напрямом розвитку систем протидії РЕБ. Подальші дослідження доцільно спрямувати на розробку адаптивних моделей машинного навчання та вдосконалення методів аналізу сигналів у реальному масштабі часу. Отримані результати показують, що використання алгоритмів штучного інтелекту дозволяє підвищити точність класифікації сигналів джерел РЕБ та скоротити час аналізу електромагнітного середовища. Запропонований підхід забезпечує адаптивність системи до зміни параметрів сигналів і може бути використаний у перспективних системах підтримки прийняття рішень для протидії засобам радіоелектронної боротьби.

1. Haykin S. Neural Networks and Learning Machines. New York: Pearson, 2009. 936 p.
2. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge : MIT Press, 2016. 775 p.
3. Richards M. Fundamentals of Radar Signal Processing. New York: McGraw-Hill, 2014. 689 p.
4. Конахович Г.Ф., Пузиренко О.Ю. Основи радіоелектронної боротьби. Київ : НТУУ «КПІ», 2018. 320 с.

ШІ як інструмент практичної підготовки фахівців з кібербезпеки

УДК 004.85

Лілія Білокриницька

Відокремлений структурний підрозділ "Тернопільський фаховий коледж" Тернопільського національного технічного університету імені Івана Пулюя, bilokrynytskali@gmail.com

Розвиток інформаційних технологій супроводжується стрімким зростанням кіберзагроз, що висуває принципово нові вимоги до підготовки фахівців у сфері захисту інформації. За даними IBM, понад 90% кібернападів виникають через людські помилки [1], що підкреслює критичну роль якісної освіти у формуванні культури кібербезпеки. Академічна освіта не завжди встигає за темпом змін у галузі, залишаючи відчутний розрив між теоретичними знаннями та практичними вимогами ринку праці. У цьому контексті штучний інтелект все частіше розглядається як інструмент, здатний суттєво підвищити якість та ефективність підготовки майбутніх фахівців з кібербезпеки.

Класична система підготовки будується переважно на теоретичній базі, що об'єктивно не завжди встигає за темпом розвитку реальних кіберзагроз. Сучасні ШІ-інструменти натомість здатні створювати динамічне навчальне середовище, що адаптується до рівня знань кожного студента індивідуально. Платформи на основі машинного навчання аналізують прогрес учня, виявляють слабкі місця та автоматично підбирають відповідні завдання і сценарії, що дозволяє перейти від стандартизованого навчання до персоналізованого підходу. Крім того, ШІ здатний симулювати реальні кібератаки у безпечному середовищі, надаючи студентам практичний досвід без ризику для реальних систем.

Сучасний ринок освітніх технологій пропонує широкий спектр інструментів для практичної підготовки. Як зазначають фахівці, "вакансії провідних

компаній — Cisco, Google, Siemens, Deloitte, SoftServe, EPAM — прямо вимагають посилань на профілі в лабораторіях на кшталт TryHackMe та HackTheBox, оскільки реальний досвід розв'язання практичних задач у бойових умовах говорить більше за сертифікати та оцінки" [2]. Обидві платформи використовують адаптивні алгоритми для підбору завдань відповідно до рівня студента — від базових сценаріїв до складних симуляцій корпоративної інфраструктури. Актуальність цього підходу підтверджує і статистика: минулого року понад 67% фішингових атак покладалися на штучний інтелект [3], що вимагає від фахівців глибокого розуміння принципів роботи ШІ-інструментів як у захисті, так і в нападі.

Водночас надмірна залежність від автоматизованих інструментів несе в собі серйозні педагогічні ризики. Українські дослідники зазначають, що "відсутність глибоких знань і критичного мислення призводить до того, що студенти легко обходять інтелектуальні виклики, отримуючи сертифікати без реальних компетенцій" [4]. У кібербезпеці це є особливо небезпечним — фахівець без справжнього розуміння матеріалу стає слабкою ланкою у системі захисту організації. "Штучний інтелект автоматизує дедалі більше когнітивних завдань, але людські навички — критичне мислення, емпатія, етичне судження та творчість — залишаються поза його досяжністю" [5] — а саме ці якості є вирішальними під час реагування на нестандартні інциденти.

Штучний інтелект кардинально змінює підходи до підготовки фахівців з кібербезпеки — від пасивного засвоєння теорії до активної взаємодії з реальними сценаріями загроз. За прогнозами, ринок ШІ у кібербезпеці досягне 46,3 мільярда доларів до 2027 року [6] — що свідчить про масштаб трансформації галузі та зростаючу потребу у фахівцях, здатних ефективно працювати з цими технологіями. Оптимальна модель підготовки поєднує можливості штучного інтелекту з традиційними педагогічними підходами — саме такий синтез здатний сформувати фахівця, готового до реальних викликів цифрового світу.

1. synchron.ua — Кібератаки на бізнес України 2025. https://synchron.ua/cyberattacks-on-ukrainian-business-2025-uk/
2. oksim.ua — ТОП-10 платформ для практики з кібербезпеки.
3. https://www.oksim.ua/top-10-platform-dlya-praktiki-z-kiberbezpeki/3.synchron.ua — Кібератаки на бізнес України 2025. https://synchron.ua/cyberattacks-on-ukrainian-business-2025-uk/
4. kreschatic.kiev.ua — Чому студенти вразливі перед штучним інтелектом, 2025. https://kreschatic.kiev.ua/tehno/2025/05/15/chomu-studenty-vrazlyvi-pered-shtuchnym-intelektom-i-yak-universytety-mozhut-cze-zminyty.html
5. focus.ua — Епоха штучного інтелекту: яка освіта і які професії вціліють. https://focus.ua/uk/ukraine/751608-epoha-shtuchnogo-intelektu-yaka-osvita-i-yaki-profesiji-vciliyut
6. bdo.ua — Роль штучного інтелекту в кібербезпеці. https://www.bdo.ua/en-gb/insights-1/information-materials/2024/the-role-of-ai-in-cybersecurity-anticipating-and-preventing-attacks