УДК 004.8

Дорогий Я. Ю., д.т.н., професор,
Донецький національний технічний університет
Цуркан В. В., к.т.н., доцент,
Інститут спеціального зв'язку та захисту
інформації КПІ ім. Ігоря Сікорського
Дорога-Іванюк О. О., вчитель вищ. кат.,
Пологівський ліцей Ковалівської територіальної громади
Білоцерківського району Київської області

ЗАСТОСУВАННЯ ШІ ПРИ ВИВЧЕННІ ДИСЦИПЛІН З КІБЕРБЕЗПЕКИ

Інтенсифікація кіберзагроз останніми роками викликає зростаючий попит на висококваліфікованих фахівців з кібербезпеки. Університети адаптують освітні програми, включаючи актуальні інструменти ШІ, щоб забезпечити студентам практичні навички захисту інформаційних систем. Наразі ШІ все частіше використовується не лише для автоматизованого виявлення атак, але й для навчання: наприклад, студенти можуть тренуватися в безпечному симульованому середовищі з імітацією реальних атак і відповідей.

В університетській освіті з кібербезпеки ШІ використовується для забезпечення реалістичних практичних вправ та персоналізації навчального процесу. Різноманітність ШІ-технологій у цьому контексті охоплює кілька напрямів:

- *Генеративні AI-моделі*. Інструменти на кшталт ChatGPT широко застосовуються для створення навчальних сценаріїв та пояснень складних тем. Наприклад, generative AI показує високу ефективність у допомозі студентам-початківцям при підготовці до CTF-змагань: ChatGPT узагальнює і пояснює базові поняття (шифрування, мережеві атаки тощо) на доступному рівні [1]. Університетські курси використовують такі моделі для генерації завдань та автоматичного зворотного зв'язку, що підвищує залученість студентів та глибину розуміння. При цьому важливо, щоб учасники навчання критично оцінювали AI-результати, а викладачі коригували їхню роботу.
- *Моделі симуляції та кіберарені*. ШІ-інструменти покращують якість симуляцій «живих атак». Наприклад, концепція Red Team/Blue Team широко використовується для відпрацювання реалістичних сценаріїв: IT-інфраструктура моделюється віртуально, і студенти у ролі нападників (Red) і захисників (Blue) змагатимуться за контроль. Системи штучного інтелекту можуть генерувати сценарії атак, створювати автоматизованих агентів-опонентів або оцінювати

результати дій студентів. У цій категорії активно розвиваються технології цифрових двійників – віртуальних копій мережевих систем (DT), які дозволяють проводити високодеталізовані симуляції кібератак у безпечному середовищі. Так, згадуваний «Red Team Knife» інтегрується з DT-екосистемою для послідовного практичного вивчення всіх фаз атаки та захисту [2].

- *Гейміфікація та адаптивне навчання*. ШІ-системи дозволяють реалізувати адаптивні навчальні шляхи: наприклад, програма виявляє слабкі місця студента і автоматично пропонує додаткові вправи або теоретичні матеріали. Аналізують греп-інформацію про спосіб вирішення задачі, модифікують складність. Хоча конкретні університетські кейси описані переважно у внутрішніх звітах, поєднання AI з гейміфікацією (змагання в режимі он-лайн, персональний прогрес, рейтинги) рекомендується практиками, оскільки підвищує конкурентний дух і ефективність засвоєння матеріалу.

Таким чином, широке застосування ШІ – від глибоких нейромереж до генеративних мовних моделей і реалістичних симуляцій – робить вивчення кібербезпеки більш інтерактивним і наближеним до реальності.

Висновки. Використання технологій штучного інтелекту в університетських курсах з кібербезпеки відкриває нові можливості для інтерактивного і практично орієнтованого навчання. Поєднання нейронних мереж для виявлення загроз, генеративних моделей для створення освітнього контенту та платформ симуляції атак сприяє тому, що студенти набувають практичних навичок у безпечному середовищі зворотного зв'язку. Зі зростанням ролі ШІ у реальних кібероперація адаптація освітніх програм із включенням цих технологій стає незаперечною вимогою для підготовки конкурентоспроможних фахівців.

Список використаних джерел:

1. Lam L. Capturing the Flag with ChatGPT: Generative AI for Cyber Education. Center for Security and Emerging Technology (CSET), Georgetown University, 2023. URL: https://surli.cc/aoymhp.

2. Barletta V.S., Bavaro V., Calvano M., Curci A., Piccinno A., Posa D.P. Enabling Cyber Security Education through Digital Twins and Generative AI. arXiv:2507.17518, 2025. URL: https://surli.cc/xggzvx.