

УДК 004.8+378

DOI: 10.31733/15-03-2024/2/365-366

Олександр МІЛЮТІН

аспірант кафедри аналітичної
економіки та менеджменту

Тетяна АЛЬОШИНА

професор кафедри аналітичної
економіки та менеджменту
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ВИЩІЙ ОСВІТІ УКРАЇНИ

Поява та стрімкий розвиток Big Data, хмарних обчислень, штучних нейронних мереж та машинного навчання дозволила інженерам створити технології, що можуть імітувати людський інтелект. Відповідні технології зможуть замінити низку професій у майбутньому. Маємо зазначити, що штучний інтелект є інноваційним інструментарієм, який людина може ефективно застосовувати у різноманітних сферах діяльності, що обумовлює актуальність вивчення обраної теми.

На сучасному етапі розвитку інноваційних технологій, штучний інтелект розглядається науковцями як рушійна сила четвертої промислової революції, яка здатна безумовно спровокувати революцію у освіті. [1].

Зростаюча увага, яку привертає розвиток штучного інтелекту, сьогодні вже не просто стає областю досліджень науковців, а й частиною шкільних та університетських програм. Однак, подібно тому, як колись рекламували появу телебачення та комп'ютерів як зміни в освіті, штучний інтелект розглядають як розширений доступ до інформації, не змінюючи суттєво основні компоненти.

На думку авторів, доречно переглянути можливості штучного інтелекту та визначити можливі шляхи оптимізації для освітньої сфери. Саме тому доречно проаналізувати останні тенденції розвитку штучного інтелекту у сфері освіти, щоб надати освітянам оновлене розуміння цієї галузі як революційного інструменту для ефективного освітнього процесу.

Штучний інтелект набуває стратегічного значення для освіти, оскільки останній може бути ефективним інструментом навчання, який зменшує навантаження як на вчителів, так і на студентів. У поєднанні з сучасними освітніми реформами, такими як цифровізація освітніх ресурсів, гейміфікація та персоналізований досвід навчання, штучний інтелект дає можливість розробки інноваційних додатків для оптимізації освітнього процесу. Потенціал методів штучного інтелекту використовується для розробки реактивних та адаптивних навчальних посібників для побудови індивідуалізованих навчальних середовищ, що у майбутньому стане альтернативою навчання «face to face» та компенсацією нестачі вчителів шляхом використання інтелектуальної системи навчання.

Інтелектуальні системи навчання є персоналізований способом навчання за чотирма основними способами: моніторинг успіхів студента; виконання відповідних завдань; забезпечення ефективного зворотного зв'язку; застосування інтерфейсів для спілкування між людиною та комп'ютером [2].

Протягом останніх років інтерес до використання штучного інтелекту в освіті значно збільшився, про свідчать численні публікації статей, доповідей та результатів експериментів впровадження штучного інтелекту у навчальні процеси та поєднання останнього з різними навчальними методиками.

До прикладів використання штучного інтелекту доречно віднести наступне: автоматизація оцінювання успішності студентів [3]; надання рекомендацій та відгуків студентам; виявлення студентів з груп ризику [4]; підтримка процесу навчання студентів, репетиторство, надання навчальних матеріалів на основі потреб студента, автоматизація перевірки домашніх завдань [3]; діагностика сильних і слабких сторін студентів і прогалин в знаннях [4]; підтримка саморегульованого навчання студентів; допомога адміністраторам

і менеджерам відстежувати тенденції та департаментам в прийнятті рішень щодо розвитку їх навчальних програм.

Таким чином, впровадження систематичного використання штучного інтелекту в роботі закладів вищої освіти, залучення працівників освіти до вивчення, впровадження освітніх методологій з використанням сучасних технологій та інструментів мають стати ключовим фактором успіху та надійним інструментарієм розвитку вищої освіти України. Студенти, як користувачі штучного інтелекту, отримують інструмент для ефективної підготовки до здачі заліку, що в свою чергу дозволяє отримати більш конкурентоспроможних випускників для розвитку економіки всередині країни та мати конкурентні переваги у всьому світі.

1. Amir H. Alavi, Bruce M. McLaren, Fan Ouyang, Pengcheng Jiao «*Artificial Intelligence in STEM Education The Paradigmatic Shifts in Research, Education, and Technology*», 460 с. 2022р.
2. Maki K. Habib, «*Revolutionizing Education in the Age of AI and Machine Learning*», 264с., 2019р.
3. Genaro Rebolledo-Mendez, Ning Wang, Noboru Matsuda, Olga C. Santos, Vania Dimitrova, збірник матеріалів конференцій, «*Artificial Intelligence*
4. Eric C. K. Cheng, Tianchong Wang, Tim Schlippe, збірник матеріалів конференцій, «*Artificial Intelligence in Education Technologies: New Development and Innovative Practices Proceedings of 2023 4th International Conference on Artificial Intelligence in Education Technology*», 340с., 2023р.

УДК 004.738.5:351.862.4

DOI: 10.31733/15-03-2024/2/366-367

Олександр НІКОЛАЄНКО

курсант Інституту підготовки
юридичних кадрів
для Служби безпеки України
Національного юридичного
університету імені Ярослава Мудрого

ПРІОРИТЕТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

У сучасному світі кібербезпека є одним із ключових факторів національної безпеки. Кіберзагрози постійно зростають та еволюціонують, ставлячи під загрозу не лише критичну інфраструктуру, але й особисті дані громадян. Російська агресія проти України значно посилила вплив кіберзагроз, роблячи їх більш складними та масштабними. Кібератаки на українські держустанови, банки, та інші організації стали звичним явищем [1]. В цих умовах забезпечення кібербезпеки стає не просто завданням, а нагальною потребою.

Особисто на мою думку підвищення кіберсвідомості та кіберкультури – це ключовий пріоритет забезпечення кібербезпеки України. Це обумовлюється тим що, людський фактор є одним із найслабших місць у кібербезпеці. Так наприклад у травні 2017 року відбулася наймасштабніша атака вірусу WannaCry направлена саме на ураження не захищених комп'ютерних систем. Під час такої атаки кіберзлочинці сканували мережу на наявність комп'ютерів із незахищеним портом SMB (порт SMB дозволяє клієнтам спілкуватися та обмінюватися файлами один з одним, використовуючи сервер як посередник), після чого запускали код для будь-яких виявлених уразливих пристроїв, а потім завантажували шкідливий компонент [2]. Більшість експертів кібербезпеки вважали, що глобальний спалах WannaCry буде цінним уроком для користувачів мережі і адміністраторів підприємств, однак це не так. Люди все одно недооцінюють значення уразливостей своїх комп'ютерних систем та важливість дотримання основних правил безпеки.

Це демонструє що високий рівень кіберсвідомості серед громадян сприятиме ефективнішій реакції на потенційні кіберзагрози. Свідомий і навчений користувач не лише усвідомлює основні правила кібербезпеки, але й може допомагати в розповсюдженні цих знань серед свого оточення. Значне підвищення рівня кіберкультури також сприяє формуванню етичного ставлення до використання інформаційних технологій. Це включає в себе усвідомлення правил етикету в Інтернеті, розуміння принципів безпеки при роботі з