

заборону можна обійти – дитина швидко навчиться користуватися VPN, знайде альтернативні джерела. По-друге, заборонене, як відомо, приваблює. Тобто такий метод не вирішує проблему, а лише її відкладає.

Другий – більш складний, але дієвий – полягає в системному навчанні. З раннього віку дитина повинна отримувати знання про інформаційну гігієну, цифрову етику, безпеку в мережі. Це має бути послідовна політика на всіх рівнях освіти: від дитячого садка до старшої школи. Необхідна також підготовка педагогів, створення навчальних програм, адаптованих до віку дітей.

Висновки. Інформаційна гігієна у цифрову епоху – це питання, яке має стратегічне значення для розвитку особистості, захисту прав дитини та формування безпечного суспільства. Сучасні діти виростають у середовищі, де інформація впливає на всі аспекти їхнього життя. Тому лише завдяки поєднанню обізнаності, критичного мислення та освітніх стратегій можна забезпечити формування цифрово грамотного покоління, здатного протистояти загрозам інформаційного світу.

ШТУЧНИЙ ІНТЕЛЕКТ В ОСВІТІ І ЦИФРОВА БЕЗПЕКА ДИТИНИ: ТЕРМІНОЛОГІЯ ТА ОФІЦІЙНІ НАСТАНОВИ.

Пінчук О.П.

кандидат педагогічних наук, старший
науковий співробітник,
Інститут цифровізації освіти НАПН
України
ORCID ID: 0000-0002-2770-0838

Штучний інтелект (ШІ) – «організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час

роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань» [1, с.32]. У наукових джерелах, офіційних документах, освітніх і аналітичних матеріалах, публіцистичній літературі використовують як синоніми такі формулювання як: сервіси на основі штучного інтелекту, цифрові сервіси; інструменти зі штучним інтелектом; інтелектуальні сервіси та штучноінтелектні сервіси.

Рамкова конвенція Ради Європи про штучний інтелект та права людини, демократію та верховенство права [4] є першим в історії міжнародним юридично обов'язковим договором у цій галузі. Україна – один з підписантів цього документу. Одним із базових принципів Конвенція визначає повагу до приватного життя та захист персональних даних, що є критичним для захисту прав дітей у цифровому середовищі. Конвенція пропонує державам-учасницям два способи дотримання її принципів та зобов'язань під час регулювання: 1) ухвалити рішення бути безпосередньо зобов'язаними відповідними положеннями Конвенції, 2) вжити інших заходів для дотримання положень договору, повністю дотримуючись своїх міжнародних зобов'язань щодо прав людини, демократії та верховенства права.

Діти потребують особливого захисту в умовах цифрової трансформації суспільства. Тут доречно згадати дослідження [5] 2024 року, що проведене серед 12-17-річних дітей з різних європейських країн (7 тис. учнів з Німеччини, Греції, Португалії, Румунії, Іспанії, Туреччини та Великої Британії). Згідно з дослідженням, майже 74% підлітків у Європі вважають, що ШІ суттєво вплине на їхнє професійне життя. Але лише менше половини вірить, що школа їх до цього готує.

Ми вступаємо в еру, де ШІ вже не фантастика, а частина шкільного щодення: від текстових чатботів до рекомендацій у навчальних платформах. Але разом із можливостями приходить і відповідальність. У рекомендаціях [2]-[3], розроблених Міністерством цифрової трансформації та МОН

України, акцент робиться на прозорості алгоритмів, добровільній згоді та обмеженні дискримінаційного впливу. Зокрема, рішення, що впливають на освітню траєкторію особи, не повинні прийматися автоматизовано без участі людини (принцип «контроль з боку людини»).

Захист персональних даних дітей має бути невід'ємним елементом цифрової інфраструктури освітнього закладу. Це вимагає наявності чітких політик конфіденційності та технічного захисту при впровадженні ІІІ в закладі освіти.

Перед використанням будь-яких цифрових платформ або ІІІ-сервісів має проводитись правова та технічна експертиза щодо безпеки персональних даних, що особливо важливо у випадку неповнолітніх. Одна з ключових рекомендацій щодо цифрової безпеки: мінімізація введення чутливої інформації. Учні та вчителі, адміністрація закладу освіти не повинні вводити персональні, конфіденційні або таємні дані в будь-яку систему ІІІ. Категорично заборонено вводити у системи ІІІ імена учнів, контактні дані, інформацію про здоров'я, психологічний стан тощо без спеціального дозволу. Це положення має бути частиною кодексу поведінки та етичного навчання у сфері ІІІ.

Безпека в цифровому середовищі має починатися з базової обізнаності про ризики та способи самозахисту. Учасники процесу мають володіти інструментами цифрової гігієни. При використанні інструментів на основі ІІІ учитель повинен перевіряти їх на відповідність психоемоційним і віковим особливостям учнів, враховувати особливості сприйняття та емоційного розвитку дитини певного віку. Це особливо важливо при використанні генеративних інструментів у початковій школі. Для всіх без виключення учнів віком до 18 років потрібна згода батьків або законних представників.

Професійний розвиток педагогічних працівників у галузі ІІІ-компетентності має ключове значення для забезпечення відповідального використання технологій. Це передбачає не лише технічну, а й етичну, юридичну та дидактичну підготовку.

Ми порівняли деякі аспекти настанов Міністерство освіти і науки України та Мінцифри [2]-[3] щодо захисту дітей у цифрову епоху.

Аспект	ЗЗСО, 2024 [3]	ЗВО, 2025 [2]
Захист персональних даних (ПД)	Наголос на забороні введення учнями персональних і конфіденційних даних у системи ІІІ (с. 23).	Зазначено необхідність забезпечення легітимного доступу, згоди на обробку, надійного зберігання та якісного управління даними (с. 24-25).
Інформована згода	Необхідність інформування та отримання згоди батьків або їх законних представників (для учнів до 18 років) перед використанням ІІІ (с. 11, 23).	Уточнюється вимога поінформованості здобувачів щодо збору й обробки їхніх даних у межах університетських політик, але згода пов'язана з повноліттям і самотійною відповідальністю.
Регламентація доступу до даних	Адміністрація має забезпечити відповідність сервісів законодавству про захист ПД (с. 10).	Впроваджуються політики конфіденційності на інституційному рівні: управління доступом, аудит, мінімізація використання чутливої інформації (с. 13, 24).
Ризики автоматизованого оцінювання	Автоматизоване оцінювання вважається високо ризиковим і має супроводжуватись людським контролем.	ІІІ-системи для оцінювання мають містити механізми перегляду викладачами, що гарантує дотримання прав здобувачів (с. 11, 13).
Політики використання ІІІ	Вимагається локальна регламентація і запобігання збору даних учнів без згоди.	Обов'язкове створення політик ІІІ на рівні ЗВО, включаючи обмеження на обробку конфіденційної інформації та заборону несанкціонованого використання (с. 13, Дод. 6).

Етична складова	Містить рекомендації щодо виховання етичного ставлення до використання ШІ у школі (с. 24).	Запроваджуються принципи прозорості, підзвітності, уникнення дискримінації, дотримання конфіденційності (с. 11–12).
------------------------	--	---

У підсумку варто зауважити, що обидва документи визнають обробку персональних даних у ШІ як вектор підвищеної загрози. У закладах загальної середньої освіти акцентовано на захисті дітей як уразливої категорії, у закладах вищої освіти – на інституційному управлінні та на внутрішніх політиках. Механізми інформованої згоди та обмеження збору даних більш строго прописані у документі для шкіл, де діти виступають як правові суб'єкти, що потребують додаткового захисту. Використання ШІ без людського контролю в оцінюванні розглядається як неприпустиме в обох документах, проте у [2] деталізовано механізми запобігання та зроблено більший акцент на автономії інституції та її політик, що врегульовують не лише захист даних, а й академічну доброчесність, етику, зокрема й авторське право.

Визнаючи відповідальність за використання автоматизованих інструментів, а також з метою сприяння утвердженню нових етичних норм у добу цифрових технологій маю зазначити, що задля стилістичної узгодженості тексту в окремих формулюваннях було використано інструмент ChatGPT, змістовне наповнення повністю ґрунтується на авторському дослідженні.

Список використаних джерел

1. Міністерство цифрової трансформації України. *Словник термінів у сфері штучного інтелекту*. Упоряд. Д. Чумаченко, Д. Мішкін, О. Андрієнко, О. Краковецький, О. Турута, О. Дубно, Д. Хрущова, А. Кобрін, Т. Авдєєва, І. Кравець, В. Герасимяк, О. Шабанов, А. Бистрицька. Київ, 2024. Дата звернення: 27 травня 2025. <https://surl.li/ppgtki>.

2. Міністерство цифрової трансформації України, та Міністерство

освіти і науки України. *Рекомендації щодо відповідального впровадження та використання технологій штучного інтелекту в закладах вищої освіти*. Київ, 2025. <https://doi.org/10.33407/lib.NAES.id/eprint/745301>

3. Міністерство освіти і науки України. *Інструктивно-методичні рекомендації щодо впровадження та використання технологій штучного інтелекту в закладах загальної середньої освіти*. Київ, 2024. <https://mon.gov.ua/static-objects/mon/sites/1/news/2024/05/21/Instruktyvno.metodychni.rekomendatsiyi.shc.hodo.SHI.v.ZZSO-22.05.2024.pdf>.

4. Council of Europe. *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. Strasbourg: Council of Europe, 2024. <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>

5. OECD. *Empowering Learners for the Age of AI: An AI Literacy Framework for Primary and Secondary Education*. Paris: OECD Publishing, 2025. https://ailiteracyframework.org/wp-content/uploads/2025/05/AILitFramework_ReviewDraft.pdf.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ДІТЕЙ В УМОВАХ ЦИФРОВІЗАЦІЇ ОСВІТИ: ПРАВОВІ ТА ІНФОРМАЦІЙНО-БЕЗПЕКОВІ АСПЕКТИ. Корж І. Ф.

доктор юридичних наук, старший науковий співробітник,
Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»
ORCID ID: 0000-0003-0446-5975

Цифровізація освіти, яка значно посилилася під час пандемії COVID-19, спричинила широке використання електронних платформ, мобільних застосунків, відеозв'язку та електронних щоденників. Діти активно