Олійник Б. М.
Інститут цифровізації освіти НАПН України

Використання штучного інтелекту в процесі розвитку цифрової компетентності з інформаційної безпеки майбутніх учителів інформатики

Стрімкий розвиток штучного інтелекту (ШІ), який відбувався протягом останніх років, значно покращив життя звичайних людей. Ще недавно використання технологій з застосуванням ШІ був обмеженим або майже недоступним для звичайних користувачів, та зараз це кардинально змінилось. Його популярність різко зросла завдяки появі потужних мовних моделей, зокрема ChatGPT-3, ChatGPT-4o та DeepSeek, а поширеність активно зростає завдяки доступності: тепер кожен може скористатися чат-ботами, генераторами зображень, автоматичним перекладачем тексту та іншими розумними інструментами безкоштовно та з будь-якою пристрою, будь це комп'ютер, смартфон чи розумний годинник. Сьогодні технології з застосуванням штучного інтелекту широко застосовуються в різних областях: від охорони здоров'я до освітнього процесу, радикально трансформуючи способи роботи, навчання та взаємодії з сучасними технологіями. Не є винятком і галузь інформаційної безпеки.

У процесі розвитку цифрової компетентності з інформаційної безпеки майбутніх вчителів інформатики ШІ може мати різноманітне застосування, від чат-ботів до спеціальних інструментів з застосуванням штучного інтелекту для проведення певної діяльності. "У перспективі сучасний педагог має бути спроможним здійснювати добір систем ШІ для підтримки навчання у школі та університеті", — зазначають О. Спірін та В. Олексюк [1].

Використання чат-ботів для отримання певної інформації є ефективним рішенням для майбутніх учителів інформатики в ході розвитку цифрової компетентності з інформаційної безпеки. Р. Ходход, Ш. Ван та Ш. Хан наголошують, що "інтелектуальні системи можуть відігравати важливу роль у прискоренні формування навичок з кібербезпеки, допомагаючи вчителям розробляти навчальні матеріали та програми" [2]. Чат-боти сприяють розвитку цієї компетентності, допомагаючи швидко знаходити актуальні матеріали, моделювати реальні небезпечні ситуації, формувати та удосконалювати навички розпізнавання вразливостей та загроз. А їх інтерактивність дозволяє навчатись в зручний для себе час і у доступній формі, що сприяє глибшому розумінню сучасних потреб у галузі інформаційної безпеки.

Застосування штучного інтелекту може бути ефективним у виявленні та запобіганні фішингу та інтернет шахрайству. Технології ШІ, які навчені на величезних наборах даних фішингових електронних листів і відомих моделей шахрайств, дозволяє їм розпізнавати непомітні для людини сигнали, які вказують на потенційну загрозу. Наприклад, ШІ може виявляти аномалії в метаданих електронної пошти, такі як незвичайні шаблони надсилання або розбіжності між відображуваним іменем відправника та адресою електронної пошти. Як зазначає індійська науковиця Рішита Чоккаппагарі: "З часом штучний інтелект стає все кращим завдяки своїй здатності вивчати нові методи фішингу, що робить його найефективнішим інструментом у розпізнаванні атак кіберзлочинців, які постійно розвиваються" [3]. Алгоритми штучного інтелекту виявилися дуже ефективними у виявленні спроб фішингу та інших шахрайських дій, аналізуючи вміст електронної пошти, поведінку відправника та інші показники, ШІ досить точно ідентифікує та позначає підозрілі дії, які могли б залишитися непоміченими.

Використання спеціалізованих інструментів з застосуванням штучного інтелекту може автоматизувати процеси сканування вразливостей шкільної мережі, полегшуючи усунення недоліків безпеки. Це дуже схоже на те, що робили б кіберзлочинці, щоб знайти вразливі місця. Завдяки безперервному моніторингу мережі штучний інтелект може виявляти та визначати пріоритети вразливостей на основі їх потенційного впливу, забезпечуючи оперативне вирішення найбільш критичних проблем. Ця безперервна оцінка дозволяє керувати вразливостями в реальному часі, звужуючи коло можливостей для кіберзлочинців використовувати слабкі місця. С. Пала у своїй статті "Дослідження з розробки моделей ШІ

для раннього виявлення вразливостей мережі" зазначає: "Моделі штучного інтелекту можуть ефективно обробляти великі обсяги даних мережевого трафіку та надавати своєчасні сповіщення про інциденти з кібербезпеки, забезпечуючи швидке реагування та вжиття заходів для зменшення наслідків" [4]. Справжньою перевагою тут є швидкість, адже за допомогою ШІ можна знайти вразливості, оцінити та виправити їх набагато швидше, ніж людина може зробити це вручну.

Штучний інтелект є ефективним інструментом, який може значно покращити забезпечення інформаційної безпеки, але він також створює нові виклики. З одного боку, ШІ може суттєво підвищити нашу здатність виявляти кіберзагрози та реагувати на них, швидко й точно аналізуючи величезні обсяги даних. Це означає, що школи чи інші організації можуть ефективніше виявляти та зменшувати ризики, захищаючи конфіденційну інформацію та забезпечуючи безперебійну роботу. З іншого боку, ту саму технологію можуть використовувати кіберзлочинці з метою розробки більш продуманих і переконливих атак. Оскільки штучний інтелект та методи атак продовжують розвиватися, дуже важливо, щоб вчителі інформатики, персонал школи та учні залишалися проінформованими про нові загрози.

Список використаних джерел

1. Спірін О.М., Олексюк В.П. Досвід та перспективи використання технологій штучного інтелекту у навчанні майбутніх учителів інформатики. Теорія і практика використання інформаційних технологій в умовах цифрової трансформації освіти: матеріали Всеукраїнської науково-практичної конференції, 29 червня 2023 року м. Київ. URL: https://lib.iitta.gov.ua/id/eprint/736338/1/%D0%A1%D0%BF%D1%96%D1%80%D1%96%D0%BD_%D0%9E.%D0%9C.%2C%20%D0%9E%D0%BB%D0%B5%D0%BA%D1%81%D1%8E%D0%BA%20%D0%92.%D0%9F._2023.%20%D0%A1.63-67.pdf
2. Hodhod, R., Wang, S., & Khan, S. Cybersecurity curriculum development using ai and decision support expert system. International Journal of Computer Theory and Engineering, 2018, 10.4: 111. URL: https://www.researchgate.net/profile/Rania-Hodhod/publication/330320538_Cybersecurity_Curriculum_Development_Using_AI_and_Decision_Support_Expert_System/links/5c5dc101a6fdccb608b0be80/Cybersecurity-Curriculum-Development-Using-AI-and-Decision-Support-Expert-System.pdf
3. Chokkappagari Rishitha. How AI Detects Phishing Scams. Insights2Techinfo, pp.1. 2024. URL: https://insights2techinfo.com/how-ai-detects-phishing-scams/
4. Pala Sravan Kumar. Study to Develop AI Models for Early Detection of Network Vulnerabilities. International Journal of Enhanced Research in Science, Technology & Engineering ISSN: 2319-7463. URL: https://www.researchgate.net/profile/Sravan-Kumar-Pala/publication/380712170_Study_to_Develop_AI_Models_for_Early_Detection_of_Network_Vulnerabilities/links/664a789a0b0d284574482839/Study-to-Develop-AI-Models-for-Early-Detection-of-Network-Vulnerabilities.pdf