виклики, пов’язані з його впровадженням у систему освіти.

Однією з основних проблем є недостатній рівень цифрової грамотності педагогічних працівників. Для ефективного використання сучасних технологій необхідно організовувати курси підвищення кваліфікації та навчання викладачів.

Також важливим є питання академічної доброчесності, оскільки використання штучного інтелекту може призводити до нечесного виконання навчальних завдань.

Крім того, існують етичні та правові аспекти використання штучного інтелекту, зокрема питання захисту персональних даних та відповідальності за використання цифрових технологій.

Отже, штучний інтелект є важливим інструментом модернізації системи професійної освіти та підготовки фахівців. Його використання сприяє підвищенню ефективності освітнього процесу, персоналізації навчання, розвитку цифрових компетентностей та впровадженню інноваційних освітніх технологій.

Інтеграція штучного інтелекту в освітній процес відкриває нові можливості для вдосконалення професійної підготовки та формування сучасних фахівців, які здатні ефективно працювати в умовах цифрової економіки.

Водночас впровадження штучного інтелекту в освіті потребує комплексного підходу, який передбачає розвиток цифрової інфраструктури, підвищення кваліфікації педагогічних працівників та забезпечення дотримання етичних норм використання технологій.

Таким чином, використання штучного інтелекту є важливим напрямом розвитку сучасної професійної освіти, що сприяє підвищенню її якості та конкурентоспроможності.

Список використаних джерел

1. Биков В. Ю. Цифрова трансформація освіти і науки. Київ: Академперіодика, 2020.
2. Морзе Н. В. Інформаційні технології в освіті. Київ: Університетська книга, 2019.
3. Кремень В. Г. Філософія освіти XXI століття. Київ: Педагогічна думка, 2021.
4. UNESCO. Artificial Intelligence in Education: Guidance for Policy-makers. Paris, 2021.
5. Holmes W. Artificial Intelligence in Education. Boston, 2019.
6. OECD. Artificial Intelligence and the Future of Education. Paris, 2022.

БЕЗПЕКА ВИКОРИСТАННЯ ЦИФРОВИХ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМІ РЕФОРМУВАННЯ БЕЗПЕЧНОЇ ТА СТІЙКОЇ ШКІЛЬНОЇ ОСВІТИ

Джурило А. П., *Інститут педагогіки НАПН України, Україна*

Ключові слова: штучний інтелект в освіті, цифрова безпека, стійкість шкільної освіти, реформи безпеки, цифрова компетентність учителя

Прискорена цифровізація освітнього простору, зумовлена технологічними зрушеннями початку XXI століття, поставила перед школою принципово нові виклики, що виходять за межі традиційної дидактики. Поширення генеративних систем штучного інтелекту (ШІ) у навчальному процесі відкриває безпрецедентні можливості для персоналізації навчання, автоматизації рутинних завдань і підвищення доступності освітніх ресурсів. Водночас їхнє некероване впровадження продукує системні ризики – від витоків персональних даних учнів до алгоритмічних упереджень, що відтворюють нерівності в освіті (UNESCO, 2023). Зазначені ризики набувають особливої гостроти в контексті ширших реформ з безпеки та стійкості шкільної освіти, які охоплюють фізичну, психологічну та інформаційну безпеку освітнього середовища.

Актуальність дослідження визначається тим, що в Україні та інших країнах, які проводять системні реформи шкільної освіти в умовах безпекових криз, питання цифрової

безпеки ШІ-інструментів залишається недостатньо інтегрованим у загальну архітектуру безпекових реформ. Це формує концептуальний розрив між технологічною практикою та нормативно-стратегічним регулюванням.

Концепти «стійкості освіти» та «освітньої резильєнтності» розглядається в сучасній науковій літературі у двох взаємопов'язаних вимірах: як здатність освітньої системи зберігати функціональність в умовах зовнішніх потрясінь (збройні конфлікти, пандемії, кліматичні катаклізми); як спроможність захищати учасників освітнього процесу від нових форм ризику, до яких дедалі більше відносять і ризики цифрового середовища. ЮНЕСКО у своїх нормативних документах безпосередньо пов'язує «*safe and resilient education*» з необхідністю вироблення регуляторних механізмів щодо генеративного ШІ в навчальних закладах, наголошуючи, що відсутність таких механізмів є самостійним чинником уразливості освітніх систем (UNESCO, 2023).

Реформи безпеки шкільної освіти традиційно фокусувалися на фізичній безпеці приміщень, психологічному кліматі та врегулюванні булінгу. Однак під впливом Рамкової програми ЄС з цифрової освіти (European Commission, 2020) відбувається розширення поняття «шкільна безпека» за рахунок включення до нього компонента цифрової безпеки, що охоплює: (а) захист персональних даних неповнолітніх; (б) протидію маніпулятивним алгоритмам; (в) формування критичного мислення щодо ШІ-генерованого контенту. Таким чином, безпека ШІ-інструментів стає структурним елементом – а не лише периферійним доповненням – до сучасних реформ стійкості шкільної освіти.

Для систематичного аналізу було виокремлено три рівні ризиків, що асоціюються із застосуванням ШІ в шкільній освіті: технологічно-правові, педагогічно-когнітивні, системно-інституційні.

1. Технологічно-правові ризики пов'язані з обробкою персональних даних учнів платформами ШІ, переважна більшість яких розроблена поза межами юрисдикції, де функціонує навчальний заклад. Дослідження свідчать, що лише 34% опитаних систем освіти мають затверджені протоколи перевірки відповідності ШІ-інструментів національному законодавству про захист даних до їхнього впровадження в навчальний процес (UNESCO, 2020). Це означає, що в переважній більшості випадків учні взаємодіють з інструментами, що не пройшли правової експертизи.

2. Педагогічно-когнітивні ризики включають залежність від ШІ-генерованих відповідей (явище «алгоритмічного аутсорсингу» мислення), некритичне сприйняття «галюцинацій» генеративних моделей як достовірної інформації, а також поглиблення «цифрового розриву» між учнями з різним рівнем ШІ-грамотності. Без цілеспрямованої педагогічної медіації цифрові технології можуть посилювати, а не нівелювати нерівності у навчальних досягненнях (Биков та ін., 2021).

3. Системно-інституційні ризики зумовлені відсутністю у більшості шкіл чітких політик використання ШІ, розмитістю відповідальності за цифрову безпеку між адміністрацією, вчителями та батьками, а також недостатньою підготовкою педагогічного персоналу до виявлення та реагування на ШІ-пов'язані інциденти.

У системній архітектурі безпеки ШІ-інструментів учитель займає позицію першої лінії захисту – суб'єкта, який безпосередньо опосередковує взаємодію учнів з технологічним середовищем. Ця позиція передбачає, що цифрова компетентність педагога має включати не лише технічні навички роботи з ШІ-платформами, але й специфічний компонент безпекової грамотності (*AI safety literacy*), що охоплює три виміри:

1. *Аналітичний вимір:* здатність ідентифікувати потенційні ризики конкретного ШІ-інструменту до його застосування в класі (аналіз умов використання, перевірка відповідності GDPR / вітчизняному законодавству, оцінка алгоритмічної прозорості);

2. *Дидактичний вимір:* проєктування педагогічних ситуацій, у яких учні набувають навичок критичного оцінювання ШІ-контенту, що є одночасно і захисним механізмом, і елементом формування цифрової компетентності;

3. *Інституційний вимір:* участь учителя у розробці та впровадженні шкільної політики

безпечного використання ШІ як частини ширшої стратегії безпеки освітнього закладу.

Рамковий документ DigComp 2.2 (Vuorikari et al., 2022) включає «безпеку» як одну з п’яти базових компетентнісних сфер, однак переважно у сенсі захисту пристроїв і приватності. Наразі тривають дискусії щодо розширення цієї сфери з урахуванням специфічних ризиків ШІ-систем. Вбачається, що саме в рамках реформ безпеки та стійкості шкільної освіти має здійснюватися конкретизація та впровадження цих теоретичних рамок у вимогах до підготовки вчителів.

На основі проведеного аналізу запропоновано такі напрями інтеграції безпеки ШІ-інструментів у загальну рамку реформ стійкості та безпеки шкільної освіти:

- *нормативна інтеграція*: включення вимог щодо перевірки ШІ-інструментів у шкільні безпекові протоколи та плани управління ризиками, аналогічно до протоколів захисту від фізичних загроз;
- *інституційна координація*: призначення відповідальних за цифрову безпеку ШІ на рівні школи (роль «ШІ-координатора з безпеки») з чітко окресленими функціями та підзвітністю;
- *підготовка вчителів*: впровадження обов’язкового модуля «Безпека ШІ в освіті» у програми підвищення кваліфікації педагогів, що поєднує правовий, технічний та педагогічний компоненти;
- *учнівська медіаграмотність*: включення критичного аналізу ШІ-контенту до навчальних програм як обов'язкового елемента формування цифрової грамотності;
- *моніторинг та оцінювання*: розробка індикаторів безпеки використання ШІ, що можуть бути інтегровані в загальні системи моніторингу стійкості шкільної освіти.

Безпека застосування цифрових інструментів штучного інтелекту в шкільній освіті не є ізольованою технічною проблемою – вона є органічним компонентом ширших реформ з безпеки та стійкості шкільної освіти. Фрагментарне ставлення до ШІ-безпеки, відірване від системної безпекової рамки школи, веде до накопичення структурних ризиків, які з часом можуть підривати не лише цифровий, а й загальний безпековий потенціал навчального закладу. Підвищення цифрової компетентності вчителя, зокрема в аспекті «безпекової грамотності щодо ШІ», є необхідною умовою успішної реалізації обох векторів – технологічної модернізації освіти та зміцнення її стійкості й безпеки. Подальші дослідження мають бути спрямовані на розробку конкретних індикаторів та інструментів вимірювання рівня інтегрованості ШІ-безпеки у шкільні безпекові системи.

Список використаних джерел

1. Биков, В. Ю., Спірін, О. М., & Пінчук, О. П. (2017). Проблеми та завдання сучасного етапу інформатизації освіти. *Наукове забезпечення розвитку освіти в Україні: актуальні проблеми теорії і практики (до 25-річчя НАПН України)*, 191–198. https://lib.iitta.gov.ua/709026/
2. European Commission. (2020). *Digital Education Action Plan 2021–2027*. Publications Office of the European Union. https://education.ec.europa.eu/focus-topics/digital-education/action-plan
3. UNESCO IITE. (2020). *AI in Education: Change at the Speed of Learning*. UNESCO IITE Policy Brief. Author: Steven Duggan. https://iite.unesco.org/wp-content/uploads/2021/05/Steven_Duggan_AI-in-Education_2020-2.pdf
4. UNESCO. (2023). *Guidance for generative AI in education and research*. UNESCO. DOI: 10.54675/EWZM9535
5. Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens — With new examples of knowledge, skills and attitudes*. Publications Office of the European Union. DOI: 10.2760/490274