

Правові аспекти використання ШІ у вищій освіті

Використання штучного інтелекту у ЗВО не лише створює багато можливостей для вдосконалення освітнього процесу та адміністрування, а й уможливорює різноманітні ризики для інтелектуальної власності, інформаційної безпеки, конфіденційності та захисту персональних даних, що потребують аналізу, оцінки та управління.

9.1. Авторське право при використанні систем ШІ

Відповідно до **Закону України «Про авторське право і суміжні права»**, неоригінальні об'єкти, згенеровані комп'ютерною програмою (а саме такими об'єктами є матеріали, створені ШІ), охороняються правом особливого роду (**sui generis**).

Поняття «автор», «авторські права» до таких матеріалів не застосовні, оскільки за українським законодавством автором визнається виключно фізична особа, яка власною інтелектуальною творчою працею створила оригінальний твір.

Відповідно до Закону України «Про авторське право і суміжні права» в узагальненому вигляді права особливого роду (**sui generis**) на матеріали, створені ШІ, можуть належати:

- або особам, яким належать майнові права чи ліцензійні повноваження на відповідну комп'ютерну програму (систему ШІ), тобто авторам системи ШІ, їх спадкоємцям, особам, яким автори чи їх спадкоємці передали (відчужили) відповідні права;
- або правомірним користувачам комп'ютерної програми (системи ШІ).

У кожному окремому випадку відповідь на питання, кому саме належать права особливого роду (**sui generis**) на неоригінальні об'єкти, згенеровані відповідними комп'ютерними програмами (системами ШІ), і які саме права надаються користувачеві системи ШІ, визначаються договором, роль якого зазвичай виконують ліцензійна угода з кінцевим користувачем (end-user license agreement, EULA) або Умови користування сервісом (Terms of Service).

Приклади умов користування окремими продуктами — системами ШІ — наведено в **Рекомендаціях щодо відповідального використання ШІ**: питання права інтелектуальної власності, де детально розкриваються питання охорони прав інтелектуальної власності та прав особливого роду, пов'язані з використанням ШІ, та надаються конкретні рекомендації користувачам щодо відповідального використання ШІ без порушення прав інтелектуальної власності.

9.2. Захист персональних даних та конфіденційної інформації при використанні систем ШІ

Захист персональних даних, приватність та право на невтручання в особисте життя є не менш важливим аспектом при використанні ШІ в ЗВО. Один із ключових принципів — мінімізація обробки даних — збір лише тих відомостей, які необхідні для роботи системи. Наприклад, якщо систему ШІ використовують для аналізу успішності студентів, немає потреби зберігати інформацію, яка не стосується освітнього процесу, наприклад, дані про їхню медичну історію.

Викладачі та студенти не повинні вводити персональних, конфіденційних або таємних даних у будь-яку систему ШІ без необхідності та за відсутності дозволу з боку ЗВО. У системах ШІ функція тренування системи на нових введених даних має бути вимкнена за замовчуванням.

Інформування студентів і співробітників про обробку їхніх персональних даних має бути прозорим та зрозумілим. Заклади повинні надавати доступ до повідомлення про обробку персональних даних, яке пояснює, хто збирає дані, які дані збирають для яких цілей обробляють тощо. Це може бути забезпечено через публікацію такого повідомлення на вебсайті закладу або проведення інформаційних сесій для студентів.

Законність обробки персональних даних має забезпечуватися наявністю однієї із шести підстав для обробки персональних даних, зокрема: виконання договору, виконання законодавчого обов'язку, захисту законних інтересів, здійснення повноважень, захисту життєво важливих інтересів та згоди.

Залежно від контексту та цілей обробки підстави будуть різні. У багатьох випадках згода не є доречною підставою і має розглядатися після вичерпання необхідності інших підстав. У разі обрання згоди вона повинна бути добровільною, чітко сформульованою та передбачати можливість її відкликання в будь-який момент без негативних наслідків.

Важливим елементом захисту приватності є забезпечення права суб'єктів даних на доступ, виправлення або видалення їхньої інформації, зокрема якщо така інформація міститься в системах ШІ. Заклади вищої освіти повинні впроваджувати механізми, які дають змогу студентам або співробітникам легко подати відповідний запит і швидко отримати відповідь.

Для забезпечення належного рівня захисту персональних даних рекомендується створювати структурний підрозділ або призначати відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних. Крім того, договори з постачальниками систем ШІ повинні містити положення про обов'язковий захист даних і передбачати їхню відповідальність за будь-які порушення безпеки даних.

Окрему увагу варто приділити транскордонній передачі даних, якщо їх передають за межі України. У таких випадках необхідно мати підставу для транскордонної передачі даних, зокрема, однією з них може бути надання гарантій щодо невтручання в особисте й сімейне життя, що може бути реалізовано шляхом наявності організаційних та технічних заходів безпеки даних у закордонних системах ШІ.

9.3. Інформаційна безпека при використанні систем ШІ

Одним із перших кроків до безпечного впровадження та використання систем ШІ є розробка політик інформаційної безпеки та управління ризиками з метою впровадження процесів ідентифікації ризиків, загроз і вразливостей, як-от несанкціонований доступ до даних студентів чи викладачів, витік конфіденційної інформації або компрометація моделей ШІ. Визначення пріоритетів ЗВО для управління цими ризиками має базуватися на їхній імовірності та потенційних наслідках для ЗВО.

Сучасні технології дають змогу ефективно захищати дані завдяки впровадженню багаторівневих заходів безпеки. Наприклад, для зберігання інформації про студентів рекомендується використовувати методи шифрування, що забезпечують недоступність даних навіть у разі витоку. Додатково важливо запровадити контроль доступу, які допомагають визначити ролі та права користувачів, а також обмежити доступ до конфіденційної інформації лише тим особам, які дійсно потребують цього для виконання своїх обов'язків.

Системи ШІ мають бути перевірені на відповідність стандартам безпеки. Упроваджуючи системи ШІ, необхідно укладати договори з розробниками та/або постачальниками систем ШІ, які містять гарантії безпеки, забезпечення регулярних оновлень, виправлення виявлених вразливостей тощо. Багато сервісів надають можливість налаштувати заходи безпеки, як-от багатофакторна автентифікація. Перед упровадженням систем ШІ доцільно проводити тестування на вразливості та здійснювати регулярний аудит, щоб упевнитися у відсутності потенційних загроз. Окрім того, важливий постійний моніторинг систем ШІ за допомогою спеціалізованих інструментів, які допомагають виявляти підозрілу активність у реальному часі та своєчасно реагувати на неї.

Ці поради сприятимуть відповідальному та ефективному впровадженню систем штучного інтелекту в закладах вищої освіти та освітньому процесі, забезпечуючи належне виконання завдань і функцій держави, а також оптимізацію управлінських процесів.

У додатках, що наводяться нижче, подано корисну інформацію щодо коректності написання запитів (промптів), оцінки успішності отриманих результатів, аналізу ризиків при виборі системи ШІ для роботи, а також корисні ШІ-інструменти й найкращі міжнародні практики використання ШІ в освіті.