УДК 004.056:004.8

Шинкарьов Є. Ю.
Кирилащук Т. Г.

АНАЛІЗ АРХІТЕКТУР ГЛИБОКОГО НАВЧАННЯ ТА ПЕРСПЕКТИВНИХ НАПРЯМІВ ЗАХИСТУ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ

Вінницький національний технічний університет

Анотація *У роботі проведено аналіз застосування алгоритмів глибокого навчання для виявлення кіберзагроз. Розглянуто основні архітектури нейронних мереж, їх переваги у розпізнаванні аномалій трафіку та вразливості до змагальних атак. Визначено перспективні напрями підвищення надійності інтелектуальних систем безпеки.*

Ключові слова: штучний інтелект, кібербезпека, глибоке навчання, виявлення вторгнень, змагальні атаки, захист даних.

Abstract *The paper analyzes the application of deep learning algorithms for cyber threat detection. The main neural network architectures, their advantages in traffic anomaly recognition, and vulnerabilities to adversarial attacks are considered. Promising directions for improving the reliability of intelligent security systems are identified.*

Keywords: artificial intelligence, cybersecurity, deep learning, intrusion detection, adversarial attacks, data protection.

У сучасних реаліях 2021–2026 років кібербезпека перетворилася на динамічне протистояння автономних систем. Складність загроз зростає експоненціально, що вимагає переходу від реактивних до проактивних методів захисту. Актуальність дослідження зумовлена необхідністю систематизації існуючих методів штучного інтелекту (ШІ) для виявлення складних цілеспрямованих атак (APT), які імітують легітимну поведінку користувачів.

Методичне підґрунтя роботи базується на порівняльному аналізі алгоритмів глибокого навчання, які є найбільш ефективними для аналізу великих масивів мережевих даних. Зокрема, розглядається використання контрольованого навчання для класифікації відомих сигнатур шкідливого ПЗ, методів кластеризації для виявлення раніше невідомих аномалій (Outlier detection) та глибокого підкріплюваного навчання для адаптації стратегій захисту в реальному часі залежно від поведінки атакуючої сторони.

Важливим практичним наслідком впровадження цих алгоритмів є суттєве зниження частки хибнопозитивних спрацювань порівняно з традиційними системами. Це дозволяє розвантажити аналітиків безпеки та скоротити час реагування на інциденти з кількох годин до лічених хвилин.

Особливу увагу слід приділити концепції безпеки самого штучного інтелекту. Дослідження показують, що хоча ШІ посилює захист, він одночасно створює нові вектори загроз, такі як інверсія моделі та змагальні атаки (adversarial attacks). Це підкреслює необхідність розробки надійних моделей, які зберігають точність класифікації трафіку навіть в умовах навмисного спотворення вхідних даних зловмисником.

Спираючись на аналіз сучасних тенденцій, можна стверджувати, що майбутні дослідження мають фокусуватися на створенні гібридних систем. Поєднання експертних знань фахівців з кібербезпеки та обчислювальної потужності ШІ дозволить нівелювати проблему «чорної скриньки» та підвищити довіру до автоматизованих систем прийняття рішень у критичній інфраструктурі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dasgupta D. Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions / D. Dasgupta, Z. Akhtar, S. Sen // IEEE Access. – 2023. – Vol. 11. – P. 102-115. URL: https://ieeexplore.ieee.org/document/10080928

Шинкарьов Євгеній Юрійович, студент гр. 2БС-24б, Факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, shinkaryov.evgen@gmail.com.

Науковий керівник: ***Кирилащук Тетяна Геннадіївна***, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, tan099838@vntu.edu.ua.

Shynkarov Yevhenii Yuriiovych, student of group 2BS-24b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, shinkaryov.evgen@gmail.com.

Scientific advisor: ***Kyrylaschuk Tetiana G***, Associate Professor, Department of Information Security, Vinnytsia National Technical University, Vinnytsia, tan099838@vntu.edu.ua.