DOI: https://doi.org/10.36059/978-966-397-477-4-189

Юлія СИНЯВІНА
кандидат економічних наук, доцент, доцент кафедри
інформаційних технологій, кібернетики та захисту інформації
Державного біотехнологічного університету (Харків)
0959106133@btu.kharkov.ua

ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПІДГОТОВКУ СПЕЦІАЛІСТІВ З КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

У наш час кібербезпека є одним з найважливіших аспектів захисту інформації. З розвитком цифрових технологій кількість кіберзагроз зростає, тому ефективна підготовка спеціалістів у цій галузі стає надзвичайно важливою. Збільшення випадків хакерських атак, шкідливого програмного забезпечення, фішингових схем та витоків даних створює нагальну потребу у висококваліфікованих спеціалістах з кібербезпеки, здатних запобігати цим ризикам. Інтеграція штучного інтелекту (ШІ) у процес навчання дозволяє значно підвищити рівень компетенцій майбутніх фахівців, активно трансформує процеси навчання, роблячи їх персоналізованими, інтерактивними та ефективними.

Концепція розвитку штучного інтелекту, затверджена Кабінетом Міністрів України [1] є важливим кроком на шляху до інноваційного розвитку країни. Одним із ключових напрямів Концепції є впровадження технологій штучного інтелекту у такі сфери, як освіта, економіка, публічне управління, кібербезпека, оборона та інші, що сприятиме зміцненню довгострокової конкурентоспроможності України на глобальному ринку. Важливо зазначити, що серед основних пріоритетів документа виділяються освіта, наука та професійна підготовка, що вимагає адаптації національного законодавства щодо використання технологій штучного інтелекту до міжнародних стандартів [2]. Отже, освіта у сфері кібербезпеки та захисту інформації може стати однією з найбільш перспективних сфер застосування ШІ.

В умовах зростання кіберзагроз сучасному світу потрібні спеціалісти, здатні швидко адаптуватися до нових викликів. Інтеграція ШІ в цей процес дозволяє модернізувати навчальні підходи, розробляти навчальні системи, які враховують індивідуальні особливості студентів, створюючи персоналізовані освітні траєкторії. Ці системи враховують попередній рівень знань, швидкість засвоєння нового матеріалу та особливості навчальних уподобань.

Однією з ключових переваг ШІ є створення симуляцій для навчання у середовищах, максимально наближених до реальних умов.

Використовуючи технології машинного навчання, можна моделювати складні сценарії кібератак, тестуючи навички студентів щодо їхнього запобігання або нейтралізації. Такі симуляції дозволяють студентам отримати практичний досвід без ризику для реальних систем.

Використання чат-ботів та віртуальних помічників на базі ШІ виступають інструментами, які надають студентам додаткову підтримку у навчанні. Вони можуть відповідати на питання студентів, надавати пояснення до складних тем або навіть допомагати вирішувати практичні завдання. Такі інструменти працюють цілодобово, надаючи доступ до навчальних ресурсів у будь-який час. Наприклад, ChatGPT Edu є потужним інструментом, який може значно покращити якість вищої освіти. ChatGPT Edu – це адаптована версія популярної Великої Мовної Моделі (з англ. Large Language Model) ChatGPT, яка спеціально розроблена для застосування в освітніх цілях. Використовуючи сучасні технології обробки природної мови (з англ. Natural Language Processing), ChatGPT Edu може відповідати практично на будь-які запитання, генерувати тексти, надавати пояснення та навіть брати участь у дискусіях на різноманітні теми. Однією з головних переваг ChatGPT Edu є його здатність надавати студентам швидкі та точні відповіді на запити. Це особливо знадобиться тим, хто працює над складними завданнями або потребує додаткової допомоги під час підготовки до іспитів. ChatGPT Edu також може надавати рекомендації ресурсів для самостійного вивчення та пояснювати складні концепції зрозумілими словами [3].

ШІ також відіграє значну роль у впровадженні гейміфікованих елементів у навчання. Наприклад, інтерактивні вікторини на основі кібербезпеки, де студенти аналізують дії зловмисників, симуляції розслідувань інцидентів або квести, спрямовані на виявлення вразливостей у системах. Це не лише покращує залучення студентів, а й формує навички вирішення реальних завдань у сфері кібербезпеки.

Застосування алгоритмів машинного навчання (ML) та обробки великих даних (Big Data) дозволяє виявляти та класифікувати загрози на основі аналізу аномалій у мережевому трафіку. Серед інструментів, які використовуються, варто виділити SIEM-системи (Security Information and Event Management), такі як Splunk, ELK Stack (Elasticsearch, Logstash, Kibana). Студенти можуть створювати моделі машинного навчання для аналізу мережевого трафіку та виявлення несанкціонованого доступу або аномальних дій. Наприклад, модель на основі нейронних мереж може виявляти дії, що не відповідають типовим шаблонам користувацької поведінки. Використання платформ з елементами ШІ дозволяє створювати віртуальні середовища, де

студенти можуть імітувати атаки на мережу, проводити її захист і відпрацьовувати методи відновлення після атак.

Віртуальні лабораторії та симуляційні платформи, такі як кіберполігон Cyber Range UA, надають українським кіберфахівцям можливість пройти навчання та відпрацювати навички для активної протидії кіберзагрозам. Cyber Range UA – це віртуальне середовище для емуляції інфраструктур і кібератак, доступне всім кіберспеціалістам країни. На кіберполігоні можуть одночасно тренуватися кілька десятків фахівців, працюючи в командах, щоб навчитися реагувати на інциденти в умовах, максимально наближених до реальних [4]. Це, також, дозволяє отримати реальний досвід роботи у команді професіоналів.

Завдяки віртуальним інструментам та ресурсам навчання стає доступним для ширшого кола осіб, незалежно від місця проживання. Студенти можуть отримувати якісну освіту та консультуватися з фахівцями, виконувати симуляційні вправи щодо розробки та впровадження рішень з кібербезпеки. Використання віртуальних лабораторій та пісочниць для тестування програмного забезпечення та аналізу загроз у безпечному середовищі дає можливість роботи з кіберзагрозами без ризику для реальних систем. Практичні заняття з аналізу шкідливого програмного забезпечення (ШПЗ) у безпечному середовищі дозволяють студентам експериментувати з різними техніками та інструментами, такими, як наприклад, Cuckoo Sandbox, для автоматичного аналізу ШПЗ та генерації звітів.

Пісочниці можуть використовуватися і для тренування навичок реагування на інциденти. Студенти можуть вчитися ідентифікувати, аналізувати та реагувати на різні типи загроз у реальному часі, моделювати та аналізувати мережеві атаки, такі як DDoS-атаки, фішинг та інші.

Здатність штучного інтелекту аналізувати великі обсяги даних у реальному часі дозволяє ефективно виявляти підозрілу активність та потенційні загрози. Студенти, які вивчають кібербезпеку, можуть навчитися використовувати алгоритми машинного навчання для розробки систем автоматизованого виявлення загроз, що значно підвищує ефективність їхньої роботи.

Інтеграція штучного інтелекту в підготовку студентів відкриває нові можливості у навчальному процесі. ШІ не тільки підвищує ефективність навчання, але й дозволяє краще підготувати фахівців до вирішення сучасних викликів [5].

Водночас, використання ШІ у підготовці фахівців з кібербезпеки має свої виклики та ризики, які потребують ретельного аналізу та врахування. Незважаючи на численні переваги, важливо зберігати

баланс між автоматизацією процесів та роллю людського фактору, а також забезпечувати відповідність етичним та юридичним нормам. Також важливо враховувати ризики, пов'язані з конфіденційністю даних і потенційним зловживанням технологіями, з метою створення безпечного освітнього середовища.

Надмірна залежність від ШІ може знижувати самостійність мислення та аналізу студентів, які можуть розраховувати лише на автоматичні системи.

Потреба в постійному оновленні навчальних програм відповідно до новітніх досягнень у сфері ШІ може бути складною задачею для освітніх установ. Також, впровадження ШІ в навчальні процеси вимагає значних фінансових та технічних ресурсів, що може бути складним для деяких навчальних закладів.

Незважаючи на виклики, використання ШІ в підготовці майбутніх спеціалістів з кібербезпеки має великі перспективи. Він допоможе створювати більш ефективні та інтерактивні навчальні програми, зробити навчання більш доступним, стимулюватиме студентів до розробки нових рішень в області кібербезпеки.

Штучний інтелект поступово змінює традиційну модель взаємодії між викладачем і студентом, створюючи нові можливості для навчання та розвитку. Він дозволяє зробити навчання більш персоналізованим, ефективним та інтерактивним. Отже, ШІ не замінює викладача, а доповнює його можливості, створюючи нові перспективи для розвитку освіти.

Впровадження штучного інтелекту в освіту з кібербезпеки – це крок до створення нового покоління фахівців, готових до вирішення складних завдань у динамічному цифровому світі. Такий підхід не тільки підвищує рівень підготовки спеціалістів, але й зміцнює кібербезпеку нашої країни.

Література:

1. Концепція розвитку штучного інтелекту в Україні. 2020. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#n8

2. Андрощук А. Г., Малюга О. С. (2024). Використання штучного інтелекту у вищій освіті: стан і тенденції. *International Science Journal of Education & Linguistics*, *3*(2), 27–35. URL: https://doi.org/10.46299/j.isjel.20240302.04

3. Використання ChatGPT Edu у вишах: коли варто очікувати революції? URL: https://speka.media/vikoristannya-chatgpt-edu-u-visax-koli-varto-ocikuvati-revolyuciyi-9qyq0m

4. Офіційний сайт Ради національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/en/Diialnist/6969.html

5. Luckin, R., Holmes, W., Griffiths, M., & Forcier, L. B. (2016). Intelligence unleashed: An argument for AI in education. Pearson. URL: https://www.researchgate.net/publication/299561597_Intelligence_Unleashed_An_argument_for_AI_in_Education