Література:

1. Про затвердження Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах) : Постанова Кабінету Міністрів України від 23 березня 2016 року № 261. URL: https://zakon.rada.gov.ua/laws/show/261-2016-%D0%BF#Text (дата звернення: 14.08.2024).

2. Про внесення змін до деяких постанов Кабінету Міністрів України з питань підготовки та атестації здобувачів наукових ступенів : Постанова Кабінету Міністрів України від 19 травня 2023 року № 502. URL: https://zakon.rada.gov.ua/laws/show/502-2023-%D0%BF#Text (дата звернення: 14.08.2024).

3. Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії: Постанова Кабінету Міністрів України від 12 січня 2022 року № 44. URL : https://zakon.rada.gov.ua/laws/show/44-2022-%D0%BF#Text (дата звернення: 14.08.2024).

ШТУЧНИЙ ІНТЕЛЕКТ У СУДОВО-ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ: ПОТЕНЦІАЛ ТА ЕТИЧНІ ПРОБЛЕМИ

Дзюбак Катерина,
кандидатка економічних наук,
головна судова експертка лабораторії економічних видів досліджень
Одеського науково-дослідного інституту судових експертиз
Міністерства юстиції України

Використання штучного інтелекту (ШІ) у судочинстві останніми роками привертає значну увагу. Постійний розвиток технології відкриває нові можливості для боротьби зі злочинністю та ідентифікації злочинців. Системи штучного інтелекту можуть аналізувати великі обсяги даних, розпізнавати закономірності та робити точні прогнози, що може призвести до більш ефективного та результативного розслідування злочинів.

Однак, незважаючи на багатообіцяючий потенціал ШІ у судочинстві, існують також етичні проблеми, які не можна ігнорувати. Використання систем штучного інтелекту для боротьби зі злочинністю порушує питання про конфіденційність, дискримінацію та вплив на верховенство права. Вкрай важливо, щоб технологічний прогрес супроводжувався глибоким розумінням етичних принципів, які лежать

в його основі, щоб гарантувати, що використання ШІ відповідає нашим суспільним цінностям і нормам.

Проведення судових експертиз із використанням штучного інтелекту (ШІ) має великий потенціал, який є як корисним, так і етично суперечливим [1]. Технології штучного інтелекту можна використовувати в різних аспектах судово-експертної роботи – від відтворення та аналізу місць злочинів до ідентифікації осіб, що вчинили певні правопорушення. Також ШІ дозволяє проводити аналіз мовлення: алгоритми ШІ можуть аналізувати аудіозаписи і шукати певні шаблони або характеристики, які можуть вказувати на злочин або підозрілу поведінку. Автоматичне розпізнавання «мовних шаблонів» може допомогти судовим експертам, які проводять судові експертизи аудіо- та відеозаписів виявити важливу інформацію з наданих слідчими органами розмов або телефонних дзвінків.

Однією з видатних особливостей штучного інтелекту у судово-експертній діяльності є його надійність. Завдяки використанню машинного навчання ШІ може безперервно навчатися і вдосконалюватися на основі великих обсягів даних, щоб надавати точні результати. На відміну від людей-експертів, на нього не впливають втома і емоції, що забезпечує більшу послідовність і точність. Точність систем штучного інтелекту в судовому розслідуванні вражає. У багатьох випадках ці системи можуть розпізнавати закономірності та кореляції, невидимі для людського ока.

Однак важливо враховувати етичні проблеми, пов'язані з використанням ШІ у судово-експертній практиці. Наприклад, алгоритми ШІ можуть бути упередженими і призводити до помилок або несправедливих результатів. Важливо, щоб ці алгоритми були ретельно вивчені і перевірені, щоб переконатися, що вони не посилюють дискримінацію або несправедливість [2]. Крім того, необхідно враховувати питання конфіденційності, оскільки використання технологій ШІ може призвести до розкриття конфіденційної інформації про людей.

Ретельне планування, нагляд і регулювання необхідні для повної реалізації переваг ШІ в судово-експертній діяльності при одночасному вирішенні етичних проблем. Дослідження і розробки повинні бути спрямовані на вдосконалення систем штучного інтелекту і гарантувати, що їх застосування буде високоточним, прозорим і справедливим. Тільки так можна реалізувати весь потенціал штучного інтелекту при проведенні судово-економічних експертиз.

Одне з важливих питань полягає в тому, як слід інтерпретувати і використовувати результати роботи алгоритмів ШІ. Чи повинні вони використовуватися як єдиний доказ у судовому процесі, чи їх слід

розглядати лише як допоміжну інформацію? Ще однією етичною проблемою є прозорість систем штучного інтелекту. Алгоритми та «процеси прийняття рішень», що лежать в основі систем ШІ, часто є складними та незрозумілими. Це може призвести до сумнівів у справедливості та неупередженості результатів.

Для вирішення цих етичних проблем необхідне всебічне обговорення і регулювання. Співпраця між науковцями, судовими експертами та фахівцями з етики має вирішальне значення для розробки правильної політики і процедур використання ШІ в судово-експертних дослідженнях.

Одне з головних занепокоєнь полягає в тому, що використання ШІ в судово-експертній роботі може призвести до автоматизації, яка зменшує роль і повноваження людей-експертів у прийнятті рішень. Хоча системи ШІ здатні аналізувати великі обсяги даних за дуже короткий час і можуть виявляти потенційні докази або закономірності, штучному інтелекту часто бракує людського судження і здатності розуміти контекст.

Інша етична проблема пов'язана з чесністю і прозорістю алгоритмів ШІ в судово-експертній діяльності. При розробці систем штучного інтелекту їм надаються навчальні дані, отримані з реальних справ. Однак базові дані можуть бути нерівномірними і надмірно представляти певні групи підозрюваних або жертв. Така упередженість може призвести до того, що системи ШІ будуть неточними або несправедливими при прогнозуванні підозрюваних або ідентифікації правопорушників.

Ще одне занепокоєння пов'язане з конфіденційністю і безпекою даних криміналістичних технологій на основі ШІ. При аналізі доказів системи ШІ можуть отримати доступ до конфіденційних даних, таких як особиста інформація, медичні записи або соціальні профілі. Важливо забезпечити, щоб ці дані не зловживалися і не використовувалися в інших цілях, а також забезпечити відповідні засоби захисту для запобігання несанкціонованому доступу.

Відповідно до п. 1.4 Інструкції про призначення та проведення судових експертиз та експертних досліджень, затвердженої наказом Міністерства юстиції України від 08.10.1998 № 53/5 [3], під час проведення експертиз (експертних досліджень) з метою виконання певного експертного завдання експертами застосовуються відповідні методи дослідження, методики проведення судових експертиз, а також нормативно-правові акти та нормативні документи, а також чинні республіканські стандарти колишньої УРСР та державні класифікатори, галузеві стандарти та технічні умови колишнього СРСР, науково-технічна, довідкова література, програмні продукти тощо.

Тому для вирішення зазначених вище етичних проблем необхідно розробити чіткі керівні принципи і стандарти використання ШІ при проведенні судових експертиз. Прозора документація алгоритмів і навчальних даних, що використовуються, має важливе значення для забезпечення об'єктивності та точності результатів, а системи ШІ повинні регулярно переглядатися і оновлюватися, щоб забезпечити їхню відповідність сучасним стандартам.

Крім того, експерти в судовій практиці повинні бути належним чином підготовлені до роботи з системами штучного інтелекту. Подальше навчання та тренінги з використання та інтерпретації результатів аналізу мають вирішальне значення для уникнення непорозумінь і неправильних інтерпретацій [4]. Такі кваліфіковані експерти мають відігравати важливу роль у забезпеченні відповідального використання ШІ в судово-експертній діяльності.

Підсумовуючи, можна сказати, що застосування штучного інтелекту (ШІ) в судово-експертній практиці має величезний потенціал для підвищення ефективності і точності надання висновків судових експертиз. Впровадження систем штучного інтелекту дозволяє судовим експертам аналізувати складні дані швидше і ефективніше, а отже, може призвести до покращення розкриття злочинів. Роль людей-експертів повинна залишатися центральною для впливу на прийняття рішень і забезпечення справедливого і прозорого використання систем штучного інтелекту.

Однак не менш важливо враховувати етичні проблеми, пов'язані з використанням ШІ у судовій експертизі. Автоматизація та делегування рішень системам ШІ вимагає ретельного осмислення питань верховенства права, конфіденційності та захисту прав людини. Тому визначення чітких керівних принципів і стандартів відповідального використання ШІ в судово-експертній практиці має вирішальне значення.

Література:

1. Richter Th. KI in der Forensik: Potenzial und ethische Bedenken. URL: https://das-wissen.de/ki-in-der-forensik-potenzial-und-ethische-bedenken/ (дата звернення: 10.08.2024).

2. Shevchuk V. (2023). Artificial Intelligence in Law Enforcement and Justice Bodies: Domestic and European Experience. *Theory and Practice of Forensic Science and Criminalistics.* 29(4):12-46. URL: https://www.researchgate.net/publication/375929350_Artificial_Intelligence_in_Law_Enforcement_and_Justice_Bodies_Domestic_and_European_Experience (дата звернення: 10.08.2024).

3. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень: Наказ Міністерства

юстиції України від 08.10.1998 № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 10.08.2024).

4. Крат В., Голубовський І. Штучний інтелект і судочинство. URL: https://yur-gazeta.com/publications/practice/sudova-praktika/shtuchniy-intelekt-i-sudochinstvo.html (дата звернення: 10.08.2024).

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ

Долженко Любов,
старший судовий експерт
сектору дослідження звуко- та відеозапису
відділу досліджень у сфері інформаційних технологій
Харківського науково-дослідного
експертно-криміналістичного центру
Міністерства внутрішніх справ України

Захист національної безпеки визначається Конституцією України як найважливіша функція держави (стаття 17) [1]. В умовах воєнного стану інформаційна безпека стає однією з ключових складових національної безпеки. Ворог використовує кіберпростір для проведення інформаційних атак, дезінформації, пропаганди та інших деструктивних дій, спрямованих на дестабілізацію ситуації всередині країни. З огляду на це, захист інформаційних систем, даних та комунікаційних мереж стає пріоритетним завданням для держави та її громадян.

Ось кілька ключових аспектів та рекомендацій:

1) захист інформаційних систем та даних під час воєнного стану. Особливо важливо захищати критичну інфраструктуру, державні бази даних та комунікаційні мережі від кіберзагроз [2]. Це включає використання сучасних технологій шифрування, брандмауерів, антивірусного програмного забезпечення та інших засобів захисту. Також важливо забезпечити фізичну безпеку серверів та інших елементів інформаційної інфраструктури;

2) моніторинг та аналіз загроз. Постійний моніторинг кіберпростору дозволяє виявляти та запобігати потенційним атакам. Використання сучасних інструментів для аналізу загроз і виявлення аномалій допомагає своєчасно реагувати на інциденти та мінімізувати їхні наслідки. Моніторинг включає як автоматизовані системи, так і аналітичну роботу фахівців;