УДК 004

**Д. В. Кисюк**
**С. Б. Стоцька**

# ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМАХ КІБЕРБЕЗПЕКИ

Вінницький національний технічний університет

***Анотація***

*У роботі розглянуто перспективи використання штучного інтелекту у системах кібербезпеки сучасних комп'ютерних систем. Проаналізовано основні підходи до застосування алгоритмів машинного навчання та глибинного навчання для виявлення кіберзагроз, зокрема вторгнень, шкідливого програмного забезпечення та аномальної поведінки у мережах.*

**Ключові слова**: Штучний інтелект, кібербезпека, машинне навчання, комп'ютерні системи, інформаційна безпека, виявлення атак, нейронні мережі

***Annotation***

*The paper examines the prospects for using artificial intelligence in cybersecurity systems of modern computer systems. The main approaches to the application of machine learning and deep learning algorithms for detecting cyber threats, including intrusions, malware, and anomalous behavior in networks are analyzed.*

**Keywords:** Artificial intelligence, cybersecurity, machine learning, computer systems, information security, attack detection, neural networks.

## Вступ

Стрімкий розвиток інформаційних технологій та цифровізація практично всіх сфер діяльності призвели до суттєвого зростання кількості кіберзагроз. Сучасні комп'ютерні системи та мережі стають об'єктами складних і багаторівневих атак, які важко виявити за допомогою традиційних методів захисту. Класичні системи кібербезпеки, що базуються на сигнатурному аналізі та статичних правилах, не завжди здатні ефективно протидіяти новим, модифікованим або цільовим атакам.

У зв'язку з цим зростає інтерес до застосування методів штучного інтелекту (AI), які дозволяють автоматизувати аналіз великих обсягів даних, виявляти приховані закономірності та адаптуватися до змін у поведінці комп'ютерних систем. Використання AI відкриває нові можливості для підвищення ефективності систем кібербезпеки та забезпечення надійного захисту інформаційних ресурсів.

## Результат розробки

Застосування алгоритмів штучного інтелекту в системах кібербезпеки дозволяє значно підвищити точність та швидкість виявлення загроз. Методи машинного навчання ефективно використовуються для аналізу мережевого трафіку, журналів подій та поведінки користувачів з метою виявлення аномалій.

Результати обробки даних за допомогою AI свідчать про зниження кількості хибних спрацювань у порівнянні з традиційними методами захисту. Глибинні нейронні мережі демонструють високу ефективність у виявленні складних атак, зокрема атак нульового дня та прихованого шкідливого програмного забезпечення. Крім того, інтелектуальні системи здатні працювати в режимі реального часу, що є критично важливим для забезпечення безпеки сучасних комп'ютерних систем. Додатково, такі системи здатні адаптуватися до нових загроз шляхом самонавчання на основі актуальних даних. Це забезпечує підвищення стійкості механізмів кіберзахисту та зменшує потребу в ручному оновленні правил безпеки.

## Виклики впровадження

Незважаючи на значні переваги, впровадження AI у системи кібербезпеки супроводжується рядом викликів. Однією з основних проблем є потреба у великих обсягах якісних та репрезентативних навчальних даних. Недостатня або некоректна підготовка даних може призвести до зниження ефективності моделей.

Іншим викликом є складність інтерпретації результатів роботи AI-алгоритмів, особливо глибинних нейронних мереж. Відсутність прозорості прийняття рішень ускладнює довіру до таких систем. Крім того, існує ризик використання штучного інтелекту зловмисниками для створення більш складних і адаптивних атак.

## Шляхи подолання викликів

- Поєднання методів AI з традиційними засобами кіберзахисту.
- Підготовка та регулярне оновлення якісних навчальних даних.
- Використання пояснюваного штучного інтелекту (Explainable AI) для прозорості рішень.
- Впровадження багаторівневого захисту та постійний моніторинг ефективності.
- Адаптація моделей до нових типів атак та обмеження доступу до критичних компонентів системи.

## Висновки

Штучний інтелект є потужним інструментом підвищення ефективності систем кібербезпеки сучасних комп'ютерних систем. Його використання дозволяє автоматизувати процеси виявлення загроз, зменшити кількість хибних спрацювань та забезпечити адаптивність до нових типів атак. Водночас впровадження AI потребує вирішення низки технічних і організаційних проблем. Подальший розвиток інтелектуальних методів захисту та їх інтеграція з класичними підходами є перспективним напрямом забезпечення інформаційної безпеки.

## СПИСОК ЛІТЕРАТУРИ


1. Goodfellow I., Bengio Y., Courville A. *Deep Learning*. — MIT Press, 2016.
2. Bishop C. M. *Pattern Recognition and Machine Learning*. — Springer, 2006.
3. Stallings W. *Cryptography and Network Security: Principles and Practice*. — Pearson, 2020.
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. Buczak A. L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. — *IEEE Communications Surveys & Tutorials*, 2016.
6. Mitchell T. *Machine Learning*. — McGraw-Hill, 1997.



***Кисюк Дмитро Васильович*** — старший викладач кафедри обчислювальної техніки, Вінницький національний технічний університет, вул. Хмельницьке шосе 95, м. Вінниця, Україна, kneimad@gmail.com

***Стоцька Софія Богданівна*** — студентка групи 2 КІ-25б, факультету інформаційних технологій та комп'ютерої інженерії, кафедри обчислювальної техніки, Вінницький національний технічний університет, вул. Хмельницьке шосе 95, м. Вінниця, Україна, stockasofia571@gmail.com

***Kysiuk Dmytro V.*** - Senior Lecturer at the Department of Computer Engineering, Vinnytsia National Technical University, 95 Khmelnytske Shose St., Vinnytsia, Ukraine, kneimad@gmail.com

***Stotska Sofia B.*** - Student of the Department of Computer Engineering, 2KI-25b group, Vinnytsia National Technical University, 95 Khmelnytske Shose St., Vinnytsia, Ukraine, stockasofia571@gmail.com