ВИКОРИСТАННЯ НЕЙРОМЕРЕЖ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У КІБЕРПРОСТОРІ

Макогон Ю.О.

Харківський національний університет

радіоелектроніки, Україна.

E-mail: yurii.makohon@nure.ua

Abstract

The study explores the application of neural network architectures for anomaly detection in cyberspace as a response to the increasing complexity of cyber threats and data environments. Deep learning models, including autoencoders, recurrent and graph neural networks, demonstrate significant advantages in identifying non-trivial behavioral deviations and novel attack patterns. Experimental results confirm their superiority over classical machine learning methods in accuracy and adaptability. The research emphasizes challenges related to data quality, interpretability, and computational efficiency, advocating for the development of explainable AI frameworks to enhance autonomous, adaptive cybersecurity ecosystems.

У контексті постійного ускладнення цифрового ландшафту та ескалації спектра кіберзагроз питання забезпечення інформаційної безпеки набуває особливої наукової ваги. Ефективність класичних методів детектування порушень, заснованих на сигнатурному аналізі або правилах поведінкової евристики, виявляється недостатньою в умовах динамічної варіативності атак та стрімкої еволюції зловмисних тактик. Це детермінує потребу у впровадженні інтелектуалізованих підходів, здатних здійснювати самонавчання, формувати узагальнені репрезентації складних даних та розпізнавати нетривіальні структурні відхилення у поведінкових патернах цифрових об'єктів.

Одним із найбільш перспективних інструментів у цій сфері постають нейронні мережі, чия архітектурна гнучкість дозволяє здійснювати високорівневу апроксимацію нелінійних залежностей у багатовимірних просторах даних. Завдяки здатності до побудови латентних ознак і самостійного виокремлення релевантних кореляцій між подіями, нейронні мережі створюють передумови для автоматизованого виявлення аномалій без необхідності попереднього визначення сигнатур чи шаблонів атак [1]. У процесі дослідження розглядалася можливість використання глибинних моделей для аналізу мережевого трафіку, журналів подій та системних логів у гетерогенних середовищах, де традиційні алгоритми виявляють знижену чутливість до слабовиражених або нових типів відхилень.

Результати емпіричного моделювання продемонстрували, що застосування глибинних автокодерів та рекурентних нейромереж, зокрема архітектур типу LSTM [2], забезпечує суттєве підвищення точності виявлення аномальних подій у порівнянні з методами класичного машинного навчання. Використання графових нейронних мереж дало змогу розширити рамки аналізу, враховуючи контекстуальні та топологічні зв'язки між об'єктами кіберпростору, що, у свою чергу, призвело до суттєвого зростання достовірності класифікації складних багаторівневих атак [3]. Ці результати підтверджують гіпотезу про те, що інтелектуальні моделі, засновані на глибинному навчанні, не лише підвищують ефективність виявлення аномалій, а й сприяють переходу від реактивної до превентивної парадигми кіберзахисту.

Разом із тим слід підкреслити, що практична імплементація нейронних моделей у системах моніторингу безпеки супроводжується низкою проблем концептуального та технічного характеру. Серед них – обмеженість якісних маркованих наборів даних для навчання, схильність моделей до переобучення, а також непрозорість механізмів прийняття рішень, що породжує проблему інтерпретованості результатів. З метою подолання зазначених бар'єрів актуалізується розробка

пояснюваних архітектур (Explainable AI), які поєднують аналітичну силу глибинних нейронних мереж із можливістю формування когнітивно зрозумілих висновків для експертів із кібербезпеки [4].

У перспективі інтеграція таких інтелектуальних систем у багаторівневі платформи моніторингу безпеки (SIEM, SOAR) створює передумови для формування самонавчальних екосистем кіберзахисту, здатних до автономної адаптації в умовах змінного кіберсередовища. Таким чином, застосування нейронних мереж у задачах виявлення аномалій постає не лише технологічним інноваційним трендом, але й фундаментальною зміною епістемологічних засад сучасної кібербезпеки, де штучний інтелект виступає не як допоміжний інструмент, а як невід'ємний компонент когнітивної архітектури цифрової оборони [5].

Отримані результати дослідження підтверджують, що застосування нейронних мереж у системах виявлення аномалій формує нову якість кіберзахисту, засновану на когнітивно-адаптивних принципах аналізу даних. Глибинні архітектури дозволяють ефективно моделювати складні, багатовимірні закономірності в поведінці інформаційних об'єктів, забезпечуючи можливість детектування як відомих, так і нових, раніше невідомих типів загроз. Особливої ефективності досягнуто при інтеграції автокодерів та рекурентних мереж, які дозволяють ідентифікувати аномалії у часових послідовностях, та графових нейронних мереж, що враховують топологічні зв'язки у кіберпросторі. Водночас виявлено низку проблем, пов'язаних із необхідністю інтерпретації результатів нейронних моделей, забезпеченням стабільності їх роботи у режимі реального часу та потребою у великих, збалансованих наборах навчальних даних. Подальші дослідження мають бути спрямовані на створення пояснюваних (explainable) моделей, оптимізацію обчислювальних витрат і розробку гібридних систем, що поєднують переваги машинного навчання та експертних методів. Таким чином, використання нейромереж для виявлення аномалій у кіберпросторі слід розглядати не лише як технологічний інструмент, а як стратегічний напрям еволюції сучасної кібербезпеки, здатний забезпечити адаптивність, автономність та інтелектуальну стійкість інформаційних систем перед викликами нової цифрової епохи.

Література

1. Гнатюк С.О. Кібербезпека та захист інформації: сучасні тенденції та технології. К.: НАУ, 2020. 312 с.

2. Довженко В.А., Соколенко В.Ю. Методи виявлення аномалій у мережевому трафіку на основі штучного інтелекту // Вісник Національного технічного університету «ХПІ». 2021. № 54. С. 45–52.

3. Ільченко М.Ю., Яровий О.В. Системи технічного захисту інформації: навч. посіб. К.: КПІ ім. Ігоря Сікорського, 2019. 286 с.

4. Литвин В.В., Ляшенко В.В. Інтелектуальні системи обробки інформації: методи, моделі, технології. Львів: Видавництво Львівської політехніки, 2022. 384 с.

5. Поповський В.В., Коляденко Ю.Ю. Застосування нейронних мереж у задачах виявлення кіберзагроз // Зв'язок. 2020. № 3. С. 12–18.