

Тенденції та виклики у навчанні з кібербезпеки

УДК 004.056.5 (355.4)

Максим Делембовський¹, Денис Калениченко²

¹Київський національний університет будівництва і архітектури,
delembovskyi.mm@knuuba.edu.ua, ²Київський національний університет імені
Тараса Шевченка, denys.kalenychenko.student@knu.ua

Сучасний світ цифрових технологій постійно розвивається, а з ним і загрози кібербезпеки стають все складнішими та різноманітнішими. Ця динаміка ставить перед освітніми інституціями низку викликів у підготовці кваліфікованих фахівців у галузі кібербезпеки. Тематика зосереджується на аналізі основних тенденцій, таких як адаптація курсів до найновіших технологічних загроз, використання інтерактивних та іммерсивних технологій для підвищення ефективності навчання. Також в роботі розглядаються ключові виклики, включаючи нестачу кваліфікованих викладачів, потребу в постійному оновленні навчальних матеріалів, а також проблеми зі збалансуванням теоретичних знань та практичних навичок. Дана тематика спрямована на визначення шляхів оптимізації навчального процесу, щоб випускники могли ефективно реагувати на кіберзагрози в реальному світі [1-3].

Освітній ландшафт з кібербезпеки формується швидкою еволюцією загроз та технологічних досягнень, представляючи складний набір викликів та тенденцій, які викладачі та фахівці повинні долати.

Однією з основних тенденцій, що спостерігається, є інтеграція штучного інтелекту (AI) та машинного навчання (ML) в навчальні програми з кібербезпеки. Освітні заклади все частіше використовують ці технології для забезпечення більш адаптивного навчального досвіду, який налаштовує навчальний контент відповідно до потреб учня. Цей підхід не лише робить процес навчання ефективнішим, але й допомагає підготувати студентів до реальних сценаріїв, де AI та ML відіграють значущу роль у виявленні загроз та реагуванні на них [4].

Однак, є і значні виклики. Швидкий темп технологічних змін вимагає, щоб навчальний контент постійно оновлювався, щоб залишатися актуальним, що становить логістичний та фінансовий виклик для багатьох установ. Крім того, зростаюча складність кіберзагроз вимагає відповідного розвитку навчання та інструментів, доступних для професіоналів кібербезпеки, роблячи важливим для освітніх програм йти в ногу з потребами індустрії [5].

Більше того, Всесвітній економічний форум підкреслює важливість антиципації майбутніх викликів кібербезпеки. Вони вважають, що поле кібербезпеки повинно адаптуватися до середовища, де довіра стає все рідкіснішою, а технологічна цілісність є вирішальною. Вони також прогнозують, що освіта з кібербезпеки повинна зосереджуватися не лише на захисті, а й на підтримці стійкості та здатності відновлюватися після кіберінцидентів [1-3].

Загалом, поки галузь освіти з кібербезпеки розвивається завдяки введенню нових технологій та методологій, вона також стикається з постійним викликом адаптації до швидко змінюваного ландшафту загроз. Ця динаміка вимагає постійних інвестицій у освітні ресурси, інноваційні методики навчання та

прогресивний підхід до розробки навчальних програм, щоб ефективно підготувати наступне покоління фахівців з кібербезпеки.

Для вирішення викликів у навчанні з кібербезпеки можна застосувати кілька стратегій:

1. Регулярне оновлення навчальних матеріалів для відображення найновіших технологічних інновацій та кіберзагроз. Це забезпечує, що студенти вивчають актуальні техніки та методи кібербезпеки.

2. Інтеграція штучного інтелекту та машинного навчання для створення адаптивних навчальних платформ, які відповідають індивідуальним потребам студентів, підвищуючи ефективність навчання.

3. Надання студентам доступу до практичних лабораторій та симуляцій, що дозволяють їм застосовувати теоретичні знання в реальних сценаріях, підвищуючи їх готовність до роботи.

4. Співпраця між різними дисциплінами, такими як комп'ютерні науки, інженерія та право, для створення всебічних освітніх програм, що включають різні аспекти кібербезпеки.

5. Стимулювання неперервного навчання серед професіоналів у галузі кібербезпеки через сертифікації та регулярні тренінги для підтримки їхніх знань на високому рівні.

6. Підтримка глобальної співпраці між освітніми закладами та індустрією для обміну кращими практиками та розробки спільних навчальних ініціатив.

1. Шестаковська Т.Л. Аналіз тенденцій та викликів впливу цифрових технологій на публічне управління. *Economic Synergy*, 2023, 2: 8-22.
2. Бучма О.В.; Гнинюк Р.Ю. Особливості сучасного стану кібербезпеки України. 2018. PhD Thesis. НПУ імені МП Драгоманова.
3. Essien N.P.; Ekaiko U.A. Cyber security: trends and challenges toward educational development in 21st century. *Asia-Africa Journal of Education Research*, 2022, 2: 141-156.
4. #CybersecurityAwarenessMonth - The Evolution of Cybersecurity Education. (б. д.). Cybersecurity Certifications and Continuing Education | ISC2. <https://www.isc2.org/Insights/2023/10/Evolution-of-Cybersecurity-Education>
5. An Executive View of Key Cybersecurity Trends and Challenges in 2023. (б. д.). ISACA. <https://www.isaca.org/resources/news-and-trends/industry-news/2023/an-executive-view-of-key-cybersecurity-trends-and-challenges-in-2023>
6. 7 trends that could shape the future of cybersecurity in 2030. (2023, 3 березня). <https://www.weforum.org/agenda/2023/03/trends-for-future-of-cybersecurity/>