентів).

Результати структурованого патентного пошуку по нейромережевим архітектурам для кібербезпеки (підклас G06N 20/00: методи штучного інтелекту для моніторингу та аудиту) щодо моделей глибинного навчання (CNN, Transformer, Swin Transformer, CoAtNet, LLM), а також, по ключовим словам (neural network, attention, computer vision):

- CNN (1 патент, Elex Cybersecurity, CN, 2021р.) - метод виявлення аномальної поведінки мережевого трафіку на основі CNN та XGBoost (використовується метод перетворення потоку байтів в зображення та подальше його розпізнавання - підхід схожий на бінарну візуалізацію).
- Transformer (1 патент, IBM, US, 2024р.) - навчання та розгортання моделей для прогнозування подій кібербезпеки (для аналізу використовуються історичні дані журналу подій з хост-пристроїв).
- LLM (Large Language Model, використання архітектури трансформерів): 4 патентні заявки (всі опубліковані у 2024 році):
    - Cisco Technology (US): два патенти, що стосуються використання LLM для кібербезпеки, включаючи створення honeypot-схем та узагальнення онтологічних графів.
    - Citibank (US): патент на систему, що використовує LLM для генерації звітів про підозрілу діяльність.
    - Darktrace (WO): патент на інтерактивний користувацький інтерфейс для кібербезпеки, що використовує LLM для виконання різних завдань.

- відсутні опубліковані патентні заявки з ключовими словами: neural network, attention, computer vision, CoAtNet.

Таким чином, дослідження з застосування технологій машинного навчання в кібербезпеці мають значний науковий та комерційний потенціал, зокрема для вирішення задач з автоматизації процесів та збільшення адаптивності систем.

Список використаних джерел:

1. Frolov D., Radziewicz W., Saienko V., Kuchuk N., Mozhaiev M., Gnusov Y., Onishchenko Y. Theoretical And Technological Aspects Of Intelligent Systems: Problems Of Artificial Intelligence // International Journal of Computer Science and Network Security. 2021. Vol. 21, No. 5. P. 35-38. DOI 10.22937/IJCSNS.2021.21.5.6.

2. Frolov D., Matviychuk A. Conceptual approach to malware recognition based on machine learning techniques // Modeling and Information System in Economics. 2022. No. 102. P. 184-202. DOI 10.33111/mise.102.15.

3. WIPO PATENTSCOPE. URL: https://patentscope.wipo.int/search/en/search.jsf (дата звернення: 02.03.2025).