НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

практичні задачі для застосування алгоритмів МН - від медичної діагностики до систем безпеки.

Таким чином, МН формує інтелектуальну основу технологій комп'ютерного зору, сприяючи точному аналізу візуальної інформації, передбаченню поведінки об'єктів та розвитку сучасних автоматизованих систем.

Список використаних джерел:

1. Vraj Sheth, Urvashi Tripathi, Ankit Sharma. A Comparative Analysis of Machine Learning Algorithms for Classification Purpose. Procedia Computer Science, Volume 215, 2022, Pages 422-431, https://doi.org/10.1016/j.procs.2022.12.044.
2. Shichao Zhang. Challenges in KNN Classification. IEEE *Transactions on knowledge and data engineering*, vol. 34, № 10, 2022. pages 4663-4675. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9314060
3. Jair Cervantes, Farid Garcia-Lamont, Lisbeth Rodríguez-Mazahua, Asdrubal Lopez. A comprehensive survey on support vector machine classification: Applications, challenges and trends. *Neurocomputing*, vol. 408, 2020, pages 189-215, https://doi.org/10.1016/j.neucom.2019.10.118.
4. Iqbal H Sarker. Machine Learning: Algorithms, Real-World Applications and Research Directions. SN Comput Sci. 2021 Mar 22;2(3):160. doi: 10.1007/s42979-021-00592-x
5. Aasim Ayaz Wani. Comprehensive analysis of clustering algorithms: exploring limitations and innovative solutions. *PeerJ Computer Science*, 2024, 10, pp.e2286. ff10.7717/peerj-cs.2286ff. ffhal-05037350.

Ключові слова: машинне навчання, комп'ютерний зір, алгоритм, метод, контрольоване навчання, неконтрольоване навчання

Keyword: machine learning, computer vision, algorithm, method, supervised learning, unsupervised learning

ШТУЧНИЙ ІНТЕЛЕКТ І МАШИННЕ НАВЧАННЯ У КІБЕРБЕЗПЕЦІ

Воронянський Володимир

викладач циклової комісії Полтавського фахового коледжу нафти і газу

Шкавро Наталія

студентка спеціальності F2 Полтавського фахового коледжу нафти і газу

Розвиток цифрових технологій, що супроводжується їхнім проникненням у всі сфери життя, відкриває нові можливості, але одночасно значно підвищує вразливість інформаційних ресурсів. Класичні підходи до кібербезпеки, такі як сигнатурні системи виявлення або статичні правила доступу, дедалі частіше виявляються неефективними проти сучасних еволюціонуючих загроз. У цьому контексті штучний інтелект та машинне навчання пропонують потужні

інструменти для автоматизації виявлення аномалій, прогнозування атак та класифікації шкідливого програмного забезпечення, суттєво підвищуючи адаптивність систем захисту [1]. Метою даного дослідження є комплексний огляд застосування ШІ та МН у сфері кібербезпеки, детальний аналіз їхніх сильних і слабких сторін, а також виокремлення найперспективніших напрямків для майбутніх досліджень.

Актуальність цієї проблематики зумовлена кількома ключовими факторами: експоненційним зростанням обсягів даних, що робить ручне виявлення загроз практично неможливим; ускладненням характеру кібератак, таких як поліморфні віруси, фішинг та DDoS-атаки; а також масовим поширенням пристроїв Інтернету речей з обмеженими обчислювальними ресурсами, що вимагає розробки спеціалізованих легковагових алгоритмів [2]. Штучний інтелект і машинне навчання відкривають можливості для виявлення аномалій у мережевому трафіку, класифікації шкідливого ПЗ на основі аналізу поведінки, прогнозування потенційних векторів атак та адаптації моделей захисту в реальному часі. Сучасні дослідження демонструють особливу ефективність глибоких нейронних мереж, графових нейронних мереж (GNN), ансамблевих методів та федеративного навчання для забезпечення приватності даних [3]. Однак існують і серйозні проблеми, серед яких вразливість до адверсаріальних атак, брак стандартизованих наборів даних для навчання, низька інтерпретованість складних моделей та суворі регуляторні вимоги до їх застосування.

Методи штучного інтелекту та машинного навчання, що застосовуються в кібербезпеці, можна умовно поділити на кілька категорій: класичні алгоритми (логістична регресія, метод опорних векторів, дерева рішень), глибокі нейронні мережі (згорткові CNN, рекурентні RNN/LSTM, трансформери), графові мережі (GNN) для аналізу структурних зв'язків, а також розподілені системи навчання, такі як федеративне навчання та методи диференційного захисту приватності [4]. Класичні підходи добре підходять для вирішення порівняно простих завдань, тоді як глибокі архітектури демонструють високу ефективність для виявлення складних патернів у мережевому трафіку або послідовностях викликів API. Графові нейронні мережі дозволяють моделювати складні взаємозв'язки між системними процесами, що значно підвищує точність класифікації аномальної поведінки.

Детальне порівняння алгоритмів штучного інтелекту та машинного навчання у контексті кібербезпеки представлено в таблиці 1, яка охоплює такі аспекти, як переваги, недоліки, сфери застосування та конкретні приклади реалізації для різних підходів. Зокрема, виявлення аномалій у мережевому трафіку активно використовує методи ненавчального навчання, автоенкодери та рекурентні нейронні мережі. Сучасні гібридні системи

успішно поєднують сигнатурні правила з машинним навчанням, що дозволяє значно зменшити кількість хибно позитивних спрацювань. Для аналізу шкідливого програмного забезпечення застосовують як статичні, так і динамічні методи аналізу; графові нейронні мережі ефективно моделюють графіки викликів системних функцій, а динамічні моделі на основі LSTM здатні точно розрізняти поведінкові патерні різних типів шкідливого ПЗ.

Таблиця 1. Порівняння алгоритмів ШІ та МН у кібербезпеці

Підхід	**Переваги**	**Недоліки**	**Застосування**	**Приклади**
Класичні ML	Простота, інтерпретованість	Обмежена моделювання складності	Фільтрація, IDS	Random Forest, SVM
Глибоке навчання	Висока точність	Обчислювальна вартість, вразливість	Аналіз послідовностей, NIDS	LSTM, Transformer
GNN	Аналіз структур	Підготовка даних	Malware detection, мережевий аналіз	GCN, GAT
Федеративне навчання	Приватність, децентралізація	Отруєння, витрати	IoT, мультиорганізаційний аналіз	FedAvg
XAI	Довіра, аудит	Приблизність	Пояснення рішень	SHAP, LIME

Адверсаріальні атаки, серед яких виділяють evasion, poisoning, inference та backdoor атаки, становлять одну з найсерйозніших загроз для сучасних інтелектуальних систем кібербезпеки. Захист від цих атак включає цілий спектр методологій, таких як адверсаріальне навчання, спеціалізовані детектори аномалій, методи робастної оптимізації та застосування диференційного захисту приватності у рамках федеративного навчання. Надзвичайно важливим також є постійний моніторинг та оцінка стану моделей у виробничому середовищі. Забезпечення приватності даних досягається завдяки використанню федеративного навчання, яке дозволяє тренувати моделі без необхідності централізації чутливих даних, проте це породжує нові виклики, пов'язані з ризиками отруєння моделей та збільшенням обчислювальних витрат.

Інтерпретованість роботи складних моделей забезпечується за допомогою методів пояснюваного штучного інтелекту (XAI), таких як SHAP, LIME та GNNExplainer, що значно полегшує процес аудиту та відлагодження систем [5]. Проте застосування цих методів часто пов'язане з певним компромісом між рівнем інтерпретованості та загальною точністю моделі. Серед сучасних тенденції розвитку можна виділити зростаючий фокус на створенні стійких до маніпуляцій моделей, активне впровадження графових

нейронних мереж для аналізу структурних даних та розвиток федеративних методів навчання. Свіжі оглядові дослідження за 2023-2025 роки особливо виділяють потенціал GNN та трансформерів для завдань класифікації програмного забезпечення та виявлення мережевих аномалій, що знаходить своє відображення в порівняльній таблиці 1.

У висновку варто зазначити, що штучний інтелект та машинне навчання суттєво підвищують ефективність систем кібербезпеки у таких ключових аспектах, як виявлення аномалій, класифікація шкідливого ПЗ та прогнозування майбутніх атак. Проте залишаються серйозні виклики, пов'язані з адверсаріальними атаками, відсутністю уніфікованих стандартів, забезпеченням конфіденційності даних та інтерпретованістю прийнятих рішень. Перспективними напрямками майбутніх досліджень виглядають розробка стійких архітектур, створення динамічних графових нейронних мереж, вдосконалення комбінованих федеративних підходів, формування стандартизованих наборів даних для навчання та інтеграція методів пояснюваного ШІ для критично важливих інформаційних систем.

Список використаної літератури:

1. Kaur R., Gabrijelčič D., Klobučar T. Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. *Information Fusion*. 2023. P. 101804. URL: https://doi.org/10.1016/j.inffus.2023.101804.
2. Mohamed N. Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering*. 2023. Vol. 10, no. 2. URL: https://doi.org/10.1080/23311916.2023.2272358.
3. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques / A. H. Salem et al. *Journal of Big Data*. 2024. Vol. 11, no. 1. URL: https://doi.org/10.1186/s40537-024-00957-y.
4. Система виявлення аномалій у DNS-запитах / Ю. Кльоц та ін. *Herald of Khmelnytskyi National University. Technical sciences*. 2024. Vol. 345, no. 6(2). P. 141–148. URL: https://doi.org/10.31891/2307-5732-2024-345-6-22.
5. A Survey on the Role of Artificial Intelligence, Machine Learning and Deep Learning for Cybersecurity Attack Detection / A. Salih et al. *2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic" (IEC)*, Erbil, Iraq, 24–25 February 2021. URL: https://doi.org/10.1109/iec52205.2021.9476132.

Ключові слові: штучний інтелект, машинне навчання, кібербезпека, виявлення аномалій, графові нейронні мережі
Keywords: artificial intelligence, machine learning, cybersecurity, anomaly detection, graph neural networks

ЗМІСТ