

---

## ТЕЗИ ДОПОВІДЕЙ

### Секція 1. Інформаційна безпека

#### Секція 1

#### **АНАЛІЗ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ ШІ ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В СИСТЕМАХ КІБЕРЗАХИСТУ**

Ахтирська С.В.

Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»

Науковий керівник: Землянко. Г. А.

**Актуальність.** Стрімкий розвиток сучасних інформаційних технологій призвів до зростання кількості, складності та швидкості здійснення кібератак, що ускладнює їхнє ефективне виявлення та реагування за допомогою лише людських ресурсів. Крім того, слід зазначити, що людський фактор є частим джерелом вразливості в системах кібербезпеки, що робить ці системи менш стійкими до атак. Близько 74% кібер інцидентів мають людський елемент (помилки співробітників та користувачів програмним забезпеченням). Використання штучного інтелекту (ШІ) для автоматичного виявлення вразливостей відкриває нові можливості, дозволяючи системам швидко реагувати на потенційні загрози через глибокий аналіз даних і виявлення слабких місць [1, 2].

**Метою** даної роботи є аналіз можливого використання ШІ для виявлення вразливостей у системах кіберзахисту.

**Основні положення.** Інструменти кібербезпеки з використанням ШІ можуть бути використані для аналізу великих наборів даних, щоб ідентифікувати аномальну поведінку після виявлення закономірностей в поведінці користувачів, забезпечення безпеки в хмарі, у системах керування ідентичністю та доступом (IAM), при розслідуванні кібер інцидентів та реагуванні на них [3]. Після виявлення підозрілої активності ШІ може надіслати відповідне сповіщення фахівцю з безпеки, таким чином спрощуючи завдання співробітникам і залишаючи прийняття остаточного рішення за людиною [4].

Проте, крім користі від ШІ, існують також певні ризики, такі як: витоки даних, помилкові спрацювання, пропущені атаки та труднощі з інтерпретацією виявлених аномалій. Проте, завдяки алгоритмам машинного навчання, здатності ШІ адаптуватися до змін та навчатися на раніше виявлених незвичайних активностях, можна знизити ризики

впровадження технологій ШІ у системи захисту. Саме тому тренування ШІ та якості вхідних даних, які використовувались, має критично важливе значення для його подальшого коректного та ефективного функціонування [4, 5].

**Висновки.** Основні переваги безпеки з використанням ШІ полягає в здатності швидко виявляти вразливості, аналізуючи мережевий трафік, також у знаходженні прогалин в безпеці, які людина може пропустити. Продумане використання засобів ШІ, коректно проведене навчання та регулярне оновлення моделей ШІ допоможуть мінімізувати згадані ризики від впровадження технології та ефективніше виконувати завдання, при цьому залишаючи остаточне рішення за людиною.

### Список літератури

1. AI in cybersecurity: use cases, implementation, solution and development. *LeewayHertz*. URL – <https://www.leewayhertz.com/ai-in-cybersecurity> (дата звернення: 28.10.2024).
2. 74% data breaches are due to human error | infosec. *Cybersecurity Training*. URL – <https://www.infosecinstitute.com/resources/security-awareness/human-error-responsible-data-breaches> (дата звернення: 04.11.2024).
3. Kaur R., Gabrijelčić D., Klobučar T. Artificial intelligence for cybersecurity: literature review and future research directions. *Information fusion*. 2023. Volume 97. DOI: <https://doi.org/10.1016/j.inffus.2023.101804>.
4. Що таке ШІ для кібербезпеки? *Microsoft*. URL: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-ai-for-cybersecurity#heading-ocafd6> (дата звернення: 28.10.2024).
5. Managing cybersecurity and privacy risks in the age of artificial intelligence: launching a new program at NIST. *NIST*. URL: <https://www.nist.gov/blogs/cybersecurity-insights/managing-cybersecurity-and-privacy-risks-age-artificial-intelligence> (дата звернення: 03.11.2024).

### Відомості про авторів

Ахтирська Софія Вячеславівна, студентка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», s.v.akhtyrskaya@student.csn.khai.edu  
Землянко Георгій Андрійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», PhD з кібербезпеки, g.zemlynko@khai.edu