УДК:

Пашківський С.О

Кирилащук Т.Г

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА МАШИННОГО НАВЧАННЯ У СУЧАСНИХ СИСТЕМАХ КІБЕРБЕЗПЕКИ

Вінницький національний технічний університет

Анотація

У роботі досліджено сучасні методи застосування штучного інтелекту та машинного навчання у кібербезпеці. Розглянуто алгоритми для виявлення вторгнень, класифікації шкідливого ПЗ, поведінкового аналізу користувачів та прогнозування кіберзагроз. Виділено переваги AI/ML-систем порівняно з традиційними підходами, а також основні проблеми, пов'язані з інтерпретованістю моделей, якістю даних і захистом від атак на алгоритми. Окреслено перспективи розвитку гібридних, адаптивних та федеративних систем кіберзахисту.

Ключові слова: кібербезпека, штучний інтелект, машинне навчання, кіберзагрози, IDS, прогнозування загроз, поведінковий аналіз.

Abstract

The paper explores modern applications of artificial intelligence (AI) and machine learning (ML) in cybersecurity. Algorithms for intrusion detection, malware classification, user behavior analysis, and threat prediction are examined. The advantages of AI/ML systems over traditional approaches are highlighted, along with challenges related to model interpretability, data quality, and defenses against adversarial attacks. Prospects for hybrid, adaptive, and federated cybersecurity systems are outlined.

Keywords: cybersecurity, artificial intelligence, machine learning, cyber threats, IDS, threat prediction, behavioral analysis.

Вступ

Стрімкий розвиток цифрових технологій призводить до постійного зростання кількості кіберзагроз та ускладнення їхньої структури. Традиційні засоби захисту інформації, що базуються на сигнатурному аналізі та статичних правилах, часто не здатні ефективно протидіяти сучасним атакам, зокрема атакам нульового дня, складним шкідливим програмам та цільовим кібератакам.

У зв'язку з цим значної актуальності набуває застосування технологій штучного інтелекту та машинного навчання у системах кібербезпеки. Ці технології дозволяють автоматично аналізувати великі обсяги даних, виявляти приховані закономірності та прогнозувати потенційні загрози. Метою роботи є аналіз сучасних підходів до використання AI та ML у кіберзахисті, визначення їх переваг, обмежень та перспектив розвитку.

Основна частина

Сучасна кіберсфера характеризується високою складністю та динамічністю загроз, що робить традиційні засоби захисту, засновані на сигнатурах і статичних правилах, все менш ефективними.

Нападники застосовують складні методи, включно з атаками нульового дня, продовженими цільовими загрозами, шкідливим програмним забезпеченням та соціальною інженерією. В умовах таких викликів інтеграція технологій штучного інтелекту та машинного навчання у системи кібербезпеки стає критичною для підвищення ефективності виявлення загроз і реагування на них. AI/ML-системи дозволяють моделювати нормальну поведінку мережевих систем та користувачів і виявляти відхилення, які можуть свідчити про атаки, що не мають попередньо визначених сигнатур. Завдяки самонавчанню такі системи постійно підвищують ефективність моніторингу та здатні ідентифікувати складні сценарії атак, включно з багатофазними і прихованими вторгненнями. Глибокі нейронні мережі аналізують структуру програм, поведінкові ознаки процесів та взаємодію з системою для класифікації шкідливого ПЗ, що дозволяє виявляти модифіковані або нові загрози та підвищувати швидкість реагування.

Алгоритми поведінкового аналізу відстежують активність користувачів і адміністраторів, визначають нетипові дії та допомагають зменшити ризик внутрішніх загроз, забезпечуючи своєчасне реагування на потенційно небезпечні ситуації. Разом із широкими можливостями застосування AI/ML існують суттєві виклики. Ефективність моделей безпосередньо залежить від повноти та достовірності навчальних даних. Складність нейронних мереж ускладнює інтерпретацію їхніх рішень і формує проблему довіри до автоматизованих систем. Додатково зростає загроза атак на самі AI-системи, включно з adversarial attacks та data poisoning, що може призвести до некоректної роботи моделей. Перспективним напрямом є створення гібридних систем, що поєднують традиційні засоби безпеки з інтелектуальними алгоритмами, а також використання федеративного навчання для обміну знаннями між організаціями без централізованого зберігання конфіденційних даних. Додатково, інтеграція AI з IoT-інфраструктурами та квантовими обчисленнями дозволяє підвищити стійкість систем і криптографічний захист, а розвиток пояснюваного штучного інтелекту (Explainable AI) збільшує прозорість прийняття рішень і довіру до автоматизованих механізмів захисту. AI і ML трансформують кіберзахист, роблячи його адаптивним, автоматизованим і здатним прогнозувати загрози. Для реалізації повного потенціалу цих технологій необхідна міждисциплінарна співпраця, вдосконалення алгоритмів та розробка нормативних та організаційних механізмів впровадження.

Висновки

Штучний інтелект і машинне навчання суттєво трансформують сучасні системи кібербезпеки, забезпечуючи адаптивність, автоматизацію та здатність прогнозувати загрози. Використання інтелектуальних алгоритмів дозволяє підвищити точність виявлення атак, скоротити час реагування на інциденти та покращити захист інформаційних систем.

Водночас ефективність AI-систем залежить від якості даних, надійності алгоритмів та рівня їх захищеності від маніпуляцій. Подальший розвиток технологій штучного інтелекту у кібербезпеці потребує вдосконалення моделей, розвитку пояснюваного AI та формування нормативної бази їх впровадження.

Список використаної літератури

1. Mohamed, N. Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems, 2025.
2. Goodfellow, I., Bengio, Y., Courville, A. Deep Learning. MIT Press, 2016.
3. Buczak, A., Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 2016.

4. Sommer, R., Paxson, V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, 2010.
5. Shone, N., Ngoc, T., Phai, V., Shi, Q. A Deep Learning Approach to Network Intrusion Detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2018.
6. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., Marchetti, M. On the Effectiveness of Machine Learning for Cybersecurity. Computers & Security, 2018.

Pashkivskyi Svyatoslav O – student of group 1BKS-24b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: svatoslav5paskivskij@gmail.com

Scientific Supervisor: Tetiana H. Kyrylashchuk – assistant of the Department of Information

Protection, Vinnytsia National Technical University, Vinnytsia. kgt0998@gmail.com