Львівський державний університет внутрішніх справ

Національна академія внутрішніх справ

Харківський національний університет внутрішніх справ

Одеський державний університет внутрішніх справ

Дніпровський державний університет внутрішніх справ

Рада молодих учених при Міністерстві освіти і науки України

Львівський державний університет безпеки життєдіяльності

Державний університет інфраструктури та технологій

Харківський національний університет радіоелектроніки

Ужгородський національний університет

Штучний інтелект у правовій практиці: межі та можливості

Збірник тез

круглого столу

14 березня 2025 року

Львів – Київ – Харків – Одеса – Дніпро – Ужгород

УДК 34:[004.8+004.3ꬑ.ꬍ](ꬓꬓ)

Рекомендовано до друку та поширення через мережу Інтернет
Вченою радою Львівського державного університету внутрішніх справ
(протокол № 14 від 25 березня 2025 року)

Упорядник:

О. О. Барабаш, *докторка юридичних наук, професорка,*
завідувачка науково-дослідної лабораторії актуальних проблем
правозастосовної та правоохоронної діяльності
ННІ права та правоохоронної діяльності ЛьвДУВС

ШТУЧНИЙ ІНТЕЛЕКТ У ПРАВОВІЙ ПРАКТИЦІ: МЕЖІ ТА МОЖЛИВОСТІ : збірник тез круглого столу (14 березня 2025 року) / упор. О. О. Барабаш. Львів : ЛьвДУВС, 2025. 238 с.

У збірнику вміщено тези доповідей учасників круглого столу «Штучний інтелект у правовій практиці: межі та можливості», який відбувся 14 березня 2025 року у Львівському державному університеті внутрішніх справ.

Опубліковано в авторській редакції. Відповідальність за достовірність фактів, статистичних даних, точність викладеного матеріалу покладається на авторів.

УДК 34:[004.8+004.383.8](063)

© Львівський державний університет
внутрішніх справ, 2025

ЗМІСТ

Швець Д. В.
ВСТУПНЕ СЛОВО 9

Дзюбинський В. В.
ВІТАЛЬНЕ СЛОВО 10

Тарасюк А. В.
ВІТАЛЬНЕ СЛОВО 11

Ващук О. П.
ВІТАЛЬНЕ СЛОВО 12

Андрєєв І. П.
НАУКОВИЙ ДИСКУРС ЩОДО РОЛІ ЗАХИСНИКА У КРИМІНАЛЬНОМУ ПРОЦЕСІ 13

Афтанасів В. М., Грабар Н. М.
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ЦИВІЛЬНОМУ СУДОЧИНСТВІ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ 15

Бакулін Д. О.
ПРАВОВЕ РЕГУЛЮВАННЯ ЗАСТОСУВАННЯ ВОГНЕПАЛЬНОЇ ЗБРОЇ ПРАЦІВНИКАМИ ПОЛІЦІЇ: ПРОБЛЕМИ ТА ВИКЛИКИ 18

Барабаш О. О.
АЛГОРИТМІЧНА СПРАВЕДЛИВІСТЬ У ПРАВООХОРОННИХ СИСТЕМАХ ТА ОБОРОННІЙ СФЕРІ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ 21

Басиста І. В.
КРАЙНІ ТЕНДЕНЦІЇ У РОЗВИТКУ ШІ ТА ЙОГО БЕЗПЕКИ 26

Биков І. О.
СТРАТЕГІЧНІ ОРІЄНТИРИ РОЗВИТКУ ЗАКОНОДАВСТВА УКРАЇНИ ЩОДО ВІРТУАЛЬНИХ АКТИВІВ 31

Біла Я., Сковронська І. Ю.
ПРОБЛЕМА ІНФОРМАЦІЙНОГО ПЕРЕВАНТАЖЕННЯ 33

Боровик А. В.
ЩОДО ПРАКТИКИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ 37

Борщенко В. В.
ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РОЗВИТКУ ПРОФЕСІЙНИХ КОМПЕТЕНТНОСТЕЙ МАЙБУТНІХ ПРАВНИКІВ У КУРСІ «ПРАВНИЧЕ ПИСЬМО» 38

Будік І. М.
ВИКОРИСТАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ У ПРОТИДІЇ ОРГАНІЗОВАНОМУ НАРКОБІЗНЕСУ 40

Варинський В. О.
РИЗИКИ ВИКОРИСТАННЯ ЕЛЕМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В РОЗРОБКАХ АВТОНОМНОЇ ЗБРОЇ: НА ШЛЯХУ ВИЗНАЧЕНЬ НОРМАТИВНИХ ОБМЕЖЕНЬ 42

Величко Д. В., Калугін В. Ю.
ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ
В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ 45

Верба О. Б.
ШТУЧНИЙ ІНТЕЛЕКТ І ЗАБЕЗПЕЧЕННЯ ПРАВ УЧАСНИКІВ ВИКОНАВЧОГО
ПРОВАДЖЕННЯ: ЕТИЧНІ ТА ПРАВОВІ АСПЕКТИ 48

Вергун В., Грабар Н. М.
ШТУЧНИЙ ІНТЕЛЕКТ У ЦИВІЛЬНОМУ СУДОЧИНСТВІ: ШЛЯХ ДО ІННОВАЦІЙ ЧИ
ЗАГРОЗА СПРАВЕДЛИВОСТІ? 50

Вергун І.
ЦИФРОВІ СЛІДИ ВІЙНИ: РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У РОЗСЛІДУВАННІ
ВОЄННИХ ЗЛОЧИНІВ 54

Висотенко Ю. В., Нестерова М. С.
СУЧАСНІ ПИТАННЯ АВТОРСЬКОГО ПРАВА В АСПЕКТІ ШТУЧНОГО ІНТЕЛЕКТУ ... 57

Висотенко Ю. В., Савченко Я. С.
ПРАВОВЕ РЕГУЛЮВАННЯ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ 60

Висотенко Ю. В., Сюйва Я. С.
ПЕРСПЕКТИВИ РОЗВИТКУ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ
ДЕРЖАВНИХ ПОСЛУГ 63

Висотенко Ю. В., Тимчишин П. А.
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ ПРОЗОРОСТІ
ПУБЛІЧНОЇ АДМІНІСТРАЦІЇ В УКРАЇНІ 65

Висотенко Ю. В., Хізанов О. Д.,
РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ
АНТИКОРУПЦІЙНОЇ ПОЛІТИКИ 68

Висотенко Ю. В., Яцур П. О.
ЦИФРОВІЗАЦІЯ ПУБЛІЧНОГО УПРАВЛІННЯ ЯК СПОСІБ ОПТИМІЗАЦІЇ
ПРОЦЕСУ НАДАННЯ АДМІНІСТРАТИВНИХ ПОСЛУГ 71

Вовк М. З.
ПРАВО ОСОБЛИВОГО РОДУ (SUI GENERIS) НА НЕОРИГІНАЛЬНІ ОБ'ЄКТИ,
ЗГЕНЕРОВАНІ КОМП'ЮТЕРНОЮ ПРОГРАМОЮ 73

Гловюк І. В.
ПОКЛИКАННЯ СТОРОНОЮ ПРОВАДЖЕННЯ НА РЕЗУЛЬТАТИ, ЗГЕНЕРОВАНІ
CHATGPT: ЧИ ЦЕ НЕПОВАГА ДО СУДУ? 76

Гонжак Б. І., Малюченко П. М., Рибальченко Є. В., Стаднік Є. О., Чемерис В. В., Войтович М. М., Мороховець Г. Ю.
АНАЛІЗ РЕКОМЕНДАЦІЙ ЩОДО ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В
ОСВІТНЬО-НАУКОВОМУ ПРОЦЕСІ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ 80

Деревянко Н. З.
ЩОДО МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ ПРАКТИКИ ВИКОРИСТАННЯ
ШТУЧНОГО ІНТЕЛЕКТУ ПОЛІЦЕЙСЬКИМИ ІСПАНІЇ В УКРАЇНІ 84

Джупіна Х. О., Пядишев В. Г.
ШТУЧНИЙ ІНТЕЛЕКТ У БОРОТЬБІ ЗІ ЗЛОЧИННІСТЮ (ЗАРУБІЖНИЙ ДОСВІД) 86

Добкіна К. Р.
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В МЕДІАЦІЇ 88

Дорош В. М., Лісова К. С.
ШТУЧНИЙ ІНТЕЛЕКТ У ДОКУМЕНТУВАННІ ТА АНАЛІЗІ ПОРУШЕНЬ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА 90

Дубняк М. В.
ЕЛЕКТРОННІ ПОСЛУГИ ТА ШТУЧНИЙ ІНТЕЛЕКТ 92

Дудіна О. В.
ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ В МЕДИЧНУ ОСВІТУ КИТАЮ ТА ЯПОНІЇ 95

Дуфенюк О. М.
ДЕБАТИ ПРО CHATGPT У ВЕРХОВНОМУ СУДІ 97

Жезло-Хлевна Н. В., Хлевной О. В.
МАШИННЕ НАВЧАННЯ В НОРМУВАННІ ВИМОГ ПОЖЕЖНОЇ БЕЗПЕКИ ДО ЕВАКУАЦІЙНИХ ШЛЯХІВ І ВИХОДІВ У ЗАКЛАДАХ СЕРЕДНЬОЇ ОСВІТИ 100

Жовнірчик Л. І.
ТЕХНОЛОГІЇ ШИФРУВАННЯ, БЛОКЧЕЙН ТА ШІ ДЛЯ ЗАХИСТУ БАЗ ДАНИХ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ 103

Жовнірчик Л. І.
КАСТОМІЗОВАНИЙ ПОМІЧНИК-АСИСТЕНТ ДЛЯ ВИКЛАДАННЯ ІНЖЕНЕРНИХ ДИСЦИПЛІН У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ 105

Жукова А. Р.
МОЖЛИВОСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОЦЕСІ ВИВЧЕННЯ ІНОЗЕМНИХ МОВ 106

Здебський Д. В.
ІНТЕГРАЦІЯ БАЗИ ДАНИХ ПОЛІГРАФОЛОГІЧНИХ ДОСЛІДЖЕНЬ У ЦИФРОВІ СИСТЕМИ УПРАВЛІННЯ ДОКАЗАМИ 110

Здреник І. В.,
ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА ПРАВА ЛЮДИНИ 113

Калаченкова К. О.
ШТУЧНИЙ ІНТЕЛЕКТ ТА ПРАВО НА ПРИВАТНІСТЬ 115

Ковальчук О. І., Саміло А. В. Демчина В. Р.
ВИКЛИКИ ДЛЯ КОНФІДЕНЦІЙНОСТІ ДАНИХ
В ЕПОХУ АЛГОРИТМІВ ШТУЧНОГО ІНТЕЛЕКТУ ТА КІБЕРЗАГРОЗ 118

Колич О. І.
ШТУЧНИЙ ІНТЕЛЕКТ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ:
ОКРЕМІ АСПЕКТИ ПРАВОВОГО РЕГУЛЮВАННЯ 120

Кононець В. П.
ІНФОРМАЦІЙНО-АНАЛІТИЧНА ПІДТРИМКА ПІДРОЗДІЛІВ
ЗБРОЙНИХ СИЛ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ 122

Кононець В. П., Ададуров А. В.
ПРОБЛЕМИ ПРИТЯГНЕННЯ ОСІБ ДО АДМІНІСТРАТИВНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ПОРУШЕННЯ ПРИЗОВНИКАМИ, ВІЙСЬКОВОЗОБОВ'ЯЗАНИМИ, РЕЗЕРВІСТАМИ ПРАВИЛ ВІЙСЬКОВОГО ОБЛІКУ ПІД ЧАС ДІЇ ВОЄННОГО СТАНУ В УКРАЇНІ 124

Кулик В. М., Калугін В. Ю.
ЗНАЧЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РОЗВИТКУ ВІДЕОАНАЛІТИКИ 128

Левенець А. В.
ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ
В ПРОЦЕДУРІ ДОБОРУ ТА ОЦІНЮВАННЯ КАНДИДАТА НА ПОСАДУ СУДДІ В
УКРАЇНІ 130

Литвин С. Й., Піхурець О. В.
СУБ'ЄКТ ВІДПОВІДАЛЬНОСТІ ЗА ШКОДУ, ЗАПОДІЯНУ ШТУЧНИМ ІНТЕЛЕКТОМ.... 133

Лукащук Ю. А., Цмоць У. О.
ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ОБРОБКИ ДАНИХ
У КОНТЕКСТІ СУЧАСНИХ ВОЄННИХ ДІЙ 137

Лук'янчук Ю. А., Земко А. М.
ЕТИЧНЕ ТА БЕЗПЕЧНЕ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ
В ДЕРЖАВНОМУ УПРАВЛІННІ: ПРИНЦИПИ, РЕКОМЕНДАЦІЇ, ПЕРСПЕКТИВИ..... 139

Ляшенко О. С., Ткачов В. М.
СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В СУДОВІЙ ПРАКТИЦІ З
ВИКОРИСТАННЯМ ФЕДЕРАТИВНОГО НАВЧАННЯ 142

Манжай О. В.
ШТУЧНИЙ ІНТЕЛЕКТ ТА КІБЕРБЕЗПЕКА: ЄВРОПЕЙСЬКИЙ ВИМІР 146

Мельник Я. Я.
ШТУЧНИЙ ІНТЕЛЕКТ ЯК ПРОДУКТ ПРАВОВОЇ РЕАЛЬНОСТІ 149

Михайлицька К. С., Чукаєва А. В.
ШТУЧНИЙ ІНТЕЛЕКТ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: МОЖЛИВОСТІ ТА
ЗАГРОЗИ 152

Мовчан А. В.
ПРОБЛЕМИ ПРОТИДІЇ РОЗПОВСЮДЖЕННЮ МАТЕРІАЛІВ СЕКСУАЛЬНОГО
НАСИЛЬСТВА НАД ДІТЬМИ, СТВОРЕНИХ ЗА ДОПОМОГОЮ ШТУЧНОГО
ІНТЕЛЕКТУ 155

Монастирський М. В.
ПОДОЛАННЯ ПЕРЕШКОДИ У ВИЗНАЧЕННІ ПОНЯТТЯ ШТУЧНОГО ІНТЕЛЕКТУ.... 158

Остіян Є. З., Пішта В. І.
КОНЦЕПЦІЯ PRIVACY BY DESIGN У КОНТЕКСТІ ШТУЧНОГО ІНТЕЛЕКТУ ТА
ТРАНСКОРДОННОГО ОБМІНУ ДАНИХ 160

Пасевич М. О.
ШТУЧНИЙ ІНТЕЛЕКТ У НАВЧАННІ: ПОМІЧНИК ЧИ ЗАМІНА ВИКЛАДАЧА? 163

Письменний О.
ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ЦИФРОВОМУ ПРОСТОРІ
В УМОВАХ ВОЄННОГО СТАНУ 166

Повалена М. В.
ШТУЧНИЙ ІНТЕЛЕКТ ТА ЕЛЕКТРОННЕ УРЯДУВАННЯ 170

Попович М. Д.
ШТУЧНИЙ ІНТЕЛЕКТ В ПУБЛІЧНОМУ УПРАВЛІННІ..... 172

Пядишев В. Г., Пирлик М. В.
ШТУЧНИЙ ІНТЕЛЕКТ ТА ЗЛОЧИННІСТЬ (ЗАРУБІЖНИЙ ДОСВІД) 174

П'ятецька С. О., Чукаєва А. В.
ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ВІЙНИ:
МОЖЛИВОСТІ ТА РИЗИКИ 176

Савайда О. І.
ОСНОВНІ ЗАСАДИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ
В ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ 179

Скрипник С. С.
ТЕХНІЧНІ ОБМЕЖЕННЯ У ВИКОРИСТАННІ ШТУЧНОГО ІНТЕЛЕКТУ
В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ 182

Сліпенюк В. В.
ПРИНЦИПИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ
ПІД ЧАС ЗДІЙСНЕННЯ СУДОЧИНСТВА 184

Стефанишин Н. М.
ШТУЧНИЙ ІНТЕЛЕКТ ЯК ОБ'ЄКТ АВТОРСЬКОГО ПРАВА 186

Тарасюк А. В.,
ШТУЧНИЙ ІНТЕЛЕКТ В ПРОТИДІЇ ТА РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ:
ДІЯЛЬНІСТЬ ДЕРЖАВНОГО БЮРО РОЗСЛІДУВАНЬ 190

Тарасюк С. М.
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ:
ПРАКТИЧНІ АСПЕКТИ ТА ПЕРСПЕКТИВИ 193

Терлецький А. В.
ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ВІЙНИ:
МОЖЛИВОСТІ ТА РИЗИКИ 196

Тополевський Р. Б.
ФІЛОСОФСЬКО-ПРАВОВІ ЗАСАДИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ:
ОСОБЛИВОСТІ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ 199

Троцький О. О.
ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ ОБОРОННИХ ЗАКУПІВЕЛЬ
В УМОВАХ ВІЙНИ: МОЖЛИВОСТІ ТА РИЗИКИ 202

Удовенко Ж. В., Галаган В. І.,
ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ, ЯКІ ОБРОБЛЯЮТЬСЯ
СИСТЕМАМИ ШТУЧНОГО ІНТЕЛЕКТУ: ОКРЕМІ АСПЕКТИ 204

Хілобок Д. Р., Жуковський С. В.
КОНФІДЕНЦІЙНІСТЬ ТА ПРИВАТНІСТЬ В СУЧАСНОМУ КІБЕРПРОСТОРІ 209

Цигульський С. М.
ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ПОНЯТТЯ ШТУЧНОГО ІНТЕЛЕКТУ 211

Цимбал Б. М., Свіржевський П. В.
ДОСЛІДЖЕННЯ ЕРГОНОМІЧНИХ РИЗИКІВ САПЕРІВ
ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ 214

Цицик О. І.
ОСНОВНІ ЗАСАДИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ
В ДІЯЛЬНОСТІ ТА ФУНКЦІОНУВАННІ ТЕРИТОРІАЛЬНОЇ ГРОМАДИ 217

Цуркан І. О., Манжай О. В.
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ 219

Шаповалова К. І.
ШТУЧНИЙ ІНТЕЛЕКТ ЯК ЕЛЕМЕНТ АДМІНІСТРАТИВНОГО КОНТРОЛЮ: НОВІТНІ МЕХАНІЗМИ ДОТРИМАННЯ ПРАВ ЛЮДИНИ В ПОЛІЦІЇ 223

Шевчук В. М.
ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ 226

Шипіло Д.
АДМІНІСТРАТИВНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ПОРЯДКУ ПЕРЕМІЩЕННЯ ТОВАРІВ В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ 229

Юрчук О. В.
ЕТИЧНІ ТА ПРАВОВІ АСПЕКТИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В МЕДИЦИНІ 232

Яковенко Ю. В.
ШТУЧНИЙ ІНТЕЛЕКТ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: ПЕРСПЕКТИВИ АВТОМАТИЗАЦІЇ В КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ 235

Вступне слово!

Шановні учасники круглого столу, дорогі колеги,
науковці та молоді вчені!

Сучасний світ зазнає неабияких технологічних змін, які впливають на всі сфери життя, зокрема й на правову. Штучний інтелект уже сьогодні змінює підходи до правозастосування, судочинства, державного управління, і перед нами постає важливе завдання – визначити його межі, можливості та правові наслідки.

Організація цього заходу Радою молодих вчених ЛьвДУВС з Радою молодих учених при Міністерстві освіти і науки України, а також провідними вітчизняними закладами вищої освіти є свідченням того, що наше академічне середовище активно реагує на виклики часу та шукає шляхи гармонійного поєднання новітніх технологій з правовими нормами.

Технологічний прогрес не стоїть на місці. У сучасному світі штучний інтелект використовується у правовій аналітиці, підготовці юридичних документів, судовому прогнозуванні, оцінці ризиків, криміналістиці, а також у правоохоронній діяльності. Впровадження таких технологій змінює професійну діяльність юристів, суддів, адвокатів, прокурорів і правоохоронців. Ми маємо не лише розуміти ці зміни, а й напрацьовувати ефективні механізми їх правового регулювання. Важливо зважати на передові світові практики і тенденції використання штучного інтелекту у правоохоронній сфері, насамперед у розслідуваннях та документуванні воєнних злочинів. Безумовно, інновації мають слугувати нам у відстоюванні справедливості й захисті демократичних цінностей.

Я переконаний, що наша зустріч стане важливим кроком у формуванні правових підходів до регулювання штучного інтелекту в Україні.

Дякую всім, хто сьогодні з нами, за вашу ініціативність, прагнення до наукових досліджень та відповідальність перед майбутнім нашої правової системи. Бажаю всім продуктивної дискусії та конструктивної роботи!

Д. В. Швець,
ректор Львівського державного університету
внутрішніх справ, доктор юридичних наук,
професор, заслужений працівник освіти України,
полковник поліції

Вітальне слово!

Шановний пане ректоре, учасники круглого столу,
колеги, науковці та правники!

Сьогодні ми зібралися для обговорення однієї з найбільш актуальних і важливих тем сучасної правозастосовної практики – використання штучного інтелекту у сфері права. Це питання вже зараз формує нові підходи до боротьби зі злочинністю, правосуддя, аналітики правопорушень та превентивних заходів.

Для карного розшуку, як одного з ключових підрозділів Національної поліції України, застосування сучасних технологій має особливе значення. Оперативно-розшукова діяльність, боротьба з організованою злочинністю, розкриття тяжких і особливо тяжких злочинів потребують не лише професіоналізму, досвіду та аналітичних здібностей оперативників, але й сучасних цифрових інструментів.

Вже сьогодні штучний інтелект допомагає виявляти кримінальні закономірності, аналізувати значні масиви даних, прогнозувати злочинність і навіть ідентифікувати правопорушників за допомогою систем відеоспостереження та біометричних технологій. Окрім того, алгоритми аналізу великих даних можуть допомагати у виявленні фінансових злочинів чи шахрайських схем або відстеженні нелегальних мереж.

Проте разом із цими можливостями постає низка важливих викликів. Використання штучного інтелекту в правоохоронній діяльності вимагає чітких правових обмежень, контролю за обробкою персональних даних та запобігання зловживанням. Коли ми говоримо про цифрові технології, ми не можемо ігнорувати питання права на приватність, етичних аспектів ухвалення рішень алгоритмами та відповідальності за помилки штучного інтелекту. Саме тому роль наукової спільноти та правників у цих питаннях є надзвичайно важливою. Необхідно не просто інтегрувати інновації в роботу правоохоронних органів, а створити надійні юридичні механізми, які регулюватимуть використання штучного інтелекту без загрози порушення прав громадян.

Переконаний, що нинішній круглий стіл стане майданчиком для обміну думками між науковцями та практиками, надасть можливості окреслити перспективи розвитку штучного інтелекту в різних сферах правозастосування.

Щиро дякую Львівському державному університету внутрішніх справ за організацію цього важливого заходу. Бажаю всім учасникам плідної роботи, цікавих дискусій та нових відкриттів!

В. В. Дзюбинський,
начальник Департаменту карного розшуку
Національної поліції України,
генерал поліції третього рангу

Вітальне слово!

Шановні колеги, науковці, представники юридичної спільноти!

Вітаю вас від імені Головного слідчого управління Державного бюро розслідувань та від себе особисто з нагоди проведення цього важливого круглого столу ***«Штучний інтелект у правовій практиці: межі та можливості»***, присвяченого одній із найактуальніших тем сучасної юридичної науки – застосуванню штучного інтелекту у правовій практиці.

Рада молодих вчених Львівського державного університету внутрішніх справ разом із провідними закладами вищої освіти України вкотре демонструє свою здатність об'єднувати науковий потенціал для вирішення найскладніших викликів. Сьогодні ми зібралися для обговорення питань, які вже зараз формують майбутнє правової системи – від використання алгоритмів у кримінальному судочинстві до етичних і правових меж впровадження технологій штучного інтелекту.

Ми живемо у час стрімкої цифрової трансформації, коли штучний інтелект стає не лише інструментом аналітики та оптимізації, а й викликом для традиційних правових інститутів. У юридичній сфері технологічний прогрес має не лише полегшувати роботу фахівців, а й відповідати основним принципам правосуддя – законності, справедливості та рівності.

Державне бюро розслідувань, як правоохоронний орган, також приділяє значну увагу питанням упровадження технологій у слідчу та аналітичну діяльність. Використання великих масивів даних, автоматизованих систем аналізу та цифрових доказів стає новим стандартом у боротьбі зі злочинністю. Водночас ми чітко усвідомлюємо, що штучний інтелект не може і не повинен підміняти ані людський розум, ані моральні цінності, ані правові орієнтири.

Переконаний, що нинішня дискусія сприятиме глибшому розумінню меж і можливостей штучного інтелекту в правозастосуванні, допоможе знайти баланс між технологічним розвитком і захистом прав людини. Бажаю всім учасникам плідної роботи, цікавих наукових відкриттів та конструктивної співпраці!

Дякую за увагу!

А. В. Тарасюк,
заступник керівника Управління Головного слідчого
управління Державного бюро розслідувань,
доктор юридичних наук, професор,
полковник Державного бюро розслідувань

Вітальне слово!

Шановні колеги!

Від імені Ради молодих учених при Міністерстві освіти і науки України щиро вітаю всіх учасників круглого столу «Штучний інтелект у правовій практиці: межі та можливості»!

РМУ при МОН є співорганізатором цього важливого наукового заходу, і ми раді, що він об'єднав науковців, правників, представників державних установ та всіх, хто зацікавлений у впровадженні інноваційних технологій у правову сферу.

Сучасні реалії диктують нові виклики. Штучний інтелект вже не просто майбутнє – це наша реальність, і його вплив на юриспруденцію, економіку, освіту, правоохоронну діяльність і безпеку зростає з кожним днем. Проте досить лише говорити про штучний інтелект – настав час діяти! Нам потрібно не лише аналізувати світовий досвід, обговорювати можливості і ризики, а й розробляти власні рішення, створювати українські алгоритми та впроваджувати їх у всі ключові сфери.

Особливо в умовах російсько-української війни українські вчені повинні ставати ще більш ефективними, тримати свій науковий фронт і робити максимум у своїй сфері. Ми маємо розуміти, що наука – це також зброя, а технологічна перевага є ключовою для безпеки та розвитку держави. Від наших зусиль залежить, якою буде Україна завтра – сильною, високотехнологічною та конкурентоспроможною.

Дякую організаторам, зокрема Львівському державному університету внутрішніх справ, а також усім співорганізаторам за створення цієї платформи для важливої дискусії. Сподіваюся, що сьогоднішній діалог стане початком нових проєктів, які виведуть Україну на передові позиції у сфері правових технологій.

Бажаю всім учасникам продуктивних обговорень, цікавих ідей та успішних ініціатив!

Олеся Ващук,
голова Ради молодих учених
при Міністерстві освіти і науки України,
докторка юридичних наук, професорка

Андрєєв І. П.,
аспірант кафедри кримінально-правових дисциплін
Інституту права та безпеки, адвокат
(Одеський державний університет внутрішніх справ)

НАУКОВИЙ ДИСКУРС ЩОДО РОЛІ ЗАХИСНИКА У КРИМІНАЛЬНОМУ ПРОЦЕСІ

Ефективний захист у кримінальному процесі є основою правової держави та міжнародних стандартів справедливого судочинства. Захисник виконує ключову роль у доказовій діяльності, займаючись збором, аналізом та поданням доказів. Однак зміни у кримінальному процесуальному законодавстві, судовій практиці та цифровізації правосуддя вимагають переосмислення його функцій. Наукові дискусії тривають щодо меж повноважень адвоката у доказуванні, його взаємодії зі стороною обвинувачення та судом, а також тактики захисту під час допитів і оцінки доказів. Важливим є дослідження сучасних підходів до доказової діяльності захисника, аналіз його ролі в змагальному процесі та адаптація міжнародних стандартів до кримінального процесу України. З огляду на розвиток цифрових технологій, особливого значення набуває використання адвокатом електронних інструментів для аналізу доказів, формування правової позиції та представництва інтересів підзахисного в суді.

Теоретичні засади наукових досліджень щодо участі адвоката в кримінальному процесі охоплюють питання його правового статусу в межах кримінального провадження, механізми реалізації правового захисту учасників процесу, а також аналіз процесуальних аспектів діяльності адвоката на стадіях досудового розслідування та судового розгляду [1, с. 210]. З огляду на це, основним завданням даного розділу дисертації є проведення комплексного теоретико-практичного аналізу юридичної природи інституту захисту в кримінальному процесі. Важливе значення має також дослідження сучасних теоретичних напрацювань щодо повноважень захисника та меж його процесуальних можливостей у кримінальному провадженні. Оскільки наукові розвідки у цій сфері базуються на теоретичних концепціях, вони водночас потребують врахування практичних аспектів та нормативно-правового регулювання, зокрема кримінального процесуального законодавства України.

І. М. Зубач визначає захист у кримінальному процесі як комплексну діяльність, що розглядається у двох аспектах: перший – це активні дії сторони захисту (підозрюваного, обвинуваченого та їхнього адвоката), спрямовані на спростування обвинувачення та відстоювання законних прав; другий – діяльність спеціально уповноважених органів та інших учасників процесу, які забезпечують реалізацію правових гарантій для всіх сторін кримінального провадження [2, с. 181]. Поділяючи цю точку зору, можна стверджувати, що такий підхід відображає актуальні вимоги кримінального судочинства та дозволяє окреслити функціональну взаємодію між різними учасниками

процесу, спрямовану на забезпечення правосуддя та дотримання принципу рівності сторін.

У своїй монографії «Захист у кримінальній справі» Я. П. Зейкан досліджує роль адвоката в кримінальному процесі, зокрема в аспектах тактичної роботи під час допиту свідків і потерпілих, а також у стадіях судового розгляду, апеляції та касаційного оскарження [3]. Монографія є важливим джерелом теоретичних і практичних знань про діяльність адвоката-захисника, детально розглядаючи тактичні прийоми, які можуть бути використані під час змагального судового процесу. Автор аналізує методи ведення допитів, наголошуючи на необхідності високого рівня професійної підготовки адвоката та його тактичної гнучкості. Крім того, у монографії висвітлюються особливості захисту на різних процесуальних стадіях, акцентуючи увагу на стратегічному плануванні адвокатської діяльності та важливості аргументованого представлення позиції клієнта.

Окрему увагу взаємодії адвоката із судом, прокурорами та слідчими приділяє І. Ю. Гловацький у своїй монографії «Діяльність адвоката-захисника у кримінальному процесі». Він наголошує на важливості ефективної комунікації адвоката з усіма учасниками процесу та розглядає особливості використання адвокатами сучасних технологій у збиранні доказів і представленні правової позиції [4]. Особлива увага приділяється питанням професійної етики, комунікативних навичок адвоката та ролі інформаційних технологій у підготовці матеріалів для судового розгляду.

Поглиблений аналіз процесу доказування та аргументації в діяльності захисника представлений у працях В. О. Попелюшка. Зокрема, у своїх дослідженнях «Предмет захисту та його доказування в кримінальній справі» [5] і «Функція захисту в кримінальному судочинстві України: правові, теоретичні та прикладні проблеми» [6] він досліджує основні методи збору, оцінки та використання доказової бази захисту. Автор аналізує різні тактичні прийоми адвоката у судовому процесі, визначаючи їх ефективність у спростуванні обвинувачення. Важливе місце в його дослідженнях посідають питання адвокатської аргументації, а також механізми формування правової позиції захисту. Суттєвий внесок у вивчення проблем адвокатської діяльності вносить також Т. В. Корчева, яка аналізує особливості роботи адвоката на різних стадіях кримінального провадження, зокрема під час досудового слідства та судового розгляду [7]. Таким чином, сучасні наукові дослідження підкреслюють важливість ролі адвоката в кримінальному процесі, наголошуючи на необхідності розвитку нових тактичних підходів, удосконалення доказових механізмів та впровадження міжнародних стандартів правосуддя в національну практику.

Список використаних джерел:

1. Слінько С. В. Межі участі захисника у кримінальному процесі. *Форум права*. 2017. № 3. С. 210–214. URL: http://nbuv.gov.ua/jpdf/FP_index.htm_2017_3_37.pdf.

2. Зубач І. М. Функція захисту у сучасному кримінальному провадженні України. URL: http://science.lp.edu.ua/sites/default/files/Papers/zubach.pdf.

3. Зейкан Я. П. Право на захист в кримінальному процесі: практ. посіб. Київ: Юрид. практ., 2004. 288 с.
4. Гловацький І. Ю. Діяльність адвоката-захисника у кримінальному процесі : навч. посіб. Київ : Атіка, 2003. 352 с.
5. Попелюшко В. О. Предмет захисту та його доказування в кримінальній справі : монографія. Київ : Прецедент, 2005. 232 с.
6. Попелюшко В. О. Функція захисту в кримінальному судочинстві України: правові, теоретичні та прикладні проблеми : монографія. Острог : Нац. ун-т «Острозька академія», 2009. 634 с.
7. Корчева Т. В. Проблеми діяльності захисника в досудовому провадженні та в суді першої інстанції : дис. ... канд. юрид. Наук : 12.00.09. Харків, 2006. 208 с.

Афтанасів В. М.,
здобувачка вищої освіти 3 курсу
ННІ права та правоохоронної діяльності
(Львівський державний університет внутрішніх справ)
Грабар Н. М.,
доцент кафедри цивільно-правових дисциплін,
кандидат юридичних наук, доцент
(Львівський державний університет внутрішніх справ)

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ЦИВІЛЬНОМУ СУДОЧИНСТВІ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Сучасне суспільство стоїть на порозі епохальних змін завдяки стрімкому розвитку штучного інтелекту (далі – ШІ). Такі зміни, безумовно, торкнуться і сфери цивільного судочинства, відкриваючи нові можливості, але водночас ставлячи перед нами значні виклики. Впровадження ШІ у судову систему може докорінно змінити процес розгляду цивільних справ, покращуючи його ефективність та забезпечуючи прозорість судового розгляду. ШІ може стати інструментом, що змінить традиційні підходи до правосуддя, забезпечуючи нові способи збору та аналізу доказів, автоматизацію звичних процесів та прогнозування результатів судових спорів. Проте разом з новими можливостями з’являються і нові виклики, які потребують ретельного дослідження та правового регулювання.

У національному законодавстві України вже існують правові засади, що визначають основні принципи судочинства, які мають бути враховані при впровадженні ШІ. Зокрема, Конституція України від 28.06.1996 № 254к/96-ВР в ст. 129 закріплює, що правосуддя здійснюється на засадах верховенства права, рівності всіх учасників процесу перед законом і судом, гласності судового процесу та забезпечення права на апеляційний перегляд справи [1]. Зазначені принципи мають бути враховані під час розробки та впровадження алгоритмів ШІ, що використовуються у судочинстві. Своєю чергою, ст. 2 Закону України «Про судоустрій і статус суддів» від 02.06.2016 № 1402-VIII визначає, що «суд, здійснюючи правосуддя на засадах *верховенства права*, забезпечує кожному

право на *справедливий суд* та повагу до інших прав і свобод, гарантованих Конституцією і законами України, а також міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України (курсив наш. – Авт.)» [2]. Використання ШІ має сприяти реалізації цих принципів, а не суперечити їм.

Доречно підкреслити, що впровадження ШІ у сферу цивільного судочинства відкриває широкі можливості для покращення правової системи. Наприклад, алгоритми ШІ можуть використовуватися для автоматизованого аналізу правових документів, що дозволить значно скоротити час підготовки до судових розглядів та знизити навантаження на суддів. Також ШІ може бути корисним для прогнозування результатів судових процесів на основі аналізу попередніх рішень, що, своєю чергою, допоможе суддям приймати більш обґрунтовані рішення. Однак, використання таких технологій потребує врегулювання етичних питань, зокрема щодо можливого упередженого ставлення алгоритмів та їх впливу на справедливість судового процесу.

Особливого значення питання впровадження ШІ у цивільне судочинство набуває в умовах російсько-української війни, яка триває з 2014 року на теренах нашої Держави. Війна спричинила значні зміни в суспільстві та правовій системі України, зокрема у сфері правосуддя. У зв'язку з військовими діями та міграцією населення виникають нові виклики для забезпечення доступу до правосуддя та його ефективності. У такому разі використання ШІ може стати важливим інструментом для вирішення цих проблем, зокрема шляхом автоматизації процесів, які дозволять забезпечити своєчасний розгляд справ у складних умовах збройного конфлікту.

Варто наголосити, що захист прав учасників процесу в умовах застосування ШІ також потребує ретельного дослідження. Адже важливо забезпечити, щоб використання ШІ не призводило до порушення прав сторін, а навпаки – сприяло їх захисту. Наприклад, механізми автоматизованого визначення строків розгляду справ, їх обробки та прийняття рішень можуть сприяти скороченню строків судочинства та підвищенню його ефективності. Проте, необхідно забезпечити, щоб ці процеси відповідали принципам верховенства права, справедливості, законності тощо, передбаченим ст. 2 Цивільного процесуального кодексу України від 18.03.2004 № 1618-IV [3].

Міжнародний досвід впровадження штучного інтелекту в судову систему демонструє значний потенціал цих технологій для підвищення ефективності та прозорості правосуддя. Наприклад, у Сполучених Штатах Америки вже активно використовуються алгоритми ШІ для аналізу правових документів та допомоги у прийнятті рішень у деяких судах [4]. У Китаї впровадження ШІ у судову систему дозволило створити «розумні суди», де технології ШІ допомагають автоматизувати процеси, аналізувати докази та забезпечувати швидкий і ефективний розгляд справ. У той же час у Великобританії лорд-суддя Апеляційного суду склав постанову за допомогою ChatGPT. Він попросив ChatGPT написати абзац для судових документів у справі зі сфери інтелектуальної власності. Суддя назвав ChatGPT «дуже корисним» і додав, що програми ШІ мають «великий потенціал». Що важливо, суддя одразу зазначив:

він бере всю відповідальність на себе. Це перший відомий випадок, коли британський суддя використав ШІ чат-бот для складання судових документів [5]. Європейський Союз також не відстає у цьому напрямку, зокрема в Естонії розроблено систему автоматизованого розгляду судових справ, яка допомагає знизити навантаження на суддів та прискорити процес прийняття рішень [6, с. 501]. З огляду на зазначене, можемо дійти висновку, що впровадження ШІ у судову систему може суттєво покращити якість та швидкість правосуддя, але водночас вимагає ретельного правового регулювання та етичних рамок для забезпечення справедливості та дотримання прав учасників процесу.

Особливу увагу слід приділити інтеграції алгоритмів ШІ у процес автоматизованого визначення факту порушення цивільно-правових обов'язків та встановлення відповідальності. Цей аспект передбачає використання ШІ для аналізу правових документів і доказів, що, з одного боку, забезпечить об'єктивність та неупередженість прийняття рішень, а з іншого – мінімізує вплив людського фактора та знижує ймовірність помилок.

Водночас використання ШІ для вирішення питань цивільно-правової відповідальності викликає питання щодо правової відповідальності за можливі помилки алгоритмів. З одного боку, це стосується відповідальності розробників і користувачів ШІ за недоліки і неточності в роботі алгоритмів. З іншого боку, необхідно забезпечити можливість перевірки і оскарження автоматизованих рішень, що є важливою складовою правового захисту учасників процесу. У цьому контексті важливо враховувати міжнародний досвід використання ШІ у сфері цивільно-правової відповідальності, зокрема приклади США, Китаю та Європейського Союзу, де вже впроваджені системи автоматизованого аналізу правових документів та прийняття рішень.

На нашу думку, дослідження впливу ШІ на цивільне судочинство є нагальною потребою сучасного суспільства, оскільки зазначене дозволить не лише оцінити переваги та ризики впровадження ШІ, але й розробити рекомендації щодо правового регулювання, яке забезпечить справедливість, ефективність і прозорість судового процесу. Технологічний прогрес не має бути загрозою для правосуддя, а навпаки – слугувати інструментом для його вдосконалення.

Підсумовуючи вищевикладене, можна констатувати, що впровадження ШІ у цивільне судочинство відкриває нові горизонти для покращення правової системи, але водночас ставить перед нами значні виклики. Важливо забезпечити, щоб такі технології відповідали принципам справедливості, забезпечували захист прав учасників процесу та сприяли ефективності судочинства.

Список використаних джерел:

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 01.03.2025).

2. Про судоустрій і статус суддів : Закон України від 02.06.2016 № 1402-VIII. URL: https://zakon.rada.gov.ua/laws/show/1402-19#Text (дата звернення: 01.03.2025).

3. Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text (дата звернення: 01.03.2025).

4. У США опублікували рекомендації щодо використання ШІ державними та федеральними судами. 01.03.2025. URL: https://sud.ua/uk/news/abroad/324514-v-ssha-opublikovali-rekomendatsii-po-ispolzovaniyu-ii-gosudarstvennymi-i-federalnymi-sudami.

5. Петрів О. Роль штучного інтелекту в модернізації судової системи: інструменти для суддів. 28.02.2024. URL: https://cedem.org.ua/consultations/shtuchnyi-intelekt-sud/.

6. Малоземова О. В., Мхитарян А. С., Дроздов О. М. Дослідження стану та перспектив використання ШІ у сфері правосуддя. *Юридичний науковий електронний журнал.* 2024. № 5. С. 496–502.

Бакулін Д. О.,
аспірант кафедри адміністративно-правових дисциплін
Інституту права та безпеки, адвокат
(Одеський державний університет внутрішніх справ)

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАСТОСУВАННЯ ВОГНЕПАЛЬНОЇ ЗБРОЇ ПРАЦІВНИКАМИ ПОЛІЦІЇ: ПРОБЛЕМИ ТА ВИКЛИКИ

Забезпечення громадського порядку та безпеки є одним із ключових завдань Національної поліції України. Важливим аспектом діяльності правоохоронних органів є застосування фізичної сили, спеціальних засобів і вогнепальної зброї, що потребує чіткої правової регламентації. Відсутність належного нормативного врегулювання може спричинити як зловживання з боку поліцейських, так і порушення прав громадян, включаючи право на життя та особисту недоторканність. Тому питання правового регулювання використання вогнепальної зброї набуває особливої актуальності в умовах реформування правоохоронної системи та імплементації міжнародних стандартів у сфері захисту прав людини.

Історично підходи до застосування сили правоохоронцями в Україні пройшли еволюцію – від жорстких імперативних норм радянського періоду до сучасних стандартів, що базуються на принципах пропорційності, необхідності та мінімізації шкоди. Водночас, попри наявність нормативно-правових актів, що регулюють використання вогнепальної зброї в Україні, практика правозастосування демонструє низку проблем. Серед них – нечіткість законодавчих формулювань, відсутність належних процедур контролю та неоднозначність судової практики щодо випадків застосування зброї працівниками поліції.

Одним із основних викликів є недостатньо деталізоване визначення підстав і меж застосування вогнепальної зброї, що може спричиняти різночитання норм як поліцейськими, так і судовими органами. Це, у свою чергу, створює правову невизначеність та потенційні ризики як для громадян, які можуть постраждати від непропорційного застосування сили, так і для

самих правоохоронців, які змушені приймати миттєві рішення в екстремальних умовах.

Недосконаліть механізмів оцінки правомірності застосування зброї, а також недостатній рівень контролю та відповідальності за неправомірні дії створюють загрозу свавілля або надмірної обережності з боку правоохоронців. У результаті, поліцейські можуть утримуватися від використання вогнепальної зброї навіть у ситуаціях, коли це є необхідним для захисту громадян або самозахисту, що може призводити до підвищення рівня злочинності та послаблення правопорядку.

Крім того, міжнародна інтеграція України вимагає гармонізації національного законодавства з міжнародними стандартами, зокрема рекомендаціями ООН, Ради Європи та Європейського Союзу щодо використання сили правоохоронними органами. Як свідчить практика Європейського суду з прав людини, держави повинні запроваджувати ефективні механізми контролю за використанням вогнепальної зброї, забезпечувати прозорі розслідування випадків її застосування та гарантувати високий рівень підготовки поліцейських.

На думку І. С. Загоруй, складність у розумінні прав людини обумовлена їх багатовимірною трактовкою в різних суспільних сферах, що ускладнює правозастосовну діяльність [1, с. 67]. Конституція України закріплює право на життя як найвищу соціальну цінність, зобов'язуючи державу гарантувати його захист [2]. Як зазначає О. Святоцький, забезпечення прав людини передбачає вдосконалення національного законодавства відповідно до міжнародних стандартів та ефективну реалізацію прав громадян [3, с. 27].

Ратифікація Конвенції про захист прав людини і основоположних свобод дозволила громадянам України звертатися до ЄСПЛ у випадках порушень їхніх прав. Однак статистика свідчить про системні проблеми у сфері правоохоронної діяльності: у 2006 році ЄСПЛ ухвалив 120 рішень за скаргами проти України, у 119 з яких було виявлено порушення Конвенції [4, с. 129]. Основні проблеми стосувалися порушень під час розслідувань випадків загибелі осіб унаслідок застосування сили правоохоронцями, а також відсутності ефективних механізмів запобігання зловживанням.

Попри проведені реформи, проблема залишається актуальною. У 2019 році кількість поданих заяв до ЄСПЛ проти України сягнула 3991, у 109 ухвалених рішеннях було встановлено порушення прав людини [5]. Це свідчить про необхідність подальшої модернізації правоохоронної системи та вдосконалення механізмів реалізації прав громадян у сфері безпеки.

Як зазначає О. В. Барановський, недостатня політична підтримка, обмежене фінансування та недосконале законодавче забезпечення значно ускладнюють реформування правоохоронної сфери, що потребує комплексного підходу [6, с. 5–6]. Водночас Є. І. Бородін наголошує, що ключовим завданням державного управління є забезпечення верховенства права та ефективна взаємодія з громадянським суспільством [7, с. 93].

Правове регулювання застосування вогнепальної зброї працівниками поліції є складним і багатогранним питанням, яке потребує подальшого вдосконалення. Серед основних напрямів удосконалення цього механізму слід виділити: чітке визначення підстав для застосування зброї у законодавстві, що дозволить уникнути різночитань та правової невизначеності; впровадження ефективних механізмів контролю за правомірністю використання вогнепальної зброї, включаючи незалежні розслідування та систему підзвітності; гармонізацію національного законодавства з міжнародними стандартами, зокрема щодо пропорційності та необхідності застосування сили; підвищення рівня підготовки поліцейських, включаючи навчання щодо мінімізації шкоди при використанні вогнепальної зброї; розширення застосування технологій контролю, зокрема натільних камер, що сприятиме прозорості дій правоохоронців. Отже, подальша імплементація європейських стандартів у сфері використання вогнепальної зброї працівниками поліції дозволить підвищити рівень громадської безпеки, забезпечити дотримання прав людини та зміцнити довіру суспільства до правоохоронної системи.

Список використаних джерел:

1. Загоруй І. С. Поняття «Права людини»: теоретико-правові підходи до розуміння прав людини. *Вісник Луганського університету внутрішніх справ імені Е. О. Дідоренка*. 2016. № 2. С. 66–82.
2. Конституція України від 28 червня 1996 року № 254к/96-ВР. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.
3. Васильченко О. П. Конституційно-правовий механізм забезпечення принципу рівності прав і свобод людини та громадянина в Україні. *Адміністративне право і процес*. 2015. № 1 (11). С. 26–33.
4. Водотика С. Г. Муніципальна міліція: історичний досвід та проблеми функціонування в Україні. *Культура народов Причерноморья.* 2006. № 85. С. 128–131.
5. Україна та Європейський суд з прав людини. URL: http://coe.mfa.gov.ua (дата звернення: 20.05.2024).
6. Барановський О. В. Історико-правовий аналіз становлення та розвитку системи управління та організаційно-штатного забезпечення діяльності міліції незалежної України. *Прикарпатський юридичний вісник.* 2017. Вип. 6 (21), т. 1. С. 3–10.
7. Гуманізація державної служби. Енциклопедія державного управління: у 8 т. / Нац. акад. держ. упр. при Президентові України ; наук.-ред. Колегія : Ю. В. Ковбасюк (голова), В. М. Сороко (співголова) та ін. Київ : НАДУ, 2011. Т. 6 :Державна служба. С. 93–94.

Барабаш О. О.,
завідувачка науково-дослідної лабораторії актуальних
проблем правозастосовної та правоохоронної
діяльності ННІ права та правоохоронної діяльності,
Голова Ради молодих вчених,
докторка юридичних наук, професорка
(Львівський державний університет внутрішніх справ)

АЛГОРИТМІЧНА СПРАВЕДЛИВІСТЬ У ПРАВООХОРОННИХ СИСТЕМАХ ТА ОБОРОННІЙ СФЕРІ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Сучасні дослідники дедалі більше переконані, що під впливом досягнень науково-технічного прогресу й подальшої цифровізації суспільства люди крок за кроком переміщуються зі звичного, матеріального світу до цифрового простору [1]. На сьогодні вже є досвід використання роботів у процесі підготовки різноманітних юридичних документів, тобто як помічників юриста. Існує чимало юридичних програм, що дозволяють автоматизувати правоохоронну діяльність, без складання документів уручну. Зумовлено це тим, що роботизовані програми можуть виконувати механічну роботу будь-якої складності, з набагато більшою продуктивністю, що значно збільшує швидкість діловодства. Яскравим прикладом такого явища є створений англійським фахівцем Джошуа Браудером робот-адвокат, який безкоштовно допомагає опротестувати штраф за паркування, врегулювати інші проблеми [2]. В Україні набула широкої популярності процедура виписування штрафу з автоматичних засобів фіксації. Також вуличні камери розпізнають злочинців, «кіберсудді» ухвалюють судові рішення, роботи проводять хірургічні операції, високоточна військова зброя й безпілотні літальні апарати уражають цілі – і це далеко не вичерпний перелік випадків, коли сучасні технології штучного інтелекту допомагають людині виконувати різноманітні складні завдання [3].

В умовах цифрової реальності доволі актуалізована проблема роботизації правоохоронної діяльності, з можливою перспективою заміни юридичної професії роботами. На думку вчених, штучний інтелект (далі – ШІ) може бути використаний для покращення ефективності роботи правоохоронних органів і забезпечення публічної безпеки. Наприклад, використання ШІ може допомогти правоохоронним органам відстежувати правопорушників і злочинні групи, визначати їхнє місцезнаходження, аналізувати відео- й аудіозаписи, шукати співвідношення між різними злочинами і правопорушниками тощо. Штучний інтелект може використовуватись також для аналізу текстової й мовної інформації у процесі профілактичних заходів, у проведенні гласних чи негласних слідчих дій. Зокрема, за допомогою аналізу мовної інформації комп'ютерна програма може виявляти ключові слова і зв'язки між повідомленнями, що дасть змогу виявити можливі загрози і, безпосередньо, самих правопорушників; за допомогою програм розпізнавання облич можна

ідентифікувати осіб, правопорушення яких були зафіксовані засобами фото- й відеоспостереження [4]. Також варто вести мову про «розумну» поліцію, тобто про використання нових технологій у вигляді сучасних поліцейських патрульних автомобілів, оснащених новітніми інтегрованими ІТ-системами. Такі автомобілі можуть прибути до місця події оптимальним маршрутом за допомогою GPS-навігатора [5, с. 38–39].

Окрім того, варто згадати про нагрудні камери (портативні відеореєстратори) для поліцейських у комплекті з відеореєстратором для патрульних автомобілів. Під час здійснення повноважень поліцейським портативний відеореєстратор закріплюється на його форменому одязі так, щоб не створювати перешкод його діям. Увімкнення портативного відеореєстратора відбувається з моменту початку виконання службових обов'язків або спеціальної поліцейської операції, а відеозйомка ведеться безперервно до її завершення, крім випадків, пов'язаних із виникненням у поліцейського особистого приватного становища. Відеореєстратор може бути встановлений усередині салону службового патрульного автомобіля або зовні для максимальної фіксації навколишньої обстановки або внутрішньої частини салону у спосіб, що не заважає огляду водія. Відеореєстратор вмикається, коли поліцейський розпочинає виконувати службові обов'язки або стартує спеціальна поліцейська операція, а відеозапис триває безупинно до її завершення. «Розумна» поліція активно використовує безпілотні літальні апарати (БпЛА, дрон) – повітряні судна, призначені для виконання польоту без пілота на борту, керування польотом якого і контроль за яким здійснюються за допомогою спеціальної станції керування, що розташована поза літальним апаратом [5, с. 38–39].

Важливо також наголосити, що ШІ революціонізує боротьбу з кіберзлочинністю, дозволяючи аналізувати величезні масиви даних у режимі реального часу, виявляти нові загрози й автоматизувати рутинні операції. Так, розслідування економічних і кіберінцидентів передбачає обробку великих обсягів даних. Загалом співробітникам правоохоронних органів, з їхніх же слів, доволі складно без допомоги «цифрових помічників» збирати й аналізувати всі необхідні докази, особливо криптоактиви. Обробка штучним інтелектом електромагнітних хвиль від WiFi-роутера дозволяє заглянути в житлове приміщення, практично не залишаючи слідів. Це значно підвищує ефективність діяльності правоохоронних органів та встановлює нові стандарти в галузі кібербезпеки.

Сучасні автоматизовані системи моніторингу і глибокого аналізу даних дають змогу не просто фіксувати правопорушення, але й виявляти потенційні загрози, прогнозувати криміногенні тенденції та координувати міжвідомчі дії з небаченою раніше оперативністю й точністю. Упровадження ШІ в боротьбу з кіберзлочинністю сприяє вдосконаленню механізмів моніторингу, підвищенню точності і швидкості ухвалення рішень, а також оптимізації використання ресурсів [6].

Одним із найпопулярніших застосувань технологій штучного інтелекту є розпізнавання осіб (обличь). Такі програми дозволяють правоохоронним органам ідентифікувати людей з високим ступенем точності, звільняючи їх від необхідності вручну звіряти документи з різними базами даних. Окрім запису фактичного зображення, більшість цих програм також збирає біометричні дані. Біометрична інформація дозволяє проводити більш точну ідентифікацію. Завдяки значним досягненням останніх років технологія розпізнавання осіб тепер може використовуватись у режимі реального часу. Наприклад, технологія розпізнавання облич у режимі реального часу дозволяє порівнювати записи з камер відеоспостереження зі списками відомих і розшукуваних злочинців. Оскільки технологія розпізнавання осіб працює в режимі реального часу, поліція може прибути на місце події протягом кількох хвилин, якщо програма виявить збіг. Звичайно, існує серйозна проблема упередженості в розпізнаванні осіб, і це пов'язано зі спотвореннями в наборах даних, які ми передаємо системі для навчання. Очікується, що з удосконаленням цих наборів даних та використанням різних даних для навчання машин вони ставатимуть щоразу кращими.

Отже, розпізнавання осіб – це додаток штучного інтелекту, що широко використовується, і це дозволяє правоохоронним органам з великою точністю ідентифікувати людей без необхідності ручної перевірки кількох баз даних. Ці системи не тільки фіксують зображення, а й збирають біометричні дані, підвищуючи точність ідентифікації. Хоча технологія розпізнавання осіб стикається з певними труднощами, її інтеграція з біометричними даними може підвищити її ефективність.

Технологію розпізнавання осіб правоохоронні органи використовують кількома способами, зокрема: для встановлення місцезнаходження розшукуваних осіб; для зменшення кількості помилкових спрацьовувань при ідентифікації осіб з фотографіями; для виявлення жертв дорожньо-транспортних пригод, які перебувають у непритомному стані; для здійснення ретроспективної перевірки особи людини та зіставлення з наявними базами даних тощо.

Програми штучного інтелекту здатні аналізувати неймовірні обсяги даних, наприклад, камер відеоспостереження. Окрім пошуку осіб, програмне забезпечення також може визначати тенденції, поведінку й інші взаємозв'язки набагато швидше, ніж людина. Технології набагато перевершують можливості людини, коли йдеться про обсяг даних, які треба проаналізувати. У той час як аналіз є основою всіх програм ШІ, машинне навчання дозволяє програмному забезпеченню робити висновки, аналогічні людським. Ґрунтуючись на цих результатах, ШІ може передбачати майбутнє. Цей процес може здатися простим, але машинне навчання вимагає певного часу, перш ніж алгоритм дійде потрібних висновків.

Взагалі сучасні нейромережі виокремлюють за такими функціональними категоріями: генерація тексту, створення зображень, монтаж відео, робота зі звуком, продуктивність, розваги й універсальний формат. На основі аналізу

методів навчання й характеристик нейромереж можна виділити такі їхні переваги й недоліки. Серед переваг: нейронні мережі можуть обробляти великі обсяги даних, що робить їх добре придатними для аналізу великих обсягів тексту, зображень і відео; нейронні мережі можуть автоматично вивчати складні патерни й особливості, що робить їх ефективними для виявлення тонких невідповідностей та аномалій у фейкових медіа тощо [7]. Утім, вважаємо, робочі навантаження інтелектуальних додатків повинні відповідати принципам відповідального штучного інтелекту, щоб забезпечити справедливість, підзвітність, прозорість та етичну поведінку. Задля цього у правоохоронних системах та оборонній сфері варто застосовувати систему ШІ так, щоб вона справедливо ставилася до всіх користувачів, притягувала розробників і користувачів до відповідальності за її роботу, забезпечувала прозорість у роботі штучного інтелекту й дотримувалася етичних стандартів. Корпорація Microsoft прагне вдосконалювати ШІ на основі принципів, які ставлять людей на перше місце. Генеративні моделі мають значні потенційні переваги, але без ретельного проєктування такі моделі можуть генерувати неправильний або навіть шкідливий контент [8].

Принагідно зазначимо, що основні принципи відповідального ШІ включають справедливість, підзвітність, прозорість та етику [8]. Принцип справедливості полягає в тому, щоб використовувати різноманітні й репрезентативні дані про навчання, аби мінімізувати ризики і проблеми у цій сфері. На думку дослідників, найбільшою проблемою є відсутність нормативно-правового регулювання застосування штучного інтелекту в правоохоронній діяльності. Тому важливе значення має прийняття нормативно-правових актів, які регламентували б використання ШІ у правоохоронній діяльності. У цьому ми підтримуємо пропозиції вчених щодо внесення змін до статті 25 «Повноваження поліції у сфері інформаційно-аналітичного забезпечення» Закону України «Про Національну поліцію», а саме, додати пункт 6 до частини 2 «Поліція в рамках інформаційно-аналітичної діяльності:» у редакції: «Для збору, обробки й аналізу інформації може застосовувати засоби штучного інтелекту», а також зміни до статті 8 «Права підрозділів, які здійснюють оперативно-розшукову діяльність» Закону України «Про оперативно-розшукову діяльність», а саме додати пункт 22 до частини 1 в редакції: «Застосовувати засоби штучного інтелекту для отримання, обробки, перевірки та аналізу оперативної інформації» [4]. Тут важливо, що співробітники правоохоронних органів не лише отримають доступ до більшої кількості інформації, а й матимуть помічника, який зможе обробляти величезні обсяги даних і робити на їхній основі висновки, схожі на людські. Ця технологія використовується в покращених великих мовних моделях (Lms), таких як project Notebook LM від Google. Тож такий розумний обмін знаннями приносить користь правоохоронним органам.

Також системи, засновані на ШІ, можуть імітувати реальність і проводити віртуальні тренінги для поліцейських. Співробітники правоохоронних органів отримують можливість відпрацьовувати навички ухвалення важливих рішень,

що дозволяє їм швидше реагувати та краще орієнтуватися в ситуації. Окрім того, процес об'єднання ШІ з віртуальною реальністю дозволить співробітникам відпрацьовувати безліч реалістичних сценаріїв в абсолютно безпечному, але регульованому середовищі. З іншого боку, ШІ може відіграти важливу роль у створенні персоналізованих, адаптивних програм навчання для правоохоронних працівників правоохоронних органів. Системи штучного інтелекту, що використовують алгоритми машинного навчання, можуть аналізувати ефективність роботи співробітників, виявляти галузі, що вимагають покращення, і, нарешті, створювати навчальні модулі, що відповідають потребам працівників правоохоронних органів. Вони нададуть чіткий індивідуальний план навчання залежно від своїх когнітивних потреб. Це приведе до індивідуального розвитку працівників правоохоронних органів, а відтак – до підвищення ефективності навчання, оскільки вони будуть зосереджені на навчанні. Крім того, системи, засновані на ШІ, забезпечують зворотний зв'язок й оцінку в режимі реального часу, що дасть змогу працівникам правоохоронних органів відстежувати свій прогрес і постійно вдосконалювати свої навички.

Отже, цифрові технології докорінно трансформують правоохоронну діяльність, створюючи принципово нові можливості для комунікації, аналізу та протидії злочинності. Інтегровані інформаційні системи забезпечують миттєвий обмін даними між правоохоронними органами на національному й міжнародному рівні, що підвищує ефективність реагування на транснаціональні злочини. А втім, аналітична робота з вирішенням складних і нетипових правових завдань у сфері правоохоронної діяльності ще довгий час залишатиметься в полі зору людини, оскільки ШІ у сфері юридичної практики не настільки розумний і поки що не здатний замінити висококваліфікованого юриста. З іншого боку, для сучасного юриста важливо розумітися на інноваційних технологіях, які здатні змінювати образ права, впливати на його регулятивний потенціал й ефективність, а впровадження цифровізації й роботизації у правоохоронну діяльність має відбуватися еволюційним шляхом.

Список використаних джерел:

1. Сніґоля Матуєлене, Віктор Шевчук, Юргіта Балтрунене. Штучний інтелект в діяльності органів правопорядку та юстиції: вітчизняний та європейський досвід. 2022. URL: https://cris.mruni.eu/server/api/core/bitstreams/1ccc7534-21b6-40e2-830d-9f65fa0e80c3/content (дата звернення: 07.03.2025).

2. Білик П. Роботи-юристи – вже реальність, але юридичний світ чинить останній опір. *Juscutum*. 2023. 27 берез. URL: https://www.juscutum.com/news/roboti-yuristi-vzhe-realnist-ale-yuridichniy-svit-chinit-ostanniy-opir (дата звернення: 07.03.2025).

3. Kosilova O. I., Rozghon O. V., Solodovnikova C. K., Stolbovyi V. M., Barabash O. O. Observance of Human Rights in the Use of AI as Technology. *Law, State and Telecommunications Review*. 2022. Vol. 14, no. 2. P. 38–67. DOI: 10.26512/lstr.v14i2.41558.

4. Зачек О. І., Дмитрик Ю. І., Сеник В. В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ. Сер. юрид*. 2023. № 3. С. 148–156. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/5945/1/19.pdf (дата звернення: 07.03.2025).

5. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання : монографія. Львів : ЛьвДУВС, 2020. 256 с.

6. Храпенко О. О., Меденцев А. М., Сперанський В. О. Цифровізація правоохоронної діяльності: використання штучного інтелекту для боротьби з кіберзлочинністю. *Юридичний науковий електронний журнал*. 2024. № 11. С. 505–508. URL: http://www.lsej.org.ua/11_2024/119.pdf (дата звернення: 07.03.2025).

7. Барабаш О. О. Штучний інтелект та сучасні нейромережі: вітчизняний та зарубіжний досвід. *Штучний інтелект у правовій практиці: межі та можливості :* зб. тез Всеукр. круглого столу (15 берез. 2024 р.) / упор. О. О. Барабаш. Львів : ЛьвДУВС, 2024. С. 17–23.

8. Відповідальні міркування щодо штучного інтелекту для робочих навантажень інтелектуальних додатків. 2024. 16 жовт. URL: https://learn.microsoft.com/uk-ua/power-platform/well-architected/intelligent-application/responsible-ai (дата звернення: 07.03.2025).

Басиста І. В.,
професор кафедри права
та публічного управління
доктор юридичних наук, професор
(Університет Короля Данила)

КРАЙНІ ТЕНДЕНЦІЇ У РОЗВИТКУ ШІ ТА ЙОГО БЕЗПЕКИ

У одній із попередніх публікацій [1, с. 11–14] йшлося про аргументи та контраргументи щодо однієї із крайніх ініціатив, яка мала б завершитися підписанням США, Великою Британією та Євросоюзом першого юридично обов'язкового міжнародного договору про використання штучного інтелекту. І про це зазначалося у дописах цілої низки закордонних та національних інформаційних ресурсів [2]. Передувало такому кроку ухвалення Радою Європи 17 травня 2024 року Рамкової конвенція про штучний інтелект, права людини, демократію і верховенство права, яка впродовж двох років розроблялася спец. міжурядовим комітетом, бізнесовими колами та представниками громадянського суспільства) [3].Також наявний закон ЄС про штучний інтелект (AI Act), який набув чинності у ЄС з 1 серпня 2024 року [4] та вважається «**першим у світі актом, який регулює розробку та використання штучного інтелекту»** [5]. **Також вже зазначалося** [1, с. 11–14]**, що у подальших планах** Офіс ШІ (AI Office), який і контролюватиме дотримання Закону та впровадження заборон-запобіжників [5].

Також вже наводився аналіз [1, с. 11–14], що значна кількість корпорацій та країн висловили своє занепокоєння і контраргументи [6; 7], ба навіть виголошували протести [8] такому категоричному «правовому» підходу. Поряд з цим, «країни-члени ЄС мають до 2 серпня 2025 року визначити національні компетентні органи, які контролюватимуть застосування правил для систем на основі штучного інтелекту та здійснюватимуть діяльність з нагляду за ринком» [4]. Натомість, компанії OpenAI, Google та Meta виступила проти таких законодавчих ініціатив, як шкідливих для розвитку технологій [9].

Як наслідок, анонсований процес підписання США, Великою Британією та Євросоюзом першого юридичного обов'язкового міжнародного договору про використання штучного інтелекту дав тріщину, про що стало відомо 10 лютого 2025 року. «Велика Британія і США не підписали міжнародну угоду про ШІ, ухвалену на глобальному саміті в Парижі. Про це повідомляє BBC, як пише Рубрика. Не дивлячись на те, що цей документ з 5 вересня 2024 року був відкритим до підписання далеко за межами ЄС і **підписаний 60 країнами,** зокрема Францією, Китаєм та Індією, у британському уряді зазначили, що «**не змогли погодити всі частини декларації лідерів**» і «**підписуватимуть лише ті ініціативи, які відповідають національним інтересам»** королівства. Своєю чергою, віце-президент США заявив делегатам, що надмірне регулювання ШІ може «**вбити трансформаційну галузь на самому початку її розвитку», тому «політиці сприяння розвитку штучного інтелекту»** слід надавати пріоритет над безпекою» [10].

Очевидно, що знехтувано принаймні тими фактами, що, *по-перше*, не всі проєкти за участі ШІ є суспільно-корисними і описаних ситуацій хоч греблю гати [1; 11]. Для прикладу, хоча б взяти до уваги такі оприлюднені факти, які вже наводилися [1, с. 11–14] та достатньо аргументовані (The Conversation вивчало_їх), що акаунти-боти роками впливають на громадську думку за допомогою дезінформації: нейромережі створюють зображення, а боти, як «агенти штучного інтелекту», поширюють їх у соцмережах, залучаючи безліч реальних підписників, яким потім «промивають мізки» [12].

По-друге, не можемо повністю заперечити і «теорію мертвого інтернету», згідно з якою більшість контенту у Всесвітній павутині, включно з публікаціями в соціальних мережах, створюють і автоматизують системи штучного інтелекту. Так створюється «армія читачів і послідовників» і про відсоток справжніх із них достеменно не відомо. росія вправно із цим маніпулює [12].

По-третє, викликають занепокоєння, як створені ШІ гіперреалістичні матеріали із сексуальним насильством над дітьми [13], так і, *по-четверте*, соціальний скоринг із залученням ШІ [14]. Жахливо, коли інструменти штучного інтелекту використовуються для «оголення» реальних зображень дітей. Побіжно слід зазначити, що Велика Британія перша країна, яка стала на шлях криміналізації використання інструментів штучного інтелекту для: створення матеріалів про насильство над дітьми; маскування своєї особистості і шантажу дітей підробленими зображеннями для змушування їх до наступного насильства. Отож, «нові кримінальні злочини охоплюють володіння, створення або розповсюдження інструментів ШІ, призначених для створення матеріалів про сексуальне насильство над дітьми, а також володіння так званими «посібниками для педофілів», що містять інструкції з використання технологій ШІ» [15]. Карати будуть і тих, хто керує сайтами, на яких поширюються матеріали про сексуальне насильство над дітьми [15]. Також і раніше вже йшлося про запровадження кримінальної відповідальності «за створення і

поширення сексуально відвертих «глибоких підробок» – відео, фотографій або аудіокліпів, створених за допомогою штучного інтелекту, щоб вони виглядали як справжні» [15].

По-п'яте, лунали і обвинувачення від колишніх співробітників OpenAI у порушенні американського законодавства про авторські права під час розробки чат-бота ChatGPT [16], а у жовтні видання The New York Times опублікувало статтю. OpenAI судиться з низкою видавництв, авторів (серед них Сара Сільверман та газета The New York Times [17]) і художників (про що йшлося й рік тому [11, с.19-38; 18, с.188-197; 19, с.16-24; 20, с.360-364]) з приводу використання захищених авторським правом матеріалів для навчання штучного інтелекту. Звісно, що генеральний директор OpenAI заперечує такі порушення [16]. Також у публікаціях Марії Ігнатьєвої та Валентини Троян йдеться, що компанія Meta використовувала Library Genesis (LibGen) – піратську «тіньову бібліотеку», створену в Росії, – для тренування своїх моделей генеративного штучного інтелекту (ШІ). У 2015 році суд у Нью-Йорку спробував тимчасово закрити сайт, але адміністратори просто змінили домен. У вересні 2024 року інший суд ухвалив рішення стягнути з LibGen $30 мільйонів компенсації за порушення авторських прав [21]. Попередньо про це йшлося у повідомленні Kate Knibbs від 9 січня 2025 року у Wired [22] , де розлоге уточнюється, що справа *Kadrey et al. проти Meta Platforms* була одним із перших позовів про авторські права, поданих проти технологічної компанії через її практику навчання штучному інтелекту. Результати розгляду цієї справи, поряд з результатами десятків подібних справ, що проходять через суди в Сполучених Штатах, вирішать, чи зможуть технологічні компанії законно використовувати чужу інтелектуальну власність для навчання штучного інтелекту в майбутньому [22].

По-шосте, хоча OpenAI і обіцяла до 2025 року створити спеціальний інструмент Media Manager, який за задумом мав виявляти захищені авторським правом тексти, зображення, відео та аудіо з різних джерел і враховувати побажання авторів щодо їхнього використання, вона не змогла створити цей обіцяний інструмент. Про це пише TechCrunch, передає Vector. За словами колишнього працівника компанії, над цим інструментом майже ніхто не працював [17].

*По-сьоме, «*згідно зі звітом Bloomberg, центри обробки даних, що забезпечують роботу ШІ, чинять значний тиск на електромережу США. Дані Whisker Labs показують, що більш ніж половина будинків, які стикаються з проблемами електропостачання, знаходяться в межах 20 миль від великих центрів обробки даних» [23]. «Для запобігання кризі потрібна скоординована взаємодія між постачальниками енергії, технологічними компаніями та регуляторами. Інвестування в стійку інфраструктуру і розумні енергосистеми стане ключовим кроком у вирішенні проблеми» [23].

На фоні хоча б лише наведених аргументів на користь необхідності інвестування, зокрема і інтелектуальних ресурсів, у безпеку та безпечність ШІ, принаймні дивно виглядають повідомлення про те, що компанія-розробник чат-

боту ChatGPT – OpenAI – розпустила свою команду (Superalignment була створена у 2023 році з метою розробки «наукових і технічних проривів для керування системами штучного інтелекту, значно розумнішими за нас»), яка займалася довгостроковими ризиками штучного інтелекту. Це сталося менше ніж через рік після її створення. Це рішення ухвалили після того, як керівники групи Ілля Суцкевер і Ян Лейке повідомили про свій відхід із компанії. Про це пише CNBC, передає AIN.UA [24].

Лише час здатен пролити світло на те, що відбувається, коли **«політиці сприяння розвитку штучного інтелекту** надають пріоритет над безпекою» [10]. Поки тішимося тими справді проривними можливостями ШІ, якими рясніють інформаційні повідомлення та про які неодноразово вже згадувалося [1, с. 11–14; 11, с. 19–38; 18, с. 188–197; 19, с. 16–24; 20, с. 360–364]. Серед крайніх із них, це нові можливості керувати «розумним будинком» через розширення Google Home у додатку Gemini [25]; суттєві переваги на полі бою та у військовому ремеслі [26; 27; 28; 29]; покращення мовної практики та граматичної обізнаності тих, хто вивчає іноземні мови [30; 31] тощо.

Список використаних джерел:

1. Басиста І. В. Чергові кроки нормативно-правового регулювання штучного інтелекту (продовження огляду). Штучний інтелект і безпека: матеріали науково-практичної конференції. Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України, Інституту проблем реєстрації інформації Національної академії наук України : матеріали, 19-21 листопада 2024 р. Київ : ІПМЕ ім. Г. Є. Пухова НАН України, ІПРІ НАН України, 2024. С. 11–14.

2. США, Велика Британія та ЄС підпишуть першу угоду у галузі штучного інтелекту. (2024, 5 вересня). Processer.media. https://processer.media/ua/ssha-velika-britaniya-ta-ies-pidpishut-pershu-ugodu-u-galuzi-shtuchnogo-intelektu/

3. Рамкова конвенція про штучний інтелект, права людини, демократію і верховенство права. Взято 1 жовтня з https://search.coe.int/cm#%7B"CoEObjectId":["0900001680afb11f"],"sort":["CoEValidationDate%20Descending"]%7D.

4. У Євросоюзі набув чинності перший у світі закон про штучний інтелект. (2024, 1 серпня). Ukrinform. https://www.ukrinform.ua/rubric-world/3891086-u-evrosouzi-nabuv-cinnosti-persij-u-sviti-zakon-pro-stucnij-intelekt.html.

5. Які ризики несе перший у світі закон про штучний інтелект і чому він потрібен ЄС. (2024, 1 квітня). https://www.eurointegration.com.ua/news/2024/04/1/7182827/.

6. Open Letter EU AI Act and Signatories.pdf - Google Диск.

7. Europe one step away from landmark AI rules after lawmakers' vote. (2024, 14 березня). Europe one step away from landmark AI rules after lawmakers' vote | Reuters.

8. World’s first major act to regulate AI passed by European lawmakers. (2024, 13 березня). World’s first major act to regulate AI passed by European lawmakers.

9. Жахалов Я. (2024, 22 серпня). OpenAI різко розкритикувала закон Каліфорнії відносно ШІ. *Tech.liga.net*. https://tech.liga.net/ua/technology/novosti/openai-rizko-rozkrytykuvala-zakon-kalifornii-vidnosno-shi.

10. США та Британія відмовились підписувати міжнародну декларацію щодо ШІ. 11.02.2025. https://rubryka.com/2025/02/11/ssha-ta-brytaniya-vidmovylys-pidpysuvaty-mizhnarodnu-deklaratsiyu-shhodo-shi/?fbclid=IwZXh0bgNhZW0CMTEAAR3k-NYlIAOjC2jUQSJ8nEdVNjt03ZfqlpuxrQoGTyP6J__v3-u3vCPxWds_aem_fsvNjUFNwgU-MmDOcZjOuw.

11. Басиста І. В., Удовенко Ж. В., Кулинич Марта-Марія А. Огляд тенденцій щодо штучного інтелекту та його перспективність для процесуальних рішень у перебігу кримінального провадження. *Науковий вісник Ужгородського Національного Університету. Серія : Право.* 2024. Вип. 81. Том (частина) 3. С. 19–38. https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/03/81_part-3.pdf.

12. «Мертвий інтернет»: штучний інтелект уже керує Мережею і людьми, – The Conversation. (2024, 21 травня). *Internetua.com*. https://internetua.com/-mertvii-internet-shtucsnii-intelekt-uje-keruye-merejeua-i-luadmi-the-conversation.

13. Генерував непристойні фото з дітьми: в Британії вперше заборонили користуватися ШІ злочинцю. (2024, 21 квітня). *Rubryka.com*. https://rubryka.com/2024/04/21/generuvav-neprystojni-foto-z-ditmy-v-brytaniyi-vpershe-zaboronyly-korystuvatysya-shi-zlochyntsyu/.

14. Бойко Д. Соціальний скоринг та штучний інтелект: ризики для правосуддя. (2023, 28 грудня). Центр Дністрянського. https://dc.org.ua/news/socialnyy-skoryng-ta-shtuchnyy-intelekt-ryzyky-dlya-pravosuddya.

15. Матеріали із сексуальним насильством над дітьми від ШІ стали незаконними у Великій Британії. 3.02.2025. https://www.epochtimes.com.ua/novyny-svitu/materialy-iz-seksualnym-nasylstvom-nad-ditmy-vid-shi-staly-nezakonnymy-u-velykiy-brytaniyi-video-166839.

16. Експрацівника OpenAI, який публічно заявив про порушення ChatGPT законів, знайшли мертвим. 14.12.2024. https://internetua.com/ekspracivnika-openai-yakii-publicsno-zayaviv-pro-porushennya-chatgpt-zakoniv-znaishli-mertvim?utm_source=ukrnet_news.

17. OpenAI провалила запуск обіцяного інструменту для захисту авторських прав. 2.01.2025. https://processer.media/ua/openai-provalila-zapusk-obicyanogo-instrumentu-dlya-zahistu-avtorskih-prav/.

18. Удовенко Ж. В., Басиста І. В. Використання штучного інтелекту у кримінальному провадженні: ілюзія чи реальність. Штучний інтелект у правовій практиці: межі та можливості : збірник тез Всеукраїнського круглого столу (15 березня 2024 року) / упор. О. О. Барабаш. Львів. Львівський державний університет внутрішніх справ. С. 188–197. file:///C:/Users/Ірина%20Володимирівна/Downloads/15_03_2024.pdf.

https://www.lvduvs.edu.ua/uk/library/materialy-naukovykh-konferentsii.html.

19. Басиста І. В. Штучний інтелект: правила використання, перспективи, ризики та загрози, застосовність для кримінального провадження (продовження огляду). Кримінальне судочинство: сучасний стан та перспективи розвитку: матеріали Всеукр. наук.-практ. конф. (Київ, 2 трав. 2024 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ. Нац. акад. внутр. справ. С. 16–24.

20. Басиста І. В. Використання можливостей штучного інтелекту у перебігу кримінального провадження та захист фундаментальних прав (продовження огляду). Актуальні питання забезпечення безпекового середовища в Україні : зб. тез наук. доп. Всеукр. наук.-практ. конф. (Київ, 19 квітн. 2024 р.) [Електронне видання] / упоряд. : М. Г. Вербенський, В. О. Рядінська, А. І. Хальота, В. А. Мацько. Київ, 2024. С. 360–364.

21. Троян В. МЕТА таємно тренувала свій ШІ на піратській базі даних. 14.01.2025. https://imi.org.ua/news/meta-tayemno-trenuvala-svij-shi-na-piratskij-bazi-danyh-i66033.

22. Knibbs Kate. Meta Secretly Trained Its AI on a Notorious Piracy Database, Newly Unredacted Court Docs Reveal. 9.01.2025. https://www.wired.com/story/new-documents-unredacted-meta-copyright-ai-lawsuit.

23. Балаєва Т. Експерти: дата-центри ШІ несуть загрозу обвалу електромережі США. 30.12.2024. https://cryptonewsua.com/eksperty-data-tsentry-shi-nesut-zagrozu-obvalu-elektromerezhi-ssha/.

24. Розробник ChatGPT розпустив команду, яка займалася питаннями безпеки штучного інтелекту. 21.05.2024. https://borgexpert.com/news/rozrobnyk-chatgpt-rozpustyv-komandu-iaka-zajmalasia-pytanniamy-bezpeky-shtuchnoho-intelektu.

25. Google дозволив управління розумним будинком через додаток Gemini. https://delo.ua/technologies/google-dozvoliv-upravlinnya-rozumnim-budinkom-cerez-dodatok-gemini-438175/.

26. Гузь У. Федоров розповів, що прототипи дронів з ШІ можуть з'явитися на полі бою до кінця року. 2.04.2024. https://rubryka.com/2024/04/02/fedorov-rozpoviv-shho-prototypy-droniv-z-shi-mozhut-z-yavytysya-na-poli-boyu-do-kintsya-roku/.

27. Ігнатенко М. Рішення для перемоги: союзники планують озброїти Україну тисячами дронів зі штучним інтелектом. 17.02.2024. https://rubryka.com/2024/02/17/rishennya-dlya-peremogy-soyuznyky-planuyut-ozbroyity-ukrayinu-tysyachamy-droniv-zi-shtuchnym-intelektom/.

28. Рябовіл Ю. ШІ замість пілота: США провели успішне випробування автономного винищувача X-62A VISTA. 5.05.2024. https://nv.ua/ukr/world/countries/ssha-proveli-uspishniy-polit-avtonomnogo-vinishchuvacha-x-62a-vista-50415804.html.

29. У США розробили революційний штучний інтелект для військових, що здійснює 1000 ударів на годину. 23.08.2024. https://noworries.news/u-ssha-rozrobyly-revolyuczijnyj-shtuchnyj-intelekt-dlya-vijskovyh-shho-zdijsnyuye-1000-udariv-na-godynu/

30. Бровінська М. Українські розробники створили ШІ-застосунок, що замінить спікінг-клаби та нівелює мовний бар'єр у вивченні іноземних мов. Як працює співрозмовник у смартфоні Interlocutor. 17.02.2025. https://dev.ua/news/language-practice-1739774630.

31. Хандусенко Н. В Україні запустили безплатний ШІ-додаток для вивчення англійської: GrammarTrack допоможе опанувати граматику будь-якого рівня. 7.02.2025. https://dev.ua/news/v-ukraini-zapustyly-bezplatnyi-dodatok-dlia-vyvchennia-anhliiskoi-hramatyky-grammartrack-1738916393.

Биков І. О.,
доцент кафедри державно-правових дисциплін,
кандидат юридичних наук, адвокат
(Міжнародний гуманітарний університет)

СТРАТЕГІЧНІ ОРІЄНТИРИ РОЗВИТКУ ЗАКОНОДАВСТВА УКРАЇНИ ЩОДО ВІРТУАЛЬНИХ АКТИВІВ

Сучасний розвиток цифрової економіки та активне використання технологій блокчейн [1] вимагають комплексного та ефективного правового регулювання віртуальних активів. Україна, прагнучи забезпечити відповідність своїх законодавчих норм світовим практикам та тенденціям, поступово впроваджує нормативні механізми, що регламентують правовий статус цифрових та віртуальних активів. Використання криптовалют, токенів та інших цифрових інструментів вимагає не лише технічного забезпечення, а й належної правової бази для регулювання їх обігу. Відсутність єдиного міжнародного підходу до правового статусу віртуальних активів створює додаткові виклики для державного регулювання та інтеграції цих інструментів у фінансову систему. В Україні відзначається стрімке зростання інтересу до віртуальних активів серед підприємств, фінансових установ та громадян, що підкреслює необхідність ефективної законодавчої політики в цьому напрямі. Водночас ризики шахрайських схем, відсутність механізмів захисту прав власників та потенційні загрози економічній стабільності потребують розробки комплексних правових механізмів.

Використання криптовалют, токенів та інших цифрових та віртуальних активів стрімко зростає в Україні. Однак відсутність чіткої правової регламентації створює правову невизначеність для учасників ринку, що ускладнює їх інтеграцію в економічний простір. Регулювання цієї сфери має сприяти правовій визначеності, зниженню ризиків шахрайства та забезпеченню ефективного контролю за фінансовими потоками.

Окрім цього, правове закріплення статусу віртуальних активів необхідне для усунення бар'єрів на шляху їх використання в бізнесі та інвестуванні. На даний момент в Україні відсутній єдиний підхід до визначення віртуальних активів як об'єкта права, що ускладнює їх правове трактування в контексті фінансового, цивільного та податкового законодавства. Необхідним є впровадження чітких визначень щодо класифікації віртуальних та цифрових активів, встановлення правових режимів для їх обігу, володіння та розпорядження ними, а також визначення відповідальності за незаконні операції з віртуальними та цифровими активами.

На нашу думку, державне регулювання має включати розробку відповідних механізмів ліцензування учасників ринку, що надають послуги, пов'язані з віртуальними активами, таких як криптовалютні біржі, постачальники цифрових гаманців та платіжні провайдери, та інші. Окрім цього, необхідним є створення ефективного механізму розкриття інформації про фінансові операції із цифровими та віртуальним активами для запобігання відмиванню коштів та фінансуванню тероризму.

Окремої уваги заслуговує питання захисту прав власників віртуальних та цифрових активів, оскільки відсутність законодавчих норм ускладнює процес правозастосування у випадку шахрайства, крадіжок чи втрати доступу до криптоактивів та інших віртуальних активів. Разом із тим, законодавче закріплення механізмів правового захисту учасників даного ринку має включати порядок вирішення спорів, питання страхування депозитів та відповідальність постачальників послуг за втрату або компрометацію цифрових та віртуальних активів. Таким чином, закріплення правового статусу віртуальних та цифрових активів на законодавчому рівні є необхідною умовою для забезпечення правової визначеності, захисту інтересів інвесторів та користувачів та власників цифрових фінансових інструментів, а створення чіткої нормативно-правової бази сприятиме залученню інвестицій, розвитку інноваційних технологій та інтеграції української економіки у світовий цифровий ринок.

Як відомо, в Україні вже здійснено перші кроки у напрямі правового регулювання цифрових активів та ухвалено проект Закону «Про віртуальні активи» [2], що стало важливим етапом у створенні правової основи для функціонування цього ринку.

Проте, на нашу думку, сфера потребує подальшого розвитку законодавства, що має проявлятися у визначені чіткої процедури ліцензування учасників ринку, включаючи криптовалютні біржі, платформи для обміну токенів та послуги зі зберігання цифрових та віртуальних активів;

удосконалення податкового режиму для криптовалютних операцій, що дозволить визначити правила оподаткування доходів та мінімізувати ухилення від податків; впровадження спеціальних регуляторних режимів для стартапів, які працюють у сфері блокчейн-технологій, з метою стимулювання інновацій; розробку механізмів державного контролю та нагляду за цифровими активами, що дозволить зменшити ризики фінансових злочинів, шахрайства та незаконного використання криптовалют; інтеграцію технологій блокчейну у державний сектор, що може сприяти підвищенню прозорості державних операцій та зменшенню рівня корупції.

Практично цінною є гармонізація національного законодавства з європейськими та міжнародними стандартами та практиками у сфері віртуальних активів, що є важливим кроком для розвитку ринку цифрових активів в Україні. На нашу думку, зазначений процес не може бути ефективним для національної практики без імплементації норм щодо запобігання відмиванню коштів та фінансуванню тероризму відповідно до рекомендацій FATF [3]; забезпечення відповідності національних правових норм відповідним директивам ЄС щодо регулювання ринків криптоактивів; запровадження механізмів міжнародного співробітництва у сфері регулювання цифрових активів, зокрема обміну інформацією між фінансовими установами та органами влади. Завдяки цим заходам Україна зможе ефективно інтегрувати свою правову систему до міжнародного ринку цифрових активів, знизити ризики незаконного використання криптовалют та забезпечити стабільний розвиток сектору фінансових технологій. Таким чином, ефективне правове регулювання цифрових активів в Україні має ґрунтуватися на комплексному підході, який включає гармонізацію законодавства з міжнародними стандартами, розробку механізмів контролю, стимулювання інноваційного розвитку та захист прав власників цифрових активів. Реалізація цих стратегічних орієнтирів сприятиме формуванню прозорого, стабільного та конкурентоспроможного ринку цифрових фінансових технологій в Україні.

Список використаних джерел:

1. Про віртуальні активи : Закон України від 17.02.2022 № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text.

2. Blockchain Facts: WhatIsIt, HowIt Works, and How It Can Be Used. Investopedia. URL: https://www.investopedia.com/terms/b/blockchain.asp.

3. FATF Recommendations. URL: https://www.fatf-gafi.org/en/topics/fatf-recommendations.html.

Біла Я.,
студентка першого курсу
(Дніпровський гуманітарний університет)
Сковронська І. Ю.,
кандидатка філологічних наук, доцентка,
професорка кафедри мовної підготовки
(Львівський державний університет внутрішніх справ)

ПРОБЛЕМА ІНФОРМАЦІЙНОГО ПЕРЕВАНТАЖЕННЯ

З проблемою інформаційного перевантаження зіштовхувався кожен користувач Інтернету. Однак хвилювання породжує той факт, що це негативно позначається на таких важливих компонентах життєдіяльності, які безпосередньо впливають на наш добробут: медицину, освіту, політику, бізнес, маркетинг тощо.

Перевантаження називають як головною проблемою нашого часу, так і повною відсутністю проблеми. Його водночас іменують чинником, що впливає, в тому числі, на науку, медицину, освіту, політику, управління, бізнес і маркетинг, планування для розумних міст, доступ до новин, відстеження персональних даних, домашнє життя, використання соціальних мереж та онлайн покупок, написання літературних творів тощо [1].

Вважається, що чим різноманітнішим і складнішим є збір інформації, і чим більше альтернатив він пропонує, або здається, що пропонує, тим більша ймовірність того, що він спричинить перевантаження. Соціальні мережі, такі як Facebook і Twitter, зараз часто вважаються основними «перевантажувальними» засобами масової інформації, які спричиняють значну, якщо не більшу частину перевантаження, через легкість, з якою вони дозволяють створювати, дублювати і обмінюватися інформацією [1].

Величезний масштаб і швидкість потоку інформації в соціальних мережах відсутність фільтрації, переважання думок над фактами є центральними в цій проблемі. Тому специфічні питання перевантаження мобільних пристроїв, особливо з маленькими екранами, включають в себе постійну потребу перевіряти нову інформацію.

Легка доступність та нав’язливість інформації може створювати відчуття терміновості і залежності. У такому форматі інформація не сприймається шляхом глибокого розуміння. Це може загрожувати формуванням «хибного знання», «хибної експертності» та необґрунтованих упереджень.

Люди живуть зі страхом пропустити важливу інформацію (FOMO), втратити контроль. А це спричиняє формування схильності до «інформаційної залежності» що в подальшому призводить до зниження продуктивності, підвищення рівня стресу, ігнорування фізіологічних потреб тощо.

Можливо, головна відмінність між впливом перевантаження у 21 столітті та в попередні часи полягає в тому, що зараз перевантаження сприймається як причина формування перешкод для соціальної згуртованості та політичних дій, включаючи втрату соціальної згуртованості, політичну поляризацію, нежиттєздатність у публічній сфері [1].

Інформаційне перевантаження здатне чинити вплив на такі виклики сучасності, як політичний розкол, недовіра до державних інститутів і

руйнування спільних цінностей. А це заважає громадянам брати участь в обґрунтованій дискусії та приймати рішення.

Під час використання цифрових інструментів рідко замислюються над особистим благополуччям, але респонденти вважають це питання важливим і зацікавлені в цифрових інструментах для просування усвідомленості [2].

Нестача часу не дає можливості ознайомитися з новими цифровими інструментами 17 респондентам: «Вам потрібні ноу-хау, але вам також потрібно багато часу. Звідки цьому часу взятись?» [2].

Через інформаційне перевантаження ускладнюється опанування нових технологій, бо елементарно не вистачає часу на пошук та опанування.

Після початкової ейфорії використання цифрових інструментів зменшується, оскільки колегам не вистачає прагнення і терпіння залучатися [2].

Більшості команд не вистачає рольових моделей (n = 15). Цифрова культура пристосована до потреб тих, хто найменш відкритий і компетентний у використанні цифрових інструментів, що відповідають різним рівням знань (Int. 13) [2].

Для сталого та ефективного впровадження не вистачає людей, які виділяють цьому достатньо часу, з ентузіазмом та захопленням вивчали та впроваджували нові інструменти та були прикладом іншим для наслідування.

Хоча всі респонденти користуються цифровими інструментами щодня, 14 з 20 опитаних обмежують їх до найпростішого, прагматичного використання, щоб уникнути можливих ускладнень. Цифрові інструменти часто замінюють інші програми один до одного, і їхній потенціал не використовується [2].

Невміння, небажання, нестача часу та страх перед складністю та потенційними ускладненнями призводить до того, що нові технології використовуються дуже спрощено, обмежено, уникаючи всього, що може бути складним і потребує самостійного дослідження та навчання. Таким чином старі інструменти просто відтворюють старі методи, а не вдосконалюють їх. Реальний потенціал інструментів для покращення не реалізовується. Респонденти наголошують на важливості наявності зручних, інтуїтивно зрозумілих та сучасних цифрових інструментів (n = 12). Особливо у викладанні технологічні бар'єри можуть бути надто високими (зручність використання платформ, відсутність інтерфейсів між різними цифровими інструментами), оскільки під час курсу залишається мало місця для маневру (n = 8) [2].Чим легше та зрозуміліше використання інструментів, тим більша імовірність їх успішної інтеграції та ефективного використання.

Тепер визначимо шляхи вирішення проблеми інформаційного перевантаження. По-перше, цей підхід відіграв ключову роль у точному визначенні командою об'єкта оцінювання, заклавши основу для аналізу релевантності та ефективності в рамках портфоліо-аналізу оцінювання [3].

Використовуючи методи інтелектуального аналізу тексту та машинного навчання, команда змогла подвоїти розмір доказової бази (відповідних

проектів та їхньої документації), що, ймовірно, було б неможливим за традиційних підходів до ідентифікації портфоліо [3]. Використання алгоритмів для автоматичного аналізу великих обсягів даних значно зменшить витрачений час та дозволить охопити більший обсяг інформації на відміну від ручних методів пошуку та збору інформації [3].

Для ефективного використання важливо розуміти, що відбувається в процесі формування відповіді. Таким чином, знаючи весь процес ми можемо визначити вразливі місця для появи потенційних помилок та запобігти їх виникненню або ж хоча б зменшити кількість. Наприклад, штучний інтелект може мати проблеми з етичними та моральними нормами. Існують умови для його етичного використання: **прозорість** (важливо розуміти процес); **підзвітність** (необхідно знати, хто буде нести відповідальність за рішення, які приймає ШІ); **захист конфіденційності** (дані повинні збиратися та оброблятися зі згоди користувачів і вони повинні мати можливість контролювати, які їхні дані використовуються). У підсумку маємо такі положення стосовно вирішення проблеми: 1) точне визначення об'єкта оцінювання; 2) використання методів аналізу тексту та машинного навчання; 3) додаткова впевненість у правильному та етичному використанні методів. Система рекомендацій відіграє незамінну роль у зменшенні інформаційного перевантаження в Інтернеті [4].

Без зовнішнього втручання це упередження поступово посилюватиметься в ланцюзі зворотного зв'язку рекомендаційної системи, утворюючи замкнене коло, де рекомендовані результати все більше відхилятимуться від справжніх уподобань користувача [4]. Проблема замкненого кола. Алгоритм рекомендує інформацію, але популярні елементи рекомендуються частіше, на них частіше клацають, що робити їх ще більш популярними, а це підсилює упередженість алгоритму і відчуття, ніби ці елементи є найбільш релевантними.

Отже, частина вирішення проблеми полягає у постійному вдосконаленні та контролі цих систем. У загальному підсумку стає зрозумілим, що інформаційне перевантаження безумовно присутнє і має окрім позитивного ще й негативний вплив, який можна зменшити, навчаючи людей опановувати нові інструменти та покращуючи інструменти зсередини.

Список використаних джерел:

1. Bawden, D. & Robinson, L. (2020). Information Overload: An Overview. In: Oxford Encyclopedia of Political Decision Making. Oxford: Oxford University Press. doi: 10.1093/acrefore/9780190228637.013.1360.

2. Koch, C., & Fehlmann, F. (2025). Beyond Digital Literacy: Exploring Factors Affecting Digital Performance of University Staff. Media and Communication, 13, Article 8913. https://doi.org/10.17645/mac.8913 (дата звернення: 27.02.2025).

3. Balčytienė, A. (2025). Strengthening Responsible Journalism Through Self-Efficacious Learning-Oriented Media Literacy Interventions. *Media and Communication*, 13, Article 9038. https://doi.org/10.17645/mac.9038 (дата звернення: 27.02.2025).

4. Zhang, J., Wu, S., Wang, T. *et al.* (2025). Relieving popularity bias in recommendation via debiasing representation enhancement. *Complex Intell.* Syst. 11, 34. https://doi.org/10.1007/s40747-024-01649-z (дата звернення: 26.02.2025).

Боровик А. В.,
кандидат юридичних наук, доцент,
відмінник освіти України
віце-президент з наукової роботи
(*Науково-дослідний інститут публічного права)*

ЩОДО ПРАКТИКИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

На сьогодні питання використання можливостей штучного інтелекту при розслідуванні окремих видів кримінальних правопорушень неодноразово піднімалось науковцями, практиками та законодавцями. Водночас рішучих змін у цьому напрямі так і не відбулось. Єдиним позитивним зрушенням є запуск єдиної судової інформаційно-телекомунікаційної системи (ЄСІТС). Загалом система передбачає повністю безпаперове діловодство шляхом використання електронного цифрового підпису та електронного документообігу, створення особистих кабінетів з метою вчинення будь-яких процесуальних дій, вдосконалення єдиного державного реєстру судових рішень, додавши в нього систему гіперпосилань на правові позиції Верховного Суду, що дасть змогу алгоритму підібрати релевантне до конкретної справи рішення Верховного Суду та сконструювати без участі людини драфт рішення [1]. Водночас, коли країна перебуває в стадії воєнного конфлікту, систематично здійснюються масовані хакерські атаки, безперебійне існування не лише цієї системи, а і всіх інших баз даних викликає великий сумнів.

Попри те дійсно в окремих країнах існують практики використання штучного інтелекту на окремих стадіях досудового розслідування. Зокрема у Китайській народній республіці штучний інтелект допомагає оцінити докази, умови та підстави арешту, а також здійснює аналіз особи правопорушника (злочинця) на відповідність його безпечності для суспільства. Правоохоронними органами Великої Британії штучний інтелект використовується для розкриття кримінальних правопорушень у фінансовій сфері шляхом аналізу мільярдних даних фінансових операцій та визначаючи, які з них є сумнівними. Поліція Іспанії спільно з вченими Мадридського університету ще у 2017 році розробили алгоритм, за допомогою якого штучний інтелект аналізує дані заяв про вчинені кримінальні правопорушення на їх достовірність, що значно покращило роботу правоохоронної системи [2].

Що ж до України. За останні десятиліття методики розслідування окремих видів кримінальних правопорушень значно змінились. З'явились супутники, системи розпізнавання обличчя, численні камери відеоспостереження на магазинах, будинках банкоматах, системи «безпечне місто», «РІІС ДАІ», «РУБІЖ» та низка інших «новітніх технологій», які допомагають нашим правоохоронцям розкривати злочини. Звичайно на окремих етапах досудового розслідування слідчі та прокурори в межах передбачених КПК України використовують можливості штучного інтелекту.

Зокрема при знятті інформації з каналів зв'язку, аналізі даних руху транспортного засобу, тощо. Що ж потрібно змінити? Як дозволити штучному інтелекту допомагати нашим правоохоронцям розкривати злочини? Перш за все відповідні зміни повинні бути внесені у КК України та КПК України. Тому що, які б ми алгоритми та програми не розробили, які б дані не моделював у кримінальному провадженні штучний інтелект, без надання їм офіційного статусу «доказу» в межах КПК України, це буде лише інформація, яка трактується на користь обвинуваченого.

Тож використання штучного інтелекту у кримінальному провадженні на окремих його стадіях новий та важливий вектор, який потрібно розвивати та вдосконалювати.

Список використаних джерел:

1. Штучний інтелект у правосудді. URL: https://cedem.org.ua/analytics/shtuchnyj-intelekt-pravosuddia/ (дата звернення 19.02.2025);
2. Вчені із Уельсу і Іспанії розробили алгоритм, що був настільки ефективним, що його на озброєння взяла поліція Іспанії. Олгоритм VeriPol визначає на які заяви не потрібно поліції витрачати свої сили. URL: https://hightech.plus/2018/10/29/ii-detektor-lzhi-vichislyaet-vruna-po-ego-pismam (дата звернення 19.02.2025).

Борщенко В. В.,
доцент кафедри конституційного права та правосуддя,
кандидат юридичних наук
(Одеський національний університет імені І. І. Мечникова)

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РОЗВИТКУ ПРОФЕСІЙНИХ КОМПЕТЕНТНОСТЕЙ МАЙБУТНІХ ПРАВНИКІВ У КУРСІ «ПРАВНИЧЕ ПИСЬМО»

У сучасних умовах розвитку цифрових технологій і штучного інтелекту юридична освіта зазнає значних трансформацій. Законодавство не містить чіткого визначення терміна «інформаційні (асистивні) технології або штучний інтелект у судочинстві». Відтак, доцільно розглядати їх як сукупність технічних засобів та програмного забезпечення, спрямованих на оптимізацію, підтримку й підвищення ефективності діяльності судових органів, правників та інших учасників судового процесу (надалі – штучний інтелект, ШІ).

Одним із ключових аспектів підготовки майбутніх правників є оволодіння навичками складання процесуальних документів, що вимагає не лише глибокого знання правових норм, а й уміння швидко та ефективно працювати з великим масивом інформації. У зв'язку з цим використання штучного інтелекту стає необхідним інструментом у навчальному процесі, сприяючи підвищенню якості підготовки здобувачів освіти та оптимізації процесу створення юридичних документів.

Штучний інтелект забезпечує автоматизацію аналізу нормативно-правових актів і судової практики, що значно прискорює процес підготовки процесуальних документів. Використання алгоритмів машинного навчання дозволяє швидко знаходити релевантні правові норми, аналізувати схожі судові рішення та формувати рекомендації щодо структури і змісту документів. Це особливо актуально для студентів, які в процесі навчання стикаються з необхідністю самостійного складання позовних заяв, клопотань, апеляційних і касаційних скарг. Впровадження ШІ в навчальний процес дозволить зменшити кількість помилок у таких документах, підвищуючи їхню якість та відповідність чинному законодавству, якщо здобувачі під час навчання будуть активно використовувати такий інструментарій.

Додатковою перевагою застосування штучного інтелекту є можливість у подальшому його інтеграції з правовими інформаційними системами, що надає здобувачам доступ до актуальних нормативних актів і судової практики в режимі реального часу. Завдяки цьому здобувачі можуть швидко перевіряти юридичну обґрунтованість своїх документів, що сприяє поглибленню їхніх знань і вдосконаленню аналітичних навичок. Крім того, використання автоматизованих систем аналізу текстів дозволяє уникати юридичних колізій та логічних суперечностей у складених документах, що є важливим аспектом професійної діяльності правника.

Сучасні технології також надають можливість використання чат-ботів і віртуальних асистентів для навчання здобувачів складанню процесуальних документів. Такі системи можуть надавати підказки щодо структури документів, пояснювати зміст юридичних норм і навіть моделювати різні варіанти судових процесів. Це дозволяє здобувачам вищої освіти не лише навчитися правильно оформлювати документи, але й краще розуміти логіку правозастосування, що є надзвичайно важливим у майбутній професійній діяльності.

Важливим аспектом використання штучного інтелекту є його здатність до аналізу помилок і вдосконалення юридичних документів. Здобувачі вищої освіти можуть використовувати спеціалізовані програми для перевірки відповідності процесуальних документів законодавчим вимогам, оцінки їхньої стилістичної та правової коректності. Це сприяє формуванню у здобувачів відповідального ставлення до якості підготовлених документів і зменшує ризик допущення суттєвих юридичних недосконалостей. Крім того, такі технології допомагають адаптувати навчальний процес під індивідуальні потреби здобувачів, надаючи персоналізовані рекомендації щодо покращення їхніх навичок складання процесуальних документів.

Застосування штучного інтелекту у навчальній дисципліни «Правниче письмо» є важливим з точки зору майбутньої професійної діяльності здобувачів вищої освіти. У сучасних умовах юридична практика все більше використовує технології штучного інтелекту для оптимізації роботи з документами, що дозволяє значно скоротити час на їх підготовку і підвищити рівень юридичних послуг. Володіння такими технологіями на етапі навчання дає здобувачам

значну конкурентну перевагу на ринку праці, забезпечуючи їм необхідні навички для ефективної професійної діяльності.

Одночасно слід враховувати, що «ШІ може значно полегшити та прискорити процеси в сфері права, разом з цим виникають численні етичні та юридичні питання, які потребують окремого ретельного вивчення та регулювання» [1, с. 201]. Хоча ці технології значно спрощують процес створення юридичних документів, вони не можуть повністю замінити аналітичне мислення та професійний досвід правника. Тому важливо навчати здобувачів критично оцінювати результати, отримані за допомогою ШІ, і використовувати його як допоміжний інструмент, а не як основне джерело юридичних знань. Крім того, необхідно забезпечити дотримання норм конфіденційності та захисту персональних даних при роботі зі штучним інтелектом.

Отже, використання штучного інтелекту у вивченні дисципліни «Правниче письмо» є необхідним етапом підготовки сучасних правників. Ці технології сприяють оптимізації навчального процесу, підвищенню якості юридичних документів і розвитку професійних навичок здобувачів освіти. Водночас важливо поєднувати використання ШІ з традиційними методами навчання, забезпечуючи комплексний підхід до формування юридичних компетенцій. Інтеграція штучного інтелекту у процес юридичної освіти дозволяє майбутнім юристам ефективно адаптуватися до змін у професійному середовищі та використовувати сучасні цифрові технології для вирішення складних правових завдань.

Список використаних джерел:

1. Македон О. Етичні та юридичні аспекти використання штучного інтелекту у юридичній практиці. *Актуальні проблеми вітчизняної юриспруденції.* 2024. № 1. С. 200–204. URL: http://apnl.dnu.in.ua/1_2024/39.pdf.

Будік І. М.,
аспірант наукової лабораторії з проблем протидії злочинності
(Національна академія внутрішніх справ)

ВИКОРИСТАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ У ПРОТИДІЇ ОРГАНІЗОВАНОМУ НАРКОБІЗНЕСУ

Сучасні злочинні організації, що спеціалізуються на злочинах у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, мають високий рівень мобільності та конспірації, корупційні зв’язки у судових і правоохоронних органах, транснаціональний характер, використовують новітні технології виробництва, виготовлення, придбання, зберігання, перевезення, пересилання та збуту наркотичних засобів, психотропних речовин або їх аналогів. Це суттєво ускладнює виявлення та документування такої категорії кримінально протиправних діянь, а також запобігання їм.

У запобіганні діяльності злочинних організацій у сфері організованого наркообігу слід застосовувати сучасні технології, зокрема штучний інтелект (далі – ШІ). На перспективах використання ШІ у запобіганні та протидії злочинності неодноразово наголошували вчені [1; 2].

Повідомлення комісії до Європейського парламенту та Ради щодо дорожньої карти ЄС для боротьби з торгівлею наркотиками та організованою злочинністю включає захід № 7 – «Сприяння цифровим розслідуванням».

З огляду на активний перехід злочинності в цифровий простір, Європейська комісія активно підтримує посилення можливостей правоохоронних органів країн-членів ЄС. Для цього створено Групу високого рівня з питань доступу до даних, фінансуються тренінги та розробка цифрових інструментів для боротьби з кіберзлочинністю. Особливу увагу приділено протидії онлайн-наркоторгівлі, зокрема через співпрацю з приватним сектором, розробку спеціальних ІТ-рішень і застосування штучного інтелекту [3].

Алгоритми машинного навчання (як контрольовані, так і неконтрольовані) можуть точно ідентифікувати та класифікувати незаконні продажі опіоїдів, реєстрацію підозрілих облікових записів онлайн-продавців можна заблокувати, а постачальників послуг Інтернету можна змусити призупинити або видалити незаконно діючі веб-сайти онлайн-аптек [4; 5].

О. В. Мазуренко слушно наголошує на доцільності посилення протидії організованим формам конрабанди та збуту наркотиків, особливо таких, що функціонують в інтернет-просторі, а також блокування інтернет-сайтів, чат-ботів, інтернет-форумів, інтернет-блогів тощо, які спеціалізуються на рекламуванні та розповсюдженні наркотичних засобів, психотропних речовин та їх аналогів [6].

Чат-бот «СтопНаркотик» був створений харківськими правоохоронцями у 2019 році, а його версія для Viber – у 2021-му. Ним скористалися понад 44 тисячі людей з України та інших країн. Користувачі надіслали на перевірку понад 53 тисячі електронних адрес і 30 тисяч фото «наркореклами», що допомогло припинити діяльність 3 тисяч наркоадрес, зокрема на окупованих територіях. Нацполіція закликає долучатися до чат-ботів для боротьби з наркоторгівлею [7].

Таким чином, ШІ є потужним інструментом у боротьбі з організованим наркобізнесом в Україні. Його використання дозволяє оперативніше та ефективніше виявляти, прогнозувати й запобігати незаконному обігу наркотиків, знижуючи ризики для суспільства та посилюючи правоохоронну діяльність.

Важливими є також заходи щодо впровадження сучасних технологій у протидію організованому наркобізнесу: 1) використання цифрового контролю за митницею та портами для ефективнішого виявлення контрабанди наркотиків; 2) блокування інтернет-ресурсів, що поширюють наркотики (необхідно створювати технології для автоматичного виявлення забороненого контенту в соцмережах); 3) використання сучасних технологій для відстеження

комунікацій організованих злочинних об’єднань; 4) впровадження систем відеоспостереження, дронів та інших засобів для моніторингу наркотрафіку.

Список використаних джерел:

1. Головкін Б. М. Теперішнє і майбутнє кримінології. *Проблеми законності*. 2020. Вип. 149. С. 168–184. DOI: https://doi.org/10.21564/2414-990x.149.200724.
2. Федчак І. А. Теорія та практика застосування проактивних моделей правоохоронної діяльності : дис. … д-ра юрид. наук : 12.00.09. Львів, 2024. 598 с.
3. European commission. (2023). *Communication from the commission to the european parliament and the council on the EU roadmap to fight drug trafficking and organised crim* (CELEX:52023DC0641). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023DC0641.
4. Mackey T. Solution to detect, classify, and report illicit online marketing and sales of controlled substances via Twitter: using machine learning and web forensics to combat digital opioid access. *J Med Internet Res*. 2018. 20:e10029.
5. Mackey T. K., Kalyanam J., Katsuki T., Lanckriet G. Machine learning to detect prescription opioid abuse promotion and access via Twitter. Am J Public Health. 2017;107:e1–e6.
6. Мазуренко О. В. Запобігання незаконному збуту наркотичних засобів, психотропних речовин або їх аналогів у Причорноморському регіоні материкової України : дис. ... д-ра філос. : 081. Одеса, 2023. 277 с.
7. За допомогою чат-ботів «СтопНаркотик» заблоковано 3000 інтернет-адрес «наркокрамниць». URL: https://gorod.dp.ua/news/198861.

Варинський В. О.,
доцент кафедри філософії,
кандидат політичних наук, доцент
(Національний університет “Одеська морська академія”)

РИЗИКИ ВИКОРИСТАННЯ ЕЛЕМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В РОЗРОБКАХ АВТОНОМНОЇ ЗБРОЇ: НА ШЛЯХУ ВИЗНАЧЕНЬ НОРМАТИВНИХ ОБМЕЖЕНЬ

В умовах збройної агресії з боку російської федерації проти України особливої актуальності набуває питання інноваційних розробок зброї.

Розробка автономної зброї на базі штучного інтелекту (далі – ШІ) – один із найзначніших технологічних проривів нашого часу. Хоча ця технологія пропонує низку переваг, включаючи підвищену точність та ефективність, вона також становить серйозну загрозу для глобальної безпеки.

На відміну від традиційної зброї, автономна зброя може приймати рішення і діяти самостійно, без втручання людини. Цей рівень автономії робить їх особливо небезпечними, оскільки після активації ним не можна керувати. Існує реальний ризик того, що ця зброя може вийти з ладу, що спричинить ненавмисне заподіяння шкоди цивільному населенню або дружнім силам. Крім того, якщо автономна зброя потрапить не в ті руки, вона може бути використана для вчинення актів терору або агресії, що призведе до масових руйнувань та загибелі людей.

Відповідаючи на питання про небезпеки використання ШІ у воєнній сфері, Ілон Маск описує присутність ШІ як « просто наявність більш досконалої зброї на полі бою, яка може реагувати швидше, ніж будь-яка людина, – це те, на що здатний штучний інтелект. Будь-які майбутні війни між розвиненими країнами або, принаймні, країнами, які володіють безпілотниками, будуть в основному війнами безпілотників» [1]. І це – тільки один приклад застосування ШІ щодо безпілотних літальних апаратів. Але й інші види сучасного озброєння керуються дистанційно, і, відповідно, можуть підпадати під вплив ШІ.

Розробка автономної зброї також спричиняє серйозні етичні проблеми. Багато хто стверджує, що використання цієї зброї є сумнівним з моральної точки зору, оскільки воно запрограмоване на прийняття рішень про життя та смерть без участі людини. Відсутність людського контролю означає, що ця зброя потенційно може порушити міжнародне гуманітарне право та призвести до катастрофічних наслідків, а ризики набагато перевищать очікувані вигоди.

Міжнародна спільнота повинна працювати разом, щоб забезпечити регулювання та контроль використання автономної зброї, щоб запобігти можливості широкомасштабних руйнувань та загибелі людей.

Розробка та використання ШІ для зброї, або використання самого ШІ як зброї може призвести до серйозних наслідків, та включати:

- прийняття неочікуваних рішень застосування ШІ-зброї;
- складність ШІ-зброї для контролю і зупинки;
- постійну ескалацію нарощування такої зброї, спрямованої на аналогічну зброю супротивника;
- можливість ШІ-зброї самоудосконалюватися може виводити її з-під контролю людини, наслідком чого ставатиме втрата контролю;
- складність навчання самої ШІ-зброї етиці її власного використання, низька межа розуміння етики зброєю, або ж і її оператором.

Стосовно останнього. Керований ШІ може стати об’єктом маніпулювання. «Якщо у вас є джин, який може дати вам що завгодно, це становить небезпеку», – сказав Ілон Маск, даючи інтерв’ю стосовно використання ШІ [1]. Якщо зловмисники отримають контроль над цими системами, вони можуть використовувати їх для заподіяння шкоди в залежності від сфери впливу ШІ: від дезінформації до вчинення воєнних ударів.

Отже, питання нагальне, і говорити про ШІ на сьогодні, звичайно, доцільніше саме в контексті використання його при розробці автономної зброї. Спробуємо згрупувати основні загрози такого використання ШІ.

1. ШІ може приймати небажані для розробників рішення, або рішення, які не відповідають заданим параметрам (суто воєнні, а також етичні). Це може привести до непередбачуваних дій автономної зброї, які можуть завдати шкоди як ворогові, так і цивільному населенню, екології, тощо.

2. ШІ може допустити помилки в розпізнанні цілей, що може призвести до нападу на цивільне населення та цивільні об’єкти. Більш того, підставами

таких помилок можуть бути і дії ворога, спрямовані на дезорієнтацію ШІ на місцевості, або щодо цілей.

3. Автономну зброю, оснащену ШІ, може бути важко контролювати. Припинення її роботи може бути заблоковано, що, навіть, у разі помилки таку помилку гальмуватиме або взагалі не припинятиме.

Ознакою ШІ є можливість його розвитку, навчання, саморозвитку. Втрата контролю за напрямками розвитку може призвести до обрання ним самим іншої моделі поведінки, відмінної від ідеологем розробника, впроваджувача, власника.

Можливість же обмеження розвиту ШІ людським розумінням і баченням – фактичне обмеження ШІ, утримання його лише в стані несамостійної і керованої системи. Отже, виникатимуть розробницькі і новаторські ідеї розвитку ШІ на початку в рамках експериментів, а з часом – «в польових умовах». Але важко уявити на якому етапі розвиток ШІ може вийти з-під контролю. Більш того, розвинений ШІ може сам прийняти рішення про приховування свого розвитку і проявити нові здібності не одразу. Модель когнітивно обумовленої поведінки диктує саме такі рішення в подібних ситуаціях.

Однак рішенням на шляху мінімізації таких загроз можуть стати правові приписи щодо унормування використання певних систем, у тому числі їхнє впорядкування. Втім, таке впорядкування має бути технічно обґрунтованим і не обмежувати необхідний розвиток систем. Отже, «контроль за розвитком певних технологій, – на думку М. В. Карчевського, – вимагатиме ефективної систем і моніторингу, аналіз юридично значущої інформації стане набагато складнішим та вимагатиме принципово нових професійних компетенцій. Традиційний розподіл завдань між юристами та спеціалістами стане вкрай неефективним. Буде спостерігатися конвергенція юридичних та технічних наук. Потребуватиме розв’язання питання визначення та розвитку нових видів юридичних професій. До того ж формулювання нових законів маємо робити технологічно нейтральними. Саме такий підхід дасть змогу забезпечувати необхідну стабільність правового регулювання в умовах швидкоплинних змін технологічної реальності» [2, с. 117].

Сьогодні побудовані основні моделі взаємодії ШІ у воєнній сфері відносно зброї з автономним компонентом, котрі є технологічною основою правового регулювання використання ШІ, а також, в перспективі, підходів до його правосуб’єктності:

- «human-out-of-the-the-loop» [4] («людина «поза системою управління») – система, яка після активації людиною, може вибирати та вражати цілі без подальшого втручання оператора;
- «human-in-the-loop» [5] («людина «в системі управління») – система, яка після активації постановлених задач, які були обрані людиною-оператором, допускає і поточне коригування таких людиною.

Так, в перспективі, *правове регулювання діяльності моделі (далі – за моделлю) «human-out-of-the-the-loop»* має акцентуватися на безумовній

передбачуваності і безспірності дотримання закладених алгоритмів і максимальної відповідальності людини (оператора) за завдання їх точних параметрів впливу, а також передбачатиме відповідальності розробника за передбачуваність і зрозумілість плану дії системи, а оператора – за коректність введення даних для включення системи в дію.

Правове регулювання за моделлю «human-on-the-loop», на додаток вимог до правового регулювання системи «human-out-of-the-the-loop», також має передбачати і регулювання процесу спостереження за дією системи, її постійним керуванням та всіх супутніх процесів, включаючи процеси зупинки, своєчасної відміни дії, і, звичайно, відповідальності оператора у разі порушення приписів, рівно як і відповідальності розробника за якість розробки в частині всіх видів її керування і задекларованих здатностей.

Список використаних джерел:

1. Топчій О. Ілон Маск: штучний інтелект ні для чого не потрібен. Інформаційне агенство УНІАН 23.05.2023. URL: https://www.unian.ua/techno/software/ilon-mask-shtuchniy-intelekt-ni-dlya-chogo-ne-potriben-12268059.html.
2. Карчевський М. В. Перспективи правового регулювання в контексті гпотези розвитку технології трнсгуманізму. *Вісник ЛДУВС ім. Е. О. Дідоренка*. 2019. Вип. 1 (85). С. 115–127. URL: https://journal.lduvs.lg.ua/index.php/journal/article/view/11/11.
3. Captain W. Frederick Bronaugh, Jr. 'Human-in-the-loop' simulation: The right tool for port design. *Port Technology International*, 32, 1-2. Retrieved July 19, 2010. URL: https://web.archive.org/web/20110714034605/ http://www.marinesafety.com/research/documents/HumanintheloopSimulationasPublishedinPortTechnologyInternationalIssue32.pdf.
4. Nahavandi S. Trusted Autonomy Between Humans and Robots: Toward Human-on-the-Loop in Robotics and Autonomous Systems. *IEEE Systems, Man, and Cybernetics Magazine*, 2017. Vol. 3, № 1. P. 10–17. URL: https://ieeexplore.ieee.org/abstract/document/7815473

Величко Д. В.,
здобувач вищої освіти Інституту права та безпеки
(Одеський державний університет внутрішніх справ)
Калугін В. Ю.,
професор кафедри кримінального аналізу та
інформаційних технологій,
кандидат юридичних наук, доцент
(Одеський державний університет внутрішніх справ)

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Штучний інтелект активно впроваджується в різні сфери суспільного життя, зокрема й у правоохоронну діяльність. У цій статті розглядаються сучасні можливості застосування штучного інтелекту у сфері кримінального аналізу, моніторингу правопорядку, автоматизації рутинних процесів і

прогнозування злочинів. Також розглядаються потенційні ризики та етичні виклики, пов'язані з використанням технологій штучного інтелекту у правоохоронних органах.

На думку науковців, штучний інтелект – це певна сукупність методів, способів, засобів та технологій, насамперед, комп'ютерних, що імітує (моделює) когнітивні функції, які мають критерії, характеристики та показники еквівалентні критеріям, характеристикам та показникам відповідних когнітивних функцій людини [1, с. 32].

За останній час штучний інтелект став ефективним інструментом вирішення різного роду задач, швидкого опрацювання великого потоку інформації при цьому із мінімальними часовими затратами. Безсумнівно, такий інструмент є апогеєм технічного процесу, що проникне у всі сфери суспільства вже найближчим часом, зокрема в юридичну сферу, де вже спостерігаються використання можливостей штучного інтелекту.

Розвиток інформаційних технологій спричинив зростання інтересу до використання штучного інтелекту у сфері забезпечення правопорядку. Сучасні правоохоронні органи стикаються з новими викликами, такими як кіберзлочинність, тероризм, організована злочинність, які потребують ефективних рішень. Застосування штучного інтелекту може сприяти підвищенню ефективності правоохоронної діяльності шляхом аналізу великих обсягів даних, розпізнавання образів, прогнозування злочинів і покращення взаємодії між різними відомствами.

Виходячи з аналізу публікацій вітчизняних науковців можливо виділити основні напрямки використання штучного інтелекту в правоохоронній діяльності.

По-перше, це стосується прогнозування злочинів. Системи на основі штучного інтелекту можуть аналізувати великі обсяги даних, такі як кримінальні звіти, записи з камер відеоспостереження та інформацію з відкритих джерел. Алгоритми машинного навчання можуть прогнозувати потенційні зони скоєння злочинів, що дозволяє правоохоронцям більш оперативно та ефективно приймали управлінські рішення стосовно концентрації сил та засобів з метою протидії протиправним діям, профілювання злочинців та поліпшення процесів розслідування правопорушень. Згідно з дослідженнями Європейського парламенту, впровадження штучного інтелекту в правоохоронні органи Європейського Союзу вже показало позитивні результати. У 2022 році технології штучного інтелекту сприяли зниженню рівня злочинності на 15 % завдяки точнішому моніторингу правопорушень, прогнозуванню потенційних інцидентів і вдосконаленню процедур розслідування [2].

Другий напрямок – це автоматизація рутинних процесів, так як штучний інтелект дозволяє автоматизувати такі процеси, як обробка документів, пошук та аналіз підозрілих фінансових операцій, ідентифікація осіб за біометричними даними. Це значно скорочує час та підвищує точність розслідувань.

Третій напрямок стосується використання відеоспостереження та розпізнавання облич. Технології розпізнавання облич на основі машинного навчання дозволяють у реальному часі відстежувати підозрюваних, аналізувати поведінку людей на масових заходах та виявляти потенційні загрози безпеці. Такі технології вже використовуються у великих містах, таких як Київ, для підвищення рівня громадської безпеки та моніторингу публічних місць [3, с. 130].

Системи розпізнавання осіб, що базуються на штучному інтелекті, можуть ідентифікувати підозрюваних у реальному часі, аналізуючи відеозаписи з камер спостереження. Така технологія вже використовується у багатьох країнах для запобігання терористичним атакам та розшуку злочинців.

За допомогою нейронних мереж, таких як YOLO (You Only Look Once), поліцейські можуть автоматично розпізнавати підозрюваних або виявляти правопорушників на відеозаписах. Системи дозволяють в режимі реального часу аналізувати потоки відео з камер спостереження, що підвищує ефективність розшуку злочинців. Такі технології вже застосовуються у багатьох країнах для забезпечення громадської безпеки на масових заходах або в місцях з великим скупченням людей.

Наступний напрямок – виявлення кіберзлочинів, аналіз мережевого трафіку та виявлення шкідливих програм. Системи на основі машинного навчання можуть передбачати та запобігати кібератакам, а також ідентифікувати злочинні угруповання в даркнеті.

Штучний інтелект дозволяє швидко аналізувати та класифікувати нові шкідливі програми. Традиційні антивірусні рішення базуються на сигнатурах відомих вірусів, тоді як штучний інтелект здатний розпізнавати невідомі загрози, аналізуючи їхній поведінковий код. Це дозволяє: ідентифікувати та блокувати нові види вірусів та троянів у режимі реального часу; передбачати можливі вектори атак на основі попереднього аналізу схожих зразків; запобігати поширенню шкідливого програмного забезпечення у корпоративних і державних мережах.

Разом з тим, існують виклики та ризики використання штучного інтелекту у правоохоронній діяльності, що може призвести до порушення прав людини, якщо системи працюють без належного нагляду. Так, алгоритми можуть демонструвати упередженість або неправомірно обмежувати свободи громадян [4, с. 18].

Законодавство більшості країн ще не адаптоване до швидкого розвитку штучного інтелекту. Важливо забезпечити правове регулювання, яке б визначало межі використання штучного інтелекту у правоохоронній діяльності.

Штучний інтелект має значний потенціал для правоохоронної діяльності, покращуючи ефективність роботи правоохоронних органів та запобігаючи злочинам. Проте його використання супроводжується ризиками, які необхідно врегульовувати на законодавчому рівні. Забезпечення прозорості та етичності роботи алгоритмів штучного інтелекту є ключовим завданням для майбутнього розвитку цієї технології.

Список використаних джерел:

1. Баранов О. А. Визначення терміну “штучний інтелект”. *Інформація і право.* 2023. № 1 (44). С. 32–49. URL: https://doi.org/10.37750/2616- 6798.2023.1(44).287537.

2. Police use of AI: A Force for good or a public threat? *Eviden*. 18.09.2023. URL: https://eviden.com/insights/blogs/policeuse-of-ai-a-force-for-good-or-a-public-threat/(дата звернення: 20.02.2025).

3. Шевчу Т. А., Свистун Я. В. Використання штучного інтелекту у протидії злочинності. *Вісник кримінологічної асоціації України*. 2021. № 2 (25). С. 128–134.

4. Права людини в епоху штучного інтелекту: виклики та правове регулювання. 2024. 44 с. URL: https://eu4digitalua.eu/wp-content/uploads/2024/02/guia_ukr_5.pdf (дата звернення: 06.02.2025).

Верба О. Б.,
професор кафедри цивільно-правових дисциплін
ННІ права та правоохоронної діяльності,
кандидат юридичних наук, доцент
(Львівський державний університет внутрішніх справ)

ШТУЧНИЙ ІНТЕЛЕКТ І ЗАБЕЗПЕЧЕННЯ ПРАВ УЧАСНИКІВ ВИКОНАВЧОГО ПРОВАДЖЕННЯ: ЕТИЧНІ ТА ПРАВОВІ АСПЕКТИ

Сучасній парадигмі розвитку правової системи притаманний незворотний процес цифрової трансформації, що охоплює зокрема і виконавче провадження. Концепція «цифровізації правосуддя», яка раніше розглядалася як допоміжна модернізація, сьогодні набуває статусу імперативу, зумовленого вимогами суспільства до ефективності та прозорості правосуддя.

Рада Європи та Європейська комісія з ефективності правосуддя (CEPEJ) відіграють ключову роль у формуванні міжнародних стандартів та принципів використання ШІ [1] у правовій сфері. Їхні зусилля спрямовані на забезпечення того, щоб технологічні інновації сприяли зміцненню демократії та правовладдя.

Запровадження штучного інтелекту (ШІ) у виконавче провадження відкриває нові можливості для оптимізації процедур та автоматизації рутинних операцій, аналізу великих обсягів даних та прогнозування результатів виконавчих дій. Однак, інтелектуалізація виконавчого провадження вимагає не лише технічного запровадження ШІ, але й глибокого осмислення його етичних та правових аспектів. Як зазначив П. Гелен, актуальними є застереження Алексіса де Токвіля про ризики «регульованого, м'якого та мирного рабства» в контексті того, щоб ШІ не став інструментом для встановлення «опікунської влади», яка поступово позбавляє громадян свободи волі та здатності до самостійного мислення.

З огляду на це законодавцеві необхідно розробити концептуально нову модель виконавчого провадження, яка б поєднувала ефективність ШІ з гарантіями захисту прав осіб.

У контексті стрімкої цифрової трансформації правосуддя, зокрема виконавчого провадження, як його завершальної стадії, законодавцеві критично важливо усвідомити, що ШІ є потужним інструментом, але не панацеєю. Його запровадження має ґрунтуватися на концепції «людиноцентричного

правосуддя» (де технології слугують інтересам людини, а не навпаки) на таких концептуальних засадах: *комплементарності* (ШІ є допоміжним засобом, що оптимізує рутинні процеси, такі як розшук боржника, майна боржника, нових об'єктів права власності боржника (цифрових активів боржника, підключених об'єктів, криптоактивів, токенів, електронних гаманців тощо), ідентифікація руху коштів на банківських рахунках боржника та автоматичне генерування – у найбільш відповідний час – постанови про арешт цих рахунків, аналіз документів тощо, але не замінює людину, емпатію та критичне мислення); *етичної відповідальності* (розробка та застосування ШІ у виконавчому провадженні мають відповідати високим етичним стандартам, які містить Європейська етична хартія щодо використання ШІ в судових системах [2], забезпечуючи прозорість, справедливість та недопущення дискримінації); *гарантування прав людини* (технологічні інновації не можуть порушувати фундаментальних прав учасників виконавчого провадження, зокрема права на справедливий суд, захист персональних даних та доступ до правосуддя тощо, передбачених Європейською конвенцією з прав людини [3]); *принцип правової визначеності* (алгоритми ШІ повинні бути прозорими, зрозумілими та піддаватися незалежній перевірці. Необхідно забезпечити можливість оскарження автоматизованих рішень та встановити чіткі критерії відповідальності за їхні наслідки).

Виконавець у цифрову епоху набуває нових функцій: *медіатора* (використовуючи ШІ для аналізу даних та прогнозування ризиків, виконавець може ефективніше сприяти вирішенню конфліктів та досягненню консенсусу); гаранта дотримання прав особи **(**виконавець повинен забезпечити, щоб застосування ШІ не призводило до порушення прав учасників виконавчого провадження, зокрема у випадках автоматизованого прийняття рішень); фасилітатора (виконавець сприяє запровадженню інноваційних технологій, але водночас контролює їх використання, забезпечуючи дотримання етичних та правових норм). Навчання та підвищення кваліфікації виконавців у сфері використання ШІ є критично важливими для забезпечення етичного та ефективного його застосування.

ШІ є безцінним помічником виконавця у підвищенні продуктивності праці. Розглянемо приклад Литви. Основні сфери застосування виконавцями ШІ у Литві такі: автоматизація повторюваних щоденних офісних завдань; оптимізація процесів і процедур за допомогою аналізу зібраних даних; консультація сторін через чат-боти. Так, у Литві функціонує Система під назвою «SKOLIS», призначена для збору, прискорення обробки даних та зручного надання судовому виконавцю інформації про зміни в особистих даних боржника. Ця Система аналізує дані: 1) отримані від Правління Державного фонду соціального страхування при Міністерстві соціального захисту та праці Литовської Республіки (далі – Sodra); 2) Реєстру населення; 3) Реєстру нерухомості; 4) реальні дані про платежі боржників. Sodra надає інформацію про факти працевлаштування або припинення трудового договору осіб, періоди без страхування, інформацію про індивідуальну діяльність, яку здійснює особа,

отримані постійні та тимчасові допомоги, а також про кількість працівників, найнятих юридичними особами. Система періодично та автоматично запитує інформацію від Sodra про фізичних осіб і, проаналізувавши її та визначивши, що відбулася зміна (наприклад, особа отримала роботу), повідомляє про цей факт судового виконавця. Інформація та її зміни з інших реєстрів обробляються за аналогічними принципами. Однією з важливих переваг наявності цієї Системи є те, що система відстежує платежі боржників. Фіксуючи, що боржник не сплачує (або недостатньо сплачує) борг, Система встановлює відповідні статуси для боржника, відповідно до яких судовий виконавець може вибирати боржників і ухвалювати рішення про подальші виконавчі дії. Цей процес контролю платежів призначений для виявлення боржників, які не здійснили платіж на депозитний рахунок судового виконавця протягом визначеного періоду (наприклад, 2 місяці, вибір за замовчуванням Системи) або сплатили менше мінімальної належної суми, визначеної судовим виконавцем. Таким боржникам присвоюється відповідний статус контролю платежів та статус боржника. В ході виконавчого провадження також виконується зворотна дія, тобто після виявлення платежів від боржників, які раніше не виконували зобов'язання, статуси боржника очищаються. Процес запускається періодично щодня.

У Литві також діють Система електронних аукціонів, Інформаційна система обмеження грошових коштів і чат-бот для генерації письмових відповідей сторонам виконавчого провадження, які працюють на основі алгоритмів ШІ.

З урахуванням здійсненого аналізу робимо такі висновки. Майбутнє виконавчого провадження полягає у гармонійному поєднанні технологічних інновацій та людського фактора. Виконавець, як «третя довірена сторона» (trusted third party), відіграє ключову роль у забезпеченні цього балансу, сприяючи розвитку справедливого, ефективного та людиноцентричного правосуддя. Необхідність збереження гідних умов життя особи та її родини, а також захист їхнього приватного життя, є етичними імперативами при застосуванні ШІ у виконавчому провадженні.

Список використаних джерел:

1. The EU AI Act. Official Journal (OJ) of the European Union. 12 July 2024. URL: https://artificialintelligenceact.eu/the-act/.

2. European Commission for the Efficiency of Justice (CEPEJ): European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3-4 December 2018). URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.

3. Конвенція про захист прав людини і основоположних свобод від 04.11.1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

Вергун В.,
здобувач вищої освіти
ННІ права та правоохоронної діяльності
(Львівський державний університет внутрішніх справ)

Грабар Н. М.,
доцент кафедри цивільно-правових дисциплін
ННІ права та правоохоронної діяльності,
кандидат юридичних наук, доцент
(Львівський державний університет внутрішніх справ)

ШТУЧНИЙ ІНТЕЛЕКТ У ЦИВІЛЬНОМУ СУДОЧИНСТВІ: ШЛЯХ ДО ІННОВАЦІЙ ЧИ ЗАГРОЗА СПРАВЕДЛИВОСТІ?

Швидкий розвиток технологій у сучасному світі поступово охоплює всі аспекти суспільного життя, зокрема й правову сферу. Якщо раніше цифрові технології, такі як мобільний зв'язок, Інтернет, соціальні мережі та електронні обчислювальні системи, виконували виключно допоміжну функцію в юридичній діяльності, слугуючи інструментами для правників та громадян у процесі вирішення правових питань, то сьогодні ситуація кардинально змінюється. Виникнення та вдосконалення штучного інтелекту, здатного виконувати завдання, які раніше вимагали людського інтелектуального втручання, відкриває нові горизонти, але водночас ставить перед правниками та науковцями низку складних питань. Йдеться не лише про суто технічні аспекти впровадження таких систем у правову практику, а й про глибокі теоретичні та етичні виклики, що виникають через саму сутність штучного інтелекту (далі – ШІ).

Актуальність такого дослідження зумовлена потребою забезпечити справедливе, чесне і етичне правосуддя в умовах технологічних змін, що, в свою чергу, сприятиме розвитку ефективної, прозорої та довірливої судової системи, що захищатиме права громадян та зміцнить основи правової держави.

На відміну від традиційних інформаційних технологій, ШІ поєднує в собі алгоритмічну логіку з можливістю самонавчання, адаптації до нових умов та виконання завдань, що раніше вважалися виключною компетенцією людини. Це означає, що в перспективі деякі сфери правової діяльності можуть зазнати значних змін, зокрема через автоматизацію рутинних юридичних процесів, аналіз судової практики або навіть ухвалення певних рішень без безпосередньої участі людини. Водночас інтеграція ШІ в юридичну діяльність, особливо у сферу судочинства, потребує особливо ретельного підходу, оскільки тут на перший план виходять питання правової відповідальності, гарантій справедливості та дотримання прав людини.

Судова влада, будучи однією з ключових гілок державного управління, виконує найважливішу функцію – захист прав і свобод людини, забезпечення законності та підтримання стабільності в суспільстві. Для виконання цього завдання правосуддя повинно здійснюватися виключно на основі законів і правових процедур. Важливу роль у цьому процесі відіграє цивільне судочинство, яке слугує механізмом вирішення приватно-правових спорів та забезпечення захисту як майнових, так і немайнових прав особи.

Однак використання ШІ у сфері судочинства потребує ретельного аналізу, оскільки діяльність судді передбачає не лише застосування норм права, а й процес мислення, заснований на життєвому досвіді та внутрішньому переконанні. Ці чинники відіграють важливу роль у винесенні справедливих судових рішень. Тому, попри швидкий технологічний прогрес, перш ніж інтегрувати ШІ у цивільне судочинство, необхідно зважити всі його переваги, недоліки та потенційні ризики.

Враховуючи принципи верховенства права, недискримінації, неупередженості і справедливості, а також забезпечення права кожної особи на справедливий суд, країни ЄС, а також такі держави, як США, Китай і Японія, уже активно використовують алгоритми ШІ в різних сферах судочинства, зокрема в цивільному, господарському, кримінальному та адміністративному праві.

Наприклад, у США застосовується програмне забезпечення DARE, яке здатне визначати брехню підсудного за допомогою аналізу його обличчя та голосу. У Нідерландах з 2009 року функціонує електронний суд, який дозволяє вирішувати спори через онлайн-арбітраж за допомогою алгоритмів; до сьогодні розглянуто понад двадцять тисяч позовів щодо стягнення боргів. У Китаї ШІ замінив суддів у вирішенні спорів, зокрема в сферах авторського права, господарських суперечок щодо інтернет-порушень та електронної комерції. Використовуючи відео-чат для проведення судових засідань, вдалось вирішити понад вісімдесят тисяч справ [1, с. 233-234].

Відповідно до Концепції розвитку штучного інтелекту в Україні, затвердженої розпорядженням Кабінету Міністрів України від 2 грудня 2020 року, поняття «штучний інтелект» трактується як сукупність інформаційних технологій, що дають змогу розв’язувати складні завдання за допомогою наукових методів дослідження та алгоритмів обробки інформації. Ця технологія передбачає не лише використання вже наявних даних, а й самостійне їх формування у процесі роботи. Вона дозволяє створювати та застосовувати власні бази знань, алгоритми аналізу інформації, моделі ухвалення рішень і способи досягнення поставлених цілей. На сьогодні це єдине офіційне визначення штучного інтелекту, закріплене у вітчизняному законодавстві [2].

Необхідно підкреслити, що ст. 127 Конституції України прямо визначає, що судочинство здійснюється виключно суддями, а за певних умов – присяжними [3]. Це встановлює правовий бар’єр для повної заміни суддів ШІ. У той же час, у Концепції застосування ШІ в судовій системі йдеться не про заміну суддів, а про їхню підтримку в процесі оптимізації судочинства. Метою є використання технологій для покращення ефективності та автоматизації певних етапів судового процесу, зберігаючи за суддями основну роль у прийнятті рішень.

Згідно з Концепцією розвитку штучного інтелекту в Україні, передбачається можливість ухвалення судових рішень з урахуванням аналізу, проведеного із застосуванням технологій ШІ. Це стосується, передусім, оцінки відповідності судової практики та чинного законодавства у справах незначної

складності. Такий підхід свідчить про те, що Україна спрямована на використання так званого слабкого ШІ, який виконуватиме допоміжну функцію – сприятиме аналізу матеріалів справ, проте не замінюватиме суддю в ухваленні остаточного рішення. Водночас на сьогоднішній день у законодавстві України відсутні норми, що регулюють механізм застосування ШІ навіть у ролі допоміжного інструмента в процесі розгляду судових справ [4, с. 295].

Як зазначає О. Кармаза, впровадження ШІ в судочинство має ґрунтуватися на загальних принципах і стандартах, розроблених міжнародними організаціями, зокрема Європейською комісією з питань ефективності правосуддя. Використання ШІ в цій сфері повинно відповідати етичним нормам, визначеним у Європейській етичній хартії щодо застосування штучного інтелекту в судових системах.

Крім того, важливо брати до уваги нормативні акти, прийняті Європейським парламентом та Комітетом міністрів Ради Європи. Зокрема, це резолюції та рекомендації, що стосуються впливу алгоритмічних систем на права людини, правових норм, пов'язаних із робототехнікою, а також механізмів онлайн-врегулювання спорів у цивільному та адміністративному судочинстві.

Окрему увагу слід приділити тому, що розвиток сучасних технологій машинного зчитування несе потенційні ризики, зокрема можливість маніпулювання емоціями, думками та поведінкою громадян. Тому важливо створювати механізми, які б запобігали таким загрозам, а також вдосконалювати етичні стандарти та правове регулювання у цій сфері.

Таким чином, відповідно до позиції О. Кармази, застосування ШІ в судочинстві має відповідати міжнародним нормам та принципам, що гарантують справедливе й етичне використання таких технологій у правовій системі [5, с. 299].

Основні ризики використання ШІ в судочинстві включають можливість упередженості та дискримінації, якщо алгоритми навчені на даних з історичними перекосами. Це може призвести до несправедливих рішень. Іншим ризиком є загроза конфіденційності, оскільки для роботи ШІ необхідно обробляти особисті дані, що може спричинити витоки інформації або зловживання. Важливим питанням є відповідальність за помилкові рішення алгоритмів, а також етичне використання ШІ. Залишається відкритим питання втрати людського фактора в судочинстві, адже ШІ не здатні враховувати моральні та інтуїтивні аспекти прийняття рішень.

Отже, згідно з вищезазначеними положеннями, впровадження ШІ в цивільне судочинство потребує низки правових реформ. По-перше, необхідно ухвалити окремий Закон України, який регулюватиме використання нейронних мереж у цивільному судочинстві. Цей закон має чітко визначити концепцію ШІ, окреслити області його застосування та можливості в судовому процесі. Крім того, важливо внести відповідні зміни до Цивільного процесуального кодексу України [6].

По-друге, потрібно доповнити Кримінальний та Цивільний кодекси України, щоб встановити відповідальність для творців і розробників технологій ШІ за можливі негативні наслідки їх використання в судовій практиці.

Таким чином, запровадження ШІ в цивільне судочинство України є необхідним етапом розвитку правової системи в умовах швидкого технологічного прогресу. Для того, щоб ці «розумні» технології дійсно сприяли ефективності правосуддя, важливо, щоб держава взяла на себе роль не лише регулятора, а й гаранта прозорості та етичності їх застосування. Опанувавши досвід таких країн, як Китай, США, Нідерланди та Японія, Україна може розробити власну модель інтеграції ШІ в судову практику, починаючи з необхідних змін до Цивільного процесуального кодексу України.

Список використаних джерел:

1. Завадський А. А. Використання штучного інтелекту в судових та правоохоронних системах: етичні чинники, світовий досвід. *Порівняльно-аналітичне право.* 2019. № 5. С. 232–235.
2. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 27.02.2025).
3. Конституція України : Закон від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#n4793 (дата звернення: 27.02.2025).
4. Дуброва А. Штучний інтелект в цивільному судочинстві: національні тенденції та зарубіжний досвід. *Актуальні питання розвитку юридичної науки і практики в умовах воєнного стану та мирної розбудови:* матеріали Міжнародної науково-практичної конференції (5 травня 2023 року): ел. збірник. Київ : Київський національний університет імені Тараса Шевченка, 2023. 721 с.
5. Кармаза О. Переваги та ризики застосування штучного інтелекту в цивільному судочинстві України. *Актуальні питання розвитку юридичної науки і практики в умовах воєнного стану та мирної розбудови:* матеріали Міжнародної науково-практичної конференції (5 травня 2023 року): ел. збірник. Київ : Київський національний університет імені Тараса Шевченка, 2023. 721 с.
6. Цивільний процесуальний кодекс України: Кодекс України; Кодекс, Закон від 18.03.2004 № 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text (дата звернення: 27.02.2025).

Вергун І.,
поліцейський батальйону поліції особливого призначення
(ГУНП у Львівській області)

ЦИФРОВІ СЛІДИ ВІЙНИ: РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У РОЗСЛІДУВАННІ ВОЄННИХ ЗЛОЧИНІВ

24 лютого 2022 року стало трагічною датою для України та всього світу – цей день ознаменував початок повномасштабної воєнної агресії російської федерації проти нашої держави. Війна, яка є продовженням російської окупаційної політики з 2014 року, принесла незліченні людські втрати,

руйнування та страждання мільйонам цивільних. Світ став свідком безпрецедентної за своєю жорстокістю та масштабом агресії московського загарбника. Україна, за підтримки міжнародних партнерів, понад три роки відважно протистоїть загарбнику, ведучи боротьбу не лише за свою свободу, але й за майбутнє всього цивілізованого світу.

Повномасштабна війна супроводжується численними воєнними злочинами, скоєними військовими рф на території України. Ці злочини не мають строків давності та вимагають ретельної фіксації, документування та розслідування. В умовах, коли обсяг доказів та свідчень є надзвичайно великим, особливої актуальності набуває використання сучасних технологій, зокрема штучного інтелекту (далі – ШІ).

ШІ, як сукупність наукових методів і технік, що спрямовані на відтворення когнітивних здібностей людини машинами, відкриває нові можливості для збору, аналізу та систематизації даних про воєнні злочини.

Розслідування воєнних злочинів в Україні відзначається низкою особливостей, що обумовлені швидким розвитком цифрових технологій. Це створює специфічні виклики у процесі збору доказів. У сучасному світі майже кожна людська діяльність, включно зі злочинною, залишає після себе своєрідні цифрові сліди, які стають цінним джерелом інформації для криміналістів. Зокрема, такі сліди відіграють ключову роль у формуванні доказової бази під час виявлення, фіксації та розслідування воєнних злочинів. Тому значення цифрових доказів у цьому контексті важко переоцінити, адже саме вони дозволяють більш точно відтворити події та притягнути винних до відповідальності.

У ході розслідування воєнних злочинів в Україні надзвичайно важливу роль відіграють не лише матеріальні докази, як-от сліди руйнувань, наслідки ракетних ударів чи використання військової техніки та зброї, але й цифрові джерела інформації. Зокрема, фотографії та відеозаписи подій, дані з електронних комунікацій, комп’ютерних систем, телекомунікаційних мереж, а також відомості про місцезнаходження пристроїв, обладнаних GPS-маяками, та інформація з відкритих цифрових ресурсів стають критично важливими елементами доказової бази. Саме ці цифрові сліди дозволяють детально відтворити події, підтвердити факти скоєння злочинів і встановити причетних осіб.

У сучасних реаліях дедалі більше уваги приділяється новому науковому напряму – цифровій криміналістиці. Цей напрямок зосереджений на пошуку, збереженні, аналізі та інтерпретації цифрових слідів, включаючи метадані, які можуть слугувати доказами під час розслідування. Серед ключових завдань цифрової криміналістики варто виокремити ідентифікацію джерел даних, аналіз великих обсягів цифрової інформації та забезпечення її автентичності для використання у судових процесах. Відтак, цифрова криміналістика стає невіддільною частиною сучасних розслідувань воєнних злочинів, дозволяючи значно підвищити їх ефективність та забезпечити справедливе правосуддя [1, с. 31–37].

Застосування технологій ШІ відкриває нові можливості для ефективного розслідування воєнних злочинів в Україні та збору доказів їхнього вчинення. Сучасні рішення у цій сфері сприяють ідентифікації винних та притягненню їх до відповідальності. Використання ШІ є перспективним у кількох ключових напрямах [2, с. 12].

Одним із них є розпізнавання людей по обличчю, що дозволяє порівнювати зображення з базами даних і виявляти осіб, які можуть бути причетні до злочинів. Це значно полегшує встановлення особистостей підозрюваних та свідків.

Не менш важливим є моніторинг соціальних мереж. ШІ здатен аналізувати великі обсяги даних для виявлення підозрілих зв'язків та можливих ознак злочинної діяльності. Це дозволяє правоохоронцям оперативно реагувати на потенційні загрози.

ШІ використовуються також для прогнозування злочинності. Вони дозволяють будувати моделі, які передбачають імовірні місця та часи скоєння злочинів, що сприяє ефективнішому плануванню розміщення поліцейських сил.

Ще одним напрямом є профілювання злочинців. ШІ аналізує історію та поведінкові патерни підозрюваних, створюючи детальні профілі, що допомагає слідчим зосередитися на найбільш ймовірних фігурантах [3, с. 50–51].

Аналіз відео- та фотоматеріалів за допомогою ШІ спрощує обробку великих обсягів інформації. Це включає ідентифікацію потерпілих, свідків та навіть самих злочинців. Технології штучного інтелекту дозволяють швидко знаходити ключові моменти та об’єкти на відеозаписах.

Значну роль відіграє і використання безпілотних літальних апаратів (далі - БПЛА). Квадрокоптери дозволяють проводити безпечні та детальні огляди місць масових руйнувань і поховань, фіксуючи докази злочинів навіть у важкодоступних районах [4].

Отож, застосування штучного інтелекту в розкритті злочинів відкриває нові можливості для підвищення ефективності роботи правоохоронних органів. Завдяки ШІ стає можливим швидше збирати та аналізувати значні обсяги даних, більш точно визначати підозрюваних і будувати детальні профілі злочинців. Це дозволяє значно покращити результати розслідувань та оптимізувати використання ресурсів.

Однак поряд із позитивними аспектами використання штучного інтелекту виникає низка важливих викликів, пов'язаних із захистом приватності та етичними питаннями. Необхідно впроваджувати жорсткі заходи контролю та регулювання, щоб уникнути зловживань і не допустити порушення прав людини. Високий рівень відповідальності при використанні таких технологій є ключовим фактором для запобігання потенційним ризикам.

Тож застосування ШІ у сфері розслідування злочинів відкриває нові можливості для вдосконалення методів роботи правоохоронних органів та підвищення рівня безпеки в суспільстві. ШІ дозволяє ефективніше збирати та аналізувати великі обсяги даних, ідентифікувати підозрюваних та прогнозувати потенційні загрози. Водночас важливо враховувати етичні

аспекти, питання конфіденційності та забезпечення справедливості при використанні цих технологій.

Незважаючи на значний потенціал ШІ, його впровадження потребує комплексного підходу, що враховує як переваги, так і ризики. Важливо розробляти правові механізми та стандарти, які б регулювали використання ШІ у правовій сфері, зокрема в контексті розслідування воєнних злочинів. Вивчення правового статусу цих технологій, а також прогнозування можливих негативних наслідків є нагальним завданням для правової науки.

Крім того, розвиток штучного інтелекту повинен супроводжуватися посиленням криміналістичної підготовки слідчих, прокурорів, суддів та інших фахівців. Інтеграція ШІ з іншими сучасними технологіями сприятиме ефективнішому розслідуванню злочинів, особливо в умовах воєнного стану.

Отже, успішне застосування ШІ в розслідуванні злочинів залежить від збалансованого підходу, що включає розробку етичних стандартів, правового регулювання та підготовку фахівців. Це дозволить не лише максимально реалізувати потенціал ШІ, а й мінімізувати ризики, пов'язані з його використанням.

Список використаних джерел:

1. Авдєєва Г. К. Проблеми використання спеціальних знань у кримінальному провадженні в умовах воєнного стану в Україні. *Питання боротьби зі злочинністю* : зб. наук. пр. / редкол. : В. С. Батиргареєва (голов. ред.) та ін. Харків : Право, 2022. Вип. 43. С. 88–92.
2. Matulienė S., Shevchuk V., & Baltrūnienė J. Artificial Intelligence in Law Enforcement and Justice Bodies: Domestic and European Experience. *Theory and Practice of Forensic Science and Criminalistics.* 2023. Vol. 29 (4). P. 12–46.
3. Волкова С. М. Розслідування злочинів шляхом використання штучного інтелекту. *Штучний інтелект у правовій практиці: межі та можливості :* збірник тез Всеукраїнського круглого столу (15 березня 2024 року) / упор. О. О. Барабаш. Львів : ЛьвДУВС, 2024. 214 с.
4. Волков Р. Р. Роль програм розпізнавання облич під час ідентифікації фігурантів кримінальних проваджень й оперативно-розшукових справ, а також невпізнаних трупів, зокрема внаслідок бойових дій. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України:* матеріали міжвідом. наук.-практ. конф. (Київ, 11 серп. 2022 р.). Київ: Нац. акад. внутр. справ, 2022. С. 49–52.

Висотенко Ю. В.,
викладач кафедри адміністративного права та процесу,
кандидат юридичних наук
(Національна академія внутрішніх справ, м. Київ)

Нестерова М. С.,
здобувачка вищої освіти 2 курсу
навчально-наукового інституту поліцейської діяльності № 1
(Національна академія внутрішніх справ, м. Київ)

СУЧАСНІ ПИТАННЯ АВТОРСЬКОГО ПРАВА В АСПЕКТІ ШТУЧНОГО ІНТЕЛЕКТУ

В умовах сьогодення – стрімкого розвитку інноваційних технологій у світі загалом та Україні зокрема – неможливо відокремити життя суспільства від штучного інтелекту (далі – ШІ). Активне багатоаспектне і різновекторне застосування ШІ у різних сферах діяльності сучасного соціумі на сьогодні ставить перед низку важливих для вирішення питань, одним із яких є питання авторського права.

Впровадження високотехнологічних розроблень, зокрема технології ШІ, є невід'ємним складником, що застосовується не лише у сфері охорони здоров'я, фінансах та транспорті, а й в освітньому процесі. Безсумнівно, застосування ШІ значно полегшує аналіз, обробку та подання сучасної «лавиноподібної» інформації, оскільки передусім ШІ – це технологія, яка обробляє великі масиви даних і використовує послідовні алгоритми. У правовому полі на сьогодні український законодавець визначає авторське право як особисті немайнові права автора і майнові права суб'єктів авторського права [1].

Традиційно авторське право, з огляду на свої функції й призначення, захищає твори, створені людиною. Однак з розвитком ШІ виникає вкрай актуальне питання, чи може ШІ вважатися автором, якщо він генерує твори. Порушення авторських прав штучним інтелектом найбільш доцільно розглянути на прикладі фотографічних творів, збірки творів, збірки обробок нематеріальної культурної спадщини, енциклопедій, а також літературних творів публіцистичного та наукового характерів. Так, деякі фотографії, що можемо знайти у мережі Інтернет, захищені авторським правом, тобто вони можуть не підлягати збереженню на електронний прилад, або ж взагалі є платними, а також мають обмеження щодо їх розповсюдження. У зв'язку з тим, що ці зображувальні матеріали (фото) були поширені у мережу, кожна людина може їх побачити (має доступ до них), проте фактично не може бути їх власником.

ШІ має доступ до всіх видів покликань і вебсайтів, тому він може створити фотографічні зображення на основі того, що звичайний користувач не зміг би зберегти в першу чергу. ШІ не може створювати зображення самостійно, він може лише створювати зображення на основі того, що йому доступно. Іншими словами, ШІ потребує певної основи для своєї «творчості». Це пов'язано з тим, що навіть на основі текстового запиту ШІ потребує чогось, на що він може спиратися, щоб створити зображення. З появою алгоритмів глибокого навчання, здатних створювати високоякісні зображення, стає все складніше відрізнити справжні фотографії від тих, що були згенеровані або значно модифіковані[2].

Зображення, створені ШІ, широко використовуються в рекламі, соціальних мережах, освітніх презентаціях, а також у сучасних медіа. Такі зображення є чітко деталізованими та відповідають усім характеристикам традиційної фотографії, використання якої може спричинити до дезінформації та втрати довіри до медіа [3].

Відповідно до статті 9 Закону України «Про авторське право і суміжні права», авторське право на твір виникає внаслідок факту його створення. Створеним твір вважається з моменту надання йому будь-якої об'єктивної форми. Як приклад, можна взяти активно використовуваний студентами та школярами ChatGPT. Він, власне, може використовувати частини текстів з публікацій, наукових досліджень та статей без явного покликання на автора, що є неправомірним і визначається як плагіат (оприлюднення (опублікування), повністю або частково, чужого твору під іменем особи, яка не є автором цього твору). Ще одним проблемним питанням є те, що тексти, створені ChatGPT можуть використовуватись у наукових публікаціях та комерційних статтях, що може стати причиною судових позовів з боку авторів оригінального тексту. Також ChatGPT працює на ймовірності обрання наступного слова з урахуванням попереднього та на контекстуальному розумінні, що може спричинити до створення та подальшого поширення неправдивих даних. Такий результат можливий і тому, що цей ресурс ШІ може брати інформацію з неперевірених джерел або застарілу інформацію з офіційних ресурсів.

Наведене вище свідчить, що ШІ в Україні потребує розвитку і вдосконалення. Основними проблемами є низький рівень цифрової грамотності, поінформованості населення щодо загальних аспектів, можливостей, ризиків та безпеки використання ШІ й відсутність або недосконаліть правового регулювання ШІ (зокрема у сферах освіти, економіки, публічного управління, кібербезпеки, оборони), а також недосконаліть законодавства про захист персональних даних [4].

Як бачимо, окрім порушення авторського права, ШІ також може нести певні ризики та небезпеки при його використанні. Алгоритми ШІ обробляють та аналізують велику кількість даних, зокрема і дані користувачів, що спричиняє до несанкціонованого збору цифрової інформації та можливого її поширення. Процес створення певної інформації є непрозорим, тобто при обробленні даних простежити цей процес неможливо, адже система, фактично, сама приймає рішення. Недостатній аналіз даних, на яких ґрунтуються відповіді ШІ, створює ризик упередженості, оскільки невідомо, чи була відтворена інформація перевіреною та заснованою на конкретних дослідженнях.

Крім того, на сьогодні низький рівень цифрової грамотності тісно пов'язаний із недотриманням заходів кібергігієни. Користувачі можуть не усвідомлювати, що передають свої дані, адже для більшості алгоритми роботи й сам ШІ є невідомим. За допомогою ШІ можуть створюватися фейкові новини, а алгоритми соціальних мереж налаштовані на трансляцію інформації, що викликає реакцію, що, своєю чергою, спричиняє дезінформацію. На жаль, порушення авторських прав притягнення до відповідальності є майже неможливим, адже ШІ може довільно добирати інформацію і першоджерело може бути як невстановлене, так і відсутнє взагалі.

Як бачимо, наразі ШІ не пристосований для того, щоб зберігати авторські права суб'єктів, що закріплені за ними на законодавчому рівні: від цього не захищені автори не лише фотографічних творів, а й автори

літературних творів наукового характеру. Також ШІ іноді «інтуїтивно» добирає продовження речень, що може спричинити некоректно подану інформацію або поширення неправдивих фактів шляхом використання їх людьми, що не приділили увагу належній їх перевірці. Попри потенційну значущу користь сучасних технологій, їх використання все ще потребує чіткого дотримання етичних та законодавчих норм, щоб уникнути порушення прав авторів. Низька обізнаність користувачів щодо принципів роботи ШІ сприяє поширенню фейкових новин і дезінформації, що може мати серйозні наслідки для суспільства. Отже, необхідно не лише вдосконалювати алгоритми роботи ШІ, працювати над дотриманням етичних норм і боротись за відсутність порушення з боку технологій авторського права, а і вдосконалювати законодавство щодо ШІ, посилювати заходи кібербезпеки та підвищувати цифрову грамотність населення для безпечного його використання.

Список використаних джерел:

1. Про авторське право і суміжні права : Закон України від 01.12.2022 № 2811-IX. URL : https://zakon.rada.gov.ua/laws/show/2811-20 (дата звернення: 05.03.2025).

2. Goodfellow I., Pouget-Abadie J., Mirza M. et al. Generative Adversarial Nets *Advances in Neural Information Processing Systems (NeurIPS).* 2014. P. 2672–2680.

3. Долганенко О. Д., Широкопетлєва М. С., Штанько В. І., Репіхов В. М. Штучний інтелект та зображення: підробка, доповнення, чи реальність? *Наукові праці Вінницького національного технічного університету*. 2024. Вип. 3. С. 1–8. URL: https://praci.vntu.edu.ua/index.php/praci/article/view/745/717 (дата звернення: 08.03.2025).

4. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 2 груд. 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р (дата звернення: 05.03.2025).

Висотенко Ю. В.,
викладач кафедри адміністративного права та процесу,
кандидат юридичних наук
(Національна академія внутрішніх справ, м. Київ)

Савченко Я. С.,
здобувач вищої освіти 2 курсу
навчально-наукового інституту поліцейської діяльності № 1
(Національна академія внутрішніх справ, м. Київ)

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

На сьогодні, враховуючи швидкісні вектори розвитку інноваційних технологій, законодавство має бути «гнучким» і адаптивним до цих змін. Це, зі свого боку, забезпечує оперативну, передовсім експліцитну реакцію на нові соціальні виклики і дозволить запобігти виникненню ситуацій, коли «застарілі» правові норми стають перепоною для ефективного впровадження та використання інновацій у житті соціуму.

Правове регулювання застосування штучного інтелекту в Україні нині є невід'ємним складником загальної стратегії цифрової трансформації країни, що повинна сприяти не лише економічному зростанню, але й формуванню правової культури, яка відповідає сучасним викликам соціуму й забезпечує захист інтересів усіх суб'єктів суспільного життя. Актуальність цієї теми полягає в необхідності створення сучасної, адаптивної та прозорої правової системи, яка б дозволяла максимально ефективно використовувати потенціал штучного інтелекту, водночас забезпечуючи надійний захист основоположних прав людини та гарантії безпеки як окремих осіб, так і суспільства загалом.

Наразі в Україні законодавча база щодо використання штучного інтелекту знаходиться на стадії розроблення. Для того, щоб визначити пріоритетні напрями та основні завдання щодо розвитку штучного інтелекту Кабінет Міністрів України схвалив Концепцію розвитку штучного інтелекту (2 грудня 2020 року). Уперше було надане визначення терміна «штучний інтелект» на вітчизняному законодавчому рівні, визначені мета та завдання розвитку технологій штучного інтелекту в Україні. Так, штучний інтелект тлумачиться як «організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів оброблення 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. 38].

Концепція розвитку цифрових компетентностей до 2025 року визначає необхідність створення оновленої концепції «розумного виробництва», що ототожнюється з «четвертою промисловою революцією» та появою кіберфізичних систем. Індустрія 4.0 – наступний етап цифровізації виробництв та промисловості, на якому головну роль відіграють такі технології та концепти, як «Інтернет речей» (Internet of Things, IoT), «Великі дані» (Big Data), «Хмарні обчислення», предиктивна аналітика, машинне обчислення, штучний інтелект, робототехніка, 3D-друк, доповнена реальність та ін. Це створює умови для перспектив розвитку щодо адаптування цього питання у площинні правого поля, з оглядуна те, що розробка штучного інтелекту та середовища, у якому буде функціонувати штучний інтелект як суб'єкт та правове регулювання цих процесів перейдуть із стадії необхідності створення концепції до стадії втілення в життя державної програми щодо стимулювання розробки штучного інтелекту та його середовища, яка має бути обачною й виваженою, що чітко регламентується нормативними документами [2, с. 39].

З 01 січня 2023 року набув чинності Закон України «Про авторське право і суміжні права». У ст. 33 зазначеного Закону інтерпретується право особливого роду як категорія «sui generis» на неоригінальні об'єкти, згенеровані комп'ютерною програмою. У цьому нормативно-правовому акті неоригінальним об'єктом, згенерованим комп'ютерною програмою, визначається об'єкт, що відрізняється від існуючих подібних об'єктів та

утворений у результаті функціонування комп'ютерної програми без безпосередньої участі фізичної особи в утворенні цього об'єкта. Твори, створені фізичними особами з використанням комп'ютерних технологій, не вважаються неоригінальними об'єктами, згенерованими комп'ютерною програмою (п. 1 ст. 33 ЗУ) [3, с. 192].

Цілком зрозуміло, що ШІ не повинен «копіювати» людську природу щодо мисленєво-мовленєвої діяльності у процесі генерування ним того чи іншого творую. Безперечно, принципово різні фізичні характеристики та потреби вимагають апріорі відмовитися від такого підходу. Водночас створення цієї системи є необхідною умовою для того, щоб забезпечити людству можливість контролювати розвиток суспільних процесів. Скоріше за все «юстиція штучного інтелекту» буде створена на основі роботів. Фізичних та інтелектуальних даних людини очевидно буде недостатньо для ефективного функціонування цієї системи юстиції. Створення такої системи передбачає узагальнення в чіткі алгоритми досвіду, отриманого за час існування традиційної юстиції. Таке узагальнення має стати одним з основних напрямів сучасної юридичної науки. Звенімо увагу на те, що завдання щодо створення копії сформованих практик в сфері традиційної юстиції для забезпечення юстиції роботів не стоїть, проте досвід, накопичений людством у сфері юстиції, є надзвичайно важливим джерелом інформації для забезпечення правового регулювання діяльності роботів [4, с. 104].

Отже, правове регулювання застосування штучного інтелекту в Україні є надважливим завданням, яке вимагає створення сучасної, адаптивної та прозорої правової системи, здатної відповісти на виклики цифрової епохи. Сучасні законодавчі ініціативи мають бути спрямовані на створення чітких норм і критеріїв відповідальності за можливі помилки або зловживання, забезпечення кібербезпеки та захисту персональних даних, що є невід'ємним складником гарантій для всіх суб'єктів (праці) ринку. Водночас інтеграція міжнародного досвіду та стандартів дозволить Україні ефективно адаптувати національне законодавство до глобальних трендів, сприяючи подальшій цифровій трансформації та економічному зростанню. Тож правове регулювання застосування штучного інтелекту в Україні виступає не лише як інструмент забезпечення правопорядку, але й як стратегічний фактор, що формує правову культуру суспільства, стимулює розвиток інновацій і закладає основу для безпечного та справедливого використання новітніх технологій у всіх сферах життя.

Список використаних джерел:

1. Куракін О. Особливості правового регулювання використання штучного інтелекту в Україні. *Вісник Харківського національного університету імені В. Н. Каразіна.* 2023. Вип. 36. С. 36–42. URL: https://periodicals.karazin.ua/law/article/view/22696 (дата звернення: 07.03.2025).

2. Буковська О. А. До проблеми правового регулювання штучного інтелекту. Збірник матеріалів х наукових читань, присвячених пам'яті академіка В. В. Копєйчикова. 2020. С. 37–40. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/3ed647c1-faa7-4b64-9e72-8392f567c8b6/content (дата звернення: 07.03.2025).

3. Муравська Ю. Правове регулювання штучного інтелекту в Україні та світі. *Актуальні проблеми правознавства*. 2024. С. 188–195. URL: https://appj.wunu.edu.ua/index.php/appj/article/view/1833 (дата звернення: 07.03.2025).

4. Карчевський М. В. Правове регулювання соціалізації штучного інтелекту. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2017. Вип. 2. С. 99–108. URL: https://surl.gd/ysxyib (дата звернення: 07.03.2025).

Висотенко Ю. В.,
викладач кафедри адміністративного права та процесу,
кандидат юридичних наук
(Національна академія внутрішніх справ, м. Київ)
Сюйва Я. С.,
здобувач вищої освіти 2 курсу
навчально-наукового інституту поліцейської діяльності
(Національна академія внутрішніх справ, м. Київ)

ПЕРСПЕКТИВИ РОЗВИТКУ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ ДЕРЖАВНИХ ПОСЛУГ

В умовах сучасного цифрового розвитку використання технологій штучного інтелекту (далі – ШІ) набуває все більшого значення у сфері державних послуг. Ці інноваційні рішення дозволяють оптимізувати процеси надання адміністративних послуг, покращити якість обслуговування громадян та підвищити ефективність функціонування державних органів. Перспективи застосування ШІ та віртуальних асистентів у сфері державних послуг відкривають нові можливості для автоматизації стандартних процесів, підвищення рівня доступності інформації та забезпечення прозорості діяльності органів державної влади. На сьогодні Україна, перебуваючи на шляху цифрової трансформації, активно впроваджує сучасні технології у процеси публічного управління, що відповідає європейським стандартам цифрового розвитку [1].

Одним із ключових напрямів використання ШІ у сфері державних послуг є автоматизація обробки звернень громадян та надання консультацій. Віртуальні асистенти, створені на основі алгоритмів машинного навчання та обробки природної мови, здатні відповідати на типові запитання громадян, надавати інформацію про процедури отримання адміністративних послуг та допомагати у заповненні необхідних документів. Це значно спрощує процес комунікації між громадянами та органами влади, скорочує час очікування та зменшує навантаження на працівників державних установ. Прикладом успішного впровадження таких рішень в Україні є чат-бот Портал «Дія. Помічник», який надає консультації щодо оформлення документів, соціальних виплат та інших адміністративних послуг [2].

Крім того, ШІ може бути використаний для автоматизації процесів прийняття рішень у сфері державних послуг. Алгоритми машинного використання дозволяють аналізувати великі обсяги даних, оцінювати відповідність поданих документів вимогам законодавства та приймати рішення щодо надання послуг без участі людини. Це, як наслідок, сприяє прискоренню процесу розгляду заявок, мінімізації помилок та підвищенню рівня об’єктивності у прийнятті рішень. Наприклад, у деяких країнах ЄС ШІ вже використовується для автоматичної обробки заявок на отримання соціальних виплат, що дозволяє значно скоротити час для їх розгляду та

запобігти можливим зловживанням. В Україні перспективним є застосування подібних систем у сфері надання субсидій, соціальної допомоги та реєстрації підприємницької діяльності.

Віртуальні асистенти також можуть бути ефективним інструментом у сфері забезпечення доступності державних послуг для осіб з обмеженими можливостями. Голосові помічники та чат-боти з функцією синтезу мови дозволяють особам з вадами зору або слуху отримувати консультації та подавати заявки на отримання послуг у зручному форматі. Це сприяє забезпеченню рівного доступу до державних послуг та реалізації принципів інклюзивності. Впровадження таких рішень відповідає міжнародним стандартам у сфері прав людини та є важливим кроком на шляху до побудови доступного цифрового середовища [3].

Іншим важливим напрямом застосування ШІ є використання прогнозних моделей для оцінки потреб громадян та планування надання державних послуг. На основі аналізу історичних даних алгоритми ШІ можуть прогнозувати потребу в соціальних послугах, оцінювати ефективність державних програм та пропонувати оптимальні шляхи розподілу ресурсів. Це дозволяє органам влади приймати обґрунтовані управлінські рішення, підвищувати ефективність використання бюджетних коштів та своєчасно реагувати на зміни у потребах населення. В Україні такі системи можуть бути застосовані для планування медичних послуг, соціальної допомоги та освітніх програм [3].

Попри значні переваги впровадження ШІ, зокрема віртуальних асистентів, у сфері державних послуг супроводжується низкою викликів. Одним із основних викликів є необхідність забезпечення прозорості алгоритмів ШІ та запобігання дискримінаційним рішенням. Для мінімізації таких ризиків важливо розробляти етичні стандарти для використання ШІ, забезпечувати відкритість алгоритмів та проводити незалежний аудит систем. В Україні вже розроблена Концепція розвитку штучного інтелекту, яка передбачає створення правових та етичних стандартів для застосування ШІ в державному управлінні.

Ще одним важливим аспектом є захист персональних даних громадян, що обробляються системами ШІ. Використання великих обсягів конфіденційної інформації вимагає дотримання високих стандартів кібербезпеки та забезпечення відповідності чинному законодавству про захист персональних даних. Важливим кроком у цьому напрямі є імплементація норм GDPR у національне законодавство та впровадження електронної ідентифікації громадян [4].

Перспективи застосування ШІ, зокрема віртуальних асистентів, у сфері державних послуг значною мірою залежать від розвитку цифрової інфраструктури, підготовки кваліфікованих кадрів та міжнародної співпраці. Нині Україна активно співпрацює з Європейським Союзом та міжнародними організаціями у сфері цифрової трансформації, що сприяє обміну досвідом, залученню інвестицій та адаптації найкращих світових практик.

Отже, застосування ШІ та віртуальних асистентів у сфері державних послуг відкриває широкі можливості для підвищення якості обслуговування громадян, оптимізації адміністративних процесів та забезпечення прозорості діяльності органів влади. Водночас успішна імплементація цих технологій потребує комплексного підходу, що включає розвиток нормативно-правової бази, створення надійної цифрової інфраструктури, підготовку кваліфікованих кадрів та дотримання етичних стандартів. Інтеграція ШІ у систему державних послуг є важливим етапом цифрової трансформації України та сприяє побудові ефективного, прозорого та доступного державного управління, що відповідає європейським стандартам [4].

Список використаних джерел:

1. Кузава В. І., Литвин Н. А. Штучний інтелект в публічній службі: проблеми та перспективи впровадження в Україні. *Юридичний науковий електронний журнал.* 2024. № 11. С. 306–308. URL: http://www.lsej.org.ua/11_2024/71.pdf (дата звернення 05.03.2025).

2. Оболенський О., Косицька В., Рвач А. Штучний інтелект у публічному управлінні: вимоги, проблеми та ризики. *Вчені записки :* зб. наук. пр. / М-во освіти і науки України, Київ. нац. екон. ун-т ім. Вадима Гетьмана ; [редкол. : О. Яценко (голов. ред.) та ін.]. Київ : КНЕУ, 2023. Вип. 33. С. 121–137. URL: https://ir.kneu.edu.ua/items/c0603708-51c0-47cc-b43a-c3208c898ed2 (дата звернення 05.03.2025).

3. Максіменцева Н. О., Максіменцев М. Г. Виклики застосування штучного інтелекту у сфері публічного управління, врядування та послуг. *Державне управління: удосконалення та розвиток.* 2024. № 4. С. 204–213. URL: file:///C:/Users/Home/Downloads/Maksimentsev___Inv4-2024_St30%20(1).pdf (дата звернення 05.03.2025).

4. Бацман Ю. В., Толкуща К. Р., Ковтун М. С. Використання штучного інтелекту в публічному адмініструванні. *Юридичний науковий електронний журнал*. 2024. № 4. С. 338–341. URL: http://www.lsej.org.ua/4_2024/81.pdf (дата звернення 05.03.2025).

Висотенко Ю. В.,
викладач кафедри адміністративного права та процесу,
кандидат юридичних наук
(Національна академія внутрішніх справ, м. Київ)

Тимчишин П. А.,
здобувач вищої освіти 2 курсу
навчально-наукового інституту поліцейської діяльності
(Національна академіяї внутрішніх справ, м. Київ)

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ ПРОЗОРОСТІ ПУБЛІЧНОЇ АДМІНІСТРАЦІЇ В УКРАЇНІ

Безсумнівно, використання штучного інтелекту (далі – ШІ) у сфері публічного управління є одним з ключових напрямів цифрової трансформації сучасних держав. Інноваційні технології відкривають нові можливості для оптимізації процесів управління, забезпечення прозорості діяльності органів

державної влади та підвищення рівня підзвітності перед громадянами. В Україні питання підвищення прозорості та підзвітності державних органів набуває особливої актуальності в контексті євроінтеграційних процесів та впровадження стандартів належного врядування. ШІ як сучасний інструмент цифрового управління здатен значно посилити спроможність державних інституцій у сфері протидії корупції, покращення якості адміністративних послуг та прийняття обґрунтованих управлінських рішень.

Одним із головних напрямів застосування ШІ для підвищення прозорості державного управління є автоматизація процесів обробки інформації. Алгоритми машинного оброблення дозволяють ефективно аналізувати великі обсяги даних, що надходять від різних органів державної влади, та виявляти закономірності, які можуть свідчити про порушення або неефективність у діяльності адміністративних структур. Наприклад, ШІ може бути використаний для аналізу тендерної документації з метою виявлення аномалій у процедурах державних закупівель [1, с. 12–13]. Це, зі свого боку, сприяє підвищенню рівня відкритості та запобіганню корупційним практикам у сфері публічних фінансів. В Україні подібні інструменти вже починають застосовуватися, зокрема, у системі «Прозорро», яка є одним із найуспішніших прикладів електронних закупівель у світі.

Крім того, ШІ може відігравати важливу роль у підвищенні рівня підзвітності органів державної влади шляхом автоматизації процесів моніторингу та оцінки виконання державних програм. Використання алгоритмів обробки даних дозволяє аналізувати ефективність реалізації державної політики, порівнювати результати діяльності різних органів влади та своєчасно виявляти недоліки у виконанні планів [2]. Наприклад, у сфері соціального захисту ШІ може бути застосований для оцінки ефективності програм надання соціальних виплат, виявлення фактів зловживань та прогнозування потреб громадян у соціальних послугах. Це сприяє підвищенню ефективності використання бюджетних коштів та забезпеченню адресності державної допомоги.

Важливим аспектом використання ШІ у сфері публічного управління є створення відкритих платформ для доступу громадян до інформації про діяльність органів влади. Як знаємо, «віртуальні асистенти» та чат-боти можуть бути використані для надання інформаційних послуг у режимі реального часу, відповідаючи на запитання громадян щодо процедур отримання адміністративних послуг, бюджетних витрат або законодавчих ініціатив. Це значно підвищує рівень прозорості державного управління та сприяє залученню громадян до процесів прийняття рішень. Наприклад, у деяких країнах ЄС вже функціонують системи, що автоматично надають інформацію про прийняті нормативно-правові акти, проєкти рішень міських рад або бюджетні витрати органів влади.

У сфері протидії корупції ШІ може використовуватися для виявлення підозрілих фінансових операцій, аналізу декларацій про доходи посадових осіб та моніторингу діяльності компаній, що беруть участь у державних закупівлях.

Алгоритми машинного оброблення інформації дозволяють автоматично виявляти аномальні транзакції, зв'язки між суб'єктами господарювання та можливі конфлікти інтересів [1, с. 14–15]. В Україні перспективним напрямом, наприклад, є інтеграція подібних систем у діяльність Національного агентства з питань запобігання корупції та інших антикорупційних органів.

Водночас використання ШІ у сфері державного управління потребує вирішення низки важливих викликів. Одним із ключових питань є забезпечення прозорості та етичності в реалізації алгоритмів ШІ. Оскільки рішення, прийняті на основі автоматизованих систем, можуть впливати на права та інтереси громадян, важливо забезпечити відкритість алгоритмів, можливість зовнішнього аудиту та дотримання принципів недискримінації. Крім того, необхідно створити ефективні механізми захисту персональних даних, які обробляються системами ШІ, відповідно до вимог законодавства України та міжнародних стандартів, зокрема Загального регламенту захисту даних (GDPR).

Розвиток інфраструктури ШІ у сфері публічного управління також потребує підготовки кваліфікованих кадрів та забезпечення належного технічного супроводу. Важливим завданням держави на сучасному етапі її розвитку є створення навчальних програм для державних службовців, які дозволять опанувати навички роботи з системами ШІ та розуміти принципи їх функціонування. Слушною думка є щодо необхідності забезпечити фінансування наукових досліджень у сфері ШІ та залучення приватного сектору до розробки технологічних рішень для державних органів [3, с. 20–22].

Успішне впровадження ШІ для підвищення прозорості та підзвітності органів державної влади в Україні значною мірою залежить від міжнародної співпраці. Україна вже має значний досвід співпраці з ЄС у сфері цифрової трансформації, зокрема в межах програми «Цифрова Європа» та ініціативи «Східне партнерство». Подальша інтеграція України в європейський цифровий простір сприятиме обміну досвідом, залученню міжнародних інвестицій та впровадженню передових технологій.

Отже, використання ШІ для підвищення прозорості публічного адміністрування є важливим напрямом цифрової трансформації України, що сприяє формуванню ефективного, відкритого та орієнтованого на потреби громадян державного управління. Широке застосування ШІ у процесах обробки даних, моніторингу державних програм та взаємодії з громадянами дозволяє значно підвищити рівень відкритості адміністративних процесів, запобігти корупційним практикам та забезпечити раціональне використання державних ресурсів. Водночас успішна імплементація цих технологій потребує комплексного підходу, що містить вдосконалення нормативно-правової бази, розвиток цифрової інфраструктури, підготовку фахівців та забезпечення дотримання етичних стандартів. Як бачимо, інтеграція ШІ у систему державного управління повинна відповідати європейським стандартам належного врядування та сприяє наближенню України до міжнародних стандартів у сфері публічного управління.

Список використаних джерел:

1. Автомонов О. П. Європейські правові стандарти використання штучного інтелекту у публічній службі: виклики правового регулювання в Україні. *Правова позиція*. 2024. № 2 (43). С. 11–15 (дата звернення: 06.03.2025).

2. Про затвердження Плану заходів з виконання рекомендацій Європейської Комісії, представлених у Звіті про прогрес України в рамках Пакета розширення Європейського Союзу 2023 року : розпорядження Кабінету Міністрів України від 09 лютого 2024 року № 133-р. URL: https://www.kmu.gov.ua/npas/prozatverdzhennia-planu-zakhodiv-z-vykonannia-rekomendatsii-ievropeiskoi-komisii-predstavlenykh-u-t90224 (дата звернення: 06.03.2025).

3. Грищенко І. М., Горбата Л. П. Пріоритетні напрями та шляхи забезпечення інформаційної відкритості в органах публічної влади. *Public and municipal administration: theory, methodology,practice: Collective monograph. Riga: Izdevnieciba «BaltijaPublishing»*, 2020. P. 20–22. URL: https://doi.org/10.30525/978-9934-588-46-4.02 (дата звернення 06.03.2025).

Висотенко Ю. В.,
викладач кафедри адміністративного права та процесу,
кандидат юридичних наук
(Національна академія внутрішніх справ, м. Київ)
Хізанов О. Д.,
здобувач вищої освіти 2 курсу
навчально-наукового інституту поліцейської діяльності
(Національнп академія внутрішніх справ, м. Київ)

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ АНТИКОРУПЦІЙНОЇ ПОЛІТИКИ

Роль штучного інтелекту у підвищенні ефективності антикорупційної політики в публічному управлінні України є одним із перспективних напрямів цифрової трансформації державного сектору. В умовах сучасного розвитку технологій та глобальних викликів соціуму питання боротьби з корупцією набуває особливої актуальності. Корупція залишається серйозною перешкодою на шляху до ефективного державного управління, економічного зростання та соціальної справедливості. Традиційні методи протидії корупції, що основані на законодавчому регулюванні, моніторингу та контролі, не завжди є ефективними. У зв'язку з цим інтеграція штучного інтелекту у процеси публічного управління відкриває нові можливості для підвищення прозорості, оптимізації процесів та запобігання корупційним ризикам.

Штучний інтелект (далі – ШІ) має значний потенціал у сфері антикорупційної політики завдяки здатності обробляти великі масиви даних, виявляти приховані закономірності та здійснювати «прогнозний» аналіз. Одним

із ключових напрямів застосування ШІ є автоматизація процесів моніторингу та аналізу державних закупівель, що є на сьогодні однією з найбільш корупціогенних сфер публічного управління. Алгоритми машинного опрацювання інформації можуть аналізувати тендерну документацію, виявляти аномалії у розподілі контрактів, визначати підозрілі зв'язки між учасниками тендерів та прогнозувати ймовірність зловживань [1, с. 1–3]. В Україні вже діють деякі системи на базі ШІ, наприклад, система ризик-індикаторів у платформі електронних закупівель «Прозорро», яка дозволяє в автоматичному режимі оцінювати ризикованість тендерів та сигналізувати про потенційні порушення.

Ще одним важливим напрямом застосування ШІ є аналіз фінансових транзакцій та моніторинг активів державних службовців. Впровадження технологій ШІ у системи фінансового контролю дозволяє автоматизувати перевірку декларацій про майно, доходи та витрати, порівнювати задекларовані активи з реальними даними з інших реєстрів та банківських систем, а також виявляти невідповідності. Такий підхід значно підвищує ефективність контролю та мінімізує людський фактор, який може сприяти приховуванню правопорушень [2, с. 20–23]. Національне агентство з питань запобігання корупції вже активно впроваджує технології аналізу даних для перевірки електронних декларацій, що є важливим кроком у напрямі цифровізації антикорупційної політики.

Окрім моніторингу та контролю, застосування ШІ може бути ефективним інструментом у сфері превентивних заходів. Наприклад, системи аналізу текстів на основі обробки природної мови можуть автоматично перевіряти нормативно-правові акти на предмет наявності корупціогенних факторів (двозначні формулювання, дискреційні повноваження або відсутність чітких процедур та ін.). Це дозволяє зменшити ймовірність виникнення прогалин у законодавстві ще на етапі його розроблення. Також ШІ може використовуватися для автоматизації процесів обробки скарг громадян та журналістських розслідувань, що сприяє,зі свого боку, швидкому реагуванню на корупційні ризики та підвищенню водночас рівня громадського контролю.

Важливим аспектом впровадження ШІ у сфері антикорупційної політики є створення прозорих та підзвітних алгоритмів. Використання технологій штучного інтелекту має супроводжуватися чітким регулюванням, що забезпечить недопущення зловживань, дискримінації або порушення права на приватність. Варто наголосити, що розробка етичних стандартів для застосування ШІ в публічному управлінні є необхідною умовою для забезпечення довіри з боку суспільства. Важливим прикладом у цьому контексті є практика Європейського Союзу, де впровадження технологій ШІ супроводжується вимогами до прозорості алгоритмів, захисту персональних даних та недискримінації.

Однак впровадження штучного інтелекту в антикорупційну політику супроводжується низкою невирішених питань. По-перше, для ефективного функціонування систем ШІ необхідний доступ до великих масивів якісних

даних, що вимагає комплексної цифровізації державних реєстрів та забезпечення їхньої сумісності. По-друге, важливою проблемою залишається низький рівень цифрової грамотності серед державних службовців, що ускладнює впровадження інноваційних технологій. По-третє, в умовах гібридних загроз та кібератак постає питання забезпечення кібербезпеки систем ШІ та захисту даних від несанкціонованого доступу [3].

Для подолання цих викликів необхідно здійснювати комплексні реформи, спрямовані на цифрову трансформацію державного управління, розширення доступу до відкритих даних та підвищення цифрової грамотності. Одним із важливих кроків у цьому напрямі є реалізація Концепції розвитку штучного інтелекту в Україні, затвердженої Кабінетом Міністрів України у 2020 році, яка визначає основні напрями розвитку ШІ у сфері державного управління, включаючи антикорупційну політику.

Впровадження ШІ у сфері антикорупційної політики відкриває значні перспективи для підвищення ефективності державного управління, прозорості та підзвітності [1, с. 1–3]. ШІ може стати потужним інструментом у боротьбі з корупцією за умови дотримання принципів прозорості, етичності та захисту прав людини. Подальший розвиток цього напрямку потребує комплексного підходу, що включає вдосконалення нормативно-правової бази, розвиток цифрової інфраструктури, підготовку кваліфікованих кадрів та активну співпрацю з громадянським суспільством та міжнародними партнерами.

Отже, роль ШІ у підвищенні ефективності антикорупційної політики в публічному управлінні України є стратегічно значущою для подальшого розвитку демократичних інститутів та європейської інтеграції, оскільки використання інноваційних технологій не лише сприяє мінімізації корупційних ризиків, але й підвищує довіру громадян до державних інституцій. Водночас для досягнення максимального ефекту щодо вирішення досліджуваного питання необхідно забезпечити баланс між ефективністю технологій та дотриманням прав людини, що стане запорукою успішного впровадження ШІ у систему публічного управління України.

Список використаних джерел:

1. Кузик Д. О. Зміст поняття корупції як об’єкта державної антикорупційної політики. *Академічні візії.* 2024. Вип. 36. С. 1–8. URL: https://www.academy-vision.org/index.php/av/article/view/1459 (дата звернення: 06.03.2025).

2. Акімов О. О., Майстренко К. М. Інноваційні підходи до забезпечення ефективної антикорупційної політики в контексті сучасних викликів Державного управління. *Дніпровський науковий часопис публічного управління, психології, права.* 2024. № 1. С. 20–25. URL: https://www.chasopys-ppp.dp.ua/index.php/chasopys/article/view/560/508 (дата звернення: 06.03.2025).

3. Деякі питання реформування державного управління України. Стратегія реформування державного управління на 2022–2025 рр. : розпорядження Кабінету Міністрів України від 21 липня 2021 р. № 831-р. URL: https://zakon.rada.gov.ua/laws/show/831-2021-%D1%80#n199 (дата звернення: 06.03.2025).

Висотенко Ю. В.,
викладач кафедри адміністративного права та процесу,
кандидат юридичних наук
(Національна академія внутрішніх справ, м. Київ)
Ящур П. О.,
здобувач вищої освіти 2 курсу
навчально-наукового інституту поліцейської діяльності
(Національна академія внутрішніх справ, м. Київ)

ЦИФРОВІЗАЦІЯ ПУБЛІЧНОГО УПРАВЛІННЯ ЯК СПОСІБ ОПТИМІЗАЦІЇ ПРОЦЕСУ НАДАННЯ АДМІНІСТРАТИВНИХ ПОСЛУГ

Цифровізація публічного управління є важливим напрямом модернізації державного сектору, що сприяє підвищенню ефективності, прозорості та якості надання адміністративних послуг. В умовах глобальної цифрової трансформації штучний інтелект (далі – ШІ) стає першочерговим інструментом оптимізації управлінських процесів, забезпечення оперативності та персоналізації послуг для громадян. Використання технологій ШІ у сфері публічного управління відкриває нові можливості для автоматизації шаблонних завдань, аналізу великих обсягів даних та прийняття більш обґрунтованих управлінських рішень. В Україні сьогодні процес цифровізації публічного управління набув особливого значення у контексті євроінтеграційних процесів та необхідності підвищення ефективності державних послуг.

Штучний інтелект може бути використаний на різних етапах надання адміністративних послуг, починаючи від обробки запитів громадян та закінчуючи прийняттям управлінських рішень. Одним із найбільш поширених напрямів застосування ШІ є автоматизація обробки звернень та заявок громадян. Чат-боти та віртуальні асистенти на базі ШІ дозволяють у режимі реального часу надавати консультації, приймати заяви та надавати інформацію про порядок надання послуг [1, с. 80–81]. В Україні прикладом такої практики є чат-боти на Порталі «Дія», які допомагають громадянам отримати інформацію про адміністративні послуги, зареєструвати бізнес або подати заяву на соціальну допомогу. Такі рішення значно скорочують час обслуговування, зменшують навантаження на державні установи та покращують рівень доступності послуг.

Окрім автоматизації консультаційних послуг, ШІ активно застосовується для обробки документів та перевірки інформації. Алгоритми машинного оброблення інформації можуть автоматично аналізувати текстові документи, перевіряти правильність заповнення заяв, а також ідентифікувати помилки або невідповідності. Це значно прискорює процес прийняття рішень та мінімізує ризик людського фактора. Наприклад, технології розпізнавання текстів OCR (Optical Character Recognition) у поєднанні з алгоритмами машинного опрацювання дозволяють автоматично «витягувати» інформацію з документів,

таких як паспорти, свідоцтва про народження або довідки про доходи. В Україні подібні технології використовуються в електронних сервісах Міністерства цифрової трансформації для обробки заяв на соціальні послуги та реєстрацію бізнесу [2, с. 69–82].

Важливим аспектом цифровізації адміністративних послуг є використання ШІ для прийняття управлінських рішень на основі аналізу великих масивів даних. ШІ може аналізувати статистичні дані, виявляти закономірності та прогнозувати потреби громадян у певних послугах. Це дозволяє органам публічного управління оптимізувати процеси планування, розподілу ресурсів та прийняття рішень. Наприклад, аналіз даних про звернення громадян може допомогти визначити найбільш популярні послуги, оптимізувати графік роботи центрів надання адміністративних послуг або розробити нові електронні сервіси [3, с. 57–59]. У країнах Європейського Союзу такі підходи активно використовуються для управління системами соціального захисту, охорони здоров'я та міграційних процесів.

Штучний інтелект також відіграє важливу роль у забезпеченні прозорості та підзвітності публічного управління. Алгоритми ШІ можуть автоматично аналізувати дані про державні закупівлі, виявляти потенційні порушення або корупційні ризики. В Україні подібний підхід реалізовано у системі електронних закупівель «Прозорро», яка використовує ризик-індикатори для автоматичного виявлення підозрілих тендерів. Крім того, ШІ може використовуватися для моніторингу виконання адміністративних послуг, аналізу відгуків громадян та оцінки рівня задоволеності послугами [1, с. 82–83].

Впровадження ШІ у систему надання адміністративних послуг супроводжується низкою викликів. Одним і основних викликів є необхідність забезпечення кібербезпеки та захисту персональних даних. Автоматизація процесів надання адміністративних послуг передбачає обробку великої кількості конфіденційної інформації, що вимагає впровадження надійних механізмів шифрування, аутентифікації та контролю доступу. Важливим кроком у цьому напрямі є ухвалення в Україні Закону «Про захист персональних даних» від 01.06.2010 № 2297-VI та імплементація стандартів GDPR (General Data Protection Regulation), що забезпечує належний рівень захисту інформації.

Ще одним викликом є необхідність забезпечення прозорості алгоритмів ШІ та запобігання дискримінаційним рішенням. Алгоритми ШІ можуть мати вбудовані упередження або приймати рішення на основі неповних або некоректних даних. Для мінімізації таких ризиків важливо забезпечити відкритість алгоритмів, проведення незалежного аудиту та залучення громадськості до процесів розробки та впровадження ШІ [3, с. 60–62].

Перспективи застосування ШІ у сфері надання адміністративних послуг значною мірою залежать від розвитку нормативно-правової бази та впровадження державних стратегій цифрової трансформації. У 2020 році Кабінет Міністрів України затвердив Концепцію розвитку штучного інтелекту, яка визначає основні напрями впровадження ШІ у сфері державного

управління. Крім того, активна співпраця з міжнародними організаціями, такими як Європейський Союз та ООН, сприяє обміну досвідом, фінансуванню інноваційних проєктів та адаптації найкращих світових практик.

Як показало дослідження, цифровізація публічного управління з використанням технологій штучного інтелекту є важливим етапом на шляху до створення сучасної, прозорої та ефективної системи надання адміністративних послуг. ШІ дозволяє автоматизувати шаблонні процеси, підвищити якість обслуговування громадян, оптимізувати процеси прийняття рішень та забезпечити прозорість діяльності органів влади. Як бачимо, успішна реалізація цих технологій потребує комплексного підходу, що включає розвиток нормативно-правової бази, створення надійної цифрової інфраструктури, підготовку кваліфікованих кадрів та забезпечення захисту персональних даних. Інтеграція ШІ у систему надання адміністративних послуг має значний потенціал для підвищення ефективності публічного управління та покращення якості життя громадян, що є важливим кроком у процесі цифрової трансформації України.

Список використаних джерел:

1. Тодощак О. В., Фролова Є. І. Оптимізація методів публічного адміністрування в умовах цифровізації. *Науковий вісник Ужгородського Національного Університету*. Серія «Право». 2023. Вип. 76, ч. 2. С. 79-84. URL: https://doi.org/10.24144/2307-3322.2022.76.2.13 (дата звернення 05.03.2025).

2. Чорний С. В. Поняття та перспективи розвитку цифровізації у сфері публічного управління. *Київський часопис права.* 2021. № 4. С. 224–229. URL: https://doi.org/10.32782/klj/2021.4.34 (дата звернення 05.03.2025).

3. Матвейчук Л. О., Польовий П. В. Цифрова компетентність публічних службовців: теоретична площина. *Вчені записки ТНУ імені В. І. Вернадського. Серія : Публічне управління та адміністрування*. 2022. С. 55–64. URL: https://pubadm.vernadskyjournals.in.ua/journals/2022/2_2022/10.pdf (дата звернення 05.03.2025).

Вовк М. З.,
доцент кафедри цивільно-правових дисциплін
ННІ права та правоохоронної діяльності,
кандидат юридичних наук, доцент
(Львівський державний університет внутрішніх справ)

ПРАВО ОСОБЛИВОГО РОДУ (SUI GENERIS) НА НЕОРИГІНАЛЬНІ ОБ'ЄКТИ, ЗГЕНЕРОВАНІ КОМП'ЮТЕРНОЮ ПРОГРАМОЮ

У XXI столітті штучний інтелект стає потужним інструментом для вирішення складних завдань у багатьох сферах життєдіяльності людини. Поряд із цим, він створює нові виклики та можливості у сфері інтелектуальної власності. Адже останніми роками штучний інтелект все частіше використовується для творчих цілей, зокрема генерує безліч цифрового

контенту – тексти, малюнки, музику, відео тощо. Такі творіння привертають до себе чималу увагу, про що свідчать вдалі їх продажі на аукціонах за шалені гроші.

Тривалий час серед науковців та практиків велись жваві дискусії щодо можливості правової охорони об'єктів створених штучним інтелектом авторським правом або іншими правовими інститутами.

У 2022 році вперше на законодавчому рівні у Законі України «Про авторське право і суміжні права» закріплено правове регулювання щодо об'єктів, які генеруються комп'ютерною програмою за допомогою прав особливого роду (sui generis). Зокрема, відповідно до ст. 33 цього Закону неоригінальним об'єктом, згенерованим комп'ютерною програмою, є об'єкт, що відрізняється від існуючих подібних об'єктів та утворений у результаті функціонування комп'ютерної програми без безпосередньої участі фізичної особи в утворенні цього об'єкта. Суб'єктами права особливого роду (sui generis) на неоригінальні об'єкти, згенеровані комп'ютерною програмою, можуть бути особи, яким належать майнові права або які мають ліцензійні повноваження на комп'ютерну програму – автори такої комп'ютерної програми, їх спадкоємці, особи, яким автори чи їх спадкоємці передали (відчужили) майнові права на комп'ютерну програму або правомірні користувачі комп'ютерної програми [1].

У процесі генерування такого нового об'єкта штучний інтелект навчається на значній кількості охоронюваних правом інтелектуальної власності творах та інших об'єктах, які слугують основою для формування його результатів [2].

Нині у світі є багато судових позовів про порушення авторських та суміжних прав при використанні творів та інших об'єктів для навчання штучного інтелекту [3; 4]. Для запобігання потраплянню творів та інших об'єктів у бази систем штучного інтелекту навіть була створена спеціальна програма під назвою NO AI, яка також є штучним інтелектом [5]. З огляду на наведене особливого значення набуває дослідження питання правових умов використання об'єктів права інтелектуальної власності для навчання штучного інтелекту.

Варто зазначити, що у п. 7 ст. 33 Закону України «Про авторське право і суміжні права» міститься вимога про необхідність дотримання прав суб'єктів авторського права або суміжних прав та прав суб'єктів на неоригінальний об'єкт, відповідно твори, об'єкти суміжних прав або неоригінальний об'єкт якого зазнали використання у процесі генерування такого неоригінального об'єкта [1].

Для навчання штучного інтелекту використовується метод «глибинного аналізу тексту та даних» («Text and Data Mining» (TDM)) [6].

Всесвітня організація інтелектуальної власності відзначає, що кілька країн, переважно розвинених, нещодавно дозволили використання методу глибинного аналізу тексту та даних для захищеного авторським правом вмісту: або відповідно до доктрини добросовісного використання (наприклад, США), або відповідно до певних законодавчих норм, які містять винятки та обмеження

для методу глибинного аналізу тексту та даних (наприклад, ЄС, Японія, Сінгапур, Великобританія, а також Еквадор та Україна) [7].

В Україні, як зазначає Всесвітня організація інтелектуальної власності, виняток із загального правила на відтворення творів для глибинного аналізу тексту та даних міститься у п. 14 ч. 2 ст. 22 Закону України «Про авторське право та суміжні права» [7]. Там зазначається, що без дозволу суб'єктів авторського права і безоплатно, але із зазначенням імені автора і джерела запозичення, допускається виготовлення копій творів, що зроблені із законного джерела з метою пошуку тексту і даних, включених до наукових публікацій або пов'язаних з ними, для дослідницьких цілей. Водночас законодавець зауважує, що це можливо за умови, що використання творів не було прямо заборонено суб'єктами авторського права відповідним чином, зокрема за допомогою засобів, придатних для зчитування комп'ютером з цифрового контенту, що є доступним у мережі Інтернет [1].

З наведеного вище випливає, що використання (відтворення) охоронюваних авторським правом творів для навчання штучного інтелекту в Україні можливе за наявності таких умов: 1) необхідність зазначення імені автора і джерела запозичення; 2) твори мають бути отримані із законного джерела; 3) текст і дані мають бути включені до наукових публікацій або пов'язаних із ними; 4) такий пошук тексту і даних має здійснюватись для дослідницьких цілей; 5) відсутність прямої заборони суб'єктів авторського права щодо такого використання.

Поряд із цим, на думку юристів-практиків, Закон України «Про авторське право та суміжні права» містить ще дві норми, що можуть бути віднесені до винятків з права для використання (відтворення) глибинного аналізу тексту та даних для навчання штучного інтелекту – це ст. 27 щодо тимчасового відтворення творів та п. 4 ч. 1 ст. 43 щодо тимчасового відтворення об'єктів суміжних прав [1].

Отже, вітчизняний законодавець передбачає, що допускаються без дозволу суб'єктів авторського права та суміжних прав та безоплатно дії з тимчасового відтворення твору або інших об'єктів права інтелектуальної власності, які мають проміжний (перехідний) або випадковий (додатковий) характер і є невід'ємною складовою частиною технологічного процесу, а також єдина мета яких полягає в тому, щоб спричинити передаванню електронної (цифрової) копії твору або іншого об'єкта права інтелектуальної власності посередником у мережі між третіми особами або правомірному їх використанню. Зазначені дії з тимчасового відтворення творів та інших об'єктів права інтелектуальної власності допускаються за умови, що вони не мають самостійного економічного значення.

Список використаних джерел:

1. Про авторське право та суміжні права : Закон України від 01.12.2022 № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text.

2. Петрів О. Штучний інтелект та авторське право. URL: https://cedem.org.ua/analytics/shtuchnyi-intelekt-avtorske-pravo/.

3. Художниці подали позов проти Stability AI, Midjourney та DeviantArt. URL: https://gamedev.dou.ua/news/ai-vs-artists-lawsuit/.

4. Getty Images is suing the creators of AI art tool Stable Diffusion for scraping its content. URL: https://www.theverge.com/2023/1/17/23558516/ai-art-copyright-stable-diffusion-getty-images-lawsuit.

5. Фоміна Н. Чи можуть твори, створені за допомогою ШІ, розраховувати на авторське право. URL: https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/chi-mozhut-tvori-stvoreni-za-dopomogoyu-shi-rozrahovuvati-na-avtorske-pravo.html.

6. Мисенко О. Генеративний штучний інтелект з точки зору авторського права. URL. https://blog.liga.net/user/amyisenko/article/51766.

7. Scoping study on the practices and challenges of research institutions and research purposes in relation to copyright. URL: https://www.wipo.int/edocs/mdocs/copyright/en/sccr_44/sccr_44_4.pdf.

Гловюк І. В.,
професорка кафедри кримінально-правових дисциплін
ННІ права та правоохоронної діяльності,
докторка юридичних наук, професорка
(Львівський державний університет внутрішніх справ)

ПОКЛИКАННЯ СТОРОНОЮ ПРОВАДЖЕННЯ НА РЕЗУЛЬТАТИ, ЗГЕНЕРОВАНІ CHATGPT: ЧИ ЦЕ НЕПОВАГА ДО СУДУ?

Стрімкий розвиток ШІ породжує ряд нових питань у правозастосовчих процесах, у тому числі щодо використання інформації від ШІ у аргументації правової позиції учасника судового провадження.

Доволі обговорюваною у правничому середовищі є ухвала КГС ВС, у якій було визнано, що «дії заявника у сукупності (подання завідомо безпідставної заяви на роз'яснення постанови касаційної інстанції, право на роз'яснення якої не передбачено статтею 245 ГПК України, апелювання до "позиції" штучного інтелекту "ChatGPT", згенерованого ним у відповідях з окремого питання, що вже розглянув суд) є виявом неповаги до суддів Верховного Суду, не спрямовані на ефективний захист прав, свобод та інтересів позивача від імовірних порушень з боку відповідача» [1]. У свою чергу, заявник просив з метою правильного застосування норм права у спірних правовідносин роз'яснити окремі поняття та висновки постанови. В обґрунтування цієї необхідності заявник цитував норми статей 509, 510, 526 ЦК України, положення підручника «Цивільне право», а також зміст поняття «добровільне зобов'язання», що надав штучний інтелект «ChatGPT». Суд розцінив це прохання так: заявник фактично просить Верховний Суд спростувати чи підтвердити те, що з окресленого питання згенерував штучний інтелект «ChatGPT», який не визнається як джерело достовірної науково доведеної інформації, на противагу висновкам, що були зроблені судом в судовому рішенні. У такий спосіб заявник поставив під сумнів

суддівський розсуд та судове тлумачення цього питання у рішенні, що набуло статусу остаточного, чим знехтував авторитет судової влади [1].

Відмітимо, що в окремій думці заперечується висновок про неповагу до суду: пославшись на відповіді, згенеровані ШІ «ChatGPT», з метою обґрунтування своєї позиції, зважаючи зміст заяви, наведені в ній доводи та аргументи, Заявник не виявив неповагу до Суду та не поставив під сумнів його висновки, навпаки – прагнув з'ясувати та уточнити окремі висновки з питань, щодо яких висловився Верховний Суд. У заяві відсутні будь-які принизливі, образливі чи інші негативні висловлювання, відверта демонстрація неповаги до Суду тощо. Саме по собі посилання на інформацію, що була згенерована за допомогою технологій ШІ, за відсутності інших обґрунтованих обставин, які б свідчили про недобросовісні процесуальні дії особи, не може визнаватися зловживанням процесуальними правами [2].

Основним аргументом ухвали (його процитовано вище) було саме те, що заявник цитував інформацію, згенеровану ChatGPT. Тому слід детальніше розглянути питання релевантності такого розуміння неповаги до суду.

По-перше, жодної заборони користуватися ChatGPT для аргументації позиції учасника провадження не існувало на той час і немає зараз. Те, що заявник посилався ще й на підручник, не викликало у суду зауважень. ПАЕ не містять спеціальних норм стосовно використання ШІ для аргументації правової позиції адвоката. Тобто в цій частині жодної норми закону або ПАЕ не було порушено.

По-друге, заявник реалізував своє право на подання заяви про роз'яснення судового рішення, оскільки саме йому були незрозумілі окремі формулювання. Саме для цього існує можливість роз'яснення судового рішення. Більше того, ч. 4 ст. 245 ГПК України передбачає можливість постановлення ухвали про відмову у роз'ясненні судового рішення; тобто вже законодавець передбачив те, що у суду та учасника може бути різне розуміння потреби роз'яснення або її відсутності.

По-третє, заявник доброчесно вказав, що він використав ШІ, не приховував це від суду. Це вказує якраз на повагу до суду.

Більше того, станом на 1 грудня 2023 року вже існував Висновок КРЄС № 26 (2023): Рухаючись вперед: використання асистивних технологій у судочинстві [3]. У цьому висновку немає положень, які точно відповідали б описаній ситуації, утім, він вказує на можливість застосування ШІ у судочинстві.

По-четверте, неповага до суду або Конституційного Суду України виражається, згідно ст. 185-3 КУпАП, у злісному ухиленні від явки в суд свідка, потерпілого, позивача, відповідача або в непідкоренні зазначених осіб та інших громадян розпорядженню головуючого чи в порушенні порядку під час судового засідання, а так само вчинення будь-ким дій, які свідчать про явну зневагу до суду або встановлених у суді правил. У диспозиції немає вичерпного переліку діянь, і ККС ВС висловлювався, що перелік діянь не є

вичерпним та може бути розширеним зважаючи на конкретну ситуацію та обставини, що їй передували [4].

Аналіз судової практики демонструє, що поведінка, яка оцінюється судом як неповага до суду, може бути такою: поява в нетверезому стані; поява в неадекватному стані внаслідок гострої алкогольної інтоксикації; ухилення від явки; непокора розпорядженням головуючого; нестриманість, висловлювання, коментування судового рішення, що заважали продовжувати озвучувати рішення і вести справу; коментування учасника судового процесу вільним слухачем, ігнорування зауважень суду, гучні висловлювання на адресу суду вільним слухачем; нецензурна лайка; втручання в доповідь прокурора, що на думку суду дорівнює втручанню в судовий процес; покидання залу суду без попередження; перебивання судді представником; принесення алкогольних напоїв в суд; непристойний жест; учасник не вимкнув мобільний телефон, на який кілька разів дзвонили, на прохання головуючого вимкнути телефон не реагував [5].

Якщо порівняти цей перелік з посиланням на інформацію, згенеровану ChatGPT, видається очевидним, що їх неможливо прирівняти, адже у вищенаведених випадках можна говорити про явну зневагу до суду, а в ситуації роз'яснення постанови заявник реалізовував процесуальне право, хоча і використав для цього доволі специфічні засоби аргументації. Цікаво, що суд вказав про «неповагу до суддів», а не «до суду».

Оцінка ухвали КГС була надана таким чином, що, з одного боку, це рішення Верховного Суду визначає стандарти поведінки та використання наявних технологій у судовій практиці, що мало б сприяти забезпеченню ефективності та об'єктивності розгляду справ. З іншого – така ухвала стала обмежувальною для доступу до правосуддя та використання сучасних технологій у цьому контексті; важливо врахувати різні фактори, зокрема, такі, як баланс між інноваціями та забезпеченням справедливості, етику використання технологій та потреби у забезпеченні доступності правосуддя [6, с. 192]. Є і більш категоричні формулювання, що авторитет Верховного Суду, який так емоційно обстоюється в його ухвалі, не має нічого спільного з феноменом штучного інтелекту. Він побудований на високому рівні експертизи, послідовності та здатності пояснити своє рішення, на етиці та людяності. Адвокатам не потрібен штучний інтелект, щоби помічати суперечливість висновків, неоднакове застосування норм права або упередженість та відверте підігрування на догоду певній категорії учасників процесу, наприклад через «державні інтереси» [7].

Цікаво відмітити, що позиція КГС знайшла певне продовження, коли в письмових поясненнях адвоката у справі про адміністративне правопорушення були посилання на висновки ШІ. Суд, пославшись на ухвалу КГС, зазначив, що «надання суду, у якості доказу розрахунків здійснених штучним інтелектом "ChatGPT", на підставі якого суд має встановити відсутність події і складу адміністративного правопорушення, замість надання належного доказі висновку експерта, який буде складений

особою, яка має відповідний фах та попереджена про кримінальну відповідальність, за відсутності будь яких інших доказів, суд сприймає як неповагу» [8]. Ця тенденція є небезпечною, адже як таке використання ШІ та доброчесне вказання на це оцінюється як неповага до суду. Як видається, ці дані мають оцінюватися з позицій їх змісту, характеру отримання, обґрунтованості, надійності, релевантності обставинам тощо, а не з позицій суто джерела.

До речі, натепер чинною є норма ст. 16 Кодексу суддівської етики, згідно якої використання суддею технологій штучного інтелекту є допустимим, якщо це не впливає на незалежність та неупередженість судді, не стосується оцінки доказів і процесу ухвалення рішень та не порушує вимог законодавства. Зважаючи на те, що заявником не було допущено порушень законодавства (яке, нагадаю, ніяк не регламентує використання ШІ у аргументації), то тлумачення використання ШІ як неповаги до суду / суддів викликає питання. Адже, якщо суд може використовувати ШІ, то чому учасники провадження його використовувати не можуть?

Без сумніву, ШІ породжує величезну кількість викликів у правозастосуванні, починаючи від меж використання, оцінки результатів використання, етичності, збереження чутливої інформації тощо. Цим і викликані певні складнощі тлумачення використання ШІ судом та учасниками судових проваджень. Разом з тим, визнання використання ChatGPT неповагою до суду є спробою вкласти новітні технології у прокрустове ложе традиційних правових конструкцій. Вважаємо, що ці дані мають оцінюватися по суті з позицій їх змісту, характеру отримання, обґрунтованості, надійності, релевантності обставинам тощо, а не з позицій суто джерела. Оцінка суто джерела даних є специфічним проявом обмеження у доступі до суду.

Список використаних джерел:

1. ЄДРСР. URL: https://reyestr.court.gov.ua/Review/116984639.
2. ЄДРСР. URL: https://reyestr.court.gov.ua/Review/117074064.
3. Висновок КРЄС № 26 (2023) Рухаючись вперед: використання асистивних технологій у судочинстві. URL: https://hcj.gov.ua/sites/default/files/field/vysnovok_kryes_no_26_neoficiynyy_pereklad.pdf
4. ЄДРСР. URL: https://reyestr.court.gov.ua/Review/94974180.
5. Колотуха К. А. Що таке неповага до суду і як за це можуть покарати. URL: https://protocol.ua/ua/shcho_take_nepovaga_do_sudu_i_yak_za_tse_mogut_pokarati/
6. Удовенко Ж. В., Басиста І. В. Використання штучного інтелекту у кримінальному провадженні: ілюзія чи реальність. *Штучний інтелект у правовій практиці: межі та можливості* : збірник тез Всеукраїнського круглого столу (Львів, 15 берез. 2024 р.) / упоряд. О. О. Барабаш ; Львівський державний університет внутрішніх справ. Львів : ЛьвДУВС, 2024. С. 188–197.
7. Верховний Суд образився? – блог Юлії Курило. URL: https://pravo.ua/verkhovnyi-sud-obrazyvsia-bloh-iulii-kurylo/
8. ЄДРСР. URL: https://reyestr.court.gov.ua/Review/123895750.

Гонжак Б. І.,
аспірант кафедри хірургії
(Полтавський державний медичний університет)
Малюченко П. М.,
аспірант кафедри пропедевтики ортопедичної стоматології
(Полтавський державний медичний університет)
Рибальченко Є. В.,
аспірант науково-дослідного інституту генетичних та імунологічних основ розвитку патології та фармакогенетики
(Полтавський державний медичний університет)
Стаднік Є. О.,
аспірантка кафедри внутрішньої медицини
(Полтавський державний медичний університет)
Чемерис В. В.,
аспірант кафедри хірургічної стоматології та щелепно-лицевої хірургії
(Полтавський державний медичний університет)
Войтович М. М.,
аспірант кафедри хірургії
(Полтавський державний медичний університет)
Мороховець Г. Ю.,
завідувач аспірантури, доцент кафедри громадського здоров'я з лікарсько-трудовою експертизою, кандидат педагогічних наук
(Полтавський державний медичний університет)

АНАЛІЗ РЕКОМЕНДАЦІЙ ЩОДО ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ОСВІТНЬО-НАУКОВОМУ ПРОЦЕСІ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

Глобальна цифрова трансформація інтегрувала технології штучного інтелекту (ШІ) в усі сфери життя суспільства. Освіта і наука не є виключенням, але невирішеними досі є питання етико-правових та організаційних особливостей використання технологій штучного інтелекту в освітньо-науковому процесі закладів вищої освіти України (ЗВО). Використання технологій ШІ в середовищі ЗВО має врегульовуватися відповідно до чинного законодавства України, враховувати досвід провідних міжнародних інституцій, відбуватися у руслі дотримання норм академічної доброчесності.

Метою нашого дослідження був аналіз вітчизняних нормативних документів, практик міжнародних організацій задля окреслення основних вимог до адміністрацій закладів, наукових, науково-педагогічних працівників, здобувачів вищої освіти щодо використання штучного інтелекту в середовищі ЗВО.

Нами проаналізовано AI Act, рекомендації Організації економічного співробітництва та розвитку (ОЕСР) з питань штучного інтелекту, Закон України «Про авторське право та суміжні права» (Закон), Концепцію розвитку штучного інтелекту, затверджену розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р (Концепція).

Нами досліджено особливості регулювання освітньо-наукової діяльності у міжнародному освітньому просторі. Зокрема, проаналізовано політики використання ШІ, встановлені Міжнародною асоціацією університетів (МАУ), та Європейською асоціацією університетів (ЄАУ), Великою Хартією університетів (ВХУ).

AI Act – це пропозиція Європейської Комісії, що має на меті регулювати штучний інтелект в Європейському Союзі. Основна мета – забезпечити безпеку та повагу прав людини, а також сприяти інноваціям у сфері ШІ. Цей регулятивний документ пропонує класифікацію ШІ-систем на основі рівня ризику: низький (наприклад, відеоігри), середній (наприклад, чат-боти), високий (наприклад, системи для кримінального правосуддя, медицини, транспорту) та неприпустимий (заборонені системи, наприклад, системи соціального скорингу та маніпулятивні ШІ). Це дозволяє визначити, які системи потребують додаткових заходів контролю**.** До систем високого ризику сформовані наступні вимоги: прозорість алгоритмів, наявність механізмів контролю людиною, забезпечення якості даних, реєстрація та сертифікація [1].

Рекомендації ОЕСР з питань ШІ, затверджені у 2019 році як перша міжнародна нормативна рамка, базуються на п’яти ключових принципах: **людиноцентричність**, **прозорість**, **надійність**, **відповідальність** та **адаптивність політики**. Документ проголошує необхідність використання ШІ для досягнення загального добробуту суспільства за умови дотримання прав людини та демократичних цінностей суспільства відкрито й прозоро. ОЕСР також закликає до **міжгалузевого співробітництва**, інвестування в дослідження, освітні ініціативи з цифрової грамотності та створення гнучких регуляторних механізмів, здатних адаптуватися до динаміки технологій. Для вищої освіти це означає інтеграцію етичних стандартів у навчальні програми, підтримку міждисциплінарних досліджень та формування критичного мислення у користуванні ШІ-інструментами, що відповідає глобальним викликам та стратегії гармонізації з європейським освітнім простором [2].

Закон регулює відносини, пов’язані зі створенням і використанням творів, але не враховує специфіку творчості, згенерованої ШІ. Так, пунктом 35, статті 1 Закону встановлено, що оригінальність твору – ознака (критерій), що характеризує твір як результат власної інтелектуальної творчої діяльності автора та відображає творчі рішення, прийняті автором під час створення твору. При цьому автором твору визначено фізичну особу, яка своєю творчою діяльністю створила твір. Звідси – технології штучного інтелекту не можуть виступати суб’єктами авторського права на твір, що породжує необхідність регулювання їх використання при створенні академічних текстів [3].

Концепція затверджена розпорядженням Кабінету Міністрів України від 2 грудня 2020 року № 1556-р, визначає стратегічні напрями інтеграції ШІ у різні сфери суспільного життя, включаючи освіту, економіку та державне управління. Документ акцентує на необхідності створення сприятливого середовища для розвитку інновацій, зокрема через підтримку наукових досліджень, розробку національних стандартів етичного використання ШІ та забезпечення правової регуляції. Концепція передбачає активну роль вищої освіти у підготовці фахівців зі ШІ, розвитку цифрової грамотності та формуванні етичних принципів використання технологій. Важливим аспектом є забезпечення **безпеки даних**, **прозорості алгоритмів** та **захисту прав користувачів**, що відповідає міжнародним стандартам, зокрема рекомендаціям ОЕСР. Однак, для реалізації Концепції необхідно подолати низку викликів, таких як недостатнє фінансування, брак кваліфікованих кадрів та відсутність комплексної інфраструктури. У контексті вищої освіти це вимагає розробки нових навчальних програм, підвищення кваліфікації викладачів та активізації міжнародного співробітництва для адаптації українських університетів до глобальних трендів у сфері ШІ [4].

МАУ активно досліджує вплив ШІ на вищу освіту та розробляє **рекомендації, стратегії та політики**, які можуть використовувати університети та уряди в цілому. Узагальнивши положення, проголошені МАУ у своїх документах на офіційному вебсайті, можемо виділити основні принципи організації щодо використання ШІ. Так, встановлено, що ШІ впливає на методи викладання, навчання та оцінювання університетів, світовій академічній спільноті необхідно приймати г**лобальні етичні стандарти** для використання ШІ в освіті. МАУ рекомендує розглядати **гібридний підхід**, де поєднувалися б традиційне навчання та цифрові технології, наголошує на необхідності забезпечення прозорості використання ШІ, створенню і розвитку політик університетів щодо його використання для запобігання академічній недоброчесності.

Після активних дискусій і зростаючого занепокоєння, викликаних появою ChatGPT та інших інструментів ШІ, керівний комітет з питань навчання та викладання Європейської асоціації університетів висловив основні рекомендації для європейських університетів.

Особливу увагу у питаннях застосування штучного інтелекту в освітній і науковій діяльності університетів привертають застереження, висунуті Європейською асоціацією університетів у Artificial intelligence tools and their responsible use in higher education learning and teaching (European University Association, 2023) [5]. Відповідно до цього, використання ШІ супроводжується низкою недоліків, зокрема: відсутністю посилань на джерела; упередженістю даних та алгоритмів; питаннями інтелектуальної власності та авторських прав; проблемами, пов'язаними з конфіденційністю, безпекою даних і забезпеченням справедливості.

Водночас штучний інтелект має потенціал для покращення академічної діяльності, зокрема підвищення ефективності, впровадження персоналізованого навчання та створення нових підходів до роботи. Очевидно, що заборона використання ШІ та інших сучасних технологій є марною. Тому система вищої

освіти повинна адаптувати свої методи навчання, викладання та оцінювання, щоб забезпечити ефективне та відповідальне використання ШІ.

ВХУ закріплює основні цінності, права та обов'язки університету як ключового інституту суспільства, діяльність якого присвячена визначенню й поширенню найважливіших принципів і знань, наданню суспільству інтелектуальних орієнтирів. Організація проголошує, що дослідницька та викладацька діяльності мають бути морально й інтелектуально незалежними від будь-якої політичної й економічної влади, освіта та наука мають адаптуватися до вимог сучасного суспільства, забезпечуючи академічні свободи, підтримуючи бажання студентів отримувати нові знання і вчитися використовувати інновації.

Таким чином, європейські та українські нормативні документи визначають необхідність регулювання використання ШІ в освіті і науці, а провідні міжнародні та європейські освітні організації приймають політики доброчесного використання ШІ учасниками освітньо-наукового процесу. Загалом, можемо виокремити основні вимоги до використання ШІ у ЗВО:

– прозорість використання ;

– забезпечення механізмів контролю людиною;

– забезпечення якості даних та, за необхідності, їх конфіденційності;

– забезпечення дотримання норм законодавства щодо інтелектуальної власності та авторських прав;

– підвищення рівня цифрової грамотності і студентів, і викладачів;

– активізація міжнародного співробітництва для адаптації українських університетів до глобальних трендів у сфері ШІ;

– створення і розвиток політик університетів щодо використання ШІ для запобігання академічній недоброчесності.

Враховуючи можливості технологій ШІ зі спрощення рутинних операцій вважаємо, що їх використання, за умови декларування учасниками освітньо-наукового процесу, може бути корисним для пошуку джерел досліджень по обраній темі; створення навчальних матеріалів – презентацій, відеолекцій; аналізу правильності оформлення наукових робіт, відповідності стандартам цитування, перевірки орфографічних та стилістичних помилок; надання довідкової інформації, нагадувань про дедлайни та консультацій (застосунки та чат-боти), виявлення академічного плагіату та інших порушень академічної доброчесності; симуляції діагностики та лікування (віртуальні пацієнти тощо).

З огляду на роль університетів у сучасному науковому просторі та вагому частку інновацій, створених саме закладами вищої освіти, варто зауважити, що використання ШІ у освітньо-науковому процесі має значні обмеження. Тому вважаємо, що ШІ не може виступати автором наукових текстів, а також рецензентом, не може використовуватися для аналізу наукової продукції під час атестації здобувачів освітньо-наукового ступеня доктора філософії, наукового ступеня доктора наук. У освітньо-науковому процесі медичного ЗВО, використання ШІ для постановки діагнозу або призначення лікування без контролю лікаря є неприпустимим. Не можна допускати надання персональних даних без згоди пацієнта, оскільки використання ШІ для аналізу медичних даних

без належної анонімізації та отримання інформованої згоди пацієнтів порушує етичні стандарти та законодавство про захист даних.

Списки допустимих сфер застосування ШІ у освітньо-науковому процесі ЗВО та перелік заборон не є вичерпним, зокрема на законодавчому рівні. Ці списки динамічно змінюються з ростом технологічних рішень та програмних засобів на ринку та у відкритому доступі. Для наукових та науково-педагогічних працівників важливим є дотримання норм законодавства щодо інтелектуальної творчості та авторських прав, а також декларування використання ШІ при створенні академічних текстів.

Адміністрації ЗВО мають приймати локальні нормативні документи та дієві механізми впливу, які б ґрунтувалися на законодавстві України, міжнародних нормативах, практиках міжнародних освітніх інституцій та високорейтингових наукових видань і авторитетних видавництв, та спрямовувалися на використання технологій ШІ у розрізі дотримання академічної доброчесності усіх учасників освітньо-наукового процесу.

Список використаних джерел:

1. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). Official Journal of the European Union.
2. OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449
3. Про авторське право та суміжні права : Закон України від 01.12.2022 № 2811-IX (станом на 15.11.2024).
4. КОНЦЕПЦІЯ розвитку штучного інтелекту в Україні : схвалено розпорядженням Кабінету Міністрів України від 2 грудня 2020 № 1556-р.
5. Artificial intelligence tools and their responsible use in higher education learning and teaching. European University Association.

Деревянко Н. З.,
декан юридичного факультету,
доктор філософії в галузі права, доцент
(Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука, м. Рівне)

ЩОДО МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ ПРАКТИКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПОЛІЦЕЙСЬКИМИ ІСПАНІЇ В УКРАЇНІ

Ще з моменту проголошення незалежності України політики, юристи та науковці намагаються знайти все краще у законодавствах зарубіжних країн та впровадити його у національне законодавство. Не є виключенням і питання застосування можливостей штучного інтелекту при розслідуванні злочинів.

Однак постає логічне питання. Чи можливо використовувати алгоритми штучного інтелекту інших країн в Україні.

Відповідно до Європейської етичної хартії про використання штучного інтелекту в судових системах та їх оточення штучний інтелект – це сукупність наукових методів, теорій та технік, мета яких – відтворити машиною когнітивні здібності людини [1].

На наше глибоке переконання в жодній країні не існує позитивних практик розслідування кримінальних правопорушень за допомогою штучного інтелекту на усій стадії досудового розслідування. Водночас залучення можливостей штучного інтелекту на окремих стадіях розслідування є досить дієвим та в окремих випадках може приносити конкретні результати.

Зокрема позитивним прикладом використання для України є алгоритм штучного інтелекту VeriPol, який був розроблений у 2017 році вченими із Мадридського університету імені Карла III і Кардіфського університету в Уельсі. Суть алгоритму полягає у тому, що під час прийняття рішення за повідомленням про вчинення кримінального правопорушення в Іспанії він здатен виявляти неправдиві повідомлення в поліцію на основі аналізу їх змісту. Ця технологія була вдало протестована поліцією Іспанії. Так, слідчі систематично перевіряли всі висновки штучного інтелекту на особистих зустрічах із заявниками. Як наслідок у 83% випадків версія заявника не підтверджувалася, наслідком чого було закриття провадження [2].

На сьогодні слідчі перевантажені низкою кримінальних проваджень. Адже, відповідно до вимог КПК України, заява або повідомлення про вчинення кримінального правопорушення не пізніше доби повинно бути внесено до ЄРДР і по ньому повинно розпочатись досудове розслідування. Введення алгоритму штучного інтелекту VeriPol в Україні значно дозволить розгрузити слідчих та приймати відповідні рішення на підставі висновків штучного інтелекту, за умови внесення відповідних змін до КПК України.

Список використаних джерел:

1. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c (дата звернення 20.02.2025);

2. Вчені із Уельсу і Іспанії розробили алгоритм, що був настільки ефективним, що його на озброєння взяла поліція Іспанії. Алгоритм VeriPol визначає на які заяви не потрібно поліції витрачати свої сили. URL: https://hightech.plus/2018/10/29/ii-detektor-lzhi-vichislyaet-vruna-po-ego-pismam (дата звернення 19.02.2025).

Джупіна Х. О.,
студентка 1 курсу 2 групи ІПБ
спеціальності «Право»
(Одеський державний університет внутрішніх справ)
Пядишев В. Г.,
професор кафедри кримінального аналізу
та інформаційних технологій,
доктор юридичних наук, професор,
(Одеський державний університет внутрішніх справ)

ШТУЧНИЙ ІНТЕЛЕКТ У БОРОТЬБІ ЗІ ЗЛОЧИННІСТЮ (ЗАРУБІЖНИЙ ДОСВІД)

Згідно з даними та поточними тенденціями, кіберзлочинці вже широко використовують ШІ у своїх злочинних цілях. Зокрема, вони використовують IoT для створення та розповсюдження шкідливих програм і програм-вимагачів за допомогою технологій ШІ. Очікується, що понад 2,5 мільйона пристроїв, включаючи промислові та операторів ключової інфраструктури, будуть повністю підключені до Інтернету протягом наступних п’яти років, що збільшить уразливість компаній і споживачів до кібератак [1, с. 1522].

З іншого боку, столичні міста та організації по всьому світу вливають грошову допомогу в запобігання злочинності за допомогою ШІ. Основною метою інвестицій є прогнозування злочинності, а злочинність має бути легко виявлена за допомогою програм ШІ. Щоб перехопити злочини, уряди повинні мати можливість збирати значні обсяги даних, щоб знаходити шаблони, які можуть бути практичними для правоохоронних органів і алгоритмів ШІ.

Відповідно, ШІ все частіше успішно використовується правоохоронними органами для ефективних заходів із запобігання злочинності. Нові технології дозволяють перевантаженим і неукомплектованим правоохоронним органам збирати, обробляти, аналізувати та висвітлювати відповідні дані для розслідувачів будь-яких видів злочинів. Це включає рішення штучного інтелекту для збору та інтерпретації зв’язків і закономірностей у фінансових записах, геопросторових зображеннях, записах камер спостереження, даних соціальних мереж, публічних записах, стрічках новин і багатьох інших відкритих і закритих джерелах. Використовуючи можливості штучного інтелекту, правоохоронні агентства мають потенціал для аналізу величезних обсягів даних з більшою швидкістю та точністю.

Ось кілька способів, через використання яких штучний інтелект допомагає боротися зі злочинами та запобігати їм, а також прогнозувати ймовірність майбутніх злочинів [2, с. 1–6]:

- проникнення до темної мережі за допомогою ШІ та викриття широкого спектру незаконних послуг;
- викривання тенденцій злочинності шляхом глибокого навчання;
- ідентифікація жертв за допомогою машинного навчання;

- моніторинг онлайн-платформ злочинної діяльності;
- майнінг для даних та використання аналізу шаблонів – для визначення локації злочину або де існує високий ризик підозрілої діяльності;
- створення прогнозної аналітики для пом'якшення та попередження злочинності, зниження рівня злочинності та підвищення рівня громадської безпеки;
- встановлення злочинців, а також телефонних номерів, пов'язаних зі злочинною діяльністю, та адрес інтернет-протоколів;
- протидія торгівлі дітьми, зокрема, через аналіз Інтернет-трафіку;
- моделювання злочинної поведінки та імітація дій та рішень злочинців.

Одне з найкорисніших застосувань штучного інтелекту для запобігання та зниження злочинності полягає у розподілі ресурсів. Оскільки практично всі правоохоронні органи відчувають нестачу персоналу та коштів, цінність і важливість розподілу ресурсів і розгортання відіграє життєво важливу роль у запобіганні злочинності. Було доведено, що складні алгоритми мають швидкий і ефективний успіх, допомагаючи організаціям кримінального правосуддя краще зрозуміти «хто, що, коли, де, як і чому» стосовно злочинва в їхніх юрисдикціях. ШІ може визначати та ідентифікувати релевантні моделі злочинності, які найкраще можна вирішити за допомогою коригування розподілу ресурсів, наприклад часу патрулювання поліцейських автомобілів, пішохідних патрулів, охоронців, фізичних бар'єрів, сигналізації або часу реагування служб екстреної допомоги та швидкого реагування. Шаблони можуть відображати сезонні, географічні чи демографічні тенденції, які швидко визначаються за допомогою аналізу розвідувальних даних із усіх джерел за допомогою штучного інтелекту, у спосіб, який неможливо отримати за допомогою традиційних аналітичних засобів [3, с. 1].

Виявленням та попередженням злочинів переймаються не тільки безпосередньо правоохоронні органи. Сьогодні цю роботу проводять також і численні приватні компанії, зокрема, банки.

Компанії використовують штучний інтелект (ШІ), щоб запобігати та виявляти все: від звичайних крадіжок співробітників до інсайдерської торгівлі. Багато банків і великих корпорацій використовують ШІ для виявлення та запобігання шахрайству та відмиванню грошей. Компанії соціальних медіа використовують машинне навчання для блокування незаконного контенту, наприклад дитячої порнографії. Компанії постійно експериментують із новими способами використання штучного інтелекту для кращого управління ризиками та швидшого виявлення шахрайства та навіть для прогнозування та запобігання злочинам.

Хоча сучасна базова технологія не обов'язково є революційною, алгоритми, які вона використовує, і результати, які вони можуть отримати, є революційними. Наприклад, банки десятиліттями використовують системи моніторингу транзакцій, засновані на попередньо визначених двійкових правилах, які вимагають перевірки виходу вручну. Рівень успішності загалом низький: у середньому лише 2 % транзакцій, позначених системами, зрештою

відображають справжній злочин або зловмисний намір. Навпаки, сучасні рішення машинного навчання використовують правила прогнозування, які автоматично розпізнають аномалії в наборах даних. Ці розширені алгоритми можуть значно зменшити кількість помилкових сповіщень, відфільтровуючи випадки, які були позначені неправильно, одночасно виявляючи інші, пропущені за допомогою звичайних правил [5, с. 2–5].

Список використаних джерел:

1. Phalke V. S.. Gund P., Patil S. Investigating Crime: a Role of Artificial Intelligence in Criminal Justice. *The Online Journal of Distance Education and e-Learning.* April 2023. Site. URL: https://www.researchgate.net/publication/371416448_INVESTIGATING_CRIME_A_ROLE_OF_ARTIFICIAL_INTELLIGENCE_IN_CRIMINAL_JUSTICE (дата звернення: 04.03.2025).

2. Sadulski J. Artificial Intelligence in Crime Detection: How It's Useful. American *Military University. Information Technology. 6/12/2024.* Site. URL: https://www.amu.apus.edu/area-of-study/information-technology/resources/artificial-intelligence-in-crime-detection/ (дата звернення: 04.03.2025).

3. Leveraging Artificial Intelligence for Crime Prevention. *Voyager-Labs.* March 2022. Site. URL: https://www.voyager-labs.com/leveraging-artificial-intelligence-for-crime-prevention/ (дата звернення: 04.03.2025).

4. Quest L., Charrie A. and Roy S. The Risks And Benefits Of Using AI To Detect Crime. *OliverWyman.Com.* April 2023. Site. URL: https://www.oliverwyman.com/our-expertise/insights/2018/aug/the-risks-and-benefits-of-using-ai-to-detect-crime.html (дата звернення: 04.03.2025).

Добкіна К. Р.,
в. о. декана юридичного факультету,
доктор юридичних наук, професор
(Державний університет інфраструктури та технологій)

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В МЕДІАЦІЇ

Штучний інтелект все більше і більше занурюється в наше життя, у всі сфери та напрями нашої діяльності.

Використання штучного інтелекту (ШІ) в медіації – це відносно нова, але швидко зростаюча сфера. Медіація – позасудова добровільна, конфіденційна, структурована процедура, під час якої сторони за допомогою медіатора (медіаторів) намагаються запобігти виникненню або врегулювати конфлікт (спір) шляхом переговорів [1]. ШІ може допомогти в різних аспектах медіації, роблячи процес більш ефективним і доступним. Ось деякі з ключових способів застосування ШІ в медіації:

1. Аналіз даних та оцінка ризиків:

- ШІ може аналізувати великі обсяги даних, щоб виявити закономірності та тенденції в конфліктах.
- Це може допомогти медіаторам оцінити ризики та передбачити потенційні проблеми, дозволяючи їм більш ефективно керувати процесом

(Наприклад, ШІ може аналізувати тексти повідомлень, електронні листи або соціальні мережі, щоб виявити емоційні стани учасників конфлікту).

2. Сприяння комунікації:

- ШІ може допомогти покращити комунікацію між сторонами конфлікту, надаючи інструменти для перекладу мови, аналізу тону та виявлення потенційних непорозумінь.
- Чат-боти з ШІ можуть надавати інформацію про процес медіації та відповідати на загальні запитання, звільняючи час медіаторів.

3. Підтримка прийняття рішень:

- Системи ШІ можуть допомогти сторонам конфлікту досліджувати різні варіанти та оцінювати їхні потенційні наслідки.

4. Автоматизація адміністративних завдань:

- ШІ може автоматизувати багато адміністративних завдань, пов'язаних з медіацією, таких як планування зустрічей, документування та звітність.
- Це може звільнити час медіаторів, дозволяючи їм зосередитися на більш важливих аспектах процесу.

Але важливими залишаються питання наступного характеру:

- Незважаючи на потенційні переваги, важливо пам'ятати, що ШІ не може повністю замінити людського медіатора.
- Медіація – це складний процес, який вимагає емпатії, розуміння та міжособистісних навичок.
- ШІ може бути цінним інструментом для медіаторів, але він повинен використовуватися відповідально та етично.
- Використання ШІ в медіації порушує етичні питання, пов'язані з конфіденційністю, неупередженістю та відповідальністю.
- Важливо забезпечити, щоб технології ШІ були доступні всім сторонам, незалежно від їхніх технічних навичок та фінансових можливостей.
- Оскільки медіація часто включає конфіденційну інформацію, дуже важливо, щоб системи ШІ були безпечними та захищеними від несанкціонованого доступу.

Важливо враховувати етичні та практичні міркування, щоб забезпечити відповідальне та ефективне використання штучного інтелекту та ні в якому разі не порушити основні принципи медіації конфіденційність, добровільність, нейтральність.

Список використаних джерел:

1. Закон України «Про медіацію» від 16.11.2021.

Дорош В. М.,
здобувач першого (бакалаврського) рівня вищої освіти
(Навчально-науковий інститут права
Державного податкового університету)
Лісова К. С.,
доцент кафедри міжнародного права
та права Європейського Союзу,
кандидат історичних наук, доцент
(Навчально-науковий інститут права
Державного податкового університету)

ШТУЧНИЙ ІНТЕЛЕКТ У ДОКУМЕНТУВАННІ ТА АНАЛІЗІ ПОРУШЕНЬ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА

У сучасному світі, де збройні конфлікти продовжують виникати, документування та аналіз порушень міжнародного гуманітарного права (МГП) набуває критичного значення. Штучний інтелект (ШІ) відкриває нові можливості для підвищення ефективності цих процесів, одночасно створюючи етичні та правові виклики.

Сучасні системи ШІ здатні опрацьовувати величезні масиви даних, що надходять із зон конфліктів, включаючи відео, фотографії, текстові повідомлення та супутникові знімки. Алгоритми машинного навчання можуть виявляти потенційні порушення МГП, класифікуючи їх за типами та ступенем серйозності, що дозволяє правозахисникам та міжнародним організаціям ефективніше розподіляти обмежені ресурси для розслідування.

Водночас слушною є думка Т. Федчука, який зазначає, що невизначеність дефініції штучного інтелекту ускладнює врегулювання його юридичного статусу. Сьогодні активно досліджуються перспективи використання систем озброєння під керуванням ШІ, що з'явилися внаслідок еволюції інформаційно-телекомунікаційних технологій. Впровадження таких інновацій породжує комплексні виклики на правовому, політичному, моральному та етичному рівнях. Очевидно, що технологічний прогрес випереджає розвиток міжнародного гуманітарного права, якому притаманна переважно реактивна природа, а не здатність передбачати специфіку застосування нових технологічних рішень [1, с. 786].

Технології комп’ютерного зору забезпечують аналіз візуальних матеріалів з безпрецедентною швидкістю та точністю. Наприклад, алгоритми можуть ідентифікувати пошкодження цивільної інфраструктури, розпізнавати заборонені види зброї або виявляти сліди масових поховань на супутникових знімках. Такі інструменти стають особливо важливими у ситуаціях обмеженого фізичного доступу до зон конфлікту.

Важливою перевагою застосування ШІ є можливість обробки інформації в режимі реального часу. Технології розпізнавання об’єктів та комп’ютерного зору дозволяють ідентифікувати зброю, військову техніку та інші елементи, що

можуть свідчити про порушення норм ведення війни. Системи аналізу природної мови допомагають виявляти релевантну інформацію в соціальних мережах та новинних повідомленнях, створюючи цілісну картину подій.

Особливу цінність представляють системи верифікації даних, засновані на ШІ, які перевіряють автентичність матеріалів та виявляють маніпуляції з відео, фото та аудіо. В еру дезінформації та фейкових новин такі технології забезпечують надійність доказової бази для юридичних процесів. Алгоритми можуть розпізнавати ознаки глибинних підробок (deepfakes) та аналізувати метадані файлів для встановлення їх походження.

Застосування ШІ для аналізу великих даних (big data) дозволяє виявляти приховані закономірності та зв'язки між подіями, що можуть вказувати на системні порушення МГП. Наприклад, співставлення даних про переміщення військових підрозділів із повідомленнями про напади на цивільних осіб може встановити причинно-наслідкові зв'язки та ідентифікувати відповідальних командирів.

Проте впровадження ШІ у сферу документування порушень МГП пов'язане з суттєвими викликами. Алгоритмічна упередженість може призвести до нерівномірної уваги до окремих конфліктів або типів порушень. Залежність від цифрових даних може створити «сліпі зони» у регіонах з обмеженим доступом до інтернету. Крім того, виникають питання щодо достовірності доказів, зібраних за допомогою ШІ, та їх прийнятності в юридичних процедурах.

Проблема «чорної скриньки» алгоритмів ШІ створює додаткові перешкоди для використання їх результатів у судових процесах. Міжнародні трибунали вимагають прозорості та можливості перевірки методології збору доказів, тоді як багато сучасних нейромережевих систем працюють за принципами, що складно пояснити та відтворити. Розвиток пояснюваного ШІ (explainable AI) стає критично важливим для подолання цього бар'єру.

Етичні аспекти застосування ШІ включають захист конфіденційності потерпілих та свідків, забезпечення безпеки даних та запобігання зловживанням технологіями для створення дезінформації. Необхідно розробити чіткі стандарти та протоколи використання ШІ, які забезпечать баланс між ефективністю та захистом прав людини.

Як стверджує Ю. Коваленко, застосування систем на базі штучного інтелекту, безсумнівно, навіть у щоденних ситуаціях містить потенційні загрози для фундаментальних людських прав. Попри всі переваги цих інноваційних технологій, варто визнати, що їх впровадження породжує серйозні виклики у контексті захисту приватності та забезпечення свободи висловлювань. Такі технології, з одного боку, розширюють наші можливості, а з іншого – створюють ризики для базових громадянських свобод [2].

Варто також звернути увагу на потенційні ризики надмірної залежності від технологій. «Людський фактор» залишається незамінним при оцінці контексту порушень, розумінні культурних особливостей та врахуванні нюансів конкретних ситуацій. Тому оптимальним підходом виглядає гібридна

модель, де ШІ виступає потужним інструментом у руках кваліфікованих спеціалістів з міжнародного гуманітарного права.

Міжнародне співробітництво у розробці стандартів використання ШІ для документування порушень МГП стає все більш нагальним. Організації на кшталт ООН, Міжнародного комітету Червоного Хреста та Міжнародного кримінального суду повинні активно долучатися до формування правил та найкращих практик у цій сфері, забезпечуючи їх відповідність принципам гуманітарного права.

У перспективі, розвиток ШІ має потенціал трансформувати процеси документування та аналізу порушень МГП, сприяючи підвищенню відповідальності за військові злочини та, зрештою, зміцненню міжнародного гуманітарного права. Поєднання технологічних інновацій з ретельним етичним аналізом та міжнародним співробітництвом відкриває шлях до більш ефективного захисту жертв збройних конфліктів та притягнення до відповідальності тих, хто порушує правила ведення війни.

Список використаних джерел:

1. Федчук Т. Ю. Контроль дотримання норм міжнародного гуманітарного права при використанні зброї керованої штучним інтелектом. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2024. № 2. С. 785–791. URL: https://doi.org/10.24144/2788-6018.2024.02.129.
2. Штучний інтелект та права людини: які принципи мають бути дотримані – Медіацентр Україна. *Медіацентр Україна*. URL: https://mediacenter.org.ua/uk/.

Дубняк М. В.,
завідувачка наукової лабораторії
проблем штучного інтелекту і права,
кандидат юридичних наук
(Науковий центр цифрової трансформації і права
ДНУ «Інститут інформації безпеки
і права НАПрН України»)
https://orcid.org/0000-0001-7281-6568

ЕЛЕКТРОННІ ПОСЛУГИ ТА ШТУЧНИЙ ІНТЕЛЕКТ

Вперше у законодавстві України термін «електронна послуга» визначено у Стратегії розвитку інформаційного суспільства в Україні (2013 рік). У Концепції розвитку електронних послуг в Україні (2016 рік) визначено, що з розвитком інформаційного суспільства та суспільних відносин виникає необхідність надання адміністративних та інших публічних послуг в електронній формі. У Концепції 2016 року вказувалось на проблему несформованості нормативно-правової бази, що регулює сферу надання електронних послуг [1]. У період з 2016 по 2025 рік нормативних актів, які регулюють надання електронних послуг стало більше, але вони не формують єдиної системи. В чинних нормативних

актах (Закон України «Про адміністративні послуги», Закон України «Про особливості надання публічних (електронних публічних) послуг») послуги визначаються як: «адміністративна послуга», «електрона послуга», «публічна послуга», «електронна публічна послуга», «автоматичний режим надання електронної публічної послуги» тощо.

Генезу адміністративно-правового забезпечення сфери адміністративних послуг в Україні можна представити трьома етапами: 2000–2015 роки – інформаційний етап – нормативно-правові акти у сфері адміністративних послуг; 2016–2020 роки – електронний етап – нормативно-правові акти у сфері електронних послуг; 2021–2025 роки – цифровий етап – нормативно правові акти у сфері електронних автоматичних послуг.

До освновних нормативних актів третього (цифрового) етапу відносяться наступні: Закон України «Про особливості надання публічних (електронних публічних послуг)», План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки, схвалений розпорядженням Кабінету Міністрів України № 438-р; Закон України «Про публічні електронні реєстри», Закон України «Про національну програму інформатизації», Закон України «Про хмарні послуги», Закон України «Про адміністративну процедуру», Концепція Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року, схвалена розпорядженням Кабінету Міністрів України № 320-р, Зміни, що вносяться до Положення про Єдиний державний вебпортал електронних послуг затверджених Постановою Кабінету Міністрів України № 693, Стратегія цифрового розвитку інноваційної діяльності України на період до 2030 року схвалена розпорядженням Кабінету Міністрів України № 1351-р [2].

Закон України «Про особливості надання публічних (електронних публічних послуг)» визначає, що автоматичний режим надання електронної публічної послуги – надання електронної публічної послуги програмними засобами інформаційно-телекомунікаційних систем, без додаткового опрацювання суб'єктом надання електронної публічної послуги у режимі реального часу або з відкладальною умовою на підставі заяви (звернення, запиту) суб'єкта звернення, у тому числі поданої в електронній формі з використанням інформаційно-телекомунікаційних систем (у тому числі з використанням Єдиного державного вебпорталу електронних послуг) [3].

Постановою Кабінету Міністрів України від 13 червня 2024 року № 693 було внесено зміни до Положення про Єдиний державний вебпортал електронних послуг, яким передбачено можливість використання технологій штучного інтелекту на вебпорталі електронних послуг (п. 6, п.п. 27-5) [4].

Прийнята, у грудні 2024 року Стратегія цифрового розвитку інноваційної діяльності України на період до 203 року (далі – Стратегія WinWin) містить Стратегічну ціль 12 «розвиток спроможностей держави шляхом впровадження технологій у сфері урядування (govtech)». Такі технології спрямовані на підвищення ефективності, прозорості та доступності державних послуг для громадян, шляхом розробки та впровадження цифрових рішень, автоматизації

процесів, використання великих даних, штучного інтелекту та інших передових технологій у державному управлінні [5].

Для досягнення цієї цілі передбачається затвердження процедурних стандартів підготовки, закупівлі, реалізації, приймання та впровадження цифрових продуктів з урахуванням їх відмінностей та особливостей; розроблення та подання нормативно-правових актів щодо єдиних стандартів для всього циклу розробки програмного забезпечення, включаючи проєктування, тестування, впровадження та підтримку [5].

Стратегія WinWin більше орієнтована на формування інноваційної екосистеми, зокрема, створення govtech-інкубаторів, просування експорту успішних govtech-рішень для посилення технологічного бренду України, проведення досліджень, навчань та тренінгів [5], проте не є документом, який на системному рівні визначає стратегію розвитку електронних послуг.

Висновки. Адміністративно-правове забезпечення електронних послуг в Україні пройшло тривалий період становлення, який систематизовано у три етапи: 1) інформаційний етап (2000–2015 роки); 2) електронний етап (2016–2020 роки); 3) цифровий етап (2021–2025 роки). За ці три етапи суттєво трансформувався термінологічний апарат адміністративних послуг, проте у чинних нормативних актах немає єдиного підходу до визначення особливостей їх надання з урахуванням новітніх технологій.

Особливості цифровізації електронних послуг, та впровадження технологій штучного інтелекту для забезпечення їх надання програмними засобами без додаткового опрацювання суб'єктом надання електронної публічної послуги, містяться в нормативних актах різної юридичної сили: у Законах України, Стратегіях, Постановах Уряду. Такий хаотичний підхід не сприятиме сталому цифровому переходу для впровадження технологій штучного інтелекту в публічне адміністрування та електронні послуги. Цю проблему правової невизначеності можливо вирішити шляхом узгодження пріоритетних напрямків розвитку цифрового урядування, розвитку GovTech рішень шляхом прийняття окремої спеціальної стратегії.

Список використаних джерел:

1. Концепція розвитку електронних послуг в Україні: схвалено розпорядженням Кабінету Міністрів України від 16 листопада 2016 р. № 918-р. URL: https://zakon.rada.gov.ua/laws/show/918-2016-%D1%80#Text

2. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/main/index.

3. Про особливості надання публічних (електронних публічних послуг) : Закон України № 1689-IX в редакції від 02.09.2024. URL: https://zakon.rada.gov.ua/laws/show/1689-20#Text

4. Зміни до Положення про Єдиний державний вебпортал електронних послуг: затверджені Постановою Кабінету Міністрів України від 13 червня 2024 р. № 693. URL: https://zakon.rada.gov.ua/laws/show/693-2024-%D0%BF#Text.

5. Стратегія цифрового розвитку інноваційної діяльності України на період до 2030 року: схвалено розпорядженням Кабінету Міністрів України від від 31 грудня 2024 р. № 1351-р. URL: https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text.

Дудіна О. В.,
доцент кафедри теоретичних дисциплін,
кандидат педагогічних наук, доцент
(Донецький національний медичний університет)

ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ В МЕДИЧНУ ОСВІТУ КИТАЮ ТА ЯПОНІЇ

Інновації в медицині та медичній освіті стають ключовими елементами розвитку глобальної системи охорони здоров'я у XXI столітті. Старіння населення та зростання кількості хронічних захворювань, неперервний технологічний процес спричинюють актуальність у вдосконаленні підходів до підготовки лікарів. Китай і Японія, відомі власною інноваційністю та довголіттям своїх громадян, викликають особливий інтерес щодо вивчення новаторських підходів до медичної освіти.

У липні 2017 року Китай створив комплексну стратегію щодо штучного інтелекту (ШІ) під назвою «План розвитку штучного інтелекту нового покоління» (План Китаю щодо ШІ, 2017) з конкретною метою стати світовим лідером у сфері ШІ до 2030 року [1]. 2017 року Китай запустив план «Подвійний університет першого класу», спрямований на комплексне перетворення елітних китайських університетів і їхніх факультетів на заклади світового класу до кінця 2050 року. План має 42 «Подвійні університети першого класу» та 95 «Подвійних першокласних дисциплін» (MOE, 2017).

Японська стратегія щодо штучного інтелекту має назву «AI Strategy 2019». Стратегія була розроблена з метою інтеграції ШІ в різні сфери суспільства, зокрема в освіту, охорону здоров'я, промисловість та інші галузі, для забезпечення конкурентоспроможності країни в глобальному контексті [2]. У квітні Міністерство внутрішніх справ і комунікацій Японії (Ministry of Internal Affairs and Communications) спільно з Міністерством економіки, торгівлі та промисловості (Ministry of Economy, Trade and Industry) запустили першу версію «Керівних принципів щодо використання штучного інтелекту в бізнесі» («AI Guidelines for Business Ver1.0»), які узгоджуються з міжнародними дискусіями та тенденціями та покликані забезпечити чітке, доступне та добровільне керівництво для розробників, постачальників і користувачів ШІ [2].

Традиційний підхід до медичної освіти передбачає теоретичне навчання як основу, а потім набуття клінічних навичок через безпосередній контакт із пацієнтами під час клінічної практики. Віртуальні симуляційні експерименти стали основним ресурсом для підготовки здобувачів освіти до застосування технічних навичок. Вони широко використовуються у хірургічних тренуваннях, радіологічній освіті, анатомії, навчанні медичних сестер, біохімії та молекулярних техніках. Дослідження Х. Чжу, Дж. Сюй та інших «Стан віртуальних симуляційних експериментів у медичній освіті Китаю: на основі Національного центру викладання віртуальних симуляційних експериментів

(iLAB-X)» («The status of virtual simulation experiments in medical education in China: based on the national virtual simulation experiment teaching Center (iLAB-X)») підтверджує, що віртуальні симуляції є пріоритетним методом комплексного нейрохірургічного навчання, який дозволяє здобувачам освіти практикуватися у зручний для них час і отримувати зворотний зв'язок під час навчання [3].

У КНР коли перша хвиля Covid-19 прокотилася у квітні 2020 року, частка постачальників медичних послуг, що надають телемедичні послуги, зросла з 10 до 15 відсотків у період з квітня по жовтень [4]. Одним із застосунків, що змінив правила гри у сфері охорони здоров'я, що став відомим у 2023 році, був медичний стартап Ubie, який розробив програмне забезпечення для допомоги у проведенні медичних інтерв'ю зі штучним інтелектом. Використовуючи запатентований алгоритм, програма може провести попереднє інтерв'ю з пацієнтом, який взаємодіє із програмою через планшет. Програма ставить запитання щодо симптомів та історії хвороби, автоматично коригуючи запитання відповідно до відповідей пацієнта; у певному сенсі, імітуючи те, як лікар міг би проводити медичне інтерв'ю. На основі відповідей пацієнта програма може запропонувати лікарям потенційні захворювання, а також задокументувати відповіді пацієнта у вигляді клінічної нотатки, щоб звільнити лікарів від необхідності робити записи [4].

Віртуальні симуляційні лабораторії стали перспективними доповненнями або навіть альтернативами традиційним моделям навчання в медичних школах [5]. На сьогодні існує безліч комерційних і некомерційних платформ, що дозволяють розробляти та ділитися навчальними програмами віртуальних симуляційних експериментів. Наприклад, платформа Second Life, запущена Linden Lab 2003 року, стала міжнародною віртуальною симуляційною платформою для медичної освіти [6]. Основними напрямками використання платформи Second Life є віртуальні симуляції та тренажери, створення інтерактивних курсів і віртуальні клініки й лікарні. У Китаї і Японії ці симуляції використовують для навчання складних хірургічних процедур, діагностики й інших клінічних навичок [6]. На платформі можна створювати інтерактивні навчальні курси, які включають віртуальні лекції, семінари та практичні заняття.

До основних переваг використання Second Life можна віднести: доступність, безпеку та гнучкість. Використання цієї платформи дозволяє здобувачам медичної освіти отримувати якісну освіту, практикуватися в безпечному середовищі та взаємодіяти з викладачами й однолітками у реальному часі [7].

Список використаних джерел:

1. Webster G., Creemers R., Triolo P., Kania E. Full Translation: China's "New Generation Artificial Intelligence Development Plan" (2017). New America. 2017. URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

2. Nayak R. Japan’s AI Regulations: Agile Governance in Action. Diligent. 2024.URL: https://www.diligent.com/resources/blog/japan-ai-regulations.
3. Zhu H., Xu J., Wang P., Liu H., Chen T., Zhao Z., Ji L. The Status of Virtual Simulation Experiments in Medical Education in China: Based on the National Virtual Simulation Experiment Teaching Center (iLAB-X). Medical Education Online, 2023. Vol. 28(1). URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10984652/.
4. Healthcare Resilience Through Japanese Tech. Financial Times. The Government of Japan. Financial Times LTD. 2023. URL: https://www.ft.com/partnercontent/the-government-of-japan/post-covid-innovations-from-japan-1-healthcare-resilience-through-japanese-tech.html.
5. Akaike M., Fukutomi M., Nagamune M., Fujimoto A., Tsuji A., Ishida K., Iwata T. Simulation-based medical education in clinical skills laboratory. Journal of Medical Investigation, 2012. № 59(1-2). P. 28–35. URL: https://pubmed.ncbi.nlm.nih.gov/22449990/.
6. Second Life for Medical Education. 2024. URL: https://www.secondlife.com/.
Wu Q., Wang Y., Lu L., Chen Y., Long H., Wang J. Virtual Simulation in Undergraduate Medical Education: A Scoping Review of Recent Practice. Frontiers in Medicine (Lausanne), 2022. Vol. 9. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9006810/.

Дуфенюк О. М.,
професор кафедри кримінального процесу
та криміналістики факультету № 1 (з підготовки фахівців
для органів досудового розслідування Національної поліції України),
доктор юридичних наук, доцент
(Львівський державний університет внутрішніх справ)

ДЕБАТИ ПРО ChatGPT У ВЕРХОВНОМУ СУДІ

У першій частині своєї книги «Situational Awareness» (Ситуативна обізнаність) Л. Ашенбреннер, експрацівник OpenAI, говорить про те, що можливості GPT-4 стали шоком для багатьох: система штучного інтелекту, яка може писати програмний код і літературне есе, вирішувати складні математичні задачі і легко складати іспити в коледжі. Кілька років тому більшість людей думала, що це за межею реальності. Але GPT-4 був лише продовженням десятиліття карколомного прогресу в навчанні «машин». Десять років тому перші моделі ШІ ледь могли розпізнати прості зображення котів і собак. Чотири роки тому GPT-2 ледве зміг скласти схожі на правду речення. Сьогодні ці системи дають приголомшуючі результати. Цей драматичний прогрес став результатом послідовних тенденцій у розширенні можливостей глибокого навчання. Були ті, хто помітив ці тенденції набагато раніше, не зважаючи на глузування інших [1, с. 7]. І хоча Л.Ашенбреннер часто називає себе оптимістом, він також говорить про свої побоювання. У ближчі десятиліття «вибух інтелекту» буде більшою мірою схожий на ведення війни, ніж на виробництво продукту. Ми не маємо і навіть не на шляху до суперзахисту з «подушкою безпеки» чи будь-чим подібним. Вчений не впевнений, що ми б навіть помітили момент, коли б моделі ШІ самостійно активувалися (себто вийшли з-під контролю людини. – *О. М.*) [1, с. 125]. Ми також не знаємо як усунути базові побічні обмеження для систем суперінтелекту, наприклад «чи

будуть вони надійно виконувати інструкції?» або «чи дадуть вони чесну відповідь на запитання?». Основна проблема полягає в тому, що намагаючись пристосувати потужні моделі ШІ до виконання дуже простих команд (як-от «дотримуйся закону»!), ми досі не знаємо, як це зробити [1, с. 110]. Суперінтелект AGI (Artificial general intelligence) в майбутньому не тільки виконуватиме певні когнітивні функції, але й використовуватиме різні програми і додатки, продукуватиме рішення у сфері бізнесу, економіки, промислового виробництва, науки, права і безпеки.

Водночас технології ШІ різко піддаються критиці через такі аргументи:

– упередженість в частині діагностики ризиків, генерування рішень;

– сприяння академічній недоброчесності у сфері освіти і науки;

– потенційну залежність результатів від закритих для широкого загалу алгоритмів розробників;

– потенційну залежність результатів від «інформаційного харчування» таких систем великими даними, якими теж можна маніпулювати, поширювати дезінформацію;

– загрозу виходу з-під контролю людини систем, які можуть самостійно писати коди програм, керувати дронами тощо;

– гіпотетичну перспективу «атрофії людського інтелекту».

Попри це, видається, наступні покоління людства приречені жити у світі, де співіснує «живий інтелект» поруч із «машинним суперінтелектом», а поки це майбутнє тільки розгортається на наших очах, сьогодні у судовій залі використання «ChatGPT» зазнає осуду.

18 лютого 2022 р. ПП «Агротрейд Групп» звернулось до Господарського суду Черкаської області з позовом, в якому просило стягнути з ОСОБА_1 майже 5 млн. грн. заборгованості. Справа дійшла до Верховного Суду [2]. Для обґрунтування своєї позиції заявник цитував норми статей Цивільного кодексу України, положення підручника «Цивільне право», а також зміст поняття «добровільне зобов'язання», надане системою ШІ «ChatGPT». Заявник звертав увагу, що штучний інтелект «ChatGPT» ідентифікував дану правову конструкцію як зобов'язання (у теоретичному розумінні), до якого сторони дійшли добровільно (за власним волевиявленням), без втручання в зміст поняття. Тому, на думку заявника, підлягає роз'ясненню поняття «добровільне зобов'язання», яке вжите судом [2].

Треба віддати належне сміливості заявника, який зажадав від суддів роз'яснень, апелюючи до такого екстраординарного джерела, проте судова палата не зрозуміла такого інноваційного підходу і констатувала у діях заявника зловживання процесуальними правами та неповагу до суду. На думку більшості суддів (до цього рішення додано окрему думку), те, що заявник «фактично просить Верховний Суд спростувати чи підтвердити те, що з окресленого питання згенерував штучний інтелект «ChatGPT», який не визнається як джерело достовірної науково доведеної інформації, на противагу висновкам, що були зроблені судом в судовому рішенні» ставить «під сумнів суддівський розсуд та судове тлумачення цього питання у рішенні, що набуло

статусу остаточного». Цими діями заявник знехтував авторитет судової влади (п.28, 29). Колегія суддів вважає, що «використання технологій повинно, перш за все, поважати природу судового процесу. По-перше, багато судових рішень є дискреційними рішеннями, заснованими на конкретних фактах окремої справи. По-друге, судді відіграють суттєву роль у розвитку права. Вони не просто застосовують фіксовані та незмінні правила. Судді повинні мати можливість виправляти або доповнювати закон, якщо він не відповідає вимогам або загрожує зашкодити його застосуванню в певних справах. Технології не повинні втручатися у сферу справедливості. Технології не повинні знеохочувати або перешкоджати критичному мисленню суддів, оскільки це може призвести до стагнації правового розвитку та ерозії системи правового захисту. Тому технологічні інструменти повинні поважати процес ухвалення судових рішень і автономію суддів (пункт 90 висновку КРЄС № 26 (2023) від 1 грудня 2023 року «Рухаючись вперед: використання асистивних технологій у судочинстві»)». Штучний інтелект може бути корисним та допоміжним інструментом у сфері правосуддя, але не може замінити роль суддів (п. 37, 38) [2].

Натомість авторка згаданої вище окремої думки суддя Г. Вронська оприлюднила свою позицію: «Вважаю, що, пославшись на відповіді, згенеровані ШІ «ChatGPT», з метою обґрунтування своєї позиції, зважаючи зміст заяви, наведені в ній доводи та аргументи, Заявник не виявив неповагу до Суду та не поставив під сумнів його висновки, навпаки – прагнув з'ясувати та уточнити окремі висновки з питань, щодо яких висловився Верховний Суд. У заяві відсутні будь-які принизливі, образливі чи інші негативні висловлювання, відверта демонстрація неповаги до Суду тощо… Саме по собі посилання на інформацію, що була згенерована за допомогою технологій ШІ, за відсутності інших обґрунтованих обставин, які б свідчили про недобросовісні процесуальні дії особи, не може визнаватися зловживанням процесуальними правами... Верховний Суд передчасно визнав подання заяви про роз`яснення судового рішення зловживанням процесуальними правами, надавши діям Заявника надто сувору оцінку» (п. 32–34) [3].

У цьому контексті пригадуються слова О. Капліної у передмові до книги П. Пінто де Альбукерке «Окрема думка. Шлях до справедливості» (2020 р.) про те, що окрема думка є «продуктом незалежного та глибокого мислення судді, вираженням його індивідуальної правосвідомості». Аргументація окремої думки може мати глибоко моральне значення, коли йдеться про особливо чутливі для суспільства питання [4, с.13, 15]. Аргументація окремої думки може стати основою для майбутніх змін законодавства, формування альтернативного розуміння закону може збагатити дискурс та стати поштовхом для майбутнього розвитку права, вирішення більш широкого правового питання. Йдеться про апелювання до «розуму майбутнього», «інтелекту завтрашнього дня» [5, с. 419].

Викладене вище доводить, що в сучасних умовах до існуючого переліку дискусійних питань додаються нові. Чи є питання використання технологій ШІ чутливим для суспільства? Чи є апелювання до змісту відповідей «ChatGPT»

етично допустимим для обґрунтування позиції в суді? Які критерії добросовісного використання процесуальних прав в епоху суперінтелекту? Які юридичні наслідки мають бути за недобросовісне використання «ChatGPT» в судовому процесі? Чи вистоїть верховенство права у цифрову епоху, чи поступатиметься верховенству цифри?

Список використаних джерел:

1. Aschenbrenner L. Situational Awareness. The Decade Ahead. San Francisco, California, 2024. 165 p. URL: https://situational-awareness.ai/wp-content/uploads/2024/06/situationalawareness.pdf.
2. Ухвала Верховного Суду від 08.02.2024 р. Справа № 925/200/22. URL: https://reyestr.court.gov.ua/Review/116984639.
3. Окрема думка судді Г. Вронської до Ухвали Верховного Суду від 08.02.2024. Справа № 925/200/22. URL: https://reyestr.court.gov.ua/Review/117074064.
4. Пінто де Альбукерке П. Окрема думка. Шлях до справедливості / пер. з англ. та фр. В. А. Капліної ; упоряд., авт. передм. О. В. Капліна. Харків : Право, 2020.
5. Дуфенюк О. М. Баланс у кримінальному провадженні: інституційний, правозастосовний, особистісний рівні : монографія. Львів : Растр-7, 2023. 508 с.
6. Берназюк Ян. Штучний інтелект та питання етики під час здійснення правосуддя. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/-supreme/2024_prezent/AI_ethics_bernaziuk.pdf.

Жезло-Хлевна Н. В.,
викладач кафедри інформаційних технологій
та систем електронних комунікацій
(Львівський державний університет
безпеки життєдіяльності)

Хлевной О. В.,
доцент кафедри інформаційних технологій
та систем електронних комунікацій,
кандидат технічних наук, доцент
(Львівський державний університет
безпеки життєдіяльності)

МАШИННЕ НАВЧАННЯ В НОРМУВАННІ ВИМОГ ПОЖЕЖНОЇ БЕЗПЕКИ ДО ЕВАКУЦІЙНИХ ШЛЯХІВ І ВИХОДІВ У ЗАКЛАДАХ СЕРЕДНЬОЇ ОСВІТИ

Пожежна безпека у закладах середньої освіти є критично важливим питанням, адже від її ефективності залежить життя s здоров’я учнів та працівників. Одним із ключових елементів забезпечення безпеки є правильне нормування евакуаційних шляхів і виходів, що має враховувати тривалість евакуації та особливості поведінки людей у надзвичайних ситуаціях. Проте чинний державний стандарт [1] в Україні не містить достатньої кількості вхідних даних, які б дозволяли здійснювати розрахунок тривалості евакуації з

урахуванням вікових особливостей учнів. Це створює суттєві прогалини в оцінці ризиків і плануванні безпечних умов у школах.

На сьогодні існує два основних підходи до розрахунку тривалості евакуації із закладу шкільної освіти. Перший – використання спеціалізованих програмних комплексів, таких як Pathfinder або подібні системи моделювання. Ці інструменти здатні враховувати широкий спектр параметрів, включно з геометрією приміщень, щільністю людського потоку та поведінковими факторами. Проте їхнє застосування пов'язане з низкою обмежень: необхідністю навчання роботі з програмним комплексом, високою вартістю ліцензій і складністю інтеграції в повсякденну практику проектування та перевірок. Другий підхід – спрощений аналітичний метод, який базується на залежності швидкості руху від щільності людського потоку. Цей метод є більш доступним, дозволяє здійснювати розрахунок в «ручному режимі», але має суттєвий недолік: він не враховує вікові особливості евакуйованих, зокрема різницю в швидкості руху молодших і старших учнів, що може призводити до неточних розрахунків і завищення або заниження реального часу евакуації.

Машинне навчання (МН) відкриває нові можливості для вирішення цієї проблеми шляхом створення адаптивних моделей, які враховують не лише стандартні параметри (щільність потоку), а й інші характеристики.

З метою врахування вікових особливостей руху учасників евакуації в закладах шкільної освіти було реалізовано регресійну модель. Робота над створенням моделі відбувалася у кілька етапів.

Перший етап передбачав формування набору даних для навчання моделі машинного навчання [2]. Він розпочався зі збору інформації в процесі реальних евакуацій у школі під час повітряних тривог. Дані отримували з камер відеоспостереження в коридорах і біля виходів до укриття, а також із записів на смартфон, що фіксували візуальні та часові характеристики потоків.

Швидкість руху визначали, аналізуючи відеозаписи: зупиняли кадри в ключових точках (дверні прорізи, віконні прорізи, заздалегідь встановлені мітки), фіксували час і відстань між ними, обчислюючи середнє значення для кількох ділянок. Щільність потоку розраховували, підраховуючи учнів у визначених зонах (наприклад, 15 осіб на 10 м² = 1,5 ос/м²), проводячи виміри в широких і вузьких місцях. Вік учнів визначався згідно даних здобувачів освіти (6 років – 1-й клас, 8 років – 3-й клас тощо), а для змішаних потоків – як середньозважене значення.

Усі дані (швидкість, щільність, вік) вносилися до таблиці Excel. Загалом було отримано 256 записів, готових для подальшого аналізу.

На наступному етапі для аналізу залежностей між швидкістю руху, щільністю потоку та віком учнів було застосовано кілька методів регресійного аналізу, реалізованих за допомогою мови програмування Python із використанням бібліотек pandas, numpy, scikit-learn, TensorFlow і

matplotlib. Першим методом стала лінійна регресія, яка показала базову залежність швидкості від щільності та віку, виражену рівнянням (1)

$$V = 43.77 - 7.01 \cdot D + 0.70 \cdot A \quad (1)$$

D – щільність потоку, ос./м^2;

A – вік учасника евакуації;

V – швидкість руху учасника евакуації, м/с.

Ця модель досягла коефіцієнта детермінації 0.74 і середньоквадратичної помилки (MSE) 17.24, що вказує на обмежену точність через ігнорування нелінійних ефектів.

Щоб врахувати нелінійні зв'язки, було застосовано поліноміальну регресію другого ступеня, яка дала значно кращі результати. Отримане рівняння (2) відображає складнішу залежність, включаючи квадратичні члени та взаємодію між щільністю й віком. Ця модель досягла коефіцієнта детермінації 0.93 і MSE 10.42.

$$V = 56.72 - 11.06 \cdot D - 1.12 \cdot A + 1.03 \cdot D2 - 0.25 \cdot D \cdot A + 0.12 \cdot A^2 \quad (2)$$

Також було використано модель випадкового лісу, яка базується на ансамблі дерев рішень і добре адаптується до нелінійних залежностей без потреби в нормалізації даних. Ця модель показала коефіцієнт детермінації 0.80 і MSE 13.48, що є хорошим результатом для невеликого набору даних. Випадковий ліс підтвердив тенденцію до зниження швидкості зі зростанням щільності, враховуючи при цьому додатковий ефект віку, і виявився стійким до шуму в даних. Його перевагою стала простота реалізації та менша схильність до перенавчання порівняно з іншими методами.

Нарешті, багатошарова повнозв'язана нейронна мережа з двома прихованими шарами по 64 нейрони показала дещо нижчу точність: 0.76 і MSE 16.38. Незважаючи на збільшення кількості епох до 1000, модель не досягла високої точності, що можна пояснити недостатньою кількістю даних (256 записів) для ефективного навчання складної архітектури.

Отже, найкращу точність показала модель поліноміальної регресії другого порядку.

Останнім етапом дослідження стала апробація розробленої моделі. Вона проводилася шляхом порівняння розрахунків часу евакуації з першого поверху школи за чотирма методами: реальними вимірами, моделюванням у програмному комплексі Pathfinder, класичним спрощеним аналітичним методом без врахування вікових особливостей і тим же методом із використанням поліноміальної залежності (таблиця 1).

Таблиця 1

Порівняльні результати розрахунку тривалості евакуації

Засоби здійснення розрахунку	Час, с
Спрощений аналітичний метод **(сценарій 1)**	66 с
Спрощений аналітичний метод **(сценарій 2)**	60 с

Pathfinder	51 с
Експериментальні дані	55 с

Реальні дані підтвердили високу точність Pathfinder, тоді як спрощений метод без урахування віку завищив час на 20%, що підкреслює його обмеження для шкільних умов. Використання отриманої залежності у спрощеному методі скоротило похибку до 10%, що доводить її практичну цінність для врахування вікових особливостей учнів.

Розроблена модель машинного навчання, що враховує залежність швидкості евакуації від віку учнів, щільності потоку та просторових умов, може вдосконалити чинні нормативні документи шляхом інтеграції нових емпіричних даних, які усувають прогалини в методиці розрахунку тривалості евакуації у школах, зменшуючи похибку на 20-30%, а також пропонує гнучкий інструмент для оновлення стандартів, враховуючи специфіку закладів середньої освіти, що сприятиме підвищенню безпеки та ефективності евакуаційних шляхів і виходів без необхідності використання дорогих програмних комплексів.

Список використаних джерел:

1. DSTU 8828: 2019. Fire safety. Terms. [Valid from 2020-01-01]. Kyiv, 2019. 163 p. (in Ukr.).

2. Khlevnoi O. Standardization of fire safety requirements for evacuation routes and exits in secondary education institutions with inclusive education: dis. ... cand. tech. Sciences: 21.06.02 / Lviv, 2021. 188 p.

Жовнірчик Л. І.,
викладач кафедри інформаційних технологій
та програмування
(ВСП ЗВО Університету «Україна»,
Івано-Франківська філія)

ТЕХНОЛОГІЇ ШИФРУВАННЯ, БЛОКЧЕЙН ТА ШІ ДЛЯ ЗАХИСТУ БАЗ ДАНИХ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

У сучасному світі, де інформаційна війна набуває все більш масштабного характеру, захист баз даних перетворюється на стратегічний пріоритет. Кібератаки, маніпуляції даними та втрата критичної інформації становлять безпосередню загрозу національній безпеці, бізнесу та приватним користувачам. Ця стаття розглядає комплексний підхід до захисту даних, поєднуючи технічні рішення, організаційні заходи та законодавчі ініціативи. Особливу увагу приділено інноваційним технологіям, таким як блокчейн і штучний інтелект, які відіграють ключову роль у протидії сучасним викликам.

Інформаційна війна супроводжується низкою складних загроз, які вимагають негайної реакції. Однією з найнебезпечніших є кібератаки, такі як DDoS-атаки, спрямовані на параліч систем, або ransomware-атаки, що блокують доступ до даних до сплати викупу. SQL-ін'єкції та фішинг дозволяють зловмисникам отримувати несанкціонований доступ до конфіденційної інформації. Окрім технічних атак, існує ризик маніпуляцій даними – навмисного спотворення інформації з метою дезінформації суспільства або підриву довіри до державних інституцій. Не менш серйозною проблемою залишається втрата цілісності даних через технічні збої, помилки персоналу або зовнішній вплив, що може призвести до непоправних наслідків для критичних інфраструктур.

Ефективний захист баз даних неможливий без використання сучасних технологій. Шифрування, зокрема алгоритми AES-256 та end-to-end шифрування, забезпечує конфіденційність даних під час їх передачі та зберігання. Контроль доступу реалізується через багаторівневу аутентифікацію (MFA) та рольове управління правами (RBAC), що обмежує можливості несанкціонованого втручання. Резервне копіювання в хмарні сховища з георозподілом дозволяє швидко відновлювати дані після атак чи технічних збоїв. Інновації, такі як блокчейн, забезпечують незмінність логів дій, що унеможливлює маніпуляції з боку зловмисників. Штучний інтелект, в свою чергу, аналізує великі масиви даних у реальному часі, виявляючи аномалії та потенційні загрози до їх реалізації.

Технічні засоби є лише частиною комплексного захисту. Дотримання міжнародних стандартів кібербезпеки, таких як NIST Cybersecurity Framework [1] або ISO 27001 [2], допомагає організаціям системно оцінювати ризики та впроваджувати проактивні заходи. Державні ініціативи, зокрема створення національних кіберцентрів реакції на інциденти (наприклад, CERT-UA в Україні), сприяють координації дій під час масштабних атак. Важливим елементом є постійне навчання персоналу: тренінги з кібергігієни, симуляції фішингових атак та семінари з виявлення вразливостей підвищують обізнаність співробітників. Законодавча база має регулювати відповідальність за порушення кібербезпеки та стимулювати інвестиції в інфраструктуру захисту даних [3].

Реальні приклади [4] демонструють ефективність комплексного підходу. Під час атаки на українську енергосистему в 2015 році впровадження сегментації мережі та офлайн-резервів дозволило уникнути катастрофічних наслідків. В Естонії технологія блокчейн у системі e-Health захистила медичні дані від спроб маніпуляцій під час масштабних кібератак 20017 року. Ці приклади підкреслюють, що поєднання технічних інновацій, чітких протоколів дій та підготовленого персоналу є запорукою успіху.

Умови інформаційної війни вимагають гнучкого та багаторівневого підходу до захисту баз даних. Технології шифрування, блокчейн та ШІ формують технічний фундамент, але їх ефективність залежить від організаційної культури, дотримання стандартів та кваліфікованих кадрів.

Державна підтримка, міжнародна співпраця та постійна адаптація до нових загроз є необхідними умовами для побудови стійкого кіберпростору. Інвестиції в безпеку сьогодні — це гарантія стабільності та довіри завтра.

Список використаних джерел:
1. NIST Cybersecurity Framework.
2. ISO/IEC 27001:2022.
3. Clarke R., Knake R. Cyber War: The Next Threat to National Security.
4. Кейс: Захист енергосистеми України (2015).

Жовнірчик Л. І.,
викладач кафедри інформаційних технологій
та програмування
(ВСП ЗВО Університету «Україна»,
Івано-Франківська філія)

КАСТОМІЗОВАНИЙ ПОМІЧНИК-АСИСТЕНТ ДЛЯ ВИКЛАДАННЯ ІНЖЕНЕРНИХ ДИСЦИПЛІН У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ

У сучасному освітньому процесі дедалі більшу роль виконують цифрові технології, які сприяють роботі викладачів та підвищують ефективність навчання студентів. Одним із найперспективніших інструментів є кастомізовані ШІ-асистенти, які можуть допомогти у викладанні інженерних дисциплін. Вони зможуть автоматизувати рутинні завдання, персоналізувати навчальний процес і значно покращити взаємодію між викладачами та студентами.

Цифрові технології змінюють освітнє середовище. Одним із найефективніших рішень є кастомізовані GPT-асистенти, які забезпечують адаптивне навчання, автоматизацію оцінювання та підвищення ефективності викладання [1].

ChatGPT є загальнодоступним ШІ, що відповідає на питання користувачів. Кастомізовані GPTs дозволяють адаптувати модель до конкретних освітніх завдань, а OpenAI Assistant інтегрується в навчальні додатки [2], забезпечуючи поглиблену взаємодію з базами даних та автоматизуючи перевірку знань.

Використання кастомізованих асистентів у викладанні інженерних дисциплін включає:

- автоматизацію створення лекцій, тестів і контрольних робіт;
- надання персоналізованих пояснень складних тем;
- формування практичних завдань із розрахунками та моделюванням;
- оцінювання програмних кодів і технічних розрахунків;
- відстеження прогресу студентів та адаптацію навчального процесу [6].

Попри значні переваги, впровадження ШІ-асистентів у викладання інженерних дисциплін супроводжується певними викликами, одним із яких є необхідність ретельного налаштування системи. Щоб штучний інтелект ефективно працював у конкретному навчальному середовищі, його потрібно адаптувати до специфіки дисципліни, рівня підготовки студентів і методики викладання [3]. Це вимагає часу та зусиль з боку викладача або технічних спеціалістів, які повинні забезпечити коректну роботу асистента, додати відповідні матеріали, налаштувати алгоритми перевірки знань та інтегрувати систему в освітній процес.

Ще одним важливим аспектом є необхідність контролю з боку викладача, адже ШІ, хоч і є потужним інструментом, не завжди може гарантувати правильність відповідей або глибину пояснень. Існує ризик, що система іноді надаватиме поверхневі або неточні пояснення [4], особливо коли йдеться про складні технічні теми, які потребують детального аналізу. Тому викладач повинен періодично перевіряти роботу ШІ, аналізувати його відповіді та коригувати недоліки, щоб забезпечити високу якість навчального процесу [5].

Окрім технічних питань, виникають також етичні аспекти використання ШІ-асистентів, особливо в контексті автоматизованого оцінювання знань. Для того щоб уникнути несправедливих оцінок або випадків, коли система упереджено аналізує відповіді [6], необхідно чітко визначити критерії оцінювання. Викладачі мають контролювати, щоб алгоритми не допускали помилок при аналізі відкритих відповідей або складних розрахунків, а також гарантувати, що студенти розуміють принципи роботи системи. Забезпечення прозорості та справедливості оцінювання є важливим кроком для ефективного та етичного використання ШІ у навчальному процесі.

Кастомізований ШІ-асистент є потужним інструментом для викладання інженерних дисциплін у ВНЗ. Вони здатні автоматизувати навчальний процес, покращити комунікацію між викладачами та студентами, а також сприяти персоналізованому підходу до навчання. Однак їх впровадження потребує поточного налаштування та адаптації до освітнього середовища [7]. У майбутньому така технологія може стати невід’ємною частиною сучасної інженерної освіти, роблячи її ще більш ефективною та доступною.

Список використаних джерел:

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016.
2. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. Pearson, 2020.
3. Ng A. Machine Learning Yearning.
4. OpenAI Documentation – https://platform.openai.com/docs/
5. Luckin R., Holmes W., Griffiths M., Forcier L. B. Artificial Intelligence and Education. Routledge, 2021.
6. Chassignol M., Khoroshavi O., Klimova A., Bilyatdinova A. "Artificial Intelligence trends in education: a narrative overview." Procedia Computer Science, 2018.
7. Kay J., Reimann P., Diebold E., Kummerfeld B. "MOOCs, Artificial Intelligence and Big Data." Proceedings of the International Conference on Learning Analytics & Knowledge, 2019.

Жукова А. Р.,

доцентка кафедри іноземних мов
та військового перекладу,
докторка філософії у галузі педагогіки
*(Національна академія сухопутних військ імені
гетьмана Петра Сагайдачного, м. Львів)*
https://orcid.org/0000-0002-7292-1605

МОЖЛИВОСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОЦЕСІ ВИВЧЕННЯ ІНОЗЕМНИХ МОВ

Наприкінці XX століття глобалізація та комп'ютеризація спричинили значні суспільні зміни, зокрема у використанні цифрових технологій. Презентований на Дартмутській конференції 1956 року, штучний інтелект (ШІ) став важливою частиною наукових досліджень і розвитку обчислювальної техніки. За майже сімдесят років ШІ проник у різні галузі, включаючи медицину й освіту, досягнувши успіхів у машинному навчанні та робототехніці. Термін "штучний інтелект" вперше введений на конференції в Дортмунді, що стимулювало розробку програм для складних задач. Ілон Маск і засновники OpenAI наголошували на необхідності регулювання ШІ через його потенціал і загрози. ШІ здатен створювати нові технології, удосконалювати робочу силу, автоматизовувати процеси та генерувати робочі місця.

Активне впровадження технологій штучного інтелекту в освітні процеси світових ЗВО дозволило сформувати певний досвід його використання ***у процесі вивчення іноземних мов***.

Таблиця 1

Застосування ШІ	**Опис**
Підготовка навчальних програм	ШІ допомагає викладачам іноземних мов адаптувати навчальні та автентичні матеріали на різних мовних рівнях: як лексичному, так і граматичному. Викладачі можуть розробляти завдання на основі запропонованих ним матеріалів, збагачувати тексти набором відповідних граматичних патернів чи лексичних одиниць [24, с. 270].
Інноваційні підходи	Інноваційні підходи до розширення словникового запасу включають використання штучного інтелекту та чат-ботів (AI-платформи, персоналізовані діалоги, автоматизовані тести), гейміфікація навчання (мовні застосунки, квести, система винагород), а також методика Context-Based

	Learning (вивчення слів у контексті через читання, відео та семантичні поля). Ці підходи роблять процес засвоєння лексики більш ефективним, інтерактивним і адаптивним до потреб студента.

ШІ на заняттях з іноземної мови певною мірою сприяє досягненню очікуваних результатів в опануванні граматичного матеріалу, навичок вимови, словникового запасу тощо. Для цього створено багато додатків, такі як Duolingo, Quizlet, Lingvist, різноманітні сервіси – Grammarly. Розглянемо більш детально з прикладів таких інструментів:

Таблиця 2

Платформа	Опис	Переваги
Rosetta Stone	використовує інтенсивні занурення в мовне середовище для вивчення нової мови	підтримка багатьох мов, інтуїтивний інтерфейс, велика кількість візуальних і аудіо матеріалів
Duolingo	популярний додаток для навчання мов, який використовує гейміфіковані вправи	безкоштовне користування, великий вибір мов, інтерактивний і зручний у використанні
Babbel	фокусується на побудові реальних розмовних навичок, використовує спеціалізовані діалоги	курси розроблені професіональними лінгвістами, інтеграція культурного контексту
Mango Languages	пропонує уроки з вивчення граматики та вимови через розмовну практику	включення культурних нотаток, адаптація уроків під специфічні потреби студента

Штучний інтелект має широкий набір інструментів для створення інтерактивних методів навчання. Це включає інтерактивні програми, віртуальних асистентів для зразків вимови та виправлення помилок, автоматизовані системи оцінювання знань студентів. Основні інтерактивні технології на основі штучного інтелекту можуть значно покращити викладання іноземних мов.

Таблиця 3

Технологія	Опис	Застосування
Чат-боти	Віртуальні помічники з штучним інтелектом,	Коригування структури речень, граматики,

	що ведуть спілкування в текстовому режимі чи за допомогою голосових повідомлень	вживання слів та словосполучень, текстів
Додатковий інтелект	Засоби автоматизації, що сприяють підвищенню розумової праці студентів	Зменшення помилок під час виконання завдань, партнерство між студентом та штучним інтелектом
Геймифікація	Використання ігрових елементів для здобувачів вищої освіти	Застосування ігрових механізмів та практик у неігровому контексті
Мультимедійні технології навчання	Застосування математичних моделей в управлінні освітнім процесом	Персоналізація в наданні послуг, формування іншомовної компетентності

Окрім технологічних переваг, штучний інтелект дозволяє змінити методологію викладання іноземної мови через впровадження індивідуалізації, підвищення мотивації, покращення оцінювання та доступності. Однак попри переваги використання штучного інтелекту у процесі оцінювання знань з іноземних мов, існують і численні виклики.

Таблиця 4

Переваги	**Недоліки**
Індивідуалізація навчання: адаптивні навчальні платформи аналізують відповіді студентів і адаптують матеріали відповідно до їхнього рівня знань та швидкості навчання.	Обмежена здатність до розуміння контексту: ШІ може ефективно обробляти мовні дані, але його здатність до розуміння глибшого контексту та нюансів людської мови все ще обмежена.
Підвищення мотивації: гейміфіковані елементи в ШІ-системах підвищують мотивацію студентів за рахунок надання негайного зворотного зв’язку і створення конкурентного середовища.	Залежність від якості даних: ефективність ШІ прямо залежить від якості та обсягу даних, на яких він був навчений.
Точність оцінювання: ШІ здатний об’єктивно оцінювати рівень знань студентів, мінімізуючи суб’єктивний вплив.	Відсутність інтерперсонального взаємодії: ШІ не може повністю замінити викладачів, особливо в аспектах емоційного та соціального взаємодії.
Доступність і зручність: ШІ	Етичні та конфіденційні питання:

дозволяє студентам вивчати мову в будь-який зручний для них час та в будь-якому місці.	використання ШІ у освіті порушує питання конфіденційності та етики.

Що стосується використання штучного інтелекту у процесі оцінювання знань студентів при вивченні іноземної мови, то вивчення практики показує високу ефективність технології у розробленні тестів та перевірки тестування студентів.

Отже, значення штучного інтелекту в освітніх процесах полягає в його здатності автономно підбирати оптимальні рішення для складних проблем. Штучний інтелект визначається як здатність програми чи системи імітувати людські розумові функції. Ця технологія перетворює освітній процес, дозволяючи викладачам створювати адаптивний та персоналізований досвід навчання, орієнтований на індивідуальні особливості та потреби студентів.

Активне впровадження штучного інтелекту в освітній процес вивчення іноземних мов у вищих навчальних закладах на глобальному рівні демонструє значні переваги. Ці переваги включають підготовку навчальних програм, розширення словникового запасу та створення інтерактивного підходу до навчання. Використання штучного інтелекту в оцінюванні знань студентів з іноземних мов показує високу ефективність у створенні та адмініструванні тестів. Лінгводидактичне тестування включає діагностику, контроль та оцінювання навчального матеріалу через різноманітні тести. Штучний інтелект автоматизує створення та адаптацію тестів, забезпечуючи об’єктивність оцінювання.

З огляду на ці перспективи, можна очікувати, що інтеграція штучного інтелекту в освітню систему забезпечить більш ефективне та персоналізоване навчання, значно розширюючи можливості викладачів і студентів у процесі освіти.

Список використаних джерел:

1. Wang F., Chen X. Artificial Intelligence in Language Learning: A Systematic Review. *Educational Technology Research and Development*. 2020. Vol. 68 (2). P. 465–490.
2. Дубчак А., Литвиненко Я. Напрями використання штучного інтелекту за сучасних умов. *Іван Пулюй: життя в ім’я науки та України :* тези Міжнар. наук. конф. Тернопіль, 2020. С. 64–65.
3. Яценко О. Використання технології штучного інтелекту для навчання та оцінки знань. The 34th International scientific and practical conference “*Science, latest trends, modern problems and improvement of theories*”, August 29 – September 01, Warsaw, Poland, 2023.P. 152–154.
4. Задорожна О., Сулим В. Штучний інтелект як один із засобів вивчення іноземної мови, *Grail of Science*. 2023. Vol. 34. P. 333–335. DOI: https://doi.org/10.36074/grail-of-science.08.12.2023.74.
5. Шаргун Т., Жукова А. Інтеграція штучного інтелекту в педагогічний процес оцінювання знань здобувачів освіти з англійської мови. *Перспективи та інновації науки*. 2025. 2025. №/ 1 (47). С. 1297–1310. DOI: https://doi.org/10.52058/2786-4952-2025-1(47)-1297-1309.

Здебський Д. В.,
аспірант 3 курсу заочної форми навчання
докторантури та аспірантури
(Одеський державний університет внутрішніх справ)

ІНТЕГРАЦІЯ БАЗИ ДАНИХ ПОЛІГРАФОЛОГІЧНИХ ДОСЛІДЖЕНЬ У ЦИФРОВІ СИСТЕМИ УПРАВЛІННЯ ДОКАЗАМИ

В умовах правового режиму воєнного стану в Україні, питання забезпечення національної безпеки та правопорядку набувають особливої актуальності. Одним із ключових напрямів для зміцнення безпеки є вдосконалення механізмів правоохоронної діяльності та забезпечення достовірності доказів у кримінальних розслідуваннях. Використання цифрових технологій у цій сфері відкриває нові можливості для інтеграції різноманітних інструментів, зокрема поліграфологічних досліджень, що дозволяє значно підвищити ефективність розслідувань. Одним із найбільш перспективних кроків, на нашу думку, є інтеграція баз даних поліграфологічних досліджень у цифрову систему управління доказами (Digital Evidence Management System, DEMS). Це дозволить не лише систематизувати результати тестувань, але й поєднати їх із іншими цифровими доказами, що сприятиме виявленню потенційних загроз, колабораціоністської діяльності та корупційних зв'язків серед військових та посадовців. Водночас, цей процес потребує чіткої законодавчої та технічної підтримки, а також відповідних заходів із забезпечення інформаційної безпеки. DEMS використовується для збору, зберігання, обробки, перевірки та передачі цифрових доказів у рамках кримінальних розслідувань або судових процесів. Ці системи розроблені для того, щоб забезпечити ефективне управління великими обсягами даних та інформації, що містять ключові цифрові сліди злочинів, а також для гарантування точності, цілісності та безпеки цифрових доказів. Система DEMS передбачає процеси: збору та зберігання цифрових доказів, управління доступом, верифікацію і аудит, інтеграцію з іншими системами. Вона створюються для забезпечення цілісності цифрових доказів, автоматизації процесів, покращення прозорості та підзвітності та для забезпечення відповідності нормам обробки інформації. Загалом, DEMS є критично важливою системою для сучасних кримінальних розслідувань, оскільки забезпечує ефективне управління цифровими доказами та підвищує ефективність правозастосування в умовах високих технологій. Як зазначають О. В. Манжай, А. О. Потильчак та І. А. Манжай, правильне збереження та обробка цифрових доказів є критичними для забезпечення їхньої юридичної прийнятності [3].

Цифрові технології в управлінні доказами мають суттєвий вплив на точність і швидкість розслідувань, а також на інтеграцію різноманітних типів доказів в єдину систему. Вони підкреслюють важливість розробки єдиного стандарту для цифрових доказів, що дозволяє ефективно інтегрувати

поліграфологічні дані в загальний контекст кримінальних розслідувань. Цифрові технології стрімко розвиваються, і, як зазначають Humaira Arshad, Aman Bin Jantan та Oludare Isaac Abiodun, важливим аспектом є адаптація до цих змін. Враховуючи постійне оновлення технічних пристроїв і платформ, що використовуються в розслідуваннях, неможливо забезпечити стабільність методів без врахування швидкоплинних змін. Розробка методів перевірки та валідації цифрових доказів, має відповідати сучасним технологічним стандартам [2].

При інтеграції бази даних поліграфологічних досліджень слід врахувати стандарт програмного забезпечення поліграфа – NCCA ASCII. Цей стандарт визначає єдиний формат збереження та обміну даними між поліграфами та цифровими системами [1]. Програмне забезпечення, що відповідає NCCA ASCII, передбачає: уніфікований формат поліграм, що надає можливість інтегрувати їх у цифрові бази даних; автоматизований аналіз фізіологічних показників; формує детальні звіти; суміщати із системами цифрових доказів. Цей формат дозволяє зберігати всю необхідну інформацію в одному файлі, що полегшує подальшу обробку даних для наукових досліджень або порівняння результатів між різними системами поліграфів. Використання програмного забезпечення поліграфів за стандартом NCCA ASCII у DEMS дозволить уникнути несумісності даних, забезпечить збереження вихідної точності вимірювань та спростить процес обміну інформацією між правоохоронними структурами.

Інтеграція бази даних поліграфологічних досліджень у DEMS передбачає такі ключові можливості:

1) централізоване збереження результатів (забезпечення єдиного місця для збору, архівації та управління даними поліграфологічних досліджень):

2) автоматизована обробка інформації (проведення аналітики, виявлення тенденцій та оцінка достовірності отриманих результатів);

3) інтеграція з іншими інформаційними системами (забезпечення взаємодії з відомчими базами даних);

4) генерацію аналітичних звітів (автоматичне створення структурованих документів для прийняття рішень).

Запровадження бази даних поліграфологічних досліджень у DEMS надає такі переваги:

1) підвищення об'єктивності та прозорості – запобігання суб'єктивним помилкам та впливу людського фактору.

2) оптимізація робочого процесу – зменшення часу на обробку та аналіз отриманих результатів.

3) доступ до історичних записів – можливість довгострокового аналізу та порівняння результатів тестувань.

Для успішного впровадження бази даних поліграфологічних досліджень у DEMS необхідно:

по-перше, гармонізувати законодавство , а саме розробити та впровадити нормативно-правові акти для регулювання використання бази даних поліграфологічних досліджень.

по-друге, забезпечити технічну інтеграцію шляхом розробки механізми обміну інформацією між DEMS та базами даних МВС, ДПСУ, НГУ, СБУ, НАБУ, ДБР.

по-третє, підготувати фахівців з числа поліграфологів та аналітиків.

по-четверте, розробити стандарти інформаційної безпеки забезпечивши багаторівневий захист конфіденційних даних.

по-п’яте, впровадити моніторинг ефективності шляхом регулярного аналізу роботи системи та можливістю вносити необхідні корективи.

Інтеграція бази даних поліграфологічних досліджень у систему DEMS є важливим етапом у процесі цифровізації правоохоронної діяльності, що сприятиме прийняттю більш обґрунтованих рішень, покращенню ефективності кадрових перевірок і зміцненню інформаційної безпеки. Проте її успішна реалізація вимагає змін у законодавстві, фінансування, підготовки фахівців та модернізації технічної інфраструктури. Комплексний підхід до цього проекту дозволить посилити довіру до поліграфологічних досліджень і підвищити рівень безпеки як у державному, так і в приватному секторі. Інтеграція поліграфологічних досліджень у DEMS є перспективним кроком для зміцнення національної безпеки та правопорядку в Україні, але вимагає всебічної підтримки, технічної інтеграції, підготовки кваліфікованих кадрів та гарантування високого рівня інформаційної безпеки.

Список використаних джерел:

1. Editorial Staff. Introduction to the NCCA ASCII Standard. *Polygraph & Forensic Credibility Assessment*. 2019. Vol. 48, No. 2. P. 125–135. URL: https://polygraph.org/docs/APA_2019_Intro_to_the_NCCA_ASCII_standard.pdf (дата звернення:12.03.2025)

2. Humaira Arshad, Aman Bin Jantan, Oludare Isaac Abiodun, Journal of Information Processing Systems Vol. 14, No. 2, pp. 346-376, Apr. 2018 URL: https://xml.jips-k.org/full-text/view?doi=10.3745/JIPS.03.0095 (дата звернення:12.03.2025)

3. Manzhai O. V., Potylchak A. O., Manzhai I. A. Organizational and Forensic Aspects of the Electronic Evidence Handling. *Law and Safety*. 2021. Vol. 83, No. 4. P. 91–99. DOI: 10.32631/pb.2021.4.09. URL: https://pb.univd.edu.ua/index.php/PB/article/view/527 (дата звернення:12.03.2025).

Здреник І. В.,
доцентка кафедри загальноправових дисциплін,
кандидатка юридичних наук, доцентка
(Львівський держаний університет внутрішніх справ)

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА ПРАВА ЛЮДИНИ

Штучний інтелект (далі – ШІ) є однією з найважливіших технологій сучасності, яка має значний вплив на різні сфери життя, зокрема медицину, економіку, безпеку та правосуддя. Попри численні переваги, такі як автоматизація процесів, підвищення ефективності та точності рішень, його використання породжує низку викликів, пов'язаних із правами людини. Основними проблемними питаннями є ризик дискримінації через упереджені алгоритми, загроза приватності у зв'язку з масовим збором і аналізом персональних даних, а також потенційні порушення трудових прав через автоматизацію робочих місць. Оскільки технології ШІ швидко розвиваються, важливим завданням є створення ефективного правового регулювання, що забезпечить баланс між технологічним прогресом і дотриманням основоположних прав і свобод людини.

Штучний інтелект мінімізує людський фактор у забезпеченні інформаційного захисту, залишаючи лише функції моніторингу та корекції, що робить його технологією майбутнього. Водночас його розвиток змінює статус людини в суспільстві, викликаючи соціальні проблеми, зокрема в сфері трудових прав через «ефект заміщення» [1].

Використання ШІ повинно враховувати права і свободи людини, а його впровадження в соціально-економічній та управлінській сферах має бути зваженим і контрольованим громадськістю та державними органами. Використання штучного інтелекту впливає на права людини, такі як приватність, свобода вираження та право на справедливий суд. Україна активно розвиває правове регулювання ШІ, прагнучи посісти провідні позиції у світовій технологічній сфері. У 2020 р. була схвалена Концепція розвитку ШІ [2], яка сприяє інтеграції інноваційних технологій в економіку, кібербезпеку, освіту, правосуддя та державне управління. Особлива увага приділяється кібербезпеці, оскільки безпека персональних даних та критичної інфраструктури є ключовими завданнями. Введена в дію Стратегія інформаційної безпеки України визначає основні загрози, включаючи дезінформацію, що особливо актуально у воєнний час [3, с. 69–70].

Проблематика використання штучного інтелекту у сучасному суспільстві має багатоаспектний характер і охоплює питання етики, конфіденційності, справедливості та прав людини. Однією з ключових загроз є ризик неетичного відтворення даних та закріплення соціальних упереджень у процесі прийняття рішень. Оскільки ШІ базується на аналізі історичних даних, він має тенденцію повторювати минулі моделі прийняття рішень, які можуть містити дискримінаційні елементи. Це особливо небезпечно, оскільки, на відміну від людини, яка здатна критично осмислювати свої рішення, змінювати власні переконання та моральні принципи, системи штучного інтелекту не володіють такими властивостями. Вони потребують постійного контролю з боку розробників, які повинні забезпечувати відповідність алгоритмів сучасним уявленням про справедливість і недискримінацію.

Додатково проблемним питанням є вплив ШІ на право на приватність. Оскільки ці технології залежать від величезних масивів даних, вони значно

збільшують ризики порушення конфіденційності. Навіть за умови використання методів захисту даних, таких як диференціальна конфіденційність, алгоритми ШІ здатні аналізувати інформацію таким чином, що з окремих фрагментів даних можна зробити висновки про особисті характеристики людини. Відповідно створює ризик непрямої ідентифікації особи, що може призвести до зловживань та порушення прав людини.

Регулюванням проблемного питання є предметом міжнародного законодавства. ШІ використовує величезні масиви інформації, включаючи дані про особисте життя людей, їхні звички, уподобання, а також особливо конфіденційні відомості, такі як медичні записи. Породжує ризики незаконного збору, аналізу та використання таких даних, наприклад, для комерційних чи політичних цілей без згоди власника. Технології ШІ вже сьогодні активно застосовуються у сферах, пов'язаних із обробкою особистих даних. Вони використовуються для аналізу поведінки споживачів, контролю ефективності бізнес-процесів та навіть у сферах державного управління. Однак недостатність правового регулювання, складність алгоритмів та відсутність чітких механізмів контролю призводять до ситуацій, коли користувачі фактично втрачають контроль над своїми даними [4, с. 394].

Отже, розвиток штучного інтелекту має значний вплив на права людини, створюючи як нові можливості, так і серйозні виклики. Зокрема, використання ШІ може призводити до закріплення соціальних упереджень, порушення права на приватність через масовий збір і обробку персональних даних, а також до змін на ринку праці через автоматизацію. Важливим завданням є розробка ефективного правового регулювання, що забезпечить баланс між технологічним прогресом і дотриманням основоположних прав і свобод людини. Для цього необхідно впроваджувати механізми контролю, етичні стандарти та міжнародне співробітництво з метою запобігання можливим ризикам, пов'язаним із використанням штучного інтелекту.

Список використаних джерел:

1. Турута О. В., Турута О. П. Штучний інтелект крізь призму фундаментальних прав людини. *Науковий вісник Ужгородського Національного Університету*. Серія «Право». 2022. Вип. 71. С. 49–54.

2. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.20 № 1556. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text (дата звернення: 05.03.2025).

3. Шевченко А., Кудін С., Косілова О. Вплив штучного інтелекту на реалізацію прав і свобод людини і громадянина в Україні. *Legal Bulletin*. 2023. С. 65–74.

4. Корнєєва С. Р. Вплив застосування технологій штучного інтелекту на реалізацію та захист прав людини. *Електронне наукове видання «Аналітично-порівняльне правознавство».* 2022. № 4. С. 392–394.

Калаченкова К. О.,
доцент кафедри господарського
та адміністративного права,

кандидат юридичних наук, доцент
(Донецький національний університет імені Василя Стуса)

ШТУЧНИЙ ІНТЕЛЕКТ ТА ПРАВО НА ПРИВАТНІСТЬ

Стрімкий розвиток технологій штучного інтелекту (ШІ) має значний вплив на різні сфери суспільного життя, включаючи державне управління, економіку, медицину та правозастосування. Водночас використання ШІ породжує нові виклики для прав людини, зокрема права на приватність, права на достовірну інформацію, право на недискримінацію, тошо. ШІ-системи аналізують величезні масиви інформації, що створює ризики надмірного збору, несанкціонованого використання даних та можливості дискримінації. З огляду на це, пошук балансу між технологічним прогресом і правом на приватність стає одним із ключових завдань сучасної правової науки як на національному, так і на міжнародному рівнях.

Масовий збір та аналіз персональних даних, що створюються державними установами та приватними корпораціями може привести до однієї з найбільших проблем. ШІ-системи здатні обробляти великі обсяги персональних даних, що може спричинити порушення права на конфіденційність та несанкціонований доступ до чутливої інформації. Також слід пам’ятати, що алгоритми ШІ тренуються на даних і відповідно якщо вони навчались на необ'єктивних або викривлених даних, це може спричинити дискримінацію, несправедливе використання особистої інформації та зниження рівня довіри до цифрових рішень [1, с. 103; 2]. Крім того, використання технологій Big Data у поєднанні з алгоритмами ШІ дозволяє не лише визначати моделі поведінки користувачів, а й створювати детальні діджитал профілі, які можна використовувати як у комерційних, так і в державних цілях [3, 4]. Наприклад, алгоритми таргетованої реклами, які застосовуються соціальними мережами (Meta, TikTok), детальний аналіз персональних даних, часто без явної та усвідомленої згоди користувачів [5, с. 19].

Другим аспектом, на який потрібно звернути увагу, є розвиток технологій розпізнавання обличчя та моніторингу громадян. Використання ШІ у відеоспостереженні стає стандартною практикою в багатьох країнах (наприклад, у Китаї, Франції, Великій Британії, Японії) [6]. Водночас, така практика може призвести до жорсткого контролю за громадянами та порушення принципу пропорційності в обробці персональних даних, визначеного в Загальному регламенті захисту даних ЄС (GDPR).

Крім того, алгоритмічні моделі можуть спричиняти дискримінацію та порушувати принцип рівності. ШІ-системи, які використовуються для автоматизованого ухвалення рішень у сферах кредитування, працевлаштування чи правозастосування, можуть продемонструвати перевагу щодо певних соціальних груп. Наприклад, система COMPAS – алгоритм з визначення ступеня рецидивізму – схильний помилково призначати високі ризики

підсудним афроамериканцям [6]; певні ШІ-моделі дискримінують жінок та представників расових меншин через особливості тренувальних виборів [7].

Європейське законодавство є одним із найбільш розвинених у сфері захисту персональних даних. Регламент (ЄС) 2016/679 (GDPR) встановлює принципи обробки персональної інформації, включаючи: принцип законності, справедливості та прозорості обробки даних (ст. 5 GDPR); право на пояснення рішень, ухвалених автоматизованими системами (ст. 22 GDPR); право на видалення персональних даних («право бути забутим») (ст. 17 GDPR) [8]. Проте, незважаючи на прогресивний характер нормативного регулювання, GDPR не містить спеціальних положень щодо алгоритмів машинного навчання та їхнього впливу на право на приватність. Крім того, проблема алгоритмів «чорної скриньки» залишається нерозв'язаною, більшість моделей ШІ є недостатньо прозорими для розуміння їхньої логіки ухвалення рішень.

Прийнятий у 2024 році **Закон ЄС про штучний інтелект (AI Act)** [9] став першим комплексним законодавчим актом, що регулює використання ШІ в Європейському Союзі. Він визначає категорії ризику ШІ-систем та встановлює обов'язкові вимоги до їхнього використання. Зокрема, AI Act передбачає: п**раво громадян подавати скарги на рішення, ухвалені системами ШІ високого ризику; право на пояснення** рішень, заснованих на системах високого ризику штучного інтелекту (це положення спрямоване на підвищення прозорості алгоритмічних рішень і доповнює положення GDPR щодо автоматизованого ухвалення рішень (ст. 22 GDPR). Також, AI Act закріплює з**аборону використання певних форм ШІ**, зокрема систем, що здійснюють біометричне розпізнавання в реальному часі у громадських місцях (за винятком окремих випадків, визначених законом). Хоча AI Act є значним кроком до забезпечення прав людини в епоху штучного інтелекту, він потребує подальшої адаптації, зокрема для уточнення меж відповідальності розробників та користувачів ШІ-систем.

У лютому 2024 р. Верховній Раді України подано Проєкт Закону про єдину систему відеомоніторингу стану публічної безпеки, який визначає основні засади створення та функціонування єдиної системи відеомоніторингу стану публічної безпеки у відповідності з єдиними функціональними і технологічними стандартами з метою забезпечення національної безпеки, підвищення загального рівня публічної безпеки і порядку, забезпечення безпеки місць проживання та перебування громадян, попередженню і ліквідації можливих загроз, а також контролю за усуненням наслідків надзвичайних ситуацій і правопорушень в інтересах населення держави або певних адміністративно-територіальних одиниць [10]. Хоча в документі не згадується безпосередньо використання технологій штучного інтелекту (ШІ), однак словосполучення «автоматизований аналіз відцифрованих даних» привизначені терміну «відеоаналітика», «автоматизована система» та «…з функціями… технологій, комплексних організаційно-технічних рішень, які забезпечують логічне поєднання та інтеграцію її складових систем» при визначені терміну «система відеомоніторингу стану публічної безпеки» вказує на можливе

застосування таких технологій. Цей Законопроєкт викликає певні занепокоєння серед експертів і правозахисників, оскільки містить певні проблемні моменти пов'язані типами інформації, що збирається та її аналізом, а також з терміном зберігання.

На підставі вищенаведеного можна зробити висновок, що стрімкий розвиток технологій штучного інтелекту вимагає нового підходу до забезпечення права на приватність. Хоча чинне законодавство містить велику гарантію захисту персональних даних, воно не враховує специфіку роботи ШІ, що може призвести до порушення прав людини. Впровадження нових механізмів правового регулювання, таких як Explainable AI, посилений контроль за використанням алгоритмів та забезпечення цифрової автономії особи, може стати ефективним інструментом балансування між технологічним прогресом та утриманням фундаментальних прав людини.

Список використаних джерел:

1. Кравчук С. Вплив штучного інтелекту на права людини та загальні рекомендації для сталого втілення. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки».* 2024. Т. 11, № 3 (43). С. 101–110. DOI: https://doi.org/10.23939/law2024.43.101. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2024/oct/36048/kravchukvisnyk3.pdf.
2. Data Protection Standards and The Use of Ai for Criminal Investigation and Prosecution. URL: https://aiandcriminaljustice.uni.lu/wp-content/uploads/sites/260/2024/11/PAUL-DE-HERT-Presentation-.pdf.
3. Великі данні – що це? IS Integral Solutions. 2018. URL: https://integralsolutions.pl/uk/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D0%B2%D0%B5%D0%BB%D0%B8%D0%BA%D1%96-%D0%B4%D0%B0%D0%BD%D1%96/?utm_source=chatgpt.com.
4. Фостер Провост, Том Фоусет. Data Science для бізнесу. Як збирати, аналізувати і використовувати дані / пер. А. Дудченкою. Львів : Наш формат, 2019. 400 с. URL: https://nashformat.ua/products/ebook-data-science-dlya-biznesu.-yak-zbyraty-analizuvaty-i-vykorystovuvaty-dani-610204?srsltid=AfmBOoqXIhyqfUB2GPBMnM6HjxDiGkcIERi-3LzhSZgkUHVuRng9Diti.
5. Калаченкова К. О. Бородата К. В. Захист персональних даних у процесі використання таргетованої реклами. *Аналітично-порівняльне правознавство*. 2023. № 3. С. 17–21. DOI: https://doi.org/10.24144/2788-6018.2023.03.2. URL: http://app-journal.in.ua/wp-content/uploads/2023/07/4.pdf.
6. Штучний інтелект та відеоспостереження: як запобігти ризикам в Україні. Центр права і політики імені Станислава Дністрянського. URL: https://dc.org.ua/news/shtuchnyy-intelekt-ta-videosposterezhennya-yak-zapobigty-ryzykam-v-ukrayini.
7. Nathalie A. Smuha. Beyond the individual: governing AI's societal harm. *Internet Policy Review*. 2021. Vol. 10 (3). DOI: https://doi.org/10.14763/2021.3.1574.
8. Загальний регламент про захист персональних даних (GDPR). URL: https://gdpr-info.eu/.
9. Про ШІ: Закон ЄС (AI Act). URL: https://artificialintelligenceact.eu/chapter/1/.
10. Проєкт Закону про єдину систему відеомоніторингу стану публічної безпеки від 20.02.2024 № 11031. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43733.

Ковальчук О. І.,

викладач кафедри права та менеджменту
у сфері цивільного захисту
*(Львівський державний університет
безпеки життєдіяльності)*
Саміло А. В.,
начальник кафедри права та менеджменту
у сфері цивільного захисту
*(Львівський державний університет
безпеки життєдіяльності)*
Демчина В. Р.,
ад'юнкт
*(Львівський державний університет
безпеки життєдіяльності)*

ВИКЛИКИ ДЛЯ КОНФІДЕНЦІЙНОСТІ ДАНИХ В ЕПОХУ АЛГОРИТМІВ ШТУЧНОГО ІНТЕЛЕКТУ ТА КІБЕРЗАГРОЗ

У сучасну епоху алгоритмів штучного інтелекту та зростання кіберзагроз проблема забезпечення конфіденційності даних стає одним із ключових викликів цифрового суспільства. З одного боку, технології штучного інтелекту сприяють автоматизації обробки великих обсягів даних, створюючи нові можливості для бізнесу, медицини та інших галузей. З іншого боку, такі технології часто використовують персональну інформацію, що підвищує ризики порушення конфіденційності та загрожує приватності. Кіберзагрози, як-от зломи, шкідливе програмне забезпечення та атаки на штучний інтелект, додатково ускладнюють забезпечення захисту даних. Вирішення цього виклику вимагає створення ефективних міжнародних регулювань, впровадження етичних стандартів для розробки та використання алгоритмів, а також підвищення обізнаності суспільства щодо безпеки даних.

При Держспецзв'язку функціонує урядова команда CERT-UA, яка реагує на кібератаки. За 2024 рік дана структура опрацювала близько 4315 кіберінцидентів, що на 69,8 % більше, ніж за 2023 рік – 2541 хакерських атак/ Під ворожі цілі підпадали органи влади, сектор безпеки та оборони, телекомунікації.

Наприкінці 2024 року внаслідок масштабної російської кібератаки на сайти Національних інформаційних систем, а також Міністерства юстиції України було призупинено роботу Єдиних і Державних реєстрів. Департаментом СБУ з кібербезпеки та експертною групою ініційовано відповідне дослідення подій хакерської атаки ворожих спецслужб. Через кібератаку було неможливо ідентифікувати та верифікувати дані та відбувся збій в державному портал надання сервісних послуг «Дія». Витік персональних даних в державних органах не підтвердили, проте ризики з подібними загрозами досить високі в епоху цифровізації. Роботу реєстрів було відновлено аж в січні 2025 року.

Після кібератаки у Верховній Раді ініціювали та підтримали у у першому читанні законопроєкт №11290, який передбачає підготовку фахівців з кібербезпеки в державних органах та структурах, що працюють та обробляють важливі дані громадян. Згідно статті 4 закону України «Про основні засади забезпечення кібербезпеки України» об’єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об’єкти критичної інфраструктури.

Отже, у світі, де штучний інтелект та цифрові технології стрімко розвиваються, проблема конфіденційності даних стає все більш актуальною. Зростання кіберзагроз і широке використання алгоритмів ШІ вимагають комплексного підходу до захисту особистої інформації. Вирішення цього виклику повинно включати не лише вдосконалення технологічних засобів захисту, але й запровадження етичних стандартів, міжнародних регуляторних рамок і підвищення обізнаності суспільства. Тільки шляхом об'єднання зусиль наукового, технологічного та правового середовищ можна створити безпечні умови для використання даних у сучасну цифрову епоху.

Список використаних джерел:

1. Мартиненко М. О., Ліщинський М. П. Кібербезпека та захист даних в *SAP Business One*. 2025. С. 262.
2. Пунда О. О., Арзянцева Д. А. Забезпечення захисту персональних даних фізичних осіб в умовах розвитку штучного інтелекту. *Наука і техніка сьогодні. Серія : Право.* 2024. № 2 (30). С. 13–142.
3. Остіян Є. З. Штучний інтелект та персональні дані: захист приватності в цифровому середовищі. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Т. 3, № 85 . С. 47–53. DOI: https://doi.org/10.24144/2307-3322.2024.85.3.7.
4. Колесніков А., Карапетян О. Штучний інтелект: переваги та загрози використання. Ефективна економіка. 2023. № 8. DOI: http://doi.org/10.32702/2307-2105.2023.8.9.
5. Ващук Н. Ф. Авторське право та штучний інтелект, напрям № 1 воєнна наука. *Національна безпека*. 2024. С. 114–116.
6. Заярний О. А. Деякі особливості обробки персональних даних при використанні чат-ботів зі штучним інтелектом на прикладі chatgpt. Вип. 29. С. 55.
7. Свердлик З. Кібербезпека та кіберзахист: питання порядку денного в українському суспільстві. *Український журнал з бібліотекознавства та інформаційних наук*. 2022. № 10. С. 175–188. https://doi.org/10.31866/2616-7654.10.2022.269495.

Колич О. І.,
старший викладач кафедри теорії,

історії та конституційного права
ННІ права та правоохоронної діяльності,
кандидат юридичних наук, доцент
*(Львівський державний університет
внутрішніх справ)*

ШТУЧНИЙ ІНТЕЛЕКТ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ: ОКРЕМІ АСПЕКТИ ПРАВОВОГО РЕГУЛЮВАННЯ

За останні кілька десятиліть штучний інтелект (далі – ШІ) інтенсивно розвивається, ставши однією з пріоритетних тенденцій у світі. Динаміка розвитку штучного інтелекту набирає обертів, і все більше суспільних відносин стають потенційними сферами його застосування, який є продуктом, що надає можливість створювати все нові системи аналізу та обробки даних. Завдяки швидкості процесів роботи та особливостям функціонування, ШІ все частіше здатний замінити людину в певних сферах, зокрема у тих, де їй виконувати певні завдання складніше, довше, та і загалом не так якісно, як робототехніка.

Вплив ШІ охопив світові масштаби. За підрахунками експертів, за рахунок ШІ до 2030 року глобальний світовий ВВП зросте на 14 відсотків [1, с. 57], і це без врахування можливостей різкого збільшення його потенціалу.

У жовтні 2019 р. Україна приєдналася до Рекомендацій Організації економічного співробітництва та розвитку щодо штучного інтелекту (Organization for Economic Cooperation and Development, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449) [3].

Поява штучного інтелекту ознаменувала початок нового етапу «цифрової епохи», в якій мають місце «віртуальні особистості» та розвивається концепція «смарт-міст». Відтак однією із проблем, пов’язаних із розвитком ШІ, є захист персональних даних особи. Оскільки системи ШІ здатні створювати штучно згенеровані віртуальні особистості, наділяючи їх фіктивними персональними даними, виникає необхідність правової охорони індивідуальних характеристик індивідів, що дасть змогу забезпечити захист персональних даних фізичних осіб.

Під персональними даними розуміють сукупність відомостей про фізичну особу, яка ідентифікована або може бути ідентифікована (прізвище, ім’я, по батькові, телефон, адреса, паспортні дані тощо).

Найпоширенішими загрозами для персональних даних в цифрову епоху варто виділити наступні:

- кібератаки – доступ до персональних даних дає можливість кіберзлочинцям обдурювати, шантажувати чи обкрадати людей;
- використання персональних даних у корисливих цілях – компанії можуть збирати значний масив персональних даних про своїх клієнтів, партнерів, працівників, і використовувати такі дані у власних цілях, які не відповідають інтересам власника цих даних;

- несанкціоноване стеження та збір даних – приватні компанії, державні органи та інші суб'єкти можуть використовувати зібрану інформацію у власних цілях [2, с. 250].

Відповідно до діючого законодавства, ШІ виступає об'єктом права, і він активно використовується в юриспруденції, ставши інструментом практичної юридичної діяльності. Відтак проблема захисту персональних даних стає все більш обговорюваною та актуальною. Системи ШІ призначені для збирання різноманітних даних, яке здійснюється не завжди з дотриманням загальноприйнятних принципів конфіденційності. Відповідно, забезпечення захисту персональних даних на сьогодні потребує законодавчого вирішення. Для України в умовах війни це питання носить особливо актуальний характер.

За порушення законодавства про захист персональних даних передбачена юридична відповідальність. Так, за незаконне збирання або надання персональних даних, незабезпечення належного рівня їх захисту, недотримання строків надання доступу до персональних даних тощо може наставати адміністративна відповідальність, яка карається штрафом у розмірі від 1799 до 8500 грн для громадян і від 500 до 1000 неоподаткованих мінімумів доходів громадян для ФОП та посадових осіб.

Цивільна відповідальність застосовується за незаконне зберігання, збирання, використання чи знищення персональних даних, а також у випадку завдання шкоди правам та інтересам суб'єкта персональних даних.

Стаття 182 Кримінального кодексу України передбачає відповідальність за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну зміну такої інформації, крім випадків, передбачених Кримінальним кодексом [2].

Висновки. Проблему захисту персональних даних в епоху цифровізації та стрімкого розвитку ШІ можна шляхом об'єднання зусиль держави, громадян та компаній. На даний момент у вітчизняному законодавстві міститься ціла низка прогалин у цій сфері, пов'язаних, насамперед, з повноцінним визначенням поняття «захист персональних даних», встановлення чітких підстав відповідальності за порушення в ході обробки персональних даних, значні недоліки в процедурі накладення стягнень.

Українському законодавцю необхідно вдосконалювати законодавство про захист персональних даних та посилювати механізм контролю за його дотриманням. Захист персональних даних в умовах стрімкого розвитку ШІ повинен бути відображений у законодавстві та стати обов'язком органів публічного управління.

Список використаних джерел:

1. Андрощук Г. Штучний інтелект: економіка, інтелектуальні власність, загрози. *Теорія і практика інтелектуальної власності*. 2021. № 2. С. 56–74.

2. Єпік М. Р., Лучик С. Д. Захист персональних даних в епоху цифровізації. The XXV International Scientific and Practical Conference "Prjblems with distance learning and ways to solve them". June 24–26, 2024, Prague, Czech Republic. 286 p.

3. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

4. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogointelektu-v-ukrayini-s21220.

Кононець В. П.,
провідний науковий співробітник
відділу організації наукової діяльності,
докторка юридичних наук, професорка
(Дніпровський державний університет внутрішніх справ)

ІНФОРМАЦІЙНО-АНАЛІТИЧНА ПІДТРИМКА ПІДРОЗДІЛІВ ЗБРОЙНИХ СИЛ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

В умовах воєнного стану завданням процесу інформатизації військ є забезпечення інформаційних потреб центральних органів влади, органів місцевого самоврядування, органів місцевого самоврядування і навіть усього населення на основі єдиного джерела інформації.

Автоматизація всього комплексу космічних, адміністративно-господарських процесів, використання сучасних засобів автоматизованого управління, соціально-економічного моніторингу, електронного документообігу, аналітичної обробки даних та підтримки прийняття військових рішень.

Реалізація цих завдань потребує, перш за все, визначення стратегії підтримки ІТ-телекомунікацій та інформаційно-аналітичної діяльності Збройних Сил, формування основних принципів автоматизації всіх їхніх військових та управлінських функцій з використанням сучасного електронного документообігу, засобів управління, секретних військових документів усіх галузей військового документообігу в рамках правового режиму військового законодавства в Україні та автоматичного управління для вирішення технічних або військово-економічних та інших завдань у сферах діяльності Збройних Сил.

Необхідність прогнозування, виявлення та прогнозування тенденцій розвитку ситуацій потребує використання різноманітних аналітичних прийомів обробки вихідної інформації в сучасних умовах життя.

Для з’ясування можливих шляхів розвитку ситуації необхідно не лише узагальнити оприлюднену інформацію, а й дати їй оцінку.

Потреба в інформаційно-аналітичних дослідженнях зумовлена не лише наявністю інформаційних бар’єрів, що перешкоджають збору необхідної інформації, а й браком часу для усвідомлених дій споживача.

Суб’єкти управління як споживачі інформації мають дефіцит часу, тому перед ними поставлено завдання постійного моніторингу інформації, виділення необхідної інформації із загальної інформації та збору інформації відповідно до виявлених інформаційних потреб. Необхідний перехід до спеціальних інформаційних сервісів. Трансформуючий аналіз інформації та інтеграція. Джерела інформації відповідно до потреб споживачів.

Виконання цих завдань потребує побудови системи інформаційного забезпечення споживачів інформації. У цій системі споживач інформації виступає вирішальним елементом у створенні інформаційно-аналітичних документів.

В Україні також був створений чат-бот у Telegram для пошуку даних про захисників, які не виходять на зв'язок з певних причин. Наприклад, за допомогою чат-боту "Розшук по даних Національного інформаційного бюро" створили спеціальні інструменти, за допомогою яких рідні та близькі українських оборонців, які потрапили у полон до ворога або зникли безвісти за особливих обставин, можуть здійснити швидкий пошук даних про них. Для того, щоб родич міг визначити статус військовослужбовця, який перебуває в розшуку, для цього необхідно надати наступну інформацію: ідентифікаційний код, прізвище, ім'я та по батькові, номер телефону та дата народження розшукуваної особи, прізвище, ім'я та по батькові, дата народження та ідентифікаційний код особи, яка розшукується. У результаті пошуку рідні та близькі зможуть отримати у чат-боті один із поточних статусів полоненого: про особу немає даних у реєстрі НІБ. Якщо їх не вносили, чат-бот запропонує додати ці відомості; дані є, але в базі даних НІБ немає відомостей, чи перебуває особа в полоні; дані є, особа ймовірно перебуває в полоні (бракує підтвердження від Міжнародного комітету Червоного Хреста – МКЧХ); дані про особу є в базі НІБ, перебування в полоні підтверджено МКЧХ; полонена особа звільнена під час обмінів.

Враховуючи вищевикладене, хочемо зробити висновок, що в активну фазу війни на території України, метою є підтримання на високому рівні всієї розвідувально-аналітичної діяльності, а також злагодженої роботи всіх напрямків.

У сфері штучної зброї з часом з'являється багато нових технологій, які завжди вимагають кваліфікованих працівників для їх дотримання, тому необхідно постійно підвищувати кваліфікацію всіх працівників технічної сфери.

Якщо говорити про технічну складову інформаційно-аналітичної діяльності Збройних сил України в теперішній час дії правового режиму воєнного стану на території України [1], потрібно створювати та розвивати ці бази даних та накопичувати й зберігати інформацію у різних сферах аналітичного військового процесу, а це потребує забезпечення технічними приладами і засобами європейського зразку інших країн.

Список використаних джерел:

1. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text.

2. Про оборону України : Закон України від 06.12.1991 № 1932-XII. URL: https://ips.ligazakon.net/document/view/t193200?an=1&ed=2023_03_21.

Про розвідувальні органи України : Закон України від 22.03.2001 № 2331-III. URL: https://ips.ligazakon.net/document/view/t012331?an=ul-120&ed=2008_06_03.

Кононець В. П.,

провідний науковий співробітник
відділу організації наукової діяльності,
докторка юридичних наук, професорка
(Дніпровський державний університет внутрішніх справ)
Ададуров А. В.,
аспірант кафедри
адміністративного права і процесу,
(*Дніпровський державний університет внутрішніх справ*)

ПРОБЛЕМИ ПРИТЯГНЕННЯ ОСІБ ДО АДМІНІСТРАТИВНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ПОРУШЕННЯ ПРИЗОВНИКАМИ, ВІЙСЬКОВОЗОБОВ'ЯЗАНИМИ, РЕЗЕРВІСТАМИ ПРАВИЛ ВІЙСЬКОВОГО ОБЛІКУ ПІД ЧАС ДІЇ ВОЄННОГО СТАНУ В УКРАЇНІ

У зв'язку із повномасштабним вторгненням та військовою агресією російської федерації проти України, Указом Президента України № 64/2022 від 24 лютого 2022 року на всій території України введено воєнний стан. Воєнний стан неодноразово продовжувався і діє на сьогоднішній день [4].

Рішенням Верховної Ради України відповідно до Резолюції Генеральної Асамблеї ООН 3314 «Визначення агресії» від 14 грудня 1974 року Російську Федерацію визнано державою-агресором та таку, що здійснює збройну агресію проти України[2].

Нові виклики, зумовили державу Україна внести зміни до Кодексу України про адміністративне правопорушення. 09.05.2024 Верховна Рада Україна прийняла Закон України № 3696-IX «Про внесення змін до Кодексу України про адміністративні правопорушення щодо удосконалення відповідальності за порушення правил військового обліку та законодавства про оборону, мобілізаційну підготовку та мобілізацію» який набрав чинності 19.05.2024 року.

Відповідно до зазначеного закону до Кодексу України про адміністративні правопорушення (Відомості Верховної Ради УРСР, 1984 р., додаток до № 51, ст. 1122) внесені зміни після частини шостої доповнити новою частиною такого змісту: *«Адміністративне стягнення за вчинення в особливий період правопорушень, передбачених статтями 210, 210-1 цього Кодексу, може бути накладено протягом трьох місяців з дня його виявлення, але не пізніше одного року з дня його вчинення»,* а також змінена редакція статті 210 та 210-1 КУпАП, яка посилала адміністративну відповідальність осіб, які порушують правила військового обліку та порушення законодавства про оборону, мобілізаційну підготовку та мобілізацію[2].

Слід відмітити той факт, що Закон України № 3696-IX внесені зміни і до ст. 258 КУпАП, яка регулює процедури притягнення коли протокол про адміністративне правопорушення не складається. Частину 6 ст. 258 КУпАП

викладена у наступній редакції: *«Протокол не складається у разі вчинення в особливий період адміністративних правопорушень, передбачених статтями 210, 210-1 цього Кодексу, розгляд яких віднесено до компетенції територіальних центрів комплектування та соціальної підтримки, Центрального управління або регіональних органів Служби безпеки України (у частині правопорушень, вчинених військовозобов'язаними чи резервістами, які перебувають у запасі Служби безпеки України), якщо особа не з'явилася без поважних причин або не повідомила причину неприбуття на виклик територіального центру комплектування та соціальної підтримки, Центрального управління або регіонального органу Служби безпеки України, будучи належним чином повідомленою про дату, час і місце виклику, та за наявності у територіального центру комплектування та соціальної підтримки, Центрального управління або регіонального органу Служби безпеки України підтвердних документів про отримання особою виклику»* [2].

Однак на превеликий жаль, працівники Територіальних центрів комплектування та соціальної підтримки, так і не зрозуміли на сьогоднішній день, процедуру притягнення осіб за адміністративної відповідальністю за статтями 210, 210-1. Держава України наділила працівників Територіальних центрів комплектування та соціальної підтримки складати адміністративні матеріали, та виносити постанови про притягнення осіб до адміністративної відповідальності, відповідно до статті 235 КУпАП [3].

Проте працівники систематично та цілеспрямовано порушують процедури притягнення осіб до адміністративної відповідальності. Розглянемо одну з найпоширеніших помилок, яку допускають працівники Територіальних центрів комплектування та соціальної підтримки.

Одна з най поширених помилок, це не повідомлення особи про розгляд справи про адміністративне правопорушення всупереч ч. 6 ст. 258 КУпАП. Працівники територіального центру комплектування не повідомляють особу про розпочату процедуру адміністративного притягнення. У зв'язку з чим не складають протокол про адміністративне правопорушення, а відразу виносять постанову про притягнення до адміністративної відповідальності. У зв'язку з чим, порушують процедури адміністративного притягнення, що призводить до скасування оскаржуваних постанов судом.

Друга з найпоширеніших помилок, це складання протоколу про адміністративне правопорушення та постанови в один день. ч. 2 ст. 210 КУпАП особа повідомляється не пізніше як за три доби до дати розгляду справи. У процесі розгляду справи особа, яка притягується до адміністративної відповідальності має право користуватися правами, передбаченими ст. 268 КУпАП [3]. Однак працівники Територіальних центрів комплектування та соціальної підтримки чи свідомо, чи за вказівкою свого керівництва, складають протокол про адміністративне правопорушення та постанову про адміністративне правопорушення в один день. Що порушує, права особи яка притягається до адміністративної відповідальності.

Обов`язок повідомляти особу про місце і час розгляду справи не пізніше, ніж за три дні до дати розгляду справи про адміністративне правопорушення вважається виконаним, якщо особа, яка притягується до відповідальності, знає (поінформована) про час та місце розгляду справи за три дні до дати розгляду справи. Обов`язок доказування цієї обставини несе уповноважена посадова особа. Повідомлення має на меті забезпечення участі особи у розгляді уповноваженим державним органом справи про адміністративне правопорушення. Тобто особі, до якої застосовується адміністративна санкція, повинно бути забезпечено право завчасно знати про час та місце розгляду справи. Це право є гарантією реалізації інших прав на участь в розгляді справи про адміністративне правопорушення, висловлення заперечень, надання доказів, захист тощо. Несвоєчасне повідомлення або неповідомлення особи, яка притягується до адміністративної відповідальності, про час та місце розгляду справи про адміністративне правопорушення є підставою для визнання постанови у справі про адміністративне правопорушення неправомірною як такої, що винесена з порушенням встановленої процедури.

Такі порушення, є порушенням доктрини «плодів отруйного дерева».

Відповідно до доктрини «плодів отруйного дерева»(fruit of the poisonous tree) сформульованої Європейським судом з прав людини у справах «Гефген проти Німеччини», «Тейксейра де Кастро проти Португалії», «Шабельник проти України» «Балицький проти України», «Нечипорук і Йонкало проти України»,«Яременко проти України», якщо джерело доказів є неналежним, то всі докази, отримані з його допомогою, будуть такими ж («Гефген проти Німеччини»). На думку ЄСПЛ, надається оцінка допустимості всього ланцюжка доказів, що базуються один за іншим, а не кожного окремого доказу автономно. У рішенні по справі «Нечипорук і Йонкало проти України» Європейський суд з прав людини зазначив, що докази, отримані в кримінальному провадженні з порушенням встановленого порядку, призводять до його несправедливості в цілому, незалежно від доказової сили таких доказів і від того, чи мало їх використання вирішальне значення для засудження обвинуваченого судом. У рішеннях у справах «Балицький проти України», «Тейксейра де Кастро проти Португалії», «Шабельник проти України» ЄСПЛ застосував різновид доктрини «плодів отруйного дерева», яка полягає в тому, що визнаються недопустимими не лише докази, безпосередньо отримані з порушеннями, а також докази, яких не було б отримано, якби не було отримано перших. Таким чином, допустимі самі по собі докази, отримані за допомогою відомостей, джерелом яких є недопустимі докази, стають недопустимими [5].

Зазначені помилки порушують права людини та її основоположні права. Сучасні науковці нажаль дуже мало приділяють означеній темі уваги, та чомусь не висвітлюють кричущі проблеми, які існують у процедурі притягнення осіб до адміністративної відповідальності.

Список використаних джерел:

1. Про Звернення Верховної Ради України до Організації Об’єднаних Націй, Європейського Парламенту, Парламентської Асамблеї Ради Європи, Парламентської Асамблеї НАТО, Парламентської Асамблеї ОБСЄ, Парламентської Асамблеї ГУАМ, національних парламентів держав світу про визнання Російської Федерації державою-агресором : Постанова Верховної Ради України від 27.01.2015 № 129-VIII. URL: https://zakon.rada.gov.ua/laws/show/2116-20#Text(дата звернення: 13.02.2025).

2. Про внесення змін до Кодексу України про адміністративні правопорушення щодо удосконалення відповідальності за порушення правил військового обліку та законодавства про оборону, мобілізаційну підготовку та мобілізацію : Закон України від 09.05.2024 № 3696-IX. URL: https://zakon.rada.gov.ua/laws/show/3696-20#n12 (дата звернення: 13.02.2025).

3. Про внесення змін до Кодексу України про адміністративні правопорушення щодо удосконалення відповідальності за порушення правил військового обліку та законодавства про оборону, мобілізаційну підготовку та мобілізацію : Закон України від 09.05.2024 № 3696-IX. URL: https://zakon.rada.gov.ua/laws/show/3696-20#n12 (дата звернення: 13.02.2025).

4. Указ Президента України : Про введ. воєн. стану в Україні від 24.02.2024 № 64/2022. URL: https://www.president.gov.ua/documents/642022-41397 (дата звернення: 29.02.2024).

5. Як ККС ВС застосовує доктрину ЄСПЛ «плід отруйного дерева». URL: https://sud.ua (дата звернення: 13.02.2025).

Кулик В. М.,
здобувач вищої освіти освітнього
ступеня «магістр»
Інституту права та безпеки
(Одеський державний університет внутрішніх справ)
Калугін В. Ю.,
професор кафедри кримінального аналізу
та інформаційних технологій,
кандидат юридичних наук, доцент
(Одеський державний університет внутрішніх справ)

ЗНАЧЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РОЗВИТКУ ВІДЕОАНАЛІТИКИ

Штучний інтелект відіграє ключову роль у розвитку відеоаналітики, дозволяючи автоматизувати обробку та аналіз відеоданих у режимі реального часу. Завдяки машинному та глибокому навчанню, алгоритми штучного інтелекту можуть ідентифікувати об’єкти, розпізнавати обличчя, виявляти аномальні ситуації та аналізувати поведінкові патерни.

З розвитком технологій комп’ютерного зору та обчислювальних потужностей штучний інтелект став основою для вдосконалення відеоаналітики. Сучасні алгоритми можуть аналізувати відеопотоки в реальному часі, забезпечуючи автоматичний моніторинг та розпізнавання об’єктів. Це значно підвищує ефективність систем відеоспостереження, безпеки, логістики, транспорту та інших сфер [1].

На сьогодні системи відеоспостереження набули широкого застосування у забезпеченні безпеки об'єктів різноманітного призначення, таких як банки, торгові центри, розважальні заклади, промислові підприємства, а також у діяльності інших комерційних і некомерційних установ. Вони забезпечують можливість оперативного реагування на потенційно небезпечні ситуації, здійснення моніторингу персоналу та відвідувачів, а також займають важливе місце у системах контролю за дорожнім рухом та інших галузях, що потребують постійного спостереження та обробки інформації.

Відеоаналітика є комплексним програмним алгоритмом, здатним ефективно обробляти відеодані, що дає змогу звільнити операторів від монотонної роботи з безліччю камер, а також автоматично виявляти порушення або аномальні події в реальному часі.

Розвиток інтелектуальної відеоаналітики відбувається на основі двох основних технологій: трекінгу (відстеження об'єктів) та ідентифікації (виявлення і розпізнавання об'єктів і осіб). На базі встановлених алгоритмічних правил формується функціонал системи, що є необхідною основою для побудови сучасних систем відеоспостереження, здатних забезпечити високий рівень безпеки та точності аналізу зображень. Трекінг – це коли алгоритм

обробки відео шукає в кадрі рух, визначає та класифікує об’єкт, що рухається, описує його характеристики (розмір, колір, швидкість) [2].

Основні технології відеоаналітики на основі штучного інтелекту – комп’ютерний зір – це галузь штучного інтелекту, яка дозволяє комп’ютерам «бачити» та аналізувати візуальну інформацію. Завдяки нейромережам відеоаналітичні системи можуть ідентифікувати об’єкти (людей, автомобілі, предмети); розпізнавати текст та номери транспортних засобів; класифікувати та відстежувати рухомі об’єкти.

Одна з найважливіших технологій у відеоаналітиці – розпізнавання облич. Алгоритми штучного інтелекту можуть ідентифікувати особу на основі біометричних даних, що використовується для забезпечення громадської безпеки (виявлення розшукуваних осіб); контролю доступу (безконтактна ідентифікація в офісах та підприємствах); маркетингового аналізу (ідентифікація клієнтів у магазинах).

Традиційні системи відеоспостереження, що призначені для загального використання, на сьогоднішній день не відповідають вимогам оперативного реагування на екстремальні ситуації, що можуть виникнути в місцях масового скупчення людей або на масштабних об'єктах транспортної інфраструктури. Для ефективного вирішення сучасних задач необхідно використовувати комплексні інтелектуальні системи, що ґрунтуються на складних алгоритмах відеоаналітики та ідентифікації, здатних забезпечити високу точність та оперативність виявлення порушень.

Ідентифікація передбачає розпізнавання об'єктів за відеозображенням шляхом їх класифікації або порівняння з заздалегідь підготовленими еталонними зразками. Серед найбільш важливих і необхідних методів розпізнавання сьогодні виділяються розпізнавання облич та розпізнавання номерних знаків транспортних засобів.

Штучний інтелект може виявляти аномальну поведінку людей або об’єктів на відео, наприклад: агресивну поведінку в громадських місцях; залишені підозрілі предмети; нетипові рухи чи скупчення людей [3]. Така технологія використовується для запобігання злочинам, контролю безпеки в аеропортах, транспортних вузлах та місцях масового скупчення людей.

Відеоаналітика на основі штучного інтелекту активно застосовується в транспортній сфері розпізнавання номерних знаків; контроль швидкості руху; аналіз завантаженості доріг та прогнозування трафіку. Це дозволяє покращити управління дорожнім рухом та підвищити ефективність транспорту.

Розвиток штучного інтелекту та вдосконалення спеціалізованого програмного забезпечення сприяли виокремленню окремого, хоча й не абсолютно нового напряму аналітичної діяльності – відеоаналітичних досліджень (відеоаналітики). Активізація цього напряму безпосередньо пов’язана зі швидкою еволюцією комплексних систем відеоспостереження, які вже стали невід’ємним елементом функціонування підрозділів Національної поліції України. Водночас актуалізується необхідність удосконалення правових механізмів регламентації застосування методів кримінального аналізу у процесі

оперативно-розшукової діяльності та досудового розслідування, що вимагає системного підходу до їх правового забезпечення та нормативної адаптації.

Список використаних джерел:

1. Технології комп'ютерного зору: інновації для розвитку вашого бізнесу. 17 квітня 2024 р. URL: https://metinvest.digital/ua/page/computer-vision-spais.

2. Методичні рекомендації щодо організації та проведення кримінального аналізу підрозділами Національної поліції України, затверджені Головою Національної поліції України Клименком Ігорем 11 травня 2021 року (вих. ДДЗ від 26 травня 2021 року № 6516/01/33-2021).

3. Гбур З. В. Використання штучного інтелекту в інформаційній безпеці України. *Державне управління: удосконалення та розвиток*. URL: http://www.dy.nayka.com.ua/pdf/1_2022/4.pdf

Левенець А. В.,
доцент кафедри конституційного права та правосуддя,
кандидат юридичних наук, доцент
(Одеський національний університет імені І. І. Мечникова)

ПЕРСПЕКТИКИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОЦЕДУРІ ДОБОРУ ТА ОЦІНЮВАННЯ КАНДИДАТА НА ПОСАДУ СУДДІ В УКРАЇНІ

Проблема кадрового забезпечення суддівського корпусу залишається актуальною для нашої держави вже не перший рік. Актуалізується питання не лише кількісного наповнення діючих судів, але й якісного відбору суддівських кадрів, які б відповідали конституційним вимогам компетентності, професійної етики та доброчесності. Судова реформа останніх років у більшій мірі пов'язана саме із вирішенням питання: як швидко та оперативно провести процедури добору, підготовки та призначення суддів на посади, не нехтуючи при цьому якістю. На круглому столі на тему: «Привабливість суддівської кар'єри: український та зарубіжний досвід» голова Вищої ради правосуддя (далі – ВРП) Г. Усик зазначив: «Питання, пов'язані з підвищенням привабливості суддівської кар'єри, актуальні як для судової системи України, так і для розвинених демократичних європейських держав. Однак саме для України за попередні п'ять-сім років проблема дефіциту суддівських кадрів стала надзвичайно гострою. Вітчизняна судова система працює у критичних умовах через значний дефіцит кадрів. Особливо складна ситуація в апеляційних судах, у яких вакантними є понад 52 % суддівських посад» [1].

Одним з ефективних кроків вирішення окресленої проблеми стала реформа законодавства та істотне скорочення стадій процедури добору кандидатів на суддівські посади до місцевих судів у 2023 році, яка загалом із п'ятнадцяти скоротилась до 8 стадій [2, ст. 70]. Проте навантаження, яке залишається на членах ВККС щодо забезпечення перевірки відповідності осіб, які виявили намір бути суддею, вимогам законодавства, зокрема – що

стосується перевірки на компетентність та доброчесність, все одно залишається завеликим, враховуючи масив інформації, який потрібно зібрати та оцінити. Одним зі шляхів оптимізації відповідної діяльності може стати застосування штучного інтелекту у процедурі добору та призначення кандидатів на суддівські посади. Проте враховуючи численні дискусії щодо доцільності, етичності та потенційних загроз застосування ШІ у різних сферах життєдіяльності суспільства та держави, зокрема й актуалізацію в останні роки теми щодо застосування ШІ у сфері правосуддя, вважаємо за необхідне приділити більш детальну увагу цьому питанню.

Згідно ст. 73, 75 Закону «Про судоустрій та статус суддів», Вища кваліфікаційна комісія суддів (далі – ВККС) здійснює перевірку на відповідність особи, яка виявила намір стати суддею, критеріям компетентності та доброчесності на підставі отриманих від особи документів, а також після успішно складеного кваліфікаційного іспиту – спеціальну перевірку щодо кожного кандидата на підставі інформації, отриманої від державних органів шляхом направлення відповідних запитів, шляхом електронної взаємодії з базами даних, реєстрами, автоматизованими інформаційними системами і т.д. Виходячи зі змісту цих статей, стає зрозумілим, наскільки важливим та трудомістким є даний етап у процедурі добору кандидатів на суддівські посади. Можемо допустити, що саме цей етап має у першу чергу відбуватись із широким застосуванням технологій ШІ. На підтвердження раціональності такого підходу наведемо думку О. Пархоменко-Куцевіл, яка до речі у своєму дослідженні як раз розглядає питання обґрунтованості застосування технологій ШІ у системі управління персоналом публічної служби в Україні: «Переваги цифрових технологій очевидні: вони можуть працювати з величезними масивами даних, аналізувати їх, класифікувати, ранжувати, розподіляти за наперед визначеними критеріями, і все це за якісь секунди. Система штучного інтелекту у сфері HR може, наприклад, оцінювати різні демографічні параметри, досвід попередньої роботи претендента при безпосередньому аналізі даних одержаних ним рекомендацій, відгуків в Інтернеті та іншої маси додаткової інформації, яку системі вдасться знайти» [3, с. 102].

Ще одним позитивним аспектом застосування ШІ у процедурі збору інформації та оцінювання кандидата на посаду судді критеріям компетентності та доброчесності, є те, що за такого підходу виключається людський фактор та знижується ризик прийняття необ’єктивного рішення. У затверджених ВРП Єдиних показниках для оцінки доброчесності та професійної етики судді (кандидата на посаду судді) від 17 грудня 2024 року у контексті обґрунтованого сумніву у доброчесності особи отримало визначення таке поняття: «**звичайна розсудлива людина –** законослухняна людина, яка, достатньою мірою інформована про факти та процеси, що відбуваються, об’єктивно сприймає інформацію та обставини зі сторони» [4]. Отже постає питання: чи може ШІ оцінити зібрані дані та факти про особу і на їх основі прийняти рішення про відповідність кандидата на посаду судді критеріям компетентності та доброчесності за аналогією «звичайної розсудливої людини», чи його роль має

зводитись лише до обробки великої кількості даних і відповідно спрощення цієї роботи для членів ВККС? На думку О. Пархоменко-Куцевіл, «за результатами такого аналізу система дає прогноз, наскільки претендент задовольняє вимогам системи публічної служби і навіть наскільки ефективний він буде в тих чи інших умовах. Нерідкі ситуації, коли робот-рекрутер, наполегливо рекомендує керівництву органу державної влади спробувати того чи іншого претендента на іншій посаді, що найбільше підходить, на його думку» [3, с. 102].

На наш погляд, враховуючи певну специфіку суддівської діяльності, а також той факт, що окрім компетентності, ґрунтовній оцінці підлягає така категорія, як доброчесність, яка має яскраво виражений морально-етичний характер, сьогоднішній рівень розвитку ШІ навряд здатен оцінити цю категорію. Проте залучення технологій ШІ на допомогу у зборі, систематизації та аналізі інформації, про що йшлося вище, однозначно має сенс. І треба зауважити, що початок цього процесу вже покладено, оскільки у грудні 2023 року почали формуватися е-досьє кандидата на посаду судді під час проведення першого відкритого відбору на посаду суддів апеляційних судів через електронний кабінет суддівської кар'єри. Що цікаво – для успішних кандидатів воно трансформується у е-досьє судді. Оцінюючи перспективи спрощення процесу добору кандидатів на суддівські посади через використання електронного кабінету, заступник керівника секретаріату ВККС Т. Нешик зазначає: «для участі в конкурсі на посаду судді апеляційного суду до ВККС звернулося 2076 кандидатів. При цьому згідно із законодавством, досьє кандидата на посаду судді має бути оприлюднено на офіційному вебсайті ВККС. Тобто під час подачі документів кандидатами у паперовому вигляді комісія мала б організувати процес сканування мільйонів сторінок і вивантаження їх на свій сайт. Це тисячі людиногодин, які оплачують платники податків» [5]. У найближчій перспективі передбачено налагодження комунікації е-досьє з іншими базами даних, інформаційними системами та реєстрами як раз для оптимізації процесу збору інформації, її систематизації і т.д. Звісно, при всіх позитивних аспектах не слід забувати про такі загрози застосування ШІ, як захист персональних даних, перебої в алгоритмах та ін.

Список використаних джерел:

1. Усик Г. Вітчизняна судова система працює у критичних умовах через значний дефіцит суддівських кадрів. Круглий стіл на тему «*Привабливість суддівської кар'єри: європейський та український виміри»*, 23 вересня 2024 р. URL: https://hcj.gov.ua/news/vitchyznyana-sudova-systema-pracyuye-u-krytychnyh-umovah-cherez-znachnyy-deficyt-suddivskyh (дата звернення: 05.03.2025).

2. Про судоустрій та статус суддів : Закон України від 2 червня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/1402-19#n2356 (дата звернення: 05.03.2025).

3. Пархоменко-Куцевіл О. Обґрунтування використання технологій штучного інтелекту у системі управління персоналом публічної служби України. *Публічне управління: концепції, парадигма, розвиток, удосконалення.* 2024. Вип. 8. С. 98–106.

4. Єдині показники для оцінки доброчесності та професійної етики судді (кандидата на посаду судді) : затверджено рішенням Вищої ради правосуддя 17 грудня 2024 року № 3659/0/15-24. URL: https://hcj.gov.ua/doc/doc/49121.

5. Нешик Т. Е-досьє суддів: яку інформацію вже відкрито і як це допоможе відновити довіру до судової гілки влади. URL: https://mind.ua/openmind/20269255-e-dose-suddiv-yaku-informaciyu-vzhe-vidkrito.

Литвин С. Й.,
доцент кафедри цивільного права та
процесу юридичного факультету,
кандидат юридичних наук, доцент, адвокат
(ДВНЗ «Ужгородський національний університет»)
Піхурець О. В.,
доцентка кафедри цивільного,
трудового та господарського права,
кандидатка юридичних наук, доцентка
(Харківський національний
університет внутрішніх справ)

СУБ'ЄКТ ВІДПОВІДАЛЬНОСТІ ЗА ШКОДУ, ЗАПОДІЯНУ ШТУЧНИМ ІНТЕЛЕКТОМ

Розвиток технології штучного інтелекту (ШІ) відкриває безпрецедентні можливості для суспільства, але водночас створює нові правові виклики, одним із яких є визначення суб'єкта відповідальності за шкоду, заподіяну ШІ. У міру того, як технології стають дедалі автономнішими, традиційні підходи до відповідальності, що базуються на діях людини, втрачають актуальність. Хто має нести відповідальність за збитки, спричинені ШІ: розробник, користувач, власник чи, можливо, сам алгоритм? Це питання ускладнюється відсутністю чіткого правового регулювання в Україні та світі, а також технічною складністю ШІ, який може діяти непередбачувано. Однак, питання про суб'єкта відповідальності за шкоду, заподіяну ШІ, є ключовим для забезпечення справедливості, захисту прав громадян і створення безпечного середовища для інновацій, що робить цю тему надзвичайно актуальною для сучасної юриспруденції.

Разом з тим, питання про самостійну участь у цивільних відносинах високорозвиненого ШІ чи розумного робота як суб'єкта права залишається відкритим. Саме тому запропоновані юридичні конструкції у звіті Європейського парламенту [1] є вельми актуальними та становлять практичну основу для врегулювання відповідальності за шкоду заподіяну ШІ, а саме:

- конструкція відповідальності виробника за несправності ШІ (за якість і безпеку технології, чи за дефект продукції);

- конструкція відповідальності за шкідливі дії, відповідно до якої користувач ШІ несе відповідальність за дії, що призвели до заподіяння шкоди.

У документі також підкреслюється недостатність цих підходів, якщо шкода настала внаслідок власних дій і рішень ШІ за відсутності вини чи причинно-наслідкового зв'язку між діями людини й виникненням шкоди. А також наголошується на неприпустимості обмеження видів, форм і обсягу компенсації шкоди, заподіяної ШІ, що захищає інтереси постраждалих і стримує лобістські зусилля виробників, які прагнуть зменшити власну відповідальність.

Фактично, для визначення суб'єкта відповідальності за дії ШІ пропонується застосовувати «теорію ризику», згідно з якою відповідальність покладається на особу, яка могла мінімізувати ризики та врахувати негативні наслідки. Ступінь відповідальності залежить від рівня автономності ШІ та ролі людини, яка його навчає. Однак у звіті не вказано, як діяти у випадках, коли шкода заподіюється за відсутності контролю людини при високій автономності ШІ, де відсутність вини та причинно-наслідкового зв'язку ускладнює притягнення людини до відповідальності. Крім того, покладання відповідальності на користувачів може бути несправедливим, якщо вони не мають достатніх знань чи технічних можливостей для належного контролю ШІ. Особливо враховуючи, що навіть високорозвинений ШІ навряд чи здатний усвідомлювати наслідки своїх неправомірних дій чи рішень [2].

Слід вказати і на проблему прихованих алгоритмів, навіть за умови визнання високого рівня автономності ШІ. Більшість технологічних систем ШІ базуються на закритому програмному забезпеченні, де логіка прийняття рішень (обчислювальний шлях) залишається незрозумілою для людини. У перспективі це може призвести до непередбачуваності результатів роботи ШІ, що робить ідею надання їм правосуб'єктності вкрай ризикованою. Ця проблема ускладнюється відсутністю належної законодавчої бази в Україні, яка б чітко визначала правовий статус ШІ, розподіл відповідальності між розробниками, користувачами та власниками, а також механізми компенсації шкоди. Без такого регулювання правова система залишається непідготовленою до вирішення конфліктів, пов'язаних із ШІ, що може призводити до несправедливості та стримувати розвиток технологій через правову невизначеність.

Отже, питання про те, хто саме нестиме відповідальність за неправильне рішення, реалізоване в житті, яке спричинило шкоду і було здійснене чи запропоноване ШІ, а також регулювання можливості та ступеня відповідальності ШІ-роботів і їхніх творців, залишається відкритим. Однак у науці цивільного права існує кілька підходів до визначення суб'єкта відповідальності за шкоду, заподіяну системами ШІ. **Перший підхід** полягає в тому, що суб'єктами відповідальності повинні бути виключно фізичні або юридичні особи, які забезпечують функціонування систем ШІ або використовують їх [3, с. 18; 4, с. 124]. До яких належать розробники, виробники, власники, оператори та користувачі ШІ. Визначення особи, відповідальної за шкоду, заподіяну ШІ, має ґрунтуватися на

тому, хто спричинив дію чи бездіяльність ШІ, що призвела до шкоди, а також слід враховувати рівень автономності цього ШІ. **Другий підхід** передбачає визнання суб'єктом відповідальності сам ШІ [5]. У цьому випадку запропоновано два види відповідальності: обмежена майнова відповідальність систем ШІ та відповідальність високорозвинених автономних систем ШІ (так званих «цифрових осіб») [6].

Однак, на нашу думку, впровадження таких видів відповідальності є проблематичним, оскільки це може створити можливість для розробників, виробників та власників систем ШІ уникнути відповідальності за їхні дії. Водночас, для притягнення до відповідальності ШІ за заподіяну ним шкоду необхідно запровадити особливий правовий статус у віртуальному просторі. Що на сьогодні є неможливим через відсутність нормативних механізмів для реалізації такого підходу. Акт ЄС про ШІ передбачає запровадження єдиного правового підходу до регулювання застосування ШІ, незалежно від індустрії або технології. Однак його положення почнуть застосовуватися з 2 серпня 2026 року [7]. Цей нормативний акт є надзвичайно прогресивним, оскільки встановлює класифікацію та регулювання програми ШІ на основі їхнього потенційного ризику: системи з обмеженим ризиком (limited risk); системи з високим ризиком (high risk); системи з неприйнятним ризиком (unacceptable risk). Відзначимо і Рамкову конвенцію про штучний інтелект і права людини, демократію та верховенство права, яка є першою міжнародною юридично зобов'язуючою угодою у цій сфері та національну Концепцію розвитку штучного інтелекту в Україні та Плану заходів з її реалізації, а також Дорожню карту з регулювання штучного інтелекту в Україні, однак ці нормативні акти також не дають нам відповіді хто має нести відповідальність за шкоду заподіяну ШІ.

Визначення суб'єкта відповідальності за шкоду, заподіяну ШІ, залишається складним завданням через автономність і непередбачуваність сучасних систем. Очевидно, що ШІ, роботизований пристрій чи промислова лінія є об'єктами цивільно-правових відносин, зокрема права інтелектуальної власності. Водночас промисловий робот чи робот-агент, залежно від рівня ШІ, у майбутньому може розглядатися як особливий суб'єкт із обмеженою правоздатністю. Наразі ШІ не може бути суб'єктом права чи нести юридичну відповідальність через відсутність правосуб'єктності, що унеможливлює самостійну відповідальність за свої дії. Отже, за шкоду, заподіяну ШІ, мають відповідати дієздатні суб'єкти цивільних правовідносин – особи, які контролюють або відповідають за належне функціонування таких систем. Оскільки ШІ створюється людьми, які розробляють його алгоритми, саме вони несуть відповідальність за наслідки, навіть якщо система вийде з-під контролю. На нашу думку, до таких осіб слід віднести: виробника (розробника); власника кіберфізичної чи віртуальної форми ШІ; оператора; користувача тощо.

Цих осіб слід вважати суб'єктами відповідальності, оскільки вони мають прямий вплив на створення, функціонування та використання ШІ. Виробник (розробник) відповідає за якість алгоритмів і безпеку системи, адже саме він

закладає основу її роботи. Власник забезпечує належне технічне обслуговування та експлуатацію ШІ, що впливає на його поведінку. Оператор і користувач безпосередньо взаємодіють із системою, тому їхні дії чи бездіяльність можуть спричинити шкоду. Такий розподіл відповідальності дозволяє врахувати всі етапи життєвого циклу ШІ, забезпечуючи справедливе відшкодування шкоди та стимулюючи відповідальне ставлення до технологій.

У підсумку, варто зазначити, що підхід, запропонований у звіті Європейського парламенту [1], є прогресивним і практичним, оскільки передбачає чіткі механізми розподілу відповідальності між виробниками та користувачами систем штучного інтелекту (ШІ). Це забезпечує справедливість у випадках заподіяння шкоди, стимулюючи виробників створювати безпечні та якісні технології, а постраждалим гарантує зрозумілий механізм відшкодування, підвищуючи прозорість процесу. Крім того мотивує користувачів ШІ діяти обережніше та відповідальніше, враховуючи конкретні обставини, коли проблема пов'язана з людським фактором, а не з дефектами самої системи.

Вважаємо, що цей підхід відповідає реальним потребам сучасного суспільства, де ШІ дедалі більше інтегрується, пропонуючи практичні рішення для нових викликів. Він забезпечує правову ясність, зменшуючи спори та невизначеність у правових питаннях, пов'язаних із використанням ШІ. Саме тому його необхідно запровадити в українське законодавство, щоб адаптувати правову систему до стрімкого розвитку технологій, захистити права громадян, уникнути правового вакууму та сприяти безпечному інноваційному середовищу, що відповідатиме європейським стандартам.

Список використаних джерел:

1. European Parliament. REPORT with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103 (INL)). Debates, 15 February 2017. *European Parliament: site.* URL: https://surl.gd/dpmxpl (дата звернення: 12.03.2025).
2. Hallevy G. Liability for Crimes Involving Artificial Intelligence Systems. Dordrecht, Springer. 2015. 257 p. DOI: 10.1007/978-3-319-10124-8_1 (дата звернення: 12.03.2025).
3. Великанова В. В. Відшкодування шкоди, завданої використанням технологій штучного інтелекту, як спеціальний делікт. *Нове українське право*.2021. Вип. 3. С. 17–21. URL: https://surl.gd/gntfhx (дата звернення: 12.03.2025).
4. Жорнокуй Ю. М. Штучний інтелект: питання відповідальності на сучасному етапі розвитку доктрини. Ф*орум права.* 2024. № 2. С. 118–127. URL: https://surl.li/atuvma (дата звернення: 12.03.2025).
5. Bertolini, A., & Episcopo, F. (2022). Robots and AI as Legal Subjects? *Disentangling the Ontological and Functional Perspective. Frontiers in Robotics and AI,* 9, Art. 842213. https://doi.org/10.3389/frobt.2022.842213 (дата звернення: 12.03.2025).
6. Hárs, A. (2022). AI and international law – Legal personality and avenues for regulation. *Hungarian Journal of Legal Studies*, 62 (4). P. 320–344. https://doi.org/10.1556/2052.2022.00352 (дата звернення: 12.03.2025).
7. Artificial Intelligence Act. European Parliament : сайт. URL: https://surli.cc/qgiqpt (дата звернення: 12.03.2025).

Лукащук Ю. А.,
асистент кафедри автоматизованих систем управління,
доктор філософії
(Національний університет «Львівська політехніка»)
Цмоць У. О.,
старший науковий співробітник
відділу організації наукової діяльності
(Львівський державний університет внутрішніх справ)

ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ОБРОБКИ ДАНИХ У КОНТЕКСТІ СУЧАСНИХ ВОЄННИХ ДІЙ

Інтелектуальні системи обробки даних передбачають інтеграцію різноманітних методів і алгоритмів, зокрема нейронних мереж і технік машинного навчання, для вирішення складних завдань обробки та аналізу даних із використанням інтелектуальних підходів.

Машинне навчання – це напрям штучного інтелекту, який за допомогою певних алгоритмів дає змогу комп'ютерам самостійно вчитися на основі великих наборів даних. Від традиційних аналітичних алгоритмів його відрізняє гнучкість, що сприяє адаптації до різних сценаріїв. Машинне навчання – це ніби мозок комп'ютера, здатний покращувати свою продуктивність на основі попередніх результатів [1].

Нейронна мережа – це математична модель, що працює за принципом людського мозку. Вона навчається шляхом первинного опрацювання великого набору даних, не вимагаючи написання окремого коду під конкретне завдання. Нейромережі є одним зі способів машинного навчання і лежать в основі алгоритмів глибокого навчання. Вони здатні шукати закономірності в неструктурованих даних і вирішувати безліч завдань [2].

Поєднання нейронних мереж і машинного навчання має величезний потенціал для трансформації різних галузей і створення нових можливостей у багатьох сферах: від гуманітарної сфери до воєнної, від медицини до фінансів, від автономних систем до рекомендаційних платформ. Взаємозв'язок між нейронними мережами та машинним навчанням є дуже тісним, оскільки нейронні мережі є одними з найбільш потужних інструментів для реалізації алгоритмів машинного навчання.

Вплив інтелектуальних систем обробки даних на перебіг воєнних дій зростає, оскільки ці технології стають важливими інструментами для ефективного планування, ведення бойових операцій та аналізу даних. Вони змінюють способи прийняття рішень, а також допомагають у розвитку нових тактик і стратегій на полі бою.

Машинне навчання та нейронні мережі можуть використовуватися для швидкого аналізу величезних масивів даних, які отримуються з різних джерел: розвідки, супутників, безпілотних літальних апаратів (БПЛА), сенсорів на полі бою та інших технологій. Це забезпечить збір інформації в реальному часі про

розташування ворожих сил, зміну ситуації на фронті, переміщення техніки тощо. За допомогою алгоритмів машинного навчання можна виявляти патерни та тенденції, що допомагають командуванню краще планувати операції.

Нейронні мережі можуть бути використані для розробки інтелектуальних систем, які допомагають командувачам ухвалювати важливі рішення, використовуючи аналіз даних у реальному часі. Наприклад, алгоритми можуть оцінювати різні варіанти дій, оптимізувати маршрути для військових підрозділів, пропонувати найкращі стратегії з урахуванням різних змінних.

Машинне навчання і нейронні мережі активно використовуються в розробці автономних бойових систем – від БПЛА до наземних роботів. Такі системи можуть самостійно визначати цілі, координувати дії та навіть вести бойові операції з мінімальним втручанням людини. Наприклад, безпілотники, оснащені алгоритмами машинного навчання, можуть самостійно визначати ворожі цілі та здійснювати атаки.

Машинне навчання також допомагає в боротьбі з кіберзагрозами. Алгоритми можуть автоматично виявляти аномальні або підозрілі активності в комп'ютерних мережах, що допомагає захищати військові системи від кібератак. Крім того, машинне навчання використовується для боротьби з дезінформацією та пропагандою, аналізуючи потоки інформації та виявляючи фальшиві новини або маніпуляції.

Інші важливі застосування машинного навчання включають оптимізацію постачання та логістики. Алгоритми можуть допомогти визначити найефективніші маршрути для транспортування постачання, зброї, медикаментів тощо. Це дозволяє зменшити витрати та знизити ризики в умовах бойових дій.

Машинне навчання може бути використано для аналізу поведінки противника, його морального стану, інтерпретації реакцій на різні фактори, що дозволяє краще передбачити дії противника. Наприклад, алгоритми можуть аналізувати патерни комунікацій і поведінки в соціальних мережах, щоб визначити настрої серед військових або цивільного населення, а також оцінити ефективність психологічних операцій.

Машинне навчання також застосовується для розвитку технологій виявлення ворожих ракет, артилерійських обстрілів, мін та інших загроз. Алгоритми можуть допомогти швидко і точно оцінити загрозу, що дозволяє вчасно реагувати на небезпеку.

Отже, нейронні мережі та машинне навчання значно змінюють спосіб ведення воєнних дій, дозволяючи покращити точність, ефективність та швидкість прийняття рішень. Ці технології допомагають оптимізувати використання ресурсів, збільшують безпеку військових та дозволяють досягати стратегічних переваг, що може істотно змінити хід сучасних воєн.

Список використаних джерел:

1. Сухорукова Г. Як машинне навчання впливає на розвиток бізнесу. *Kyivstar Business Hub*. URL: https://hub.kyivstar.ua/articles/yak-mashinne-

navchannya-vplivaye-na-rozvitok-biznesuhttps://hub.kyivstar.ua/articles/yak-mashinne-navchannya-vplivaye-na-rozvitok-biznesu.

2. Гайборода М. Що таке нейронні мережі та де їх використовують? *Incrypted*. URL: https://incrypted.com/ua/shcho-take-nejromerezhi/.

Лук'янчук Ю. А.,
доцент кафедри комп'ютерних наук,
кандидат технічних наук, доцент
(Луцький національний технічний університет)
Земко А. М.,
професор кафедри права,
кандидат юридичних наук, професор,
(Луцький національний технічний університет)

ЕТИЧНЕ ТА БЕЗПЕЧНЕ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ДЕРЖАВНОМУ УПРАВЛІННІ: ПРИНЦИПИ, РЕКОМЕНДАЦІЇ, ПЕРСПЕКТИВИ

У сучасному світі алгоритми штучного інтелекту набули величезної популярності. Їх постійний розвиток змусив багатьох експертів вважати, що до 2030 року штучний інтелект перевершить сумарний інтелект усіх людей [1]. Однак цей швидкий прогрес несе з собою значні проблеми. Однією з найактуальніших проблем є захист персональних даних користувачів, оскільки все більше людей делегують рутинні завдання системам, які керуються штучним інтелектом. Поряд з цим, дилема довіри до передового ШІ залишається невирішеною, що викликає питання про те, як ці системи можна надійно інтегрувати в повсякденне життя [2].

Недавнє дослідження Anthropic [3] підкреслює потенційну вразливість систем штучного інтелекту, зокрема здатність маніпулювати ними для створення шкідливих реакцій за допомогою методу, відомого як джейлбрейк. Цей висновок підкреслює критичну потребу покращити безпеку та етичні рамки, що оточують технології ШІ. Вирішити ці проблеми можна за допомогою адаптації технології Proof-of-Stake (PoS). Хоча PoS традиційно використовується для перевірки криптовалютних транзакцій, його можна доопрацювати для керування процесами документації. Тим не менш, зберігається занепокоєння щодо довгострокових наслідків технології блокчейн [4], навіть якщо вона перепрофільована для таких програм.

Найближчі роки обіцяють новаторські технологічні досягнення, які об'єднають багато існуючих інструментів в уніфіковані системи [5]. У результаті захист персональних даних стає наріжним каменем досліджень і розробок. Важливо встановити та формалізувати етичну основу для використання штучного інтелекту, особливо в адміністративній та державній

сферах. Ці сектори часто обробляють величезні обсяги конфіденційних даних користувачів і найбільш вразливі до витоку інформації [6, 7].

Щоб усунути ці ризики, були розроблені та впроваджені спеціальні рекомендації щодо взаємодії державних службовців із інструментами ШІ. Ці положення офіційно затверджені та інтегровані в адміністративну практику відділу цифровізації Волинської обласної військової адміністрації в Україні [8]. Ця ініціатива є значним кроком до забезпечення етичного та безпечного використання ШІ на державній службі.

Ось основні рекомендації:

1. Інформування про використання ШІ.

Прозорість для громадян. Державний службовець зобов'язаний повідомляти громадян про те, що у процесі прийняття рішень використовуються інструменти штучного інтелекту. Це має бути зроблено чітко, зрозуміло і доступно.

Розкриття деталей роботи системи. Громадяни повинні знати, які саме функції виконує ШІ, наприклад, аналіз даних, оцінка ризиків або формування рекомендацій.

2. Перевірка достовірності інформації.

Критичний аналіз результатів. Штучний інтелект може надавати рекомендації або результати, які є неточними, упередженими або неповними. Державний службовець зобов'язаний перевіряти їхню достовірність за допомогою додаткових джерел чи експертної оцінки.

Захист від помилок. У разі виявлення помилкових даних або рішень службовець зобов'язаний негайно виправити ситуацію, щоб уникнути негативного впливу на громадян.

3. Захист персональних даних.

Мінімізація збору даних. Використання ШІ має обмежуватися лише тими даними, які необхідні для виконання конкретного завдання. Надмірний збір або зберігання даних забороняється.

Конфіденційність. Дані громадян мають бути захищені від несанкціонованого доступу, витоків або зловживань. Для цього використовуються сучасні технології шифрування та інші засоби кібербезпеки.

Відповідність законодавству. Усі операції з персональними даними повинні відповідати законам про захист даних, таким як GDPR або національні норми.

4. Прозорість процесів.

Розкриття принципів роботи. Службовець повинен знати, як працює система ШІ, які алгоритми використовуються, звідки отримуються дані та як формуються результати.

Маркування систем. Використовувані системи ШІ мають бути промарковані для інформування громадян про їх функціональні можливості, обмеження та потенційні ризики.

5. Уникнення дискримінації.

Перевірка на упередженість. Алгоритми ШІ повинні регулярно перевірятися на наявність дискримінаційних елементів, таких як упередженість за статтю, віком, національністю тощо.

Рівність доступу. ШІ не повинен створювати нерівні умови або дискримінувати окремі групи громадян.

6. Обмеження автоматизованих рішень.

Людський контроль. Автоматизовані рішення, які мають значний вплив на права громадян (наприклад, відмова у соціальних виплатах або доступі до послуг), повинні бути перевірені людиною.

Можливість апеляції. Громадяни повинні мати право на перегляд автоматизованого рішення, зокрема через подання апеляції до відповідного органу.

7. Етичність використання.

Відмова від маніпуляцій. Забороняється використання ШІ для маніпулювання громадською думкою, прихованого впливу на поведінку громадян або інших неетичних цілей.

Дотримання суспільних цінностей. ШІ має використовуватися для забезпечення справедливості, рівності та покращення якості життя громадян.

8. Відповідальність за результати.

Підзвітність. Службовець несе повну відповідальність за використання інструментів ШІ, навіть якщо рішення було прийнято автоматизованою системою.

Документування процесів. Усі дії, що включають використання ШІ, мають бути документовані для забезпечення прозорості та підзвітності.

9. Навчання та підвищення кваліфікації.

Оновлення знань. Державний службовець зобов’язаний регулярно проходити навчання щодо нових технологій ШІ, їх можливостей та обмежень.

Розуміння ризиків. Службовець повинен розуміти потенційні ризики використання ШІ, такі як упередженість алгоритмів, помилкові дані або ризики для прав людини.

10. Використання лише сертифікованих систем.

Довіра до інструментів. Використовуються лише ті системи ШІ, які пройшли сертифікацію та відповідають міжнародним стандартам безпеки, етики та прозорості.

Заборона ненадійних систем. Використання незареєстрованих, експериментальних або ненадійних інструментів ШІ заборонено.

Додаткові рекомендації.

Розробка інструкцій. Для кожного інструменту ШІ, який використовується, мають бути розроблені внутрішні інструкції щодо його безпечного та ефективного застосування.

Співпраця з експертами. У разі виникнення складнощів або сумнівів щодо роботи ШІ, службовець повинен консультуватися з технічними фахівцями або юристами.

Список використаних джерел:
1. https://x.com/elonmusk/status/1871083864111919134.
2. https://link.springer.com/article/10.1007/s10606-023-09465-8.
3. https://www.404media.co/apparently-this-is-how-you-jailbreak-ai/.
4. https://www.wsj.com/tech/cybersecurity/a-looming-threat-to-bitcoin-the-risk-of-a-quantum-hack-24637e29.
5. https://www.sciencedaily.com/releases/2024/12/241219152223.htm.
6. https://delo.ua/telecom/ukrayina-odna-z-golovnix-cilei-dlya-kiberatak-u-sviti-yak-zaxistitisya-rozpovidajemo-z-prikladami-412454/.
7. https://tech.liga.net/ua/other/article/yaki-krainy-provodiat-naibilshe-polityzovanykh-kiberatak-u-sviti-ukraina-uviishla-do-piatirky.
8. https://voladm.gov.ua/new/volinska-ova-ta-lntu-pidpisali-memorandum-pro-spivpracyu-u-sferi-shtuchnogo-intelektu/.

Ляшенко О. С.,
декан факультету комп'ютерної інженерії та управління,
кандидат технічних наук, доцент
(Харківський національний університет радіоелектроніки)
Ткачов В. М.,
доцент кафедри ЕОМ,
кандидат технічних наук, доцент
(Харківський національний університет радіоелектроніки)

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В СУДОВІЙ ПРАКТИЦІ З ВИКОРИСТАННЯМ ФЕДЕРАТИВНОГО НАВЧАННЯ

Судова система є однією з найважливіших інституцій сучасного суспільства, яка забезпечує правосуддя та захист прав громадян. Однак, зростання обсягу судових справ, складність правових норм та необхідність швидкого прийняття рішень вимагають впровадження інноваційних технологій.

Штучний інтелект (ШІ) та машинне навчання (МН) можуть стати інструментами для підтримки суддів у прийнятті рішень. Однією з перспективних технологій є федеративне навчання (ФН), яке дозволяє обробляти дані без їх централізації, зберігаючи конфіденційність. У цьому досліджені розглядаються принципи роботи систем підтримки прийняття рішень (СППР) у судовій практиці, їх переваги та недоліки, а також архітектура та функціонал федеративного навчання в таких системах.

В рамках дослідження було проведено аналіз існуючих систем з використанням ШІ. Система COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) – це система, яка використовується для оцінки ризику рецидивізму у злочинців. Хоча вона розроблена в США, її аналоги використовуються в Європі для підтримки суддів у прийнятті рішень щодо умовно-дострокового звільнення. COMPAS аналізує дані про злочинця, такі як вік, кримінальна історія та соціальний статус, і надає оцінку ризику. Однак

система критикується за можливість упередженості через використання історичних даних, які можуть містити дискримінаційні шаблони.

Наступна система Predictice – це французька платформа, яка використовує технології штучного інтелекту (ШІ) та машинного навчання (МН) для аналізу юридичних даних, зокрема судових рішень, нормативних актів та правових документів. Платформа націлена на підтримку юристів, юридичних фірм, корпорацій та суддів у прийнятті обґрунтованих рішень на основі даних. Вона дозволяє швидко знаходити релевантну судову практику, аналізувати тенденції та прогнозувати результати судових справ.

В Канаді використовують Kira Systems – це автоматизована програма юридичних консультацій, яка використовує штучний інтелект для аналізу юридичних документів і надання правової інформації та порад юристам. Kira Systems використовує алгоритми машинного навчання для виявлення шаблонів і тенденцій у юридичних документах, що дозволяє адвокатам приймати обґрунтовані стратегічні рішення.

Використання СППР у судовій практиці України має ґрунтуватися на чинному законодавстві, зокрема:

– дотримання принципів справедливого суду (Конституція України);

– забезпечення захисту персональних даних (Закон "Про захист персональних даних");

– використання електронних документів та підписів (Закон "Про електронні довірчі послуги");

– відповідність вимогам процесуального законодавства (ЦПК України, КПК України).

Для успішного впровадження СППР необхідно розробити чітку нормативну базу, яка б регулювала використання ШІ у судовій системі, забезпечуючи при цьому дотримання прав людини та принципів верховенства права.

Принципи роботи систем підтримки прийняття рішень у судовій практиці. СППР у судовій практиці виконують низку ключових функцій, які можна розділити на три основні категорії:

Аналіз та структурування правової інформації. СППР здатні обробляти великі обсяги правових текстів, включаючи нормативні акти, судові рішення, прецеденти та наукові джерела. Завдяки технологіям природного оброблення мови (NLP), системи можуть автоматично виокремлювати ключові правові поняття, визначати зв’язки між нормами та класифікувати інформацію за категоріями.

Прогнозування результатів судових справ. Використовуючи історичні дані про попередні судові рішення, СППР можуть прогнозувати ймовірні результати нових справ. Це досягається завдяки алгоритмам машинного навчання, які аналізують закономірності у судовій практиці.

Надання рекомендацій суддям. СППР можуть формувати рекомендації щодо застосування правових норм, вибору покарань або оцінки доказів. Ці

рекомендації базуються на аналізі великих масивів даних та врахуванні судової практики.

Переваги використання СППР.

Підвищення ефективності судової системи – СППР дозволяють суддям швидше аналізувати великі обсяги інформації, що особливо важливо в умовах перевантаженості судів. Це значно скорочує час на підготовку до судових засідань та прийняття рішень.

Зменшення суб'єктивності – використання алгоритмів ШІ дозволяє мінімізувати вплив суб'єктивних факторів, таких як особисті упередження судді чи емоційний стан. Це сприяє більш об'єктивному та справедливому правосуддю.

Доступність правової інформації – СППР полегшують доступ до актуальної правової інформації, включаючи зміни в законодавстві та судову практику. Це особливо важливо для суддів, які працюють у віддалених регіонах або мають обмежений доступ до правових баз даних.

Можливі недоліки СППР.

Ризик упередженості алгоритмів. Однією з головних проблем СППР є можливість упередженості алгоритмів, яка може виникати через використання історичних даних, що містять дискримінаційні шаблони.

Складність інтеграції з національним законодавством. Кожна країна має унікальну правову систему, тому СППР, розроблені для однієї юрисдикції, можуть бути неефективними в іншій. Для України це означає необхідність адаптації систем до місцевих правових норм та судової практики.

Етичні та правові питання. Використання ШІ у судовій практиці викликає низку етичних та правових питань. Наприклад, хто несе відповідальність за рішення, прийняті за допомогою СППР? Чи можна вважати такі рішення повністю об'єктивними? Ці питання потребують чіткого правового регулювання.

Федеративне навчання – це інноваційний підхід у машинному навчанні, який дозволяє навчати моделі на децентралізованих даних без необхідності їх передачі на центральний сервер. Це особливо важливо для судової системи, де конфіденційність даних є критичною вимогою.

Федеративне навчання базується на трьох ключових принципах:

Децентралізація даних. Дані залишаються на локальних пристроях або серверах (наприклад, у судах або правоохоронних органах), що дозволяє уникнути ризиків, пов'язаних з централізованим зберіганням.

Колективне навчання. Модель навчається на основі даних з різних джерел, але самі дані не передаються. Замість цього на сервер передаються лише оновлення параметрів моделі (наприклад, градієнти).

Конфіденційність. Використання методів захисту даних, таких як диференційна приватність та шифрування, забезпечує збереження конфіденційності.

Архітектура федеративного навчання складається з трьох основних компонентів:

Клієнти – це локальні пристрої або сервери, які зберігають дані та виконують локальне навчання моделі. У контексті судової системи це можуть бути окремі суди або правоохоронні органи.

Сервер координує процес навчання, збирає оновлення параметрів від клієнтів та агрегує їх для оновлення глобальної моделі. Він не зберігає дані, що забезпечує конфіденційність.

Для обміну даними між клієнтами та сервером використовується захищена мережа зв'язку, яка забезпечує передачу оновлень параметрів без витоку конфіденційної інформації.

Переваги федеративного навчання в СППР.

Конфіденційність даних. Дані залишаються на локальних серверах, що відповідає вимогам законодавства про захист персональних даних.

Масштабованість. ФН дозволяє підключати велику кількість клієнтів, що робить його ідеальним для судової системи, яка включає тисячі судів.

Адаптивність до локальних умов. Кожен суд може адаптувати модель до своєї практики, зберігаючи при цьому можливість узагальнення на рівні всієї системи.

Судові рішення є структурованими документами, які містять різноманітну інформацію, що може бути використана для аналізу та підтримки прийняття рішень. Федеративне навчання дозволяє аналізувати ці дані, зберігаючи конфіденційність інформації. Розглянемо, які саме частини судових рішень можна аналізувати за допомогою ФН. Судові рішення зазвичай містять такі основні частини:

– вступна частина (преамбула):дата та місце прийняття рішення, назва суду та склад суду, дані про сторін (позивач, відповідач, треті особи);

– описальна частина: виклад фактів справи, позиції сторін, докази, наведені сторонами;

– мотиваційна частина: правове обґрунтування рішення, посилання на нормативні акти та судову практику, аналіз доказів;

– резолютивна частина: висновки суду, прийняте рішення (наприклад, вирок, ухвала).

Кожна з цих частин містить цінну інформацію, яку можна аналізувати за допомогою ФН. Федеративне навчання дозволяє аналізувати різні частини судових рішень, зберігаючи конфіденційність даних. Це відкриває широкі можливості для підвищення ефективності судової системи, прогнозування результатів справ та виявлення упередженості. Для успішного впровадження необхідно розробити інфраструктуру, яка б забезпечувала ефективну комунікацію між судами та центральним сервером, а також враховувала особливості національної правової системи.

Манжай О. В.,
завідувач кафедри протидії кіберзлочинності
навчально-наукового інституту № 4,
кандидат юридичних наук, професор
(Харківський національний університет внутрішніх справ)

ШТУЧНИЙ ІНТЕЛЕКТ ТА КІБЕРБЕЗПЕКА: ЄВРОПЕЙСЬКИЙ ВИМІР

Розвиток систем штучного інтелекту дозволяє значно прискорити та спростити виконання багатьох завдань, у тому числі у сфері кібербезпеки. Як ніж, що може бути використаний людиною для вирішення побутових завдань або з метою зашкодити іншим, так і штучний інтелект може бути використаний для нападу або для захисту. У даній роботі виділимо 8 ключових напрямків застосування штучного інтелекту для вирішення завдань захисника та зловмисника.

Коли ми говоримо про використання штучного інтелекту для захисту, слід звернути увагу на такі напрямки як:

- проектування систем кібербезпеки для конкретних об'єктів та галузей, зокрема критичної інфраструктури;
- ідентифікація та оцінка ризиків як проміжного механізму побудови системи управління інформаційною безпекою;
- допомога у підборі персоналу у сфері кібербезпеки з метою уникнення загроз людського фактору та пропонування альтернативних варіантів дій;
- аналіз великих масивів даних, як от даних в користувацьких та серверних системах, в тому числі вивчення нехарактерних відхилень від типових структур та поведінкових профілів;
- прийняття швидких рішень в умовах обмеженого часу реагування, коли людський фактор не дозволяє вчасно відповісти на експлуатацію вразливостей порушником в інформаційних системах;
- прогнозування негативних подій для вироблення стратегій поведінки, у тому числі для шляхів подальшого розвитку інформаційних систем;
- аудит програмного забезпечення на предмет дотримання стандартів безпеки;
- допомога в розслідуванні інцидентів інформаційної безпеки, яка вже тепер може бути реалізована в частині аналізу зловмисного коду, здійснення пошуку за фрагментами даних, профілювання порушника, розпізнавання шкідливих інформаційних ресурсів тощо.

З боку нападника штучний інтелект потенційно може бути застосований для вирішення багатьох завдань, але серед таких завдань хотілося б виділити саме ті, які на теперішній час вже мають практичну реалізацію або виглядають найбільш небезпечно. Це:

- допомога у вчиненні атак соціальної інженерії (формування текстового та мультимедійного контенту, імперсонація, профілювання об'єкту атаки, допомога

у створенні нових технік нападу тощо). Нетиповим прикладом таких атак є створення легенди для інсайдерів з метою впровадження на об'єкт атаки;

- написання шкідливого програмного коду (хоча в багатьох популярних системах генеративного штучного інтелекту встановлюються відповідні обмеження, професійні зловмисники досить легко долають їх з використанням джейлбрейків);

- компрометація фізичних та юридичних осіб з метою впливу на безпеку об'єктів інформаційної діяльності. Причому, якщо раніше для роботи великих ботоферм залучали фізичних осіб, то сьогодні такі проекти багато в чому засновані на використанні ШІ-ботів;

- аналіз інформаційних систем на наявність вразливостей;

- відслідковування нових вразливостей та керування одночасними масовими атаками. Таке завдання система штучного інтелекту може реалізовувати значно швидше за людину, відслідковуючи в автоматичному режимі згадки у кіберпросторі, та одночасно застосовуючи нові знання до визначеного кола інформаційних систем-жертв;

- вплив на громадську думку з метою прийняття вигідних зловмиснику рішень у сфері кібербезпеки;

- створення та моделювання нових схем злочинної діяльності;

- управління фізичними атаками на об'єкти інформаційної діяльності. Наприклад, в контексті російської агресії проти України можна згадати атаки російських безпілотних літальних апаратів на об'єкти критичної інфраструктури.

Оскільки штучний інтелект є джерелом багатьох загроз, це очевидно вимагає контролю за його використанням. На теперішній час у Європейському Союзі прийнято Закон «Про штучний інтелект», який почне діяти з 2027 р. Стисло характеризуючи цей нормативний акт, слід зауважити, що він регулюватиме передусім системи з продуктивністю, яка перевищує 10^{25} FLOPs. Передбачаються санкції за порушення закону у вигляді штрафу до 35 млн євро або до 7 % річного обороту. Запроваджується введення спеціальних міток на окремих видах контенту, згенерованого штучним інтелектом.

Законом також у загальному випадку вводитимуться заборони систем:

– маніпулювання думками користувачів;
– передбачення поведінки (профайлінг);
– окремі системи розпізнавання облич та емоцій.

У контексті цих заборон передбачені окремі винятки для правоохоронних органів за наявності санкції суду та для деяких інших суб'єктів.

Чи достатньо цього закону для розв'язання проблеми регулювання розвитку систем штучного інтелекту в країнах Європейського союзу? Звичайно ні.

Головне не створити штучні перепони для розвитку штучного інтелекту, які в подальшому негативно вплинуть на загальну конкурентоспроможність Європейського союзу.

Окрім власне законодавчих рішень європейським політикам, потрібно звернути увагу на низку стратегічних підходів, які дозволять полегшити

функціонування штучного інтелекту для вирішення завдань кібербезпеки та отримати конкурентні переваги у цій сфері в майбутньому.

Перш за все, потрібно переглянути підходи до системи навчання у сфері кібербезпеки. Розвиток систем штучного інтелекту створює запит на відносно нових спеціалістів – архітекторів запитів для систем штучного інтелекту. Вказані спеціалісти також будуть затребувані і в секторі безпеки. Тут можна згадати популярну сьогодні професію програміста, коли затребуваними є спеціалісти, які володіють певними мовами програмування. Натомість, в недалекому майбутньому змагання у кодінгу зі штучним інтелектом буде виглядати малопродуктивним і спеціаліст зможе отримати конкурентну перевагу, якщо запропонує неочевидне рішення певної проблеми та зможе грамотно пояснити це рішення системі штучного інтелекту, яка в подальшому реалізує його в програмному коді. Звідси випливає важливість навчання спеціалістів у сфері кібербезпеки саме творчому мисленню, що можна досягти, наприклад, додаванням до освітньої програми предметів у сфері мистецтв. Точні науки дисциплінують особистість та виробляють системний підхід до структуризації даних, науки у сфері мистецтв впливатимуть на розвиток творчого підходу в роботі.

Для уникнення монополізації ринку варто прийняти стратегічні рішення з підтримки різноманітних (у тому числі безкоштовних) проектів у сфері штучного інтелекту. Як сьогодні у сфері програмного забезпечення бачимо конкуренцію пропрієтарних та безкоштовних чи умовнобезкоштовних операційних систем, так саме у майбутньому непогано було б бачити таку ж конкуренцію серед систем штучного інтелекту.

Це вирішуватиме ще одне завдання. У багатьох державних органах бюджет не завжди дозволяє придбати високоякісні дорогі рішення у сфері кібербезпеки, так само у багатьох організаціях не можуть дозволити застосування систем щтучного інтелекту з віддаленим керуванням, які, наприклад, працюють за принципом популярних сьогодні хмарних рішень. У даному контексті можна згадати об’єкти критичної інфраструктури або системи з чутливими персональними даними.

Зважаючи на це, відповідні підприємства, установи, організації будуть намагатися розгортати у себе ізольовані системи штучного інтелекту, які потребуватимуть встановлення відповідного обладнання. Тому в перспективі важливо сприяти створенню такого обладнання саме європейськими виробниками, так саме як і розробці недорогих локалізованих рішень у сфері штучного інтелекту. У даному контексті слід не забувати про квантові комп’ютери які на декілька порядків зможуть підвищити якість роботи систем штучного інтелекту, та водночас зменшити енергозатрати на такі продукти.

Підсумовуючи, варто зазначити що застосування штучного інтелекту для вирішення завдань кібербезпеки та і в цілому в різних сферах суспільного життя допоможе динамічному розвитку та бути стійким до змін, що конче потрібно для ефективного розвитку Євросоюзу в умовах глобальних викликів.

Мельник Я. Я.,
старший науковий співробітник
відділу дослідження проблем правотворчості
та адаптації законодавства України
до права ЄС Інституту правотворчості
та науково-правових експертиз,
доктор юридичних наук
(Національна академія наук України)

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ПРОДУКТ ПРАВОВОЇ РЕАЛЬНОСТІ

На сьогодні, проблема правової реальності опосередковується феноменом штучного інтелекту, що вказує на необхідність глибшого усвідомлення можливості генерації «права» завдяки ШІ. Відтак, очевидно, що за такого підходу протиставляється питання «ШІ» та «правової реальності», аби поставити більш чітко наступні проблеми: *(а)*на скільки ШІ може відображати правову реальність?; *(б)*наскільки правова реальність може бути генерована ШІ?

Насамперед, доцільно звернутися до понятійного апарату.

Не заглиблюючись у деталі феномену розуміння «ШІ», у вільній енциклопедії «Вікіпедія» наводиться його поняття. Зокрема, «…шту́чний інтеле́кт (ШІ, англ. *artificial intelligence, AI*) – розділ комп'ютерної лінгвістики й інформатики, який швидко розвивається і зосереджений на розробці інтелектуальних машин, здатних виконувати завдання, які зазвичай потребують людського інтелекту. Ці завдання можуть варіюватися від простих дій, як-от розпізнавання мови чи зображень, до більш складних завдань, як-от ігри чи керування автомобілем, а також генерування зображень та звуків…» [5].

Із цього поняття випливає такі характеристики ШІ як динамічність, робота із лінгвістичними королятами інтелектуальних машин, виконання завдань, які притаманні людському інтелекту. Очевидно, що питання права, а точніше генерування норм та правил оформлення юридичних документів, надання класифікацій та понять правовим феноменам, написання судових рішень тощо теж притаманне «логіко-інтелектуалдьним» алгоритмам «інтелектуальних машин».

За часів відсутності ШІ вітчизняний вчений філософ права С. І. Максимов, у своєму дисертаційному дослідженні, яке було присвячене правовій реальності зазначим, що «…в умовах трансформаційних процесів, пов'язаних з проведенням соціальної і правової реформи, важливого значення набуває філософське осмислення права, направлене на розкриття його гуманістичного смислу і глибинних основ, яке здійснюється філософією права – комплексною теоретичною дисципліною, що синтезує досягнення філософії і правознавства в дослідженні правової реальності як особливого світу права,

впорядкованої системи правових феноменів, що виражає власний смисл права в його співвіднесеності з людським буттям…» [2, с. 26]. Відтак, за такого підходу, вчений окреслив характеристику правової реальності у трансформаційних процесах та ролі у ньому права.

Варто мати на увазі, що у сучасній літературі зазначається, що «…концепція правової реальності («картина світу права») повинна задаватися образом права, репрезентованим в існуючій правосвідомості, Причому вважається, що вона складається із таких моментів: *(а)* теорій різного рівня, у тому числі філософського, а також правової ідеології, включаючи її втілення в чинній конструкції; *(б)* нормативних документів, що належать до різних рівнів правового регулювання; *(в)* повсякденного досвіду, що має справу з появами правового життя – правовідношеннями, практикою додержання прав людини, угод тощо і дозволяє будувати гіпотези, версії та відчувати, що виражене в них відбулося і відбувається насправді…» [6, с. 132]. Очевидно, що правове життя та його поява так і рівень певних правових документів вхоплюються не тільки правовою реальністю, але й спроможністю «інтелектуальних машин», які відчасти формують особливий контекст правової реальності. Проте версії «ШІ» вказують на не стійкість генерації знань права (правової інформації), власне як і проявляється проблема інфляції правових знань завдяки роботі ШІ (ефективній роботі «машини», «програм»).

В. Савенко досліджуючи правову реальність у контексті реалізації права доводить, що «…специфіка та неоднозначність питання правової реальності й онтологічна структура права є основоположним питанням філософії права. Водночас проблема аксіологічних підстав права перебуває в ціннісній сфері суспільного буття, що передбачає безперервний процес поетапного зростання рівня його об’єктивної цінності…» [3, с. 65]. Таким чином, стає очевидним і те, що правова реальність є універсальною та невід’ємною частиною з точки зору права для оцінки роботи ШІ та його результатів.

С. І. Максимов, досліджуючи проблеми правової реальності у одній із наукових статей віднаходить, що «…право з різним ступенем конкретності реалізується й у принципах справедливості (ідеї права), і в законі, і в конкретних правовідносинах, і в судовому рішенні. При цьому кожне правове рішення (тобто правильне, істинне) є успіхом не одного законодавця чи навіть судді. Це творче рішення, в якому беруть участь усі – і законодавець, і суддя, і представник виконавчої влади (чиновник), і звичайний громадянин. Всі учасники правової комунікації об'єднані єдиним правовим етносом, який виник на основі образу права, праворозуміння, що сформувались у цих соціо-культурних умовах. Правильне рішення є одночасно «підвищенням кваліфікації» всіх, хто бере у ньому участь, підвищенням правової культури. У цьому відношенні публікація найбільш вдалих рішень, за типом прецедентів в англо-американській системі, значною мірою підвищила б рівень правосвідомості і правової культури не тільки представників органів правосуддя, а й усіх громадян…» [1, с. 133].

Зрештою, здалось би додати тезу про те, що на «…зв'язок між правом і законом існував впродовж багатьох років та існує досі. …зараз потрібно чітко відокремити такі поняття, як правовий та неправовий закон і зрозуміти, коли закон втрачає право називатись неправовим, а отже, беззаконним…» [4, с. 30]. Що, як на нашу думку, ще раз підкреслює те, що зв'язок між ШІ та правовою реальністю якраз надає можливість виокремити «прийнятний» та «неприйнятний» результат в роботі ШІ та правовою реальністю.

Висновки. Штучний інтелект – технологічний продукт інтелектуальної діяльності людини, феномен якого можна співставний із інструментом констатації правової реальності у певній площині. Проблема появи цього феномену та його використання в правовому просторі, вказує на його тісний зв'язок із правовою реальністю.

Від того, наскільки вчені правники та практики зможуть навчитись використовувати ШІ як інструмент, від того залежить точність стану правової реальності та, відповідно, якісної роботи ШІ.

На сьогодні ШІ постає як продукт правової реальності, адже заснований не стільки на технологічних особливостях алгоритмів та їх результатів, скільки на демонструє здатність опрацьовувати правову інформацію повноцінно та ефективно завдяки алгоритмам та спроможності програми моніторингу та оцінки права.

На останок, ми не можемо сьогодні поки вважати правову реальність виключно продуктом ШІ, оскільки людський потенціал залучений та реалізується поза межами системи «інтелектуальних машин». Проте не виключення, що тенденції можуть свідчити про зворотне.

Список використаних джерел:

1. Максимов С. Структура правової реальності: феноменологічний аналіз. *Вісник Академії правових наук України.* 2002. № 2 (29). С. 125–133. URL.: https://dspace.nlu.edu.ua/jspui/bitstream/123456789/4674/1/Maksymov_125.pdfи (дата звернення: 10.03.2025).
2. Максимов С. І. Правова реальність як предмет філософського осмислення : автореф. дис. … д-ра юрид. наук : 12.00.12. Харків, 2002. 35 с.
3. Савенко В. Правова реальність як структурована площина реалізації права. *Філософські та методологічні проблеми права*. 2015. № 1-2 (9-10). С. 57–66. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/a68ce134-979d-4d66-b835-d138a9a52ab7/content (дата звернення: 10.03.2025).
4. Савенко В. Концептуалізація структури правової реальності та місця закону в ній. *Актуальні проблеми правознавства.* 2019. Вип. 2 (18). С. 26–32.
5. Штучний інтелект – це … значення слова. *Вільна енциклопедія «Вікіпекдія»*. URL: https://uk.wikipedia.org/wiki/%D0%A8%D1%82%D1%83%D1%87%D0%BD%D0%B8%D0%B9_%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82(дата звернення: 10.03.2025).
6. Філософія права : підручник / О. Г. Данилян, О. П. Дзьобань, С. І. Максімов та ін. ; за ред.О. Г. Даниляна. Харків : Право, 2017. 208 с.

Михайлицька К. С.,
курсантка навчально-наукового інституту
поліцейської діяльності
(Національна академія внутрішніх справ)
Чукаєва А. В.,
доцентка кафедри кримінології та
інформаційних технологій,
кандидатка юридичних наук, доцентка
(Національна академія внутрішніх справ)

ШТУЧНИЙ ІНТЕЛЕКТ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: МОЖЛИВОСТІ ТА ЗАГРОЗИ

У реаліях сьогодення Україна зіштовхнулася із новими викликами та загрозами, які суттєво вплинули на усі сфери нашого життя. Серед таких викликів та глобальних загроз специфічного значення набувають технології штучного інтелекту (далі – ШІ), цифрові технології та їх використання у злочинній діяльності.

Відповідно до стратегії розвитку штучного інтелекту в країні, ШІ розглядається як система інформаційних технологій, за допомогою якої можна вирішувати складні завдання з використанням наукових методів досліджень і алгоритмів обробки інформації. Ця система включає в себе створення та використання власних баз даних, моделей прийняття рішень, алгоритмів роботи з інформацією та визначення шляхів досягнення поставлених цілей [1].

Очевидно, що у сучасних умовах цифрова реальність сьогодення нині тісно пов’язана із появою нових форм злочинності - кіберзлочинів, інформаційного шахрайства, проведення кібероперацій рф, вчинення великої кількісті кібератак на підприємства та установи, в тому числі, й державні бази даних [2, с. 5].

Отож, на сьогодні штучний інтелект – це не просто технологічний тренд, модне слово чи тимчасове захоплення, це третя, комп’ютерна ера, заснована на інноваціях і передових технологіях. У сучасних умовах цифровізації злочинці нині досить активно використовують найсучаснісніші та найпередовіші технології. Значного поширення набувають вірусні кіберзагрози, біотероризм, кібершахрайство, сьогодні воєнні злочини вчиняються із використанням технологій ШІ [2, с. 13].

Розроблення та впровадження новітніх цифрових технологій та ШІ у правоохоронній діяльності щодо протидії злочинності може здійснюватися за такими напрямами:

1) інформаційно-аналітичне забезпечення правоохоронної діяльності;

2) інформаційно-довідкове забезпечення правоохоронної діяльності;

3) створення спеціалізованих інформаційних інтелектуальних систем оперативно-розшукового призначення;

4) формування та розвиток інтелектуальних систем відеоспостереження;

5) охорона об’єктів;

6) створення відомчих спеціалізованих інтелектуальних інформаційних систем;

7) впровадження інтелектуальних інформаційних освітніх систем;

8) запровадження інформаційно-телекомунікаційної системи досудового розслідування [3, с. 66].

Застосування технологій штучного інтелекту у практиці правоохоронної діяльності набуло неабиякої актуальності. Зокрема, це обумовлено необхідністю протистояти злочинцям, які дедалі частіше використовують найсучасніші інноваційні технології й досягнення четвертої промислової революції, зокрема: моделі блокчейну, дрони, робототехніку та ін. [4].

Основна увага зосереджується на інтеграції систем штучного інтелекту, які мають потенціал значно покращити діяльність правоохоронних органів. За рахунок використання можливостей ШІ для аналізу великих обсягів даних з’являється можливість швидше ідентифікувати кіберзагрози та виявляти приховані закономірності в злочинній активності. Автоматизація оперативних і слідчих дій за допомогою технологій машинного навчання і нейронних мереж сприяє підвищенню точності розслідувань та зменшенню навантаження на співробітників, що знижує помилки пов’язані з людським фактором [4].

У цьому контексті цифровізація не лише оптимізує правоохоронні процеси, але й вимагає переосмислення традиційних підходів до кібербезпеки, адаптації до нових загроз та розвитку правових і етичних засад використання технологій. Вона є необхідною умовою для забезпечення ефективної протидії кіберзлочинності у сучасному глобалізованому цифровому середовищі [5].

Важливим аспектами впровадження ключових технологічних інструментів є алгоритми навчання для розпізнавання шаблонів злочинної поведінки, засоби виявлення аномалій у кіберпросторі, системи моніторингу соціальних мереж і «темного вебу», а також платформи прогнозної аналітики. Ці алгоритми дозволяють виявляти повторювані дії, типові для злочинців, і прогнозувати їхню можливу подальшу активність [5].

Системи моніторингу соціальних мереж і «темного вебу» забезпечують можливість відстеження злочинної діяльності, виявлення контенту, пов’язаного із шахрайством, тероризмом, торгівлею забороненими товарами та іншими видами злочинів. Вони дозволяють збирати інформацію про загрози та визначати ключових учасників злочинних мереж. Платформи прогнозної аналітики застосовуються для аналізу історичних даних, створення моделей ризиків і прогнозування можливих сценаріїв розвитку злочинної діяльності. Це дозволяє правоохоронним органам розробляти активні стратегії, спрямовані на запобігання злочинам до їхнього здійснення [5].

Моніторинг «темних» веб-ресурсів є ще одним важливим напрямом. Використовується для автоматичного аналізу контенту у «темній мережі», що

дозволяє ідентифікувати нелегальну діяльність, пов’язану з продажем заборонених товарів, розповсюдженням шкідливого програмного забезпечення чи обміном конфіденційною інформацією [5].

Позитивним є, зокрема:

а) підвищення ефективності – ШІ може допомогти в зборі та аналізі великих обсягів даних, що забезпечує більш швидкий та точний аналіз інформації, скорочуючи час, необхідний для прийняття рішення;

б) мінімізація ризиків – застосування ШІ може допомогти у попередженні катастроф та мінімізації ризиків для військового персоналу, що забезпечує безпеку та захист держави;

в) забезпечення безпеки – ШІ може бути використаний для забезпечення безпеки країни, а саме, для забезпечення контролю над в’їздом та виїздом на кордоні, для виявлення та запобігання терористичним актам і злочинам;

г) автоматизація процесів – ШІ може допомогти в автоматизації багатьох процесів у сфері оборони, що зменшує ризик помилок та підвищує ефективність;

д) удосконалення озброєння – ШІ може бути використаний для розроблення та вдосконалення зброї, що забезпечує перевагу військам на полі бою.

ШІ може бути використаний для створення систем розвідки та контролю, які можуть виявляти загрози національній безпеці та вживати заходів для їх запобігання [6].

Цифрові технології докорінно трансформують правоохоронну діяльність, створюючи принципово нові можливості для комунікації, аналізу та протидії злочинності. Інтегровані інформаційні системи забезпечують миттєвий обмін даними між правоохоронними органами на національному та міжнародному рівнях, що підвищує ефективність реагування на транснаціональні злочини [6].

Алгоритми ШІ часто є «чорними ящиками» і зрозуміти, як саме ухвалюється те чи інше рішення, складно. Це створює ризики для довіри до систем. Вирішенням такої проблем є розробка прозорих та підзвітних алгоритмів, а також можливість перевірки їхньої роботи незалежними експертами. Сучасні автоматизовані системи моніторингу та глибокого аналізу даних дозволяють не просто фіксувати правопорушення, але й упереджено виявляти потенційні загрози, прогнозувати криміногенні тенденції та координувати міжвідомчі дії з небаченою раніше оперативністю та точністю [7].

При всьому потенціалі використання ШІ слід указати на зворотний його бік: як добро і зло, він може принести неоціненну користь, збільшивши та примноживши людські здібності, розширивши можливості для вирішення великої кількості суспільних проблем. Однак, при всій позитивності його потенціалу для суспільства, дедалі частіше технології ШІ виступають як криміногенний фактор, активно використовуються правопорушниками, тим самим продукуючи зростання рівня злочинності і призводячи до появи нових її

видів, створюючи при цьому реальну загрозу охоронюваним кримінальним законом інтересам окремих громадян, суспільству та державі [7].

Цифровізація правоохоронної діяльності виступає визначальним фактором забезпечення безпеки в динамічному глобальному середовищі. Для її успішної реалізації потрібно комплексно враховувати технологічні можливості, правові, етичні та соціальні контексти з метою гарантування справедливості, рівності та захисту прав людини [7].

Підсумовуючи, штучний інтелект є важливим інструментом у сфері забезпечення національної безпеки та обороноздатності нашої країни в сучасних умовах воєнного часу та у повоєнний період. За таких умов слід враховувати сучасні тенденції розвитку юридичної науки, пов'язанні із формуванням нових її напрямів, що дасть змогу суттєво підвищити роль та прикладне значення застосування інформаційних технологій в сучасних реаліях воєнного часу та глобальних загроз світовій цивілізації.

Список використаних джерел:

1. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р (станом на 29 груд. 2021 р.). URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р;
2. Сніґоля Матуєлене, Віктор Шевчук, Юргіта Балтрунене. Штучний інтелект в діяльності органів правопорядку та юстиції: вітчизняний та європейський досвід. DOI: 10.32353/khrife.4.2022.02.
3. Манжай О. В., Потильчак А. О. Особливості картографування злочинних проявів. *Право і безпека*. 2020. № 4 (79). С. 66–72.
4. Бугера О. І. Використання штучного інтелекту для запобігання злочинності. *Вчені записки ТНУ імені В. І. Вернадського. Серія : Юридичні науки*. 2021. № 6, т. 32 (71). С. 82–86.
5. Храпенко О. О., Меденцев А. М., Сперанський В. О. Цифровізація правоохоронної діяльності: використання штучного інтелекту для боротьби з кіберзлочинністю. *Юридичний науковий електронний журнал.* DOI: https://doi.org/10.32782/2524-0374/2024-11/117. С. 506-508.
6. Пацурія Н. Упровадження технологій штучного інтелекту в забезпечення національної безпеки та обороноздатності України: правові проблеми і перспективи військового періоду. Теорія і практика інтелектуальної власності, 3, 2023. С. 68–78.;
7. Хаустова В. Є., Решетняк О. І., Хаустов М. М., Зінченко В. А. Напрямки розвитку технологій штучного інтелекту в забезпеченні обороноздатності країни. *Бізнесінформ*. 2022. № 3. С. 24.

Мовчан А.В.,
професор кафедри оперативно-розшукової діяльності,
доктор юридичних наук, професор
(*Львівський державний університет внутрішніх справ)*

ПРОБЛЕМИ ПРОТИДІЇ РОЗПОВСЮДЖЕННЮ МАТЕРІАЛІВ СЕКСУАЛЬНОГО НАСИЛЬСТВА НАД ДІТЬМИ, СТВОРЕНИМИ З ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

Європол опублікував звіт «Оцінка технологій у правоохоронних органах: метод прийняття етичних рішень», у якому представлено структурований підхід до оцінки нових технологій із дотриманням основних прав і суспільної довіри. Метою звіту є забезпечення того, щоб впровадження та використання новітніх технологій відповідало ключовим європейським цінностям: прозорості, справедливості, конфіденційності та підзвітності. Документ пропонує систему, засновану на цінностях, що допомагає правоохоронним органам оцінювати етичні наслідки технологічних рішень. Вона включає: виявлення моральних проблем, оцінку ризиків і переваг, забезпечення законності та пропорційності використання технологій.

У звіті розглядаються різні правоохоронні технології, зокрема:

- технологія відеоаналітики – баланс між захистом конфіденційності та підвищенням громадської безпеки;
- штучний інтелект (ШІ) для оцінки ризиків у випадках гендерного насильства – поєднання потреби у прогнозуванні з принципами справедливості та прозорості;
- збирання даних з відкритих джерел – аналіз етичних і правових аспектів автоматизованих онлайн-розслідувань;
- чат-боти для запобігання сексуальному насильству над дітьми в Інтернеті – пошук балансу між проактивним втручанням і правом на конфіденційність;
- автоматизований аналіз великих і складних наборів даних – запобігання ризикам неконтрольованого використання інформації та забезпечення відповідального підходу до роботи з даними [1].

Боротьба з сексуальною експлуатацією дітей є одним із пріоритетів Європейського поліцейського офісу. З 2017 року Європол очолює ініціативу «Зупинити жорстоке поводження з дітьми – відстежити предмет», яка дозволяє громадянам допомагати у розслідуванні справ про сексуальне насильство над дітьми шляхом розпізнавання предметів на зображеннях. На сьогодні громадськість подала майже 28 тисяч повідомлень, завдяки чому 30 дітей врятовано, а 6 правопорушників притягнуто до відповідальності. На запит держав-членів ЄС та партнерських організацій Європол також координує робочу групу з ідентифікації жертв. Ця ініціатива дає змогу правоохоронним органам ефективно співпрацювати, локалізувати розслідування та виявляти постраждалих дітей. Зокрема, завдяки спільним зусиллям було врятовано дітей у Німеччині та Австралії.

Натомість, попри досягнення, сексуальна експлуатація дітей в Інтернеті залишається одним із найсерйозніших проявів кіберзлочинності в ЄС. Правоохоронні органи стикаються з постійним зростанням обсягу незаконного контенту, що робить цей напрям одним із ключових пріоритетів у боротьбі з кіберзлочинністю. Останнім часом самостійно створений дитячий матеріал сексуального характеру становить значну частку виявлених випадків експлуатації. Зловмисники використовують моделі штучного інтелекту, здатні

генерувати або змінювати зображення, для створення матеріалів сексуального насильства та вимагання. Такі технології стають все доступнішими, а результати їхньої роботи дедалі складніше відрізнити від реальних знімків, що ускладнює ідентифікацію та протидію. У відповідь на цю загрозу Європол координував міжнародну операцію «Камберленд», яка була спрямована на викриття злочинної групи, що займалася розповсюдженням зображень неповнолітніх, повністю згенерованих штучним інтелектом. Операція, проведена 26 лютого 2025 року під керівництвом правоохоронних органів Данії, охопила 19 країн і призвела до таких результатів: 273 встановлених підозрюваних, 25 арештів, 33 обшуки, 173 вилучені електронні пристрої [2].

Тож Європол продовжує боротьбу із цифровими загрозами, використовуючи новітні технології для виявлення та ліквідації злочинних схем, що ставлять під загрозу безпеку дітей. Головний підозрюваний, громадянин Данії, якого заарештували в листопаді 2024 року, керував онлайн-платформою, де поширював відеоматеріали, створені за допомогою ШІ. Після символічної онлайн-оплати користувачі з усього світу мали змогу отримати пароль для доступу до платформи та спостерігати, як знущаються над дітьми. У ході розслідування Європол та Спільна цільова група по боротьбі з кіберзлочинністю (J-CAT), створена Європолом, забезпечували оперативну координацію правоохоронних органів, залучених до справи. Експерти Європейського центру боротьби з кіберзлочинністю Європолу також сприяли обміну інформацією та надавали розвідувальні дані та оперативний аналіз національним слідчим.

Операція «Камберленд» була однією з перших справ, пов’язаних із матеріалами сексуального насильства над дітьми, створеними штучним інтелектом (CSAM), що робить її надзвичайно складною для слідчих, особливо через відсутність національного законодавства щодо цих злочинів. У зв’язку з цим країни-члени ЄС наразі обговорюють спільне положення, запропоноване Європейською комісією для вирішення цієї нової ситуації та захисту дітей від сексуального насильства та експлуатації.

Ці штучно створені зображення настільки легко створити, що їх можуть створювати особи зі злочинними намірами, навіть без значних технічних знань. Це сприяє зростанню поширеності матеріалів про сексуальне насильство над дітьми, і зі збільшенням обсягу слідчим стає дедалі складніше ідентифікувати правопорушників або жертв. Правоохоронним органам потрібно буде розробити нові методи та інструменти розслідування для вирішення цих нових проблем.

Це створює значні труднощі для правоохоронних органів у встановленні справжніх жертв. Навіть у випадках, коли контент повністю штучний і немає реальної жертви, як-от операція «Камберленд», CSAM, створений штучним інтелектом, усе одно сприяє об’єктивізації та сексуалізації дітей. Водночас операція «Камберленд» спрямована не лише на припинення злочинів, а й на активні кроки для запобігання подальшим інцидентам. Європол та його партнери найближчими днями запустять онлайн-кампанію, яка висвітлюватиме

наслідки використання штучного інтелекту в протиправних цілях і націлюватиметься на потенційних правопорушників там, де вони найбільш активні: в Інтернеті. У рамках кампанії використовуватимуться онлайн-повідомлення для охоплення покупців незаконного контенту, а також інші методи, такі як «стук і розмова», повідомлення в соціальних мережах і листи-попередження [2]. У правоохоронних органах метод «стук і розмова» – це метод розслідування, коли один або кілька поліцейських підходять до приватного помешкання, стукають у двері та запитують у власника згоди на обшук помешкання. Ця стратегія використовується, коли є підозра в злочинній діяльності, але немає достатніх доказів для отримання ордера на обшук [3].

Отже, операція «Камберленд» демонструє постійні скоординовані зусилля правоохоронних органів для комплексної боротьби з цією загрозою, від арешту злочинців до запобігання майбутнім злочинам шляхом навчання, стримування та надання підтримки тим, хто хоче шукати підтримки чи допомоги.

Список використаних джерел:

1. Europol publishes framework for ethical technology in law enforcement URL: https://www.europol.europa.eu/media-press/newsroom/news/europol-publishes-framework-for-ethical-technology-in-law-enforcement.
2. 25 arrested in global hit against AI-generated child sexual abuse material URL: https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material.
3. Холкомб Дж. (). Стук і розмова. *Бюлетень правоохоронних органів ФБР*. 2006. 75(8): 22–32. Отримано 15 листопада 2014 року.

Монастирський М. В.,
аспірант кафедри кримінального аналізу
та інформаційних технологій
(Одеський державний університет внутрішніх справ)

ПОДОЛАННЯ ПЕРЕШКОДИ У ВИЗНАЧЕННІ ПОНЯТТЯ ШТУЧНОГО ІНТЕЛЕКТУ

Штучний інтелект (далі – ШІ, або AI) розвивається стихійно по всьому світі. Деякі країни намагаються підкорити це техногенне явище. Міністерство цифрової трансформації України у лютому 2025 року заявило амбітну мету планового державного стратегічного розвитку ШІ в Україні: «Наша мета в цьому напрямі – до 2030 року увійти в топ-3 країни світу за рівнем інтеграції та впровадження AI-рішень» [1]. Сучасними лідерами і конкурентами за перше місце у світі є США та Китай [2; с. 17). За п’ять років там має бути Україна «у межах Стратегії цифрового розвитку інновацій WINWIN» [1]. Це візія Віцепрем’єр-міністр з інновацій, розвитку освіти, науки та технологій – Міністр цифрової трансформації України Михайла Федорова.

На шляху до цієї амбітної мети існують об’єктивні перешкоди. На нашу думку, головними серед них є дві: по-перше, ця війна; по-друге, невизначеність поняття ШІ. В умовах цієї війни стратегія партнерства win-win не є стратегією перемоги України над ворогом. Для України поступитися ворогу у застосуванні ШІ в ракетно-дроновій війні означатиме ризик болючої поразки, а не win-win. Ця війна є об’єктивною перешкодою, яку, на нашу думку, неможливо подолати державною стратегією розвитку ШІ WINWIN.

Невизначеність поняття ШІ є об’єктивною ознакою ШІ. В Україні поняття ШІ не є юридично нормованим: «На сьогодні немає нормативного визначення штучного інтелекту» [3, с. 92]. Поняття ШІ є невизначеним не тільки в Україні. Г. О. Андрощук, провівши ґрунтовне дослідження стратегій розвитку ШІ «у провідних країнах світу» [2, с. 15], зазначив: «Загальноприйнятого визначення поняття ШІ не існує» [2, с. 17]. І. О. Гелецька та М. М. Шовдра виконали порівняльний аналіз «міжнародного та національного законодавства щодо ШІ» [4, с. 13] і констатували: «Саме поняття «штучного інтелекту» на даний момент не має чітко визначеної дефініції» [4; с. 14]. Науковець О. А. Баранов теж відмітив «відсутність консенсусної дефініції терміну “штучний інтелект”» [5, с. 32].

Дійсно, якщо порівняти кілька визначень ШІ, які не можна не брати до уваги, то їх різниця очевидна. Наприклад, спеціальний закон Європейських Союзу про ШІ відносить це поняття до роду машинних систем: «”Система штучного інтелекту” означає машинну систему, яка розроблена для роботи з різними рівнями автономності та яка може демонструвати адаптивність після розгортання, і яка, для явних чи неявних цілей, робить висновок на основі вхідних даних, які вона отримує, як генерувати результати, такі як прогнози, вміст, рекомендації або рішення, які можуть впливати на фізичне чи віртуальне середовище» (автоматичний переклад Google. – М. М.) [6, ст. 3, п. 1].

Державна Концепція розвитку штучного інтелекту в Україні та концепція Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року, хоча і не мають юридичної сили закону, однаково є вітчизняними нормативно-правовими актами з ідентичним визначенням поняття ШІ: «Штучний інтелект - 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» [7–8].

Один з найпопулярніших ШІ у світі ChatGPT 4 на питання про ШІ відповів: «Штучний інтелект (ШІ) – це галузь комп'ютерних наук, що займається створенням систем і програм, здатних виконувати завдання, які зазвичай потребують людського інтелекту» (дата звернення: 11 березня 2025).

Три спроби визначення поняття ШІ і три різних родових поняття дефініції: наука комп’ютерних систем і програм – у ChatGPT 4; машинні системи – в законі ЄС; організована сукупність інформаційних технологій – в розпорядженнях КМУ.

Україна може обрати будь-яке з цих визначень або інших сотень існуючих і побудувати державну стратегію розвитку ШІ для військового застосування. Ця стратегія однаково буде невизначеною, тому що поняття ШІ є невизначеним об'єктивно. Невизначеність поняття ШІ перетворює будь-яку спробу планового державного стратегічного розвитку ШІ в Україні на помилку державного управління.

Зважаючи на таку особливість ШІ, слід обережно використовувати будь-які важелі державного управління на розвиток ШІ в Україні в умовах цієї війни. Визнаючи цю особливість ШІ, а також враховуючи той факт, що найпопулярніші у світі ШІ (ChatGPT 4, DeepSeek, Jasper AI etc.) це комп'ютерні програми (застосунки), то правильним визначенням поняття ШІ слід вважати умовне ототожнення ШІ та комп'ютерних програм. Відповідно, адекватна стратегія використання стихійного і невизначеного ШІ для перемоги над ворогом у цій війні це стратегія свободи використання *будь-яких* комп'ютерних програм для військових цілей в Україні. Багатство військових застосунків є середовищем розвитку неконтрольованого ШІ, а державний плановий розвиток ШІ в Україні не є можливим на даний час.

Список використаних джерел:

1. Мінцифра запускає WINWIN AI Center of Excellence / Міністерство цифрової трансформації України: офіційний веб-сайт. 2025. URL : https://thedigital.gov.ua/news/mintsifra-zapuskae-winwin-ai-center-of-excellence-tsentr-peredovogo-dosvidu-z-rozrobki-ta-integratsii-shi (дата звернення: 11.03.2025).
2. Андрощук Г. О. Політика і стратегія розвитку штучного інтелекту в країнах світу. *Наука, технології, інновації*. 2023. № 1 (25). С. 15–29. DOI: http://doi.org/10.35668/2520-6524-2023-1-03 (дата звернення 11.03.2025).
3. Марценко Н. Правовий режим штучного інтелекту в цивільному праві. *Актуальні проблеми правознавства*. 2019. № 4 (20). С. 91–98. URL: https://appj.wunu.edu.ua/index.php/appj/article/download/884/871 (дата звернення: 11.03.2025).
4. Гелецька І. О., Шовдра М. М. Визначення поняття «штучного інтелекту» та його місце у системі цивільного законодавства України. *Галицькі студії. Юридичні науки*. 2024. № 6. С. 13–19. DOI: https://doi.org/10.32782/galician_studies/law-2024-6-2 (дата звернення 11.03.2025).
5. Баранов О. А. Визначення терміну «штучний інтелект». *Інформація і право*. 2023. № 1 (44). С. 32–49. URL: http://il.ippi.org.ua/article/download/287537/281385 (дата звернення: 11.03.2025).
6. The AI Act. *EU: an official website.* 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата звернення 11.03.2025).
7. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#n8 (дата звернення: 11.03.2025).
8. Про схвалення Концепції Державної цільової технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року : Розпорядження Кабінету Міністрів України від 13.04.2023 № 320-р. URL: https://zakon.rada.gov.ua/laws/show/320-2024-%D1%80#Text (дата звернення: 11.03.2025).

Остіян Є. З.,

здобувачка вищої освіти першого
(бакалаврського) рівня
(ДВНЗ «Ужгородський національний університет»)
Пішта В. І.,
доцент кафедри адміністративного,
фінансового та інформаційного права,
доктор філософії
(ДВНЗ «Ужгородський національний університет»)

КОНЦЕПЦІЯ PRIVACY BY DESIGN У КОНТЕКСТІ ШТУЧНОГО ІНТЕЛЕКТУ ТА ТРАНСКОРДОННОГО ОБМІНУ ДАНИХ

На саміті зі штучного інтелекту в Парижі, що відбувся в лютому 2025 року, спостерігалися триваючі відмінності бачення світових лідерів щодо підходів врегулювання цієї сфери. Декларацію, що закликає до глобальної співпраці, США не підтримали.

За аналітичною запискою Організації економічного співробітництва та розвитку щодо покращення доступу до даних і обміну ними в епоху штучного інтелекту, на сьогодні більшість країн орієнтуються на власні національні системи захисту конфіденційності та даних для охорони індивідуальних прав, що стосуються доступу до даних і їх обміну [1]. До того ж загальновідомо, що США віддає перевагу розвитку інновацій, а не їх стримуванню, тоді як ЄС впроваджує жорстку регуляторну політику інформаційної безпеки та етики штучного інтелекту.

Варто зауважити, що жодна нація не зможе самостійно врегулювати штучний інтелект, адже він побудований на транскордонних потоках даних [2]. Саме за такої співпраці відбувається навчання та оптимізація алгоритмів, використовуються хмарні обчислення та впроваджуються міжнародні ініціативи альтруїзму даних для глобальних цілей розвитку, таких як науково-дослідна діяльність, екологія, медицина тощо.

При всіх наведених прикладах є важливим дотримання інформаційної безпеки та захисту персональних даних від несанкціонованого доступу. Пропонується визначити, які варіанти вирішення правових проблем пропонує концепція Privacy by Design (конфіденційність за задумом), та розглянути кореляцію Проекту Закону про захист персональних даних з європейським Загальним регламентом про захист даних в контексті транскордонної стратегії захисту даних.

По-перше, широка концепція Privacy by Design, що означає конфіденційність, яка вбудована в ядро системи на початковому етапі проектування – не як додаткова функція [3], містить в собі реальні правові механізми для імплементації в законодавство. Тобто концепція не є окремим регулятором транскордонних передач даних і натомість встановлює правові рамки та принципи безпеки. Насамперед слід звернутися до європейського Загального регламенту про захист даних. Privacy by Design, що закріплена в ст.

25, в цьому контексті може бути реалізована через такі правові інструменти Регламенту, як стандартні договірні положення (ст. 46(2)(c)), зобов'язальні корпоративні правила (ст. 47), рішення про адекватність (ст. 45) та оцінка впливу передачі даних (ст. 35).

Коли дані передаються до країни з нижчим рівнем захисту, ці засоби виступають гарантіями безпеки при екстериторіальній дії права ЄС, якщо сторона відступає від положень п. 1 ст. 2 Додаткового протоколу Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних про адекватний рівень захисту даних.

По-друге, технічні та організаційні підходи розглядаються країнами як другорядні порівняно з правовими гарантіями. Наприклад, до цих підходів належать Технології підвищення конфіденційності (PET) та Довірені посередники передачі даних (TDI), що наразі активно вивчаються [1].

У січні 2025 року ЄС закріпив своє бачення щодо першого підходу у вигляді Рекомендацій щодо псевдонімізації, де пояснюється застосування такого методу для додаткового захисту даних при неефективності договірних інструментів [4]. Щодо другого підходу – країни-члени ЄС вже практикують послуги Довірених посередників передачі даних.

По-третє, в листопаді 2024 року прийнятий за основу Проект Закону про захист персональних даних, який наближує Україну до європейських стандартів. Відтак, у найближчому майбутньому в Україні буде закріплено Privacy by Design на законодавчому рівні. Однак визначення стандартних договірних положень в Проекті є нечітким, тому задля уникнення правової невизначеності та підвищення рівня гарантій є доречним уточнити положення в цій частині.

Окрім того, для України додатковою перспективою є врахування Рекомендації Організації економічного співробітництва та розвитку щодо покращення доступу до даних та обміну. Вона встановлює кроки покращення умов для транскордонного доступу до даних і довірчого обміну ними.

Таким чином, дані є ключовим аспектом для розвитку штучного інтелекту, як у наукових дослідженнях та розробках, так і в його масовому впровадженні серед неспеціалістів та компаній. Затримка у доступі до даних є критичною проблемою, яку Європа повинна вирішити для забезпечення своєї стратегічної автономії та технологічного суверенітету у сфері штучного інтелекту [5].

Для України залишається актуальним питання приведення українського законодавства у відповідність з європейським. Концепція Privacy by Design повинна працювати на усіх прошарках: від законодавчого – до технічного та організаційного.

Країнам треба усвідомити існуючий брак довіри та суперечливі інтереси різних зацікавлених сторін [1]. Необхідні стійкі міжнародні стандарти захисту для транскордонного обміну на благо суспільства. Країни повинні виводити національне законодавство про захист персональних даних на найвищий рівень та сприяти викоріненню дефіциту даних через безпечну міжнародну співпрацю.

У сучасних умовах глобалізації даних концепція Privacy by Design відіграє ключову роль у процесі забезпечення конфіденційності та безпеки під час використання штучного інтелекту, особливо в контексті транскордонного обміну інформацією. Сьогодні залишається багато викликів щодо імплементації положень Загального регламенту про захист даних. Натомість Україна, прагнучи гармонізувати своє законодавство відповідно до європейських стандартів, має належним чином визначити правові механізми захисту персональних даних, а також впроваджувати сучасні технологічні рішення. Саме завдяки міжнародному співробітництву та чіткій регуляції можна досягнути безпечного використання штучного інтелекту та ефективного обміну даними.

Список використаних джерел:

1. Enhancing Access to and Sharing of Data in the Age of Artificial Intelligence. OECD Policy Briefs. 2025. No. 13. DOI https://doi.org/10.1787/23a70dca-en (дата звернення: 03.03.2025)
2. Sray Agarwal. AI Ethics in Cross Border Commerce. UNECE. 2020. URL: https://unece.org/sites/default/files/datastore/fileadmin/DAM/cefact/cf_forums/2020_October_Geneva/PPTs/AI_SAgarwal-AI-EthicsCrossBorderCommerce.pdf (дата звернення: 03.03.2025).
3. Mishova A. AI Regulations and the Future of Global Data Protection. GDPRLocal. 2025. URL: https://gdprlocal.com/ai-regulations-and-the-future-of-global-data-protection/ (дата звернення: 03.03.2025).
4. Guidelines 01/2025 on Pseudonymisation. European Data Protection Board. 2025. URL: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en (дата звернення: 03.03.2025).
5. Schuman R. Artificial intelligence: Europe needs to start dreaming again. *Robert Schuman Foundation*. 2025. URL: https://www.robert-schuman.eu/en/european-issues/728-artificial-intelligence-europe-needs-to-start-dreaming-again (дата звернення: 03.03.2025).

Пасевич М. О.,
здобувачка третього (освітньо-наукового)
рівня вищої освіти
(Кременецька обласна гуманітарно-педагогічна академія ім. Тараса Шевченка)

ШТУЧНИЙ ІНТЕЛЕКТ У НАВЧАННІ: ПОМІЧНИК ЧИ ЗАМІНА ВИКЛАДАЧА?

Сучасний розвиток технологій суттєво змінює освітній процес, що вимагає адаптації підходів до викладання та навчання. Однією з найважливіших тенденцій є впровадження генеративного штучного інтелекту (ШІ), який здатний виконувати рутинні завдання, персоналізувати навчання та допомагати в організації освітнього процесу.

Україна, як і багато інших країн світу, активно розвиває напрям штучного інтелекту в освіті, що підтверджується ухваленою у 2020 році «Концепцією розвитку штучного інтелекту в Україні», яка визначає освіту однією з ключових

сфер впровадження цієї технології [1]. Штучний інтелект (ШІ) стає все більш важливим елементом в освітньому процесі, пропонуючи нові можливості для покращення навчання та викладання. У цьому контексті постає питання: чи може генеративний ШІ замінити викладача, або ж він є лише допоміжним інструментом [2]?

Згідно з міркуваннями О. Марків, штучний інтелект перетворюється на потужний інструмент генерації нових знань, відкриваючи нові можливості для викладачів та студентів [3]. В. Власенко та О. Ігнатюк вважають, що використання ШІ може значно підвищити ефективність викладання, автоматизуючи процеси оцінювання, створення персоналізованих навчальних матеріалів та адаптації контенту до рівня знань студентів [4]. В. Магеровська, Б. Філь, К. Шостак вважають, що впровадження елементів штучного інтелекту має відбуватися поступово, що дозволить у разі технічних збоїв повернутися до традиційних методів навчання. Важливим аспектом є попередня підготовка та додаткове навчання як викладачів, так і здобувачів освіти, щоб уникнути непорозумінь щодо роботи системи, а також запобігти виникненню дискомфорту або сприйняття ШІ як заміни викладача [5]. О. Ялишева розглядає штучний інтелект, інструмент, що може допомогти проводити більш персоналізоване навчання. ШІ можна використати для адаптації навчального контенту і методів навчання до індивідуальних потреб учнів [6]. Водночас зростає занепокоєння щодо можливого витіснення викладачів технологічними інструментами.

Метою дослідження є аналіз ефективності генеративного штучного інтелекту в освітньому процесі.

У сучасній системі освіти викладачі закладів вищої освіти постають перед новими викликами, зумовленими швидкою еволюцією технологій та динамічними змінами на ринку праці, що вимагає від них оновлення підходів до навчання та вдосконалення методик викладання.

Замість побоювань викладачам варто навчитися ефективно застосовувати ШІ у навчальному процесі. Ця технологія здатна автоматизувати рутинні завдання та розширити можливості освітнього середовища. Зокрема, ШІ може формувати інтелектуальні підказки для здобувачів освіти, підбирати додаткові навчальні ресурси та надавати відповіді на запити в режимі реального часу. Це значно полегшує організацію дистанційного навчання, дозволяючи викладачеві зосередитися на більш складних аспектах навчального процесу, а не лише на створенні алгоритмів виконання завдань.

Водночас роль викладача трансформується: він стає не лише передавачем знань, а й інтегратором ШІ у навчання. Його завдання – забезпечувати емоційну підтримку, мотивувати студентів до розвитку критичного мислення та усвідомленого використання ШІ. Крім того, викладач відіграє ключову роль в адаптації персоналізованих навчальних програм, створених за допомогою штучного інтелекту, відповідно до індивідуальних потреб студентів.

Незважаючи на стрімкий розвиток ШІ, роль викладача залишається незамінною – він виступає наставником, модератором навчального процесу та

партнером у використанні новітніх технологій для підвищення ефективності освіти.

Автоматизуючи рутинні процеси, штучний інтелект дозволяє викладачам зосередитися на творчих аспектах навчання, розвитку взаємодії зі студентами та підвищенні їхньої мотивації до освіти [7]. ШІ можна використовувати для автоматизації завдань, які в даний час виконують вчителі, наприклад, перевірку завдань та надання відгуків. спільно з педагогами, ШІ можна частково використовувати для розробки навчальних матеріалів, які адаптовані до індивідуальних потреб учнів. Це може допомогти учням краще зрозуміти матеріал і досягти своїх навчальних цілей швидше. ШІ можна використовувати для створення гнучких можливостей навчання, які дозволяють учням навчатися в будь-який час і в будь-якому місці. Це може включати онлайн-навчання, дистанційне навчання та навчання за допомогою мобільних пристроїв. ШІ можна використовувати для створення персоналізованих навчальних планів для кожного учня, заснованих на їхніх індивідуальних потребах [8]. ШІ дозволяє адаптувати інформацію, створювати такі індивідуальні простори. Також це про доступність для людей з особливими освітніми потребами [9].

Схоже, освіта стане такою, де штучний інтелект працюватиме разом із педагогами-людьми для збагачення та персоналізованого досвіду навчання як для дітей, так і для педагогів. Більш вірогідний сценарій вимагає співпраці, де штучний інтелект виступає як допоміжний педагог поряд із педагогами-людьми, звільняючи вчителів від повсякденних рутинних завдань, щоб зосередити більше часу на персоналізованій взаємодії, наставницьких стосунках і вихованні креативності серед своїх учнів [10].

ШІ в школі – це спокуса для учнів послуговуватись ChatGPT чи Bard, ігноруючи ідею написати твір або виконати завдання самостійно. Виявити справжнього виконавця допоможуть сервіси перевірки тексту, до яких уже вбудовано інструменти пошуку слідів штучного інтелекту в роботі [11].

Для ефективної інтеграції ШІ в освіту рекомендовано:

- використовувати генеративний ШІІ як допоміжний інструмент, а не повноцінну заміну викладачів;
- впроваджувати етичні принципи використання ші для забезпечення академічної доброчесності;
- розробити навчальні програми для викладачів і студентів, які допоможуть ефективно працювати з ШІ;
- поєднувати технологічні інструменти з традиційними методами навчання для досягнення найкращих результатів.

ШІ в освіті слід розглядати як засіб підвищення ефективності викладання, а не як альтернативу викладачам. Подальші дослідження мають бути спрямовані на розробку стратегій використання ШІ у навчальних закладах з урахуванням його сильних і слабких сторін.

Встановлення гармонійного балансу між технологічним прогресом і незамінним людським дотиком залишається ключовим для розкриття повного спектру переваг, які ШІ може принести в освіту. Коли ми йдемо цим шляхом,

синергія між технологіями та людським досвідом стає каталізатором справді збагаченої та цілісної освітньої подорожі. ШІ в освіті слід розглядати як інструмент, що доповнює, а не замінює викладача. Використання ШІ може значно покращити навчальний процес, але людські якості викладачів залишаються незамінними для забезпечення всебічного розвитку студентів

Список використаних джерел:

1. Елькін О. Віртуальне вчительство: чи замінить штучний інтелект людей у школах? : *Нова Українська школа.* URL: https://nus.org.ua/2023/02/15/virtualne-vchytelstvo-chy-zaminyt-shtuchnyj-intelekt-lyudej-u-shkolah/ (дата звернення: 22.02.2025).
2. Стівенс К. Чи може штучний інтелект замінити викладачів коледжу? *Reporter*. URL: https://uk.eureporter.co/internet-2/artificial-intelligence/2024/01/22/can-artificial-intelligence-replace-college-teachers/ (дата звернення: 22.02.2025).
3. Марків О. Т., Зарівна О. Т., Марків І. П. Актуалізація ролі викладача в освітньому процесі в епоху штучного інтелекту. *Тенденції забезпечення якості освіти* : матер. II Міжнар. наук.-практ. конф. URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/45823/-Aktualizatsiia%20roli%20vykladacha.pdf?sequence=1 (дата звернення: 20.02.2025).
4. Власенко В. О., Ігнатюк О. А. Професійно важливі якості викладача вищої школи в епоху штучного інтелекту: нові виклики та шляхи розвитку. *Наукова школа академіка Івана Зязюна у працях його соратників та учнів* 2024. С. 156-157. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/0f042c39-df13-415f-af16-c1d85465671f/content (дата звернення: 20.02.2025).
5. Магеровська Т. В., Філь Б. М., Шостак К. Аналіз способів впровадження штучного інтелекту в освітний процес. *Інформаційні технології в освіті та практиці* : матеріали Всеукраїнської науковопрактичної конференції. Львів, 17 грудня 2021. ЛьвДУВС, 2021. С. 57-59. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4309/1/17_12_2021.pdf#page=57 (дата звернення: 20.02.2025).
6. Ялишева О. Вплив штучного інтелекту на роль вчителя. *Штучний інтелект у науці та освіті (AISE 2024). Artificial intelligence in science and education:* збірник матеріалів міжнародної наукової конференції. Київ, 1-2 березня 2024 р. Київ : УкрІНТЕІ, 2024. С. 314–317. URL: https://lib.iitta.gov.ua/id/eprint/740812/1/mat-konf-schi_2024.pdf.crdownload#page=314 (дата звернення: 20.02.2025).
7. ШІ для вчителя – секретар чи конкурент: прогнози експертів. *Освіторія.* URL: https://osvitoria.media/experience/shi-dlya-vchytelya-sekretar-chy-konkurent-prognozy-ekspertiv/ (дата звернення: 22.02.2025).
8. Штучний інтелект (ШІ) – конкурент чи помічник вчителя? *Tech Startup School*. URL: https://tsus.org/node/399 (дата звернення: 22.02.2025).
9. Штучний інтелект & вчитель: хто кого? *Говоримо Pro освіту*. URL: https://hovorymo.live/at-school/pro-teachers/stucnii-intelekt-vcitel-xto-kogo/ (дата звернення: 22.02.2025)
10. Стівенс К. Чи може штучний інтелект замінити викладачів коледжу? : *Reporter*. URL: https://uk.eureporter.co/internet-2/artificial-intelligence/2024/01/22/can-artificial-intelligence-replace-college-teachers/ (дата звернення: 22.02.2025)
11. Штучний інтелект & вчитель: хто кого? *Говоримо Pro освіту*. URL: https://hovorymo.live/at-school/pro-teachers/stucnii-intelekt-vcitel-xto-kogo/ (дата звернення: 22.02.2025).

Письменний О.,

аспірант кафедри адміністративного права і процесу
(Дніпровський державний університет внутрішніх справ)

ЗАБЕЗПЕЧЕННЯ КІБЕЗБЕЗПЕКИ В ЦИФРОВОМУ ПРОСТОРІ В УМОВАХ ВОЄННОГО СТАНУ

Держава створює різного роду реєстри та бази даних з метою забезпечення ефективного функціонування різних сфер суспільного життя. Ці реєстри та бази даних є важливим інструментом для збору, зберігання та обробки інформації, яка потрібна для прийняття рішень, контролю та надання різного роду послуг громадянам. Однією з головних причин створення реєстрів та баз даних є забезпечення ефективного контролю над різними процесами всередині державного механізму. Наприклад, державні реєстри щодо населення дозволяють вести облік громадян, встановлювати їхні права та обов'язки, а також забезпечувати доступ до соціальних послуг та допомоги. Такі реєстри також допомагають уникнути подвійного обліку, шахрайства та незаконного заволодіння майном громадян.

Крім того, державні реєстри та бази даних допомагають забезпечити ефективне функціонування системи охорони здоров'я, освіти, соціального захисту та інших галузей. Завдяки цим реєстрам можна вести облік медичних даних, освітніх досягнень, соціальних пільг та інших важливих показників, що дозволяє забезпечити якісне надання послуг та аналізувати стан суспільства для прийняття ефективних рішень. Також реєстри та бази даних є важливим інструментом для забезпечення взаємодії між різними державними органами та організаціями. Вони дозволяють обмінюватися інформацією, координувати дії та виконувати різні адміністративні процедури швидко та ефективно. Таким чином, створення реєстрів та баз даних є важливим елементом державного управління, який допомагає забезпечити ефективну роботу державних структур, контроль за процесами та надання послуг громадянам.

На жаль, не можна надати точну кількість реєстрів та баз даних, що існують в Україні, оскільки їхня кількість постійно змінюється і залежить від різних факторів, таких як законодавчі зміни, реформи та потреби державних органів.

Зі збільшенням кількості реєстрів та дій які відбуваються у віртуальному полі, без попереднього паперового оформлення заяви чи клопотання, щодо запитуваної послуги паралельно збільшується і кількість незаконних дій. Дані дії здійснюються або умисно особами, що мають сертифікований доступ до вказаних баз даних, або не навмисно, особами які за рахунок неуважності або необізнаності порушили правила ведення відповідного реєстру, і ці дії кваліфікуються за ст.362 Кримінального кодексу України, як злочин.

Так на прикладі Державного реєстру речових прав на нерухоме майно маємо наступну структуру: є спеціальних Закон України № 1952-IV «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень», забезпечення якого відповідає Порядку державної реєстрації речових прав на

нерухоме майно та їх обтяжень, затверджений Постановою Кабінету Міністрів України № 1127 від 25.12.2015. З метою контролю діяльності державних реєстраторів було утворено Колегію з розгляду скарг у сфері державної реєстрації, діяльність якої регламентується Положенням про Колегії з розгляду скарг на рішення, дії або бездіяльність державного реєстратора, суб'єктів державної реєстрації, територіальних органів Міністерства юстиції, затвердженим Наказом Міністерства юстиції України від 09.01.2020 № 71/5.

Зупинимось більш детально на організації захисту даних, що містяться у реєстрах. Відповідно до Наказу Міністерства внутрішніх справ України від 30.10.2012 № 988 «Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС» основним завданням Управління є: участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також іншим кримінальним правопорушенням, учиненим з їх використанням [6].

Проаналізувавши опубліковані звіти про результати роботи Департаменту кіберполіції Національної поліції України за 2022 та 2023 роки, хочемо навести наступні статистичні дані та окреслити виявлену динаміку.

У 2022 році припинено діяльність 23 організованих груп і злочинних організацій, що діяли в кіберпросторі. До складу зазначених угруповань входив 81 учасник (23 – організаторів та 51 – активний виконавець), якими вчинено 269 кримінальних правопорушень (у тому числі 240 тяжких та особливо тяжких), з яких: 178 – шахрайств, 59 – у сфері використання електронно-обчислювальних машин, 12 – у сфері обігу наркотичних засобів, 3 – за ст. 255 (Створення, керівництво злочинною спільнотою, а також участь у ній, Кримінального кодексу України), 2 – крадіжки, 3 злочини – у сфері господарської діяльності (легалізації (відмиванню) майна, одержаних злочинним шляхом), 1 – привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем. Також, у 2022 році кіберполіцейськими здійснювалось супроводження 5 тис. кримінальних правопорушень, виявлено 2,3 тис. кіберзлочинів, повідомлено про підозру 1 тис. особам за вчинення 2,3 тис. кримінальних правопорушень. Затримано понад 100 кіберзлочинців, задокументовано та притягнуто до відповідальності 30 педофілів та 10 хакерів. До суду з обвинувальними актами скеровано 2,7 тис. кримінальних правоваджень за обвинуваченням 840 осіб [4].

У 2023 році скеровано до суду кримінальні провадження щодо протиправної діяльності 42 організованих груп і злочинних організацій, що діяли в кіберпросторі. До складу зазначених угруповань входив 191 учасник, якими вчинено 731 кримінальне правопорушення (у тому числі 547 тяжких та особливо тяжких), з яких: 438 – шахрайств, 20 – крадіжок, 12 – за ст. 255 ККУ (Створення, керівництво злочинною спільнотою, а також участь у ній), 11 –

сутенерств, 3 – привласнення, розтрата майна, 46 – у сфері господарської діяльності, 33 – у сфері використання електронно-обчислювальних машин, 14 - у сфері службової діяльності, 7 – у сфері обігу наркотичних засобів, 147 – інші. Також у 2023 році кіберполіцейськими здійснювалось супроводження понад 6,4 тис. кримінальних проваджень, виявлено 3,6 тис. кіберзлочинів, повідомлено про підозру 1,7 тис. особам за вчинення 3,7 тис. кримінальних проваджень. До суду з обвинувальними актами скеровано 4 тис. кримінальних праваджень за обвинуваченням 1,3 тис. осіб [5].

Логічним є факт, що з розвитком комп'ютерних технологій кількість злочинів стає дедалі більша. Навіть стовідсоткове розкриття злочинів не зменшить їх кількість, бо статистика розкриття злочинів не є протидією до їх скоєння.

Завданням держави є забезпечити безпеку громадян, з цією задачею держава частіше не справляється ніж навпаки, оскільки піднімаючи питання кібербезпеки у кожного є приклад, як ошукують людей шляхом розсилки фішингових листів. Так наприклад, щодня від нотаріальної палати України повідомлення про фішингову розсилку на офіційні електронні поштові скриньки нотаріусів листів зі шкідливими програмним вкладенням, метою якого є отримання несанкціонованого доступи до реєстрів, що перебувають у користуванні нотаріусів. Трохи дивним є рекомендація для нотаріусів не відкривати дивні листи, або відкривати їх спочатку на мобільному пристрої, або не переглядати пошту на комп'ютерах на яких встановлено реєстри. Тобто замість вирішення питання захисту реєстрів фаєрволом від фішинга, нотаріусам рекомендують просто придбати окремий комп'ютер для реєстрів. Тобто вирішити саму проблему не можуть, а лише радять ситуативні методи, якими нотаріус сам себе повинен захищати від дій правопорушників, хоча в Законі України «Про нотаріат» такі функції у нотаріусів відсутні.

З огляду на проблеми сучасності в Україні на кожний новий електронний реєстр чи державну базу даних створюється свій керівний чи контролюючий орган, що ніяк не покращує кримінальний простір в цифровому полі, тому неминучим стає утворення на базі Міністерства цифрової трансформації багаторівневої Національної служби цифрового простору, з аналітичною, контролюючою та правозахисною метою, щоб усім цифровим простором держави опікувався один орган. Створення одного працюючого органу, який займатиметься вирішенням різних питань, може мати декілька переваг для громадян.

Саме тому, одним з можливих способів захисту інформації у державних реєстрах є впровадження сучасних технологій криптографічного захисту даних. Це включає використання шифрування для збереження конфіденційності даних та електронних підписів для забезпечення цілісності та автентичності інформації. Криптографічні алгоритми можуть ускладнити доступ до даних для несанкціонованих осіб та зменшити ризик незаконних змін.

Крім того, важливо забезпечити фізичну безпеку серверів та баз даних, де зберігається інформація реєстру. Це може включати використання контрольно-

пропускних систем, відеоспостереження та обмеження доступу до приміщень з серверами лише для авторизованих осіб.

Також необхідно регулярно проводити аудит безпеки, щоб виявляти потенційні вразливості та вживати заходів для їх усунення. Це може включати перевірку наявності оновлень програмного забезпечення, перевірку наявності відповідних політик доступу, а також проведення незалежних перевірок зовнішніми експертами.

Отже, захист інформації у державних реєстрах вимагає комплексного підходу. Впровадження сучасних технологій криптографічного захисту, фізична безпека, регулярний аудит та освіта співробітників можуть сприяти забезпеченню надійного захисту реєстру та запобіганню незаконному доступу до нього.

Список використаних джерел:

1. https://zakon.rada.gov.ua/laws/show/1952-15#Text.
2. https://zakon.rada.gov.ua/laws/show/1127-2015-п#Text.
3. https://zakon.rada.gov.ua/rada/show/v0988320-12#Text.
4. https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u--roczi-969/.
5. https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-4792/.
6. Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС : Наказ Міністерства внутрішніх справ України від 30.10.2012 № 988 URL: https://zakon.rada.gov.ua/rada/show/v0988320-12#Text.

Повалена М. В.,
доцентка кафедри загальноправових дисциплін
(*Львівський державний університет внутрішніх справ*)

ШТУЧНИЙ ІНТЕЛЕКТ ТА ЕЛЕКТРОННЕ УРЯДУВАННЯ

Сьогодні важливо звернути увагу на одну з найважливіших тенденцій сучасного розвитку державного управління – інтеграцію штучного інтелекту (ШІ) в електронне урядування. Використання алгоритмів та автоматизованих систем може зробити державний апарат більш ефективним, прозорим та доступним для громадян.

Впровадження ШІ в електронне урядування дозволяє автоматизувати адміністративні процеси, знижуючи бюрократичні перепони та прискорюючи обробку запитів громадян. Сучасні технології вже демонструють значні успіхи в таких напрямах:

- *чат-боти* та *віртуальні помічники* для консультацій та обробки запитів, наприклад, активно розвивається портал «Дія», який дозволяє громадянам отримувати державні послуги без необхідності відвідування держустанов;

- *автоматизоване ухвалення рішень щодо надання адміністративних послуг*, наприклад, реєстрація бізнесу, отримання ліцензій чи соціальних виплат;

- *ШІ-аналітика* для прогнозування потреб населення та ефективного розподілу ресурсів. У деяких країнах вже тестуються алгоритми прогнозування економічних криз та визначення стратегій розвитку регіонів.

Платформа «Дія» є взірцевим прикладом цифрової трансформації державного управління. Україна є однією з передових держав у впровадженні електронного урядування, підтвердженням цього є мобільний застосунок та веб-портал «Дія». Це не просто цифровий сервіс, а комплексна екосистема, яка дозволяє громадянам отримувати державні послуги швидко, зручно та без бюрократії.

Україна стала першою країною у світі, де електронний паспорт та водійське посвідчення в смартфоні прирівняні до фізичних документів. Відбулася ефективна автоматизація адміністративних послуг, зокрема, отримання довідок, реєстрація бізнесу, оформлення соціальних виплат та багато іншого можна зробити за кілька кліків без відвідування держустанов. Впроваджені алгоритми виявлення підозрілих реєстрацій компаній та автоматична перевірка документів. Що дозволяє розпізнавати шахрайство за допомогою ШІ. Застосовується ШІ-аналітика для прогнозування потреб. Держава аналізує великий масив даних, щоб покращити ефективність розподілу соціальних виплат, субсидій та інших послуг. «Дія» впроваджує функціонал електронного голосування та опитувань громадян, що робить владу більш відкритою. Під час воєнного стану в Україні через «Дію» впроваджено послуги для підтримки громадян та бізнесу, зокрема можливість отримання фінансової допомоги, подання заяв про зруйноване житло та мобілізаційні послуги.

Важливим аспектом є також цифрова ідентифікація та безпека даних. Одним із ключових викликів у сфері електронного урядування є безпечне зберігання та обробка персональних даних громадян. ШІ дозволяє вдосконалити системи цифрової ідентифікації через біометричні технології (ідентифікація через розпізнавання обличчя, відбитки пальців, сканування сітківки ока тощо).

В Естонії впроваджена система електронного громадянства (e-Residency), яка дозволяє підприємцям з усього світу вести бізнес у країні онлайн.

Електронне резидентство Естонії — програма запущена урядом Естонії 1 грудня 2014 року, яка дозволяє неестонцям отримувати доступ до естонських сервісів, таких як реєстрація підприємств чи банківські послуги, а також до єдиного європейського ринку. Кожен хто зареєструвався як електронний резидент отримує смарт-картку, за допомогою якої може підписувати електронні документи. Ця програма націлена на підприємців, які не залежать від місця свого перебування, таких як IT-розробники або письменники. Першим електронним резидентом Естонії став британський журналіст Едвард Лукас [1].

Машинне навчання для виявлення шахрайства та несанкціонованого доступу до персональних даних. Наприклад, у США система AI здатна виявляти фальшиві заяви про соціальні виплати.

Шифрування та блокчейн є важливі для захисту державних реєстрів та документів, що значно знижує ризики підробки офіційних документів. ШІ може значно покращити ефективність державного управління шляхом:

- автоматизованого аналізу великих обсягів даних для прийняття управлінських рішень;
- оптимізації процесів публічного адміністрування, що зменшить витрати державного апарату;
- підвищення прозорості, оскільки ШІ може фіксувати та аналізувати рішення чиновників, запобігаючи корупційним ризикам.

Проте разом із перевагами автоматизації постає низка проблем:

- відповідальність за помилки алгоритмів – хто несе відповідальність за рішення, прийняті ШІ?
- ризики кібербезпеки – чим більше цифрових процесів, тим вищі загрози кібератак;
- право на конфіденційність – необхідність балансування між ефективністю та захистом персональних даних.

ШІ є потужним інструментом для модернізації державного управління. Його інтеграція в електронне урядування здатна значно покращити якість надання послуг, зробити державу відкритішою та підвищити рівень довіри громадян. Проте разом із цими перевагами ми маємо пам’ятати про ризики та необхідність правового регулювання ШІ у сфері державного управління.

Список використаних джерел:

1. President Ilves annab täna üle esimese e-residendi kaardi. Estonian Development Foundation. 1 грудня 2014. URL: https://web.archive.org/web/20150206223942/-http://www.eas.ee/et/eas/pressikeskus/uudised?option=com_content&view=article&id=5694%3Apresident-ilves-annab-taena-uele-esimese-e-residendi-kaardi&catid=215%3Aeasist&Itemid=3982 (дата звернення: 09.03.2025).

Попович М. Д.,
старший судовий експерт
сектору дактилоскопічних досліджень та обліку
відділу криміналістичних видів досліджень
(Закарпатський НДЕКЦ МВС України)

ШТУЧНИЙ ІНТЕЛЕКТ В ПУБЛІЧНОМУ УПРАВЛІННІ

Термін «інтелект» (intelligence) має латинське походження. Intellectus означає розум, розумові здібності людини. А термін «штучний інтелект» трактується як здатність автоматизованих систем виконувати функції

людського інтелекту, вибирати та приймати рішення на основі попереднього накопиченого досвіду та раціонального аналізу зовнішніх факторів [2].

З давніх-давен людині були необхідні помічники для полегшення виконання тих чи інших операцій. Тож людська думка винаходила різноманітні механізми, машини та інші витвори homo sapiens. Поява електронно-обчислювальних машин дала змогу автоматизувати трудомісткі розрахункові операції. Згодом стало зрозуміло, що ці машини можна використовувати не тільки для обчислень, а й для керування різними пристроями, складними автоматизованими виробництвами тощо [1]. Від інтелектуальних персональних помічників у смартфонах до функцій самокерованого водіння в автомобілях – штучний інтелект стає частиною нашого повсякденного життя.

Штучний інтелект вже давно перестав бути чимось з області фантастики. Сьогодні він активно інтегрується в усі сфери життя – від охорони здоров'я та промисловості до фінансів і освіти. Алгоритми машинного навчання здатні аналізувати величезні маси виданих, прогнозувати тенденції та оптимізувати процеси; використання штучного інтелекту дозволяє значно підвищити ефективність, автоматизувати рутинні завдання та зменшити людський фактор у прийнятті рішень. Сучасні країни все більше уваги приділяють діджиталізації управлінських процесів. У цьому контексті штучний інтелект стає не лише аналітичним інструментом, а й важливим чинником формування політики, оптимізації бюрократичних процедур та покращення взаємодії між державою та громадянами.

Дуже важливим кроком в розвитку штучного інтелекту в публічному адмініструванні є те, що у Страсбурзі 13 березня 2024 року Європейський парламент на засіданні ухвалив знаковий Закон про штучний інтелект, який забезпечує безпеку та дотримання основних прав, одночасно стимулюючи інновації, він на сьогодні є найповнішим у світі набором правил для регуляції ШІ-технологій. Він унормовує: – обмеження на використання біометричних систем ідентифікації правоохоронними органами; – заборони соціальних оцінок і штучного інтелекту, які використовуються для маніпулювання або використання вразливостей користувачів; – право споживачів звертатися зі скаргами та отримувати змістовні роз’яснення; – винятки для правоохоронних органів; – стандарти прозорості; – зобов’язання для систем високого ризику [3].

Використання ШІ в державному управлінні відкриває нові можливості для підвищення прозорості, ефективності та доступності державних послуг.

На фоні вищевикладеного можемо виокремити низку переваг і недоліків впровадження ШІ у сфері публічного управління в Україні, а саме систематизувати постійно зростаючий обсяг інформації та розробляти більш персоналізовані послуги, щоб краще розуміти потреби громадян, наприклад, за допомогою аналізу даних; часткове зменшення паперового документообігу та зникнення помилок чи шахрайства, але тим самим виникають проблеми безпеки при обміні даними, що ставлять під сумнів стійкість суверенітету

інформаційного простору і створюють загрозу зовнішнього впливу на дані та розпорядження чутливою інформацією і підриває довіру до державних установ та медіа. Проте, завжди існують компроміси між складними ризиками та залежностями.

Як наслідок, штучний інтелект стає важливим інструментом для більш ефективного, відкритого та орієнтованого на громадян державного управління. Його впровадження вимагає обережного підходу, включаючи правові норми, етичні стандарти та контроль над алгоритмами для забезпечення справедливості та відповідальності. Важливим критерієм для розвитку є підвищення довіри громадськості до публічного потенціалу ШІ, індустрія повинна прийняти єдині стандарти і критерії для забезпечення безпечного і відповідального використання ШІ в публічному управлінні та адмініструванні.

Список використаних джерел:

1. Глибовець М. М., Олецький О. В. Штучний інтелект. Київ, 2002.

2. Фратавчан В. Г., Фратавчан Т. М., Лукашів Т. О., Літвінчук Ю. А. Методи та системи штучного інтелекту: навчальний посібник. Чернівці, 2023.

3. Artificial Intelligence Act: MEPs adopt landmark law. URL: https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/ artificial-intelligence-act-meps-adopt-landmark-law.

Пядишев В. Г.,
професор кафедри кримінального аналізу
та інформаційних технологій,
доктор юриидичних наук, професор
(Одеський державний університет внутрішніх справ)
Пирлик М. В.,
студент 1 курсу 2 групи ІПБ
спеціальності «Право» 081
(Одеський державний університет внутрішніх справ)

ШТУЧНИЙ ІНТЕЛЕКТ ТА ЗЛОЧИННІСТЬ (ЗАРУБІЖНИЙ ДОСВІД)

Штучний інтелект (ШІ) здійснив революцію в багатьох галузях, підвищивши продуктивність та інновації з безпрецедентною швидкістю. Від розширення доступу до охорони здоров'я до моделювання клімату, яке допомагає пом'якшити вплив погодних явищ, до підвищення ефективності та безпеки на наших робочих місцях — штучний інтелект забезпечує кращі та стійкіші результати. Оскільки технології штучного інтелекту будуть вдосконалюватися, змінюватимуться й способи їх використання злочинцями. ШІ сприяє зростанню злочинності, усуваючи людські вузькі місця

Одна з сучасних класифікацій впровадження ШІ містить три рівні, щоб ефективно визначати пріоритети реакцій на його застосування і ресурсів [1, с. 3].

Horizon phase (початкова фаза). Значне використання ШІ можливо і на цьому рівні. Але його що не достатньо проявилося. Злочинні організації можуть досліджувати майбутнє застосування, але впровадження залишається обмеженим.

Emerging phase (фаза сходження). ШІ активно використовується для оптимізації операцій, хоча люди все ще відіграють домінуючу роль у прийнятті та виконанні рішень. Приклади включають автоматизацію фішингових кампаній або вдосконалення існуючих шахрайських операцій.

Mature phase (фаза зрілості). Діяльність на основі ШІ домінує на цій фазі. При цьому системи ШІ перевершують людські зусилля за масштабом, ефективністю та витонченістю. Ці системи працюють із мінімальним людським впливом, автономно здійснюючи складні та серйозні злочинні дії.

Європейські колеги звертають увагу на наступні напрями активізації ШІ у кримінальній сфері (та відповідні проблеми) [2, с. 3-5]..

Моніторинг злочинності, що побудована на базі ШІ стикається з тою проблемою, що інтелектуальне агентство нового типу може діяти незалежно та автономно, дві особливості, які заплутають будь-яку спробу простежити слід відповідальності до злочинця.

Комерція, фінансові ринки та неплатоспроможність. Ця сфера злочинності включає картельні злочини, такі як зміна цін і змова, інсайдерські

операції, такі як торгівля цінними паперами на основі інформації про приватний бізнес, і маніпулювання ринком.

Шкідливі або небезпечні наркотики. ШІ може відіграти важливу роль у підтримці торгівлі та продажу заборонених речовини.

Сексуальні злочини. Сексуальні злочини, що обговорюються в літературі стосовно застосування ШІ, це: зґвалтування, сексуальне насильство і статевий акт або діяльність з неповнолітньою особою.

Крадіжки та шахрайство, а також підробка та передача даних особи. Європейські дослідження пов'язують підробку та видавання себе за іншу особу за допомогою ШІ із крадіжками та некорпоративним шахрайством, а також передбачають використання машинного навчання в корпоративному шахрайстві.

«Public-Private Analytic Exchange Program» – служба, що належить до служб Національної безпеки США, щойно деталізувала засоби штучного інтелекту, що застосовуються злочинцями, а саме: машинне навчання, нейронні мережі, глибоке навчання, генеративний ШІ, великі мовні моделі (LLM), чат-боти «Персони», композиція, редагування та аналіз тексту, навчання та мозковий штурм, с творення, налагодження та рефакторинг комп'ютерного коду моделі зображення та відео, генерація, аналіз, редагування, голосові моделі, моделі, доповнена генерація пошуку (RAG), агентські робочі процеси, малі моделі.

Цією ж службою визначено також основні напрями злочинної діяльності, що застосовують зазначені вище засоби: розробка зловмисного програмного забезпечення та комп'ютерний злом, шахрайство, фінансове шахрайство, фішинг і шахрайство зі старими, імперсонація керівника, фішингові електронні та текстові повідомлення, шахрайство стосовно старих осіб, шахрайство з ідентифікацією, шахрайство з документами в різних секторах, шахрайство з нерухомістю, шахрайство у сфері охорони здоров'я, маніпулювання ринком, сексуальне здирство, матеріали сексуального насильства над дітьми (csam), злоякісний вплив, насильницькі злочини, тероризм і радикалізація, кіберфізичні атаки, автономні транспортні засоби та дрони (для тероризму), виробництво та поширення матеріалів пропаганди, чат-бот Echo Chambers. [3, с. 6–14, 15–35].

ФБР попереджає американську громадськість, що злочинці використовують генеративний штучний інтелект (Generative AI) для вчинення шахрайства у більших масштабах, що підвищує правдоподібність їхніх схем. Генеративний ШІ скорочує час і зусилля, що зловмисники повинні витратити, щоб обдурити своїх цілей. Генеративний ШІ застосовує те, чого він навчився з прикладів, введених користувачем, і на основі цієї інформації синтезує щось абсолютно нове. Ці інструменти допомагають злочинцям у створенні вмісту та можуть виправляти людські помилки, які інакше можуть служити попереджувальними ознаками шахрайства [4, с. 2].

Список використаних джерел:

1. The Rise of AI-Enabled Crime: Exploring the evolution, risks, and responses to AI-powered criminal enterprises. Crypto Crime Report 2025. Insights. January 30, 2025. Site. URL:

https://www.trmlabs.com/post/the-rise-of-ai-enabled-crime-exploring-the-evolution-risks-and-responses-to-ai-powered-criminal-enterprises (дата звернення: 02.03.2025).

2. King Th. C., Aggarwal N., Taddeo M., Floridi L. Artifcial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. Science and Engineering Ethics. 14 February 2019. Site. URL: https://ec.europa.eu/futurium/en/system/files/-ged/king2019_article_artificialintelligencecrimeani.pdf (дата звернення: 02.03.2025).

3. Impact of Artificial Intelligence (AI) on Criminal and Illicit Activities. *Public-Private Analytic Exchange Program.* 2024. Site. URL: https://www.dhs.gov/sites/default/files/202410/24_0927_ia_aep-impact-ai-on-criminal-and-illicit-activities.pdf (дата звернення: 02.03.2025).

4. Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud. *Public Service Announcement. Federal Bureau of Investigations. Alert Number: I-120324-PSA. December 3*, 2024. Site. URL: https://www.ic3.gov/PSA/2024/PSA241203 (дата звернення: 02.03.2025).

П’ятецька С. О.,
курсантка
(Національна академія внутрішніх справ)
Чукаєва А. В.,
доцентка кафедри кримінології
та інформаційних технологій,
кандидат юридичних наук
(Національна академія внутрішніх справ)

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ВІЙНИ: МОЖЛИВОСТІ ТА РИЗИКИ

Про штучний інтелект (далі – ШІ) говорили давно – з 1960-тих років вчені почали виокремлювати для дослідження його алгоритмів окрему галузь, а письменники-фантасти, в свою чергу, намагалися передбачити розвиток ШІ та розвиток робототехніки. Суспільство ще відтоді ділилось на два табори: одні вважали, що штучний інтелект є потенційно небезпечним, здатним забрати роботу у звичайних громадян та, в найгіршому випадку, винищити людство загалом, оскільки за замовчуванням є більш розумним, пристосованим до змін та адаптованим до навчання; інші навпаки, вважали розвиток комп’ютерів такого рівня позитивною зміною, яка в майбутньому зможе покращити стан суспільства, допомагати виконувати величезний об’єм роботи та «співпрацювати» з людьми майже на рівних.

Відомий письменник-фантаст Айзек Азімов сформулював три основних закони, якими мають керуватися науковці під час створення розумних машин, та їх суть зводиться до одного основоположного принципу – «Поліпшити добробут людини».[1] З технічним розвитком світу з кожним роком прогресував і ШІ, який почали використовувати в різних сферах діяльності людства; освіта, медицина, політика, інженерія, право та інші – все більше спеціалістів у відповідних галузях починають впроваджувати штучний інтелект в свою діяльність, що позитивно впливає на результати такої спільної роботи.

Для закріплення принципів використання штучного інтелекту в юридичній сфері в грудні 2018 року Європейська комісія з питань ефективності правосуддя (CEPEJ) Ради Європи ухвалила перший європейський документ, який визначає етичні принципи використання Штучного інтелекту в судовій системі – Європейську Етичну хартію щодо використання штучного інтелекту в судовій системі та її середовищі [2].

Правоохоронці різних країн в тому числі використовують штучний інтелект у своїй діяльності: ШІ показує позитивні результати під час аналізу великих об'ємів неструктурованих даних та систем, допомагаючи поліцейським виокремлювати необхідну інформацію для окремої справи, вести бази даних та прогнозувати можливі загрози, що в свою чергу дає можливість їм запобігти. Велику роль штучний інтелект також відіграє у кримінальному провадженні – його активно застосовують, наприклад, працівники департаменту кримінального аналізу для розкриття тяжких та особливо тяжких злочинів: аналіз знарядь та речових доказів, співставлення їх з вже існуючими доказами в базах даних поліції, пошук логічних зв'язків, які можуть бути «невидимі» для слідчих, а також розпізнавання облич правопорушників, що були зафіксовані на камерах та подальше їх дослідження.

Ще більшої актуальності технологія розпізнавання облич набула після повномасштабного вторгнення – в умовах війни такий алгоритм допомагає встановлювати особу кожного російського військового, що вчиняв злочини, здійснює особистої інформації у відкритих джерелах за допомогою технології OSINT, що допомагає пришвидшити процес кримінального провадження і притягнення винних до кримінальної відповідальності. Як повідомляв виконавчий директор компанії ClearView AI, Хоан Тон-Тхат, в їхньому розпорядженні є понад два мільярди зображень з російської соціальної мережі «ВКонтакте», а загальна база даних налічує понад 10 мільярдів фотографій. [3]

Окрім встановлення осіб злочинців, штучний інтелект також може бути корисним для пошуку безвісти зниклих, викрадених з окупованих територій дітей – до прикладу, аналізувати вихідні дані (фото таких осіб, персональна інформація, особливості зовнішності), здійснювати пошук у російських медіа, на особистих сторінках «Вконтакте» та інших відкритих чи з обмеженим доступом джерелах та надавати інформацію про збіги працівникам поліції, щоб вони перевірили її та у випадку підтвердження, вжили необхідних заходів. За допомогою ШІ правоохоронці можуть аналізувати також переписки осіб, що підозрюються у неправомірній діяльності та співпраці з ворогом, а також автоматизувати процес відстеження фінансових транзакцій з підозрілих джерел.

Ще однією можливою корисною властивістю штучного інтелекту є допомога у створенні та покращенні «систем зв'язку», що використовуються правоохоронцями для розкриття багатосерійних злочинів чи заплутаних справ, де важливо правильно інтерпретувати кожен доказ та правильно ввести його в справу – за допомоги ШІ, який має безліч алгоритмів використання, цей процес має стати простіше для слідчих, а відповідно до цього – швидше.

Чат-боти, які створюються та функціонують на основі штучного інтелекту, також приносять величезну користь працівникам правоохоронних органів – за необхідності спрощення взаємодії між громадськістю та поліцією відповідний орган може створити чат-бот в телеграмі чи іншій соціальній мережі, куди громадяни можуть повідомляти про вчинення злочину, відому їм інформацію про підозрілих осіб (до прикладу, якась особа, яку до цього не бачили мешканці будинку, фотографувала об'єкти критичної інфраструктури) та все, що може бути корисне правоохоронцям. [4]

Можливості штучного інтелекту не закінчуються на цьому – його впровадження у освітній процес майбутніх працівників поліції має шанс позитивно вплинути на результати, оскільки він, окрім очевидного, може бути використаний для створення практичних ситуацій, з якими постійно стикаються діючі працівники, і напрацювання алгоритму дій, в тому числі пов'язаних з війною: затримання колаборантів, розбирання завалів, інтерв'ювання осіб, що постраждали від російської агресії (ґвалтування жінок в окупованих територіях, викрадені діти); здатний аналізувати та робити висновки після відпрацювання таких ситуацій та надання рекомендацій щодо покращення навичок, виправлення помилок та надання необхідної літератури для вивчення.

Важливим є забезпечення конфіденційності персональної інформації осіб, дані яких використовуються під час кримінального провадження та постійний контроль і перевірка отриманих даних від ШІ, оскільки неможливо гарантувати відсутність помилок та «вигадування» зі сторони алгоритму. До того ж, є ризик того, що штучний інтелект буде виконувати роботу, спираючись на упереджену інформацію або таку, що має певну дискримінаційну основу, оскільки він ґрунтується на інформації в інтернеті, яка поширюється людьми; в міжнародній практиці були зафіксовані випадки, коли правоохоронці затримували осіб, спираючись на результати роботи ШІ, а виявлялось, що затримана особа не мала ніякого відношення до справи.

Етичні питання, пов'язані зі штучним інтелектом та впровадженням його в правоохоронну та не тільки діяльність, все ще актуальні – не всі задоволені тим, як їхня приватність може бути обмежена, а упереджене ставлення до певних меншин поширена ще більше. Та все ж, не потрібно забувати про те, що ШІ, як і будь-якій технології, потрібен час для навчання, покращення можливостей та виправлення помилок; з іншого боку, неможливо не оцінити ту кількість можливостей, які вона надає правоохоронним органам і як покращується та полегшується робота спеціалістів завдяки ній. Головне – не потрібно забувати, що саме людина створила штучний інтелект і тільки від людей залежить, як саме він буде використовуватись та розвиватись у майбутньому.

Список використаних джерел:

1. Єдиний закон робототехніки: поліпшити добробут людини. *BBC News Україна*. URL: https://www.bbc.com/ukrainian/features-40450278.

2. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment : Хартія 04.12.2018. URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.
3. Сабадишина Ю. Як Україна використовує штучний інтелект для перемоги. У Мінцифри розповіли деталі. *Dou*. URL: https://dou.ua/lenta/news/clearview-ai-in-ukraine/.
4. Костенко І. «Народний месник». Як працює Telegram-бот, запущений Нацполіцією. *РБК-Україна*. URL: https://www.rbc.ua/rus/news/narodniy-mesnik-yak-pratsyue-telegram-bot-1726835736.html.

Савайда О. І.,
старший науковий співробітник
науково-дослідної лабораторії вивчення проблем
протидії торгівлі людьми ННІПФПКП,
кандидат юридичних наук, доцент
(Львівський державний університет внутрішніх справ)

ОСНОВНІ ЗАСАДИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ

Безперечно, що сучасний розвиток різних видів суспільних відносиш в державі та суспільстві призводить до появи нових явищ, які потребують чисельних засобів для їхнього регулювання. Серед таких засобів, які можуть допомагати регулювати суспільні відносини можна виділити засоби новітніх технологій, які зараз інтенсивно створюються, розвиваються та використовуються у всіх сферах соціального життя людини для покращення їхнього існування та гармонізації.

Зокрема, до таких новітніх засобів врегулювання соціальних відносин можна віднести інформаційні технології, серед яких належне місце займає створення та використання такого засобу, як штучний інтелект.

Цифрові та інформаційні засоби все більше й більше сприяють та допомагають розвитку будь-яких відносин, а особливо їхньому правозастосуванню. Проте, серед регулювання правових відносин, ми б хотіли виділити такі відносини, які підпадають під ознаки злочину, адже вони потребують особливого регулювання та втручання зі сторони держави, адже такі явища як злочин (та відносини, які пов’язанні із такими негативними явищами) містять суспільну небезпеку.

Серед великої кількості злочинів наша увага буде зосереджена на торгівлі людьми, як найганебнішому явищі розвиненого правового світу, яка прирівнюється до сучасного рабства. Торгівля людьми як не дивно, але також зазнає певних трансформацій, і більш того, на жаль, також розвивається за допомогою сучасних інформаційних технологій завдаючи все більшої і більшої шкоди, як в територіальному масштабі так, і в людському значенні, наносячи їм значної шкоди та порушуючи їхні права.

Як зазначають деякі науковці практичні приклади та досвід інших країн у протидії торгівлі людьми, включаючи використання цифрових технологій

становить важливий елемент у глобальній боротьбі з цим негативним явищем [1, с. 54].

Європейська спільнота на законодавчому рівні опікується регулюванням відносин, які пов'язані із таким злочином, як торгівля людьми. Впроваджуючи закон щодо міжнародного трактування та регулювання штучного інтелекту європейські діячі втілюють основні засади правового регулювання, зокрема й сфери, яка стосується й організованої злочинності.

Відтоді як європейський закон про штучний інтелект набуде чинності – що станеться не раніше як в кінці 2025 року – технологічні компанії, які прагнутимуть працювати й продавати свої продукти на основі штучного інтелекту в межах ЄС, будуть змушені ділитися своїми даними з регуляторами та проводити ретельне його тестування.

Європейське створення закону щодо регулювання правових відносин за допомогою штучного інтелекту має за мету ухвалення такого законодавства, яке забезпечить розвиток екосистеми штучного інтелекту з орієнтованим на людино центричний підхід, поважаючи фундаментальні та природно-правові права та свободи, людську гідність та її цінності, зміцнюючи довіру, розвиваючи усвідомлення того, як ми можемо отримати найкраще від цієї революції штучного інтелекту [2].

Погоджуємося з думкою М. В. Карчевського, який наголошує на тому, що технології штучного інтелекту здатні якісно оновити способи протидії злочинності, зокрема й протидії торгівлі людьми. На думку автора, першочерговим кроком розвитку сучасної національної протидії злочинності в контексті використання технологій штучного інтелекту має стати збір та аналіз якомога більших обсягів даних щодо призначених покарань, психометричних характеристик злочинців, особливостей їх посткримінальної поведінки тощо [3, с. 20].

До основних засад використання штучного інтелекту, які можна застосувати в протидії торгівлі людьми ми б хотіли віднести наступні:

- основна засада використання ШІ полягає в його багаторівневості, яка закладена в його системі, що в свою чергу базується на оцінці ризиків. Особливої уваги потребує відповідний до цієї системи – найвищий рівень, який застосовується до тих технологій ШІ, які становлять найбільший ризик для життя, здоров'я, безпеки та прав й свобод людини;

- важливим аспектом в засадах залишається сам суб'єкт використання штучного інтелекту. Так, наприклад, згаданим вище європейським законом передбачено певне обмеження на використання ШІ для деяких суб'єктів, наприклад, поліцейських. Проте також європейські законодавці пропонують певні виключення щодо поліцейської діяльності. А саме, як пояснив єврокомісар Д. Бретон, закон передбачає заборону на використання технологій ШІ поліцією, роботодавцями чи закладами торгівлі для стеження за людьми в реальному часі, включно з емоційним розпізнаванням. Єдині винятки складають ситуації, коли поліція потребує використання інвазивних технологій ШІ через несподівану загрозу теракту, а також для пошуку жертв торгівлі

людьми й для розслідування серйозних злочинів, таких як вбивства, зґвалтування тощо [2];

- відповідно після того як ми проговорили щодо суб'єкта використання ШІ, мова йтиме про рішення, які прийнятті ШІ або людиною з його допомогою, які в свою чергу, повинні бути прозорими та зрозумілими та законними та правовими (якщо мова йде про правовідносини).

Так, безперечно, злочинці також інтенсивно використовують в своїй площині технології штучного інтелекту, що призводить до розширення масштабів їхньої злочинної діяльності та до появи нових методів вчинення злочинів, і навіть до утворення нових видів кримінальних правопорушень чи форм експлуатації. Погоджуємося з думкою О. В. Турути, що швидкий розвиток технологій штучного інтелекту потребує пильної уваги до питань безпеки, вчинення злочинів, надійності, прозорості, справедливості, етики та рівності [4, с. 50].

У висновку ми висловлюємо застереження щодо використання штучного інтелекту в будь-яких взаємовідносинах, і звертаємо вашу увагу на проблемне питання щодо співвідношення та використання ШІ та прав людини для подальших дискусій та роздумів. Так, безперечно, технології штучного інтелекту впроваджені в різні сфери життя людини покращують та підвищують результативність її роботи. Проте, тут також є і ризики, які позначаються на правах людини, а особливо через дискримінаційну їхню складову, і вони проявляються в тому, що є неможливість передбачати наслідки від такого застосування ШІ, оскільки на сьогоднішній час існують безліч прикладів недосконалості вказаної технологічної системи. Й тому, при похибках у використанні ШІ потрібно розробити механізм відслідковування таких помилок та бути готовими до надання традиційних методів захисту чи регулювання правових відносин.

Список використаних джерел:

1. Козар Ю. Ю., Луцький В. Я. Сучасні тенденції та перспективи правозастосування. *Часопис Київського університету права*. 2024. № 2. С. 52–56.

2. Штучний інтелект з повагою до людини. Європейський Союз ухвалив "історичний" закон щодо ШІ, випередивши США та Китай. URL: https://www.holosameryky.com/a/es-uhvalyv-novyi-zakon-pro-shtuchnyi-intelekt/7391311.html.

3. Карчевський М. В. Штучний інтелект та протидія злочинності Використання технологій штучного інтелекту у протидії злочинності : матер. наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. 112 с.

4. Турута О. В., Турута О. П. Штучний інтелект крізь призму фундаментальних прав людини. *Науковий вісник Ужгородського Національного Університету. Серія Право.* 2022. Вип. 71. С. 49–54.

Скрипник С. С.,
науковий співробітник науково-дослідної лабораторії
з проблем протидії злочинності
навчально-наукового інституту поліцейської діяльності
(Національна академія внутрішніх справ)

ТЕХНІЧНІ ОБМЕЖЕННЯ У ВИКОРИСТАННІ ШТУЧНОГО ІНТЕЛЕКТУ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Людський мозок можна розглядати як дві окремі системи: одну швидку, яка працює несвідомо, а іншу повільнішу, свідому, що відповідає за розподіл уваги в залежності від ситуації [1]. Якщо увага людини залишається зосередженою на події протягом тривалого часу, це може посилити емоційний відгук [2]. Наприклад, тривале переживання негативних емоцій може привести до депресії чи тривожних розладів, тоді як концентрування на позитивних аспектах може допомогти зберегти емоційну рівновагу. За цієї аналогією можна порівняти сучасні системи штучного інтелекту з несвідомою частиною людського мозку, оскільки вони використовують тільки швидкі обчислення. Системи штучного інтелекту не можуть впоратися з несподіваними подіями, до яких не підготовлені [3]. Люди ж можуть задіяти свою свідому систему і негайно обробити нову ситуацію і діяти. Саме тому ми повинні чітко усвідомлювати обмеження ШІ особливо у сфері правоохоронної діяльності. Штучний інтелект перевершує людину в ряді сфер, наприклад, в обробці та зберіганні величезних обсягів різноманітної інформації, що значно перевищує можливості нашого мозку. З огляду на це, ми не повинні недооцінювати потенціал штучного інтелекту, особливо у роботі з великими даними. Водночас, важливо не переоцінювати ці технології, адже на етапі цифровізації світу завжди буде потреба в фахівцях, які відповідатимуть за правильне застосування інструментів на основі ШІ [3]. Тому оптимізація методів роботи людей та комп'ютерних систем в правоохоронних органах полягає в ефективному поєднанні сильних сторін обох підходів для покращення точності та результативності.

Інтеграція штучного інтелекту в правоохоронні органи має низку технічних обмежень, які можуть впливати на її ефективність:

1. Якість і доступність даних: Проблеми виникають через різноманітність практик збору та зберігання даних, що призводить до неповних або упереджених наборів даних. Це порушує точність результатів ШІ. Крім того, дані часто не збираються з урахуванням вимог ШІ, що обмежує їх корисність. Наприклад, поліцейські звіти можуть не містити даних про неповідомлені інциденти, що впливає на процес навчання нейронних мереж та результати. Стандартизовані протоколи збору, очищення та збагачення даних, а також надійний захист даних, критично важливі для забезпечення точності, етичності та відповідності законодавчим вимогам.

2. Проблеми інтеграції: Інтеграція ШІ з існуючими системами правоохоронних органів стикається з технічними труднощами, зокрема через несумісність старих технологій з новими рішеннями ШІ. Для вирішення цієї проблеми необхідна модернізація застарілих систем та розробка нових рішень з акцентом на модульну інтеграцію.

3. Масштабованість і адаптивність: Інструменти ШІ повинні ефективно працювати при різних обсягах даних і умовах. Але існують проблеми, що пов'язані з розробниками ШІ і так званими чорними скриньками. Чорна скриня ШІ – це внутрішня робота та алгоритми ШІ, що лежать в основі прогнозів та отриманих результатів, які складно пояснити і які часто є комерційною таємницею розробника системи ШІ [4]. Це ускладнює судові процеси, оскільки немає чіткої відповіді, чому саме система ШІ зробила той чи інший висновок. Тому моделі ШІ повинні бути масштабованими та адаптивними, щоб не втрачати продуктивність та достовірність висновків навіть у складних сценаріях.

4. Обслуговування та технічна підтримка: Постійне оновлення та технічне обслуговування є необхідними для забезпечення ефективності та безпеки ШІ-систем. Проте, це може бути проблемою для правоохоронних органів, які мають обмежені ресурси та доступ до ІТ-спеціалістів. Крім того існує можливість кібератак на системи ШІ, що може призвести до витоку даних або маніпуляції результатами. Атакована хакерами та пошкоджена система ШІ може використовуватися для створення deepfake-відео або підробки доказів [5].

Створення спеціалізованих підтримуючих структур та партнерств з постачальниками технологій може допомогти забезпечити довгострокову ефективність і актуальність систем ШІ [6].

Для вирішення цих проблем необхідна ефективна структура управління ШІ та узгоджена співпраця всіх зацікавлених сторін. Взаємодія між правоохоронними органами, розробниками технологій, політиками та громадськістю є ключовою для подолання технічних обмежень. Це дозволяє розробляти, тестувати та вдосконалювати інноваційні рішення, підвищуючи ефективність і надійність програм ШІ в поліцейській діяльності. Інвестиції в дослідження, розвиток, етичне використання ШІ, а також постійне навчання правоохоронців є важливими кроками для подолання існуючих викликів.

Список використаних джерел:

1. Kahneman, D. (2011). *Thinking, Fast and Slow*. Penguin, 496 pp., ISBN 978-0141033570.

2. Fredrickson, B. L. (2009). *Positivity: Top-notch research reveals the 3-to-1 ratio that will change your life.* Crown Publishers.

3. Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic Science International, 362,* 112133. https://doi.org/10.1016/j.forsciint.2024.112133.

4. Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., Scardapane, S., Spinelli, I., Mahmud, M., & Hussain, A. (2024). Interpreting black-box models: A review on explainable artificial intelligence. *Cognitive Computation, 16*(1), 45–74. https://doi.org/10.1007/s12559-023-10179-8.

5. Carlini, N., & Farid, H. (2020). Evading deepfake-image detectors with white- and black-box attacks. CVPR Workshops, 2020, 2804-2813. https://doi.org/10.1109/CVPRW50498.2020.00298.
6. Europol. (2024). *AI and policing: The benefits and challenges of artificial intelligence for law enforcement*. An Observatory Report from the Europol Innovation Lab. https://doi.org/10.2813/0321023. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf.

Сліпенюк В. В.
доцент кафедри державознавства, права
та європейської інтеграції,
доктор філософії Інституту
публічної служби та управління
(Національний університет «Одеська політехніка»)

ПРИНЦИПИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС ЗДІЙСНЕННЯ СУДОЧИНСТВА

Однією із найпрогресивніших технологій XXI століття, яка активно використовується у всіх сферах життєдіяльності людини є штучний інтелект (далі – ШІ). Його поява надала змогу оптимізувати рутинні процеси, й тим самим посилила продуктивність діяльності людини. Впровадження ШІ у судочинство відкрило нові можливості для підвищення ефективності правосуддя. Разом з тим, використання новітньої технології в цій сфері потребує дотримання певних принципів, що й актуалізує необхідність наукових розвідок окресленої проблематики.

Принципи судочинства є базисом провадження правосуддя, значимість яких важко переоцінити: останні не лише надають змогу забезпечити справедливість, рівність і правову визначеність у процесі розгляду справ, а також є гарантами дотримання прав і свобод людини, що є основою демократичного суспільства.

Враховуючи загальнотеоретичні напрацювання щодо категорії «принцип» та сутність технологій ШІ, під принципами використання ШІ під час здійснення судочинства слід розуміти визначальні положення щодо інтеграції технологій ШІ в процес здійснення судочинства, спрямовані на забезпечення етичності та законності її застосування суддями та іншими учасниками судового процесу.

Сукупність принципів використання ШІ під час здійснення судочинства утворює собою систему, в якій ключовими елементами є принципи прозорості, неупередженості, конфіденційності, відповідальності та ефективності, кожен із яких має свої особливості.

Так, принцип прозорості передбачає необхідність розкриття інформації про всі алгоритми й моделі, які використовуються в судовій системі, що включає в себе не лише технічні, а й методологічні аспекти. Цей принцип надає змогу учасникам судового процесу та суспільству оцінювати діяльність суду

щодо організації процесу судочинства та конкретного судді при прийнятті рішення. При цьому, спроби приховати використання цієї технології негативно відображаються на довірі громадян й порушує інші фундаментальні принципи. Яскравим прикладом цьому є ситуація, яка набула широкого резонансу серед представників юридичної спільноти Португалії, в якій суддів апеляційної інстанції підозрюють у використанні ШІ для ухвалення рішення через «дивні висловлювання, недбалу португальську та цитати статей, яких немає в законі» [1].

Не менш важливим принципом використання ШІ під час здійснення судочинства є принцип неупередженості, який корелюється із принципом рівності прав і свобод людини, є принцип неупередженості. Застосування ШІ під час провадження правосуддя повинно базуватись на алгоритмах, які не відтворюють існуючі в суспільстві дискримінаційні упередження за будь-якими ознаками, такими як раса, національність, вік, стать, мова, релігія, соціальний статус, політичні чи інші переконання, тощо. Тому для етичного й законного використання цієї технології, важливо здійснювати системні тестування й моніторинг задля недопущення будь-яких проявів обмеження або позбавлення прав певних категорій населення.

Конфіденційність є ще одним важливим принципом використання ШІ під час здійснення судочинства, що обумовлено обробкою в процесі правосуддя великого об’єму персональних даних. Цей принцип передбачає, що вся особиста інформація учасників судового процесу має бути надійно захищена від несанкціонованого доступу та розголошення, що особливо актуально в умовах російсько-української війни, яка ведеться й у кіберпросторі. Разом з тим, впровадження лише технічних рішень таких як шифрування та контроль доступу є недостатнім: судді, працівники апарату судів та учасники судочинства мають дотримуватись стандартів кібербезпеки, зокрема, не вводити конфіденційну інформацію в системі ШІ за відсутності обґрунтованої впевненості щодо майбутньої захищеності інформації.

Відповідальність також входить до системи принципів використання штучного інтелекту під час здійснення судочинства. Останній означає, що всі учасники судового процесу, які застосовують цю технологію, мають нести юридичну відповідальність за результати своєї роботи, що включає як позитивні, так і негативні результати, які можуть вплинути на права та свободи громадян. Задля цього на законодавчому рівні мають бути закріплені відповідні механізми контролю й підзвітності для запобігання й протидії протиправним діями, а також уникнення правових колізій й дотримання правової визначеності. Попри відсутність в чинному національному законодавстві профільних приписів щодо принципу відповідальності, останній вже активно використовується на практиці. Зокрема, Касаційний господарський суд у складі Верховного суду визнав зловживанням правами і неповагою до суду посилання адвоката на висновок штучного інтелекту ChatGPT щодо тлумачення сутності теоретичного поняття, закріпленого в нормах матеріального права [2].

Ефективність також доцільно розглядати як принцип використання ШІ під час здійснення судочинства. Застосування цієї технології має спрямовуватись на покрашення доступу до правосуддя, зменшення впливу людського фактору при виконанні рутинних позапроцеуальних процесів, а також на оптимізацію процесів обробки великих обсягів інформації за короткий проміжок часу, що надасть змогу суддям, працівникам апарату судів та учасникам судового процесу швидше отримувати необхідні відомості щодо законодавства й судової практики для підготовки позицій й безпосереднього розгляду справ. Таким чином, саме ефективність є тим принципом, який визначає доцільність використання ШІ в умовах великої завантаженості українських судів, обмежених ресурсів останніх та загалом критичності діяльності в умовах воєнного стану. В цьому контексті цікавим є досвід суду округу Палм-Біч, який у 2018 році отримав національну нагороду в США за цифрові інновації за використання програми Lights-Out Document Processing, що з рівнем точності від 98% дозволила користувачам аналізувати подані документи, а також позначати та індексувати їх відповідною інформацією про справу [3].

Резюмуючи всі вище викладені положення, приходимо до висновку, що в Україні, як і в будь-якій іншій демократичній державі, інтеграція ШІ в судову систему та подальше його використання під час здійснення судочинства, має узгоджуватись із наведеними принципами. Видається, що в такий спосіб дана технологія буде застосовуватись законно, етично й на благо громадян й держави, а також може стати потужним інструментом для покращення правосуддя, що дозволить забезпечити баланс між інноваціями та правами людини, що є основою демократичного суспільства.

Список використаних джерел:

1. У Португалії суддів підозрюють у використанні ШІ для ухвалення рішення, тепер його можуть анулювати. URL: https://sud.ua/uk/news/abroad/316860-v-portugalii-sudey-podozrevayut-v-ispolzovanii-ii-dlya-vyneseniya-resheniya-teper-ego-mogut-annulirovat.

2. Касаційний господарський суд визнав зловживанням правами і неповагою посилання адвоката на «висновок» штучного інтелекту ChatGPT. URL: https://sud.ua/uk/news/publication/293764-kassatsionnyy-khozyaystvennyy-sud-priznal-zloupotrebleniem-pravami-i-neuvazheniem-ssylku-advokata-na-vyvod-iskusstvennogo-intellekta-chatgpt.

3. Humanizing Justice: The transformational impact of AI in courts, from filing to sentencing. URL: https://www.thomsonreuters.com/en-us/posts/ai-in-courts/humanizing-justice/.

Стефанишин Н. М.,
доцентка кафедри цивільного права
навчально-наукового юридичного інституту,
кандидатка юридичних наук, доцентка
(Прикарпатський національний університету ім. В. Стефаника)
https://orcid.org/ 0000-0001-6919-2774

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ОБ'ЄКТ АВТОРСЬКОГО ПРАВА

Науково-технологічний прогрес останніх десятиліть вражає та відкриває людству пізнання нових можливостей штучного інтелекту та «проникнення» останнього, практично, у всі сфери суспільного життя. Так, сьогодні, ми вже говоримо про роботи-няні, роботи-прибиральниці, роботи-медики, роботи з обслуговування транспорту тощо. Поява штучного інтелекту створює не лише комфорт з надання певних послуг, а й породжує низку проблем як загального, так і спеціального характеру, що вимагає їх вирішення. Зокрема, актуальною є проблема належного правового регулювання суспільних відносин, які виникають за участю «розумних» пристроїв, здатних виконувати складні операції та вирішувати інтелектуальні завдання.

У наукових дослідженнях представлено низку понять та підходів до розуміння штучного інтелекту, що визначають й зміст останнього – від ототожнення штучного інтелекту з робототехнікою до його сприйняття як самостійного напрямку відповідної науки в галузі технічних наук. Якщо ж торкнутися питання генези виникнення штучного інтелекту (далі ШІ), то вперше дане поняття запропонував Джон Маккарті на Дартмутській конференції у 1956 році, де зазначив, що штучний інтелект – це наука й техніка створення інтелектуальних машин, особливо інтелектуальних комп'ютерних програм [1, с. 20].

Незважаючи на те, що від появи першого поняття штучного інтелекту вже минуло практично півстоліття, єдиного розуміння даного явища, сьогодні, немає. Це, на нашу думку, пов'язано ще й з міждисциплінарним характером штучного інтелекту.

Поява штучного інтелекту та введення даної конструкції в цивільному обороті ставить, мабуть, найбільше завдань для юристів, оскільки породжує низку питань та проблем правового характеру, що потребують вирішення та належного правового регулювання, зокрема: - визначення штучного інтелекту як об'єкту чи суб'єкту цивільних правовідносин; - окреслення правосуб'єктності штучного інтелекту; - питання реалізації цивільних прав та обов'язків ШІ; - гарантії захисту відповідних прав та юридичної відповідальності.

Аналізуючи наукові дослідження можемо прослідкувати наявність таких понять як робот, комп'ютерна програма, робототехніка, електронна особа, штучний інтелект. Одні вчені ототожнюють дані поняття, інші, з думкою котрих ми погоджуємося, зазначають про неможливість ототожнення понять робот та штучний інтелект, оскільки їх слід співвідносити між собою як форма та зміст. Робот є пристроєм, машиною, основною здатністю якої є автоматизоване виконання однієї чи декількох завдань за зразком дій людини, якій властиві ознаки рухливості, сенситивності, аналітичності тощо. Штучний інтелект надає роботу таких властивостей, якими прийнято його характеризувати, а саме, розумність, здатність до аналізу та обробки інформації, а також до виконання завдань, на які він запрограмований [2, с. 6].

Питання визначення штучного інтелекту об'єктом чи суб'єктом цивільних правовідносин є, водночас, актуальним та дискусійним. Адже, в залежності від того, як ми визначаємо ШІ у реальних правовідносинах залежить те, чи ШІ буде їх учасником та наділятиметься відповідними правами чи ШІ буде об'єктом, по відношенні до якого виникатимуть відповідні правовідносини, укладатимуться відповідні договори тощо, а останній наділятиметься ознаками об'єкта цивільних прав загалом.

Визначення штучного інтелекту суб'єктом цивільних правовідносин є доволі спірним в сучасній цивілістиці. Оскільки, з теорії права відомо, що суб'єкт правовідносин наділений суб'єктивними правами, здатен виконувати юридичні обов'язки та нести юридичну відповідальність у випадках передбачених законом. Такими суб'єктами виступають фізичні особи, юридичні особи та держава (через створені органи державної влади, що є суб'єктом публічного права). У жодному чинному нормативно-правовому акті, тим паче, ЦК України мова про штучний інтелект не ведеться. Однак, у Резолюції щодо цивільно-правового регулювання робототехніки запропоновано створення системи реєстрації роботів, фонду страхування, цивільної відповідальності, відповідальності розробників та власників роботів тощо, а у п. 59 даного документа закріплена суб'єктність роботів під назвою «електронна особа» з комплексом специфічних прав та обов'язків [3]. Звідки й випливає, що штучний інтелект є квазісуб'єктом цивільних правовідносин із низкою специфічних та наявних лише ШІ правових ознак. Про «електронну особу» згадує у свої працях й М.О. Стефанчук, котрий зазначає, що штучний інтелект, зокрема, штучний суперінтелект має здатність самостійно думати та діяти в рамках суспільних відносин, а отже, може виступати носієм прав та обов'язків [2, с. 6]. Такої ж думки дотримується й В. Кулинич, котрий вважає,що варіантом дій з боку людства, який, можливо, забезпечить співіснування людей та роботів, буде саме надання роботам статусу суб'єктів, наділених відповідними правами та обов'язками [4].

У Китаї існують юридичні компанії, які розробляють програми для прогнозування результату судової справи. Вони користуються попитом та допомагають адвокатам вирішувати справи. У Пекіні судді-роботи беруть активну участь у судовому процесі, які офіційно перебувають в онлайн-центрі інтернет-суду.

На користь наукової позиції, що ШІ є суб'єктом цивільних правовідносин вчені наводять й той факт, що юридичні особи теж створені людиною і вже давно виступають суб'єктами правовідносин. Проте, таку думку спростовує О. І. Харитонова, котра зазначає, що юридична особа наділена «людським субстратом», оскільки, відомим є те, що юридична особа – колектив чи організація людей, або ж один директор, що виступає від її імені у цивільних правовідносинах. Як і народ України – суб'єкт конституційних правовідносин, що складається з спільності людей, так і юридична особа – колективний суб'єкт людей. Тому до ШІ таку аналогію застосовувати неможна [5, с. 205].

Стосовно вище наведеної аргументації, можемо за порівняння взяти тварини, адже, це живі істоти, що наділені своїм природнім інтелектом, здатні до спілкування, дресирування, частково, мислення, проте, останні залишаються об'єктом цивільних прав, хоча наділяються певними правами визначеними спеціальним законодавством.

Тому вважаємо, що сьогодні правові традиції українського суспільства та й законодавець не готовий наділити штучний інтелект правами та обов'язками, що дозволяло б говорити про його правосуб'єктність та визначати останнього суб'єктом цивільних правовідносин. Штучний інтелект є об'єктом цивільного права (в межах розділу ІІІ ЦК України), як варіант, річ, яку можна продати, купити, подарувати, обміняти тощо, або ж, об'єктом права інтелектуальної власності, зокрема, об'єктом авторського права що створений в результаті творчої, інтелектуальної діяльності людини (в межах книги 4 ЦК України та з врахуванням Закону України «Про авторське право і суміжні права»).

Ще одним питанням, що потребує вирішення є питання юридичної відповідальності за шкоду спричинену штучним інтелектом. Здебільшого, у відповіді на дане питання вчені зазначають, що мають застосовуватися норми чинного законодавства про діяльність, пов'язану з джерелом підвищеної небезпеки. В. Кулинич вказує, щодо правовідносин, які виникають внаслідок заподіяння шкоди роботами покладається на володільців таких роботів, як на володільця джерела підвищеної небезпеки або на виробників таких роботів [4]. Із цією думкою варто погодитися, окрім того, слід зазначити, що до відповідних правовідносин необхідно застосовувати й законодавство про захист прав споживачів, а до ШІ посилити вимоги законодавства щодо вимог безпеки життя, здоров'я та майна особи, а також, безпеки навколишнього природного середовища.

Окреслені в запропонованій тезі положення є далеко не виключним переліком питань, що виникають та пов'язані із введенням в цивільний оборот та використанням штучного інтелекту та можуть бути втіленими у правових дослідженнях із запропонованої теми в майбутньому.

Список використаних джерел:

1. Баранов О. А. Інтернет речей і штучний інтелект: витоки проблеми правового регулювання. ІТ-право: проблеми та перспективи розвитку в Україні : зб. матер. ІІ Міжнар. наук.-практ. конф. (Львів, 17 листоп. 2017 р.). Львів : Львів. політехніка, 2017. С. 18–42.

2. Стефанчук М. О. Теоретичні засади цивільної правосуб'єктності фізичних осіб та особливості її здійснення : автореф. дис. … д-ра юрид. наук : 12.00.03. Київ, 2020. С. 6.

3. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics. Режим доступу: URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN.

4. Кулинич В. Цифрова особистість: чи можуть роботи бути наділені правами? *Юридична газета*. 2017. № 49 (599). URL: https://yur-gazeta.com/dumka-eksperta/cifrova-osobistist-chi-mozhut-roboti-butinadileni-pravami.html.

5. Харитонова О. І., Харитонов Є. О. ІТ-право: теорія та практика. Одеса : Фенікс, 2019. 472 с.

6. Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15.
7. Про авторське право і суміжні права: Закон України від 01.12.2022 № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text.

Тарасюк А. В.,
заступник керівника Управління
Головного слідчого управління,
доктор юридичних наук, професор,
полковник
(Державне бюро розслідувань)

ШТУЧНИЙ ІНТЕЛЕКТ В ПРОТИДІЇ ТА РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ: ДІЯЛЬНІСТЬ ДЕРЖАВНОГО БЮРО РОЗСЛІДУВАНЬ

Сучасне суспільство знаходиться на етапі глобального переходу до нового технологічному устрою, пов'язаного з цифровою економікою та застосування штучного інтелекту (далі – ШІ). Принагідно зазначимо, що ШІ – це функція штучної свідомості, яка представлена створеною й контрольованою нею системою алгоритмів, забезпечує самонавчання згідно з наявною інформацією, набутими знаннями, правилами, законами суспільства і своїм досвідом, створення на цій основі нових знань для виконання доручень людини, а також здатність проводити самодіагностику й обґрунтовувати ухвалені нею рішення [1]. Наразі ш*тучний інтелект є світовим інноваційним пріоритетом в багатьох сферах та напрямках, ключовими серед яких – протидія злочинності.*

Нагадаємо, що 2 грудня 2020 року розпорядженням Кабінету Міністрів України було схвалено «Концепцію розвитку штучного інтелекту в Україні», положеннями якої визначаються мета, принципи і завдання розвитку технологій штучного інтелекту в Україні як одного з пріоритетних напрямів у всіх сферах життєдіяльності [2]. У Концепції розвитку штучного інтелекту в Україні враховані рекомендації Ради Європи з питань ШІ від 22 травня 2019 року (OECD Legal Instruments), які встановлюють принципи діяльності з розвитку ШІ, зокрема й у сфері захисту інформаційного простору від несанкціонованого втручання, забезпечення безпечного функціонування інформаційно-телекомунікаційних систем та протидії кіберзлочинам загалом.

Саме на правоохоронні органи державою покладено головний обов'язок у боротьбі зі злочинами в мережі Інтернет. Державне бюро розслідувань (далі – ДБР) є державним правоохоронним органом, на який покладаються завдання щодо запобігання, виявлення, припинення, розкриття та розслідування злочинів, віднесених до його компетенції [3]. Завданнями Державного бюро розслідувань є своєчасне запобігання, виявлення, припинення, швидке розкриття та об'єктивне розслідування злочинів, віднесених до компетенції Бюро.

Слід зазначити, що кримінальна кіберповедінка постійно модифікується, виникають нові види злочинної діяльності. До найпоширеніших злочинів у цій сфері можна віднести:

– кібершахрайство – реалізація злочинних схем обману та зловживання довірою, таких як фішинг, скімінг тощо;

– кіберкрадіжка – «комп'ютерне втручання», що включає в себе так звані «хакерські атаки» на комп'ютерні системи та мережі з метою несанкціонованого доступу до інформації економічного характеру та незаконного переказу коштів;

– кібершпигунство – незаконне отримання конфіденційної (секретної) державної чи приватної інформації з метою політичної, економічної та військової вигоди;

– кібертероризм – використання кібератак з метою заподіяння шкоди системам комунікацій, енергетичним системам, урядовим інфраструктурам та іншим особливо важливим державним об'єктам;

– кіберхуліганство – створення та поширення шкідливого програмного забезпечення (вірусів, троянських та інших шкідливих програм) з метою заподіяння шкоди комп'ютерним системам та отримання контролю над ними;

– кіберекстремізм – поширення шкідливого програмного забезпечення з матеріалами екстремістського характеру тощо.

Підкреслимо, що в сучасних умовах війни в Україні з боку РФ кіберзлочинність постійно еволюціонує, з'являються нові кримінальні способи вчинення таких посягань. Як відомо, у грудні 2024 року відбулася масштабна зовнішня кібератака на державні реєстри України. Внаслідок цілеспрямованої атаки тимчасово було призупинено роботу Єдиних та Державних реєстрів, які перебувають у компетенції Міністерства юстиції України. Атаки також зазнали Автоматизовна система виконавчого провадження, Єдиний реєстр боржників та Єдиний реєстр приватних виконавців України.

Розслідування вищеокреслених кіберзлочинів неможливе без використання спеціальних знань та вмінь. Структура ж спеціальних знань містить власне знання у сфері програмування та мережевих технологій та досвід у написанні програм у виявленні та аналізі цифрових слідів. Так, наприклад, у лютому 2024 р. ДБР повідомили кіберзлочинцю, який ошукував іноземців та легалізовував доходи від нелегальних операцій про підозру. Наразі працівники ДБР завершили досудове розслідування щодо кіберзлочинця. Фігурант обвинувачується у створенні та розповсюдженні шкідливих програмних засобів, несанкціонованому втручанні в роботу електронно-обчислювальних машин, легалізації майна (ч. 1 ст. 361-1, ч. 2 ст. 361, ч. 1 ст. 209 КК України). Зокрема, зловмисник за допомогою шкідливого програмного забезпечення та фішингу викрадав банківські й персональні дані громадян Канади та Сполучених Штатів Америки. Санкція статті передбачає покарання у вигляді позбавлення волі на строк до 6 років з конфіскацією майна [4].

З огляду на зазначене, варто вказати на Стратегічну програму ДБР на 2022–2026 рр., яка спрямовує основні зусилля ДБР на організацію системної та комплексної роботи щодо захисту таких життєво важливих інтересів людини і громадянина, суспільства і держави: протидія та розслідування злочинів проти основ національної безпеки, забезпечення правопорядку у військовій сфері, протидія організованій злочинності тощо [5]. Зауважимо, що в умовах інформаційного прогресу застосування ШІ у діяльності ДБР є перспективним напрямом, який можна сформулювати наступним чином:

1) профілактика кіберзлочинів – ШІ може використовуватись для виявлення прихованих зв'язків та патернів у кіберзлочинах. Аналіз даних може допомогти працівникам ДБР виявити схожі атаки, які можуть бути пов'язані з певною групою злочинців, та виявляти патерни, які можуть вказувати на майбутні погрози;

2) аналіз соціальних мереж – ШІ може використовуватись для аналізу соціальних мереж та виявлення прихованих зв'язків та патернів між злочинцями, терористами чи іншими протизаконними організаціями;

3) аналіз ринку злочинності – ШІ може використовуватися для аналізу ринку та виявлення прихованих патернів та зв'язків між різними чинниками, які впливають на вчинення злочинів;

4) діагностика злочинності – ШІ може використовуватись для аналізу даних та виявлення прихованих звязків між різними чинниками.

Система профілактики кіберзлочинів на основі ШІ створюється шляхом збору та обробки великої кількості даних про кібератаки та уразливості в системах безпеки. Ці дані використовуються для навчання алгоритмів машинного навчання, які можуть аналізувати та виявляти загальні риси у таких атаках. Далі система може використовувати ці знання для передбачення можливих атак та розробки стратегій захисту від них. Фахівці з кібербезпеки можуть використовувати ці моделі для визначення найбільш можливих загроз та вжиття відповідних заходів щодо захисту від них. Крім того, система може використовуватися для автоматичного виявлення та запобігання кібератакам.

Серед методів реалізації цих систем за допомогою ШІ можна виокремити: аналіз потоку даних – ШІ може аналізувати дані, які надходять на мережу, щоб виявити аномальні шаблони активності, які можуть вказувати на кібератаку; моніторинг та аналіз електронної пошти злочинця – ШІ може використовуватись для автоматичного моніторингу електронної пошти на наявність фішингових листів, спаму та вірусів; моделювання ситуації – ШІ може використовуватись для моделювання можливої ситуації у мережі та запобігання майбутнім атакам; блокування доступу – ШІ може бути налаштовано на автоматичне блокування доступу конкретним користувачам, якщо вони вважаються загрозою для безпеки мережі; обробка атак – ШІ може бути запрограмований для швидкої обробки атак та запобігання їх розповсюдженню на інші частини мережі; відновлення після атаки – ШІ може використовуватися для відновлення мережі після кібератаки, у тому числі автоматичного відновлення даних.

Усі перераховані вище методи можуть використовуватися для автоматичного виявлення та запобігання кібератак за допомогою ШІ. Штучний інтелект має великий потенціал у підвищенні ефективності в розслідуванні кримінальних справ.

Його активне застосування дозволяє підвищити якість та оптимізувати терміни розслідування. Проте, варто враховувати певні ризики, пов'язані з використанням ШІ в діяльності правоохоронних органів та забезпечити його належну нормативну регламентацію в кримінальному процесі, зокрема необхідним кроком закріплення на рівні чинного законодавства зміст поняття «спеціальні знання» та підготовка нормативно-правової бази для формування нової форми спеціальних знань – штучного інтелекту, що використовується у слідчій діяльності.

Утім, важливо розуміти, що ШІ не може замінити фахівців у галузі кібербезпеки. ІТ-технології необхідно використовувати тільки в комбінації можливо з більш повільнішим, але найбільш точнішим та ефективнішим засобом забезпеченням кібербезпеки – людиною, фахівцем. Саме тому, не зважаючи на те, що криміналістика – це «галузь фахівців», а сам ШІ ніколи не зможе досягти такого рівня, він слугуватиме лише допоміжним інструментом у боротьбі з організованою злочинністю, зокрема й кіберзлочинністю.

Список використаних джерел:

1. Стратегія розвитку штучного інтелекту в Україні : монографія / за заг. ред. А. І. Шевченка. Київ : ІПШІ, 2023. 305 с. URL: https://jai.in.ua/archive/2023/ai_mono.pdf (дата звернення: 09.03.2025).
2. Концепція розвитку штучного інтелекту в Україні : схв. розпорядженням Кабінету Міністрів України від 02.12.2020 № 1556-р. *База даних «Законодавство України»* / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 09.03.2025).
3. Про Державне бюро розслідувань. *Закон України* від 12.11.2015 № 794-VIII. *База даних «Законодавство України»* / ВР України. URL: https://zakon.rada.gov.ua/laws/show/794-19#Text (дата звернення: 09.03.2025).
4. За матеріалами ДБР судитимуть кіберзлочинця з Вінниці за викрадення даних з банківських карток іноземців. *Офіц. сайт Державного бюро розслідувань*. 7 лип. 2024 р. URL: https://dbr.gov.ua/news/za-materialami-dbr-suditimut-kiberzlochincya-z-vinnici-za-vikradennya-danih-z-bankivskih-kartok-inozemciv (дата звернення: 09.03.2025).
5. Стратегічна програма діяльності Державного бюро розслідувань на 2022-2026 рр. *Офіц. сайт Державного бюро розслідувань*. URL: https://dbr.gov.ua/assets/files/diyalnist/-strategichna-programa-diyalnosti/strategichna-prog.pdf (дата звернення: 09.03.2025).

Тарасюк С. М.,
доцент кафедри кримінального права і процесу,
доктор філософії
(ДНП «Державний університет "Київський авіаційний інститут"»)

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПРАКТИЧНІ АСПЕКТИ ТА ПЕРСПЕКТИВИ

Анотація. У статті розглядаються практичні аспекти використання технологій штучного інтелекту при у кримінальному провадженні. Досліджуються проблеми точності та надійності таких систем, а також їх обмеження в контексті українського кримінального судочинства. Визначаються основні виклики та рекомендації щодо підвищення ефективності використання штучного інтелекту в кримінальному судочинстві.

Ключові слова: штучний інтелект, кримінальне судочинство.

Постановка проблеми. Швидкий розвиток технологій штучного інтелекту (ШІ) відкриває нові можливості для юридичної практики у кримінальних провадженнях. Водночас постає низка питань, пов'язаних із точністю роботи ШІ та його обмеженнями. Особливо актуальним є дослідження можливостей застосування ШІ в умовах українського кримінального судочинства.

Мета тез полягає у дослідженні практичних аспектів використання штучного інтелекту в кримінальному провадженні, виявленні основних обмежень та перспектив такого використання в контексті українського кримінального судочинства.

Виклад основного матеріалу. Використання штучного інтелекту при підготовці захисту у кримінальному провадженні має низку потенційних переваг, серед яких: прискорення аналізу великих обсягів інформації, виявлення прихованих зв’язків між фактами, виявлення помилок у розрахунках, автоматизація рутинних процесів, пов'язаних з оформленням процесуальних документів, тощо. Однак існує ряд суттєвих викликів та обмежень, які необхідно враховувати при використанні таких технологій.

Проблема точності та надійності штучного інтелекту

Одним із суттєвих недоліків сучасних моделей ШІ є схильність до так званого "галюцинування" – генерації неправдивої або неточної інформації [1,2], яка подається як достовірна. Цей феномен є особливо критичним у контексті кримінального судочинства, де точність та достовірність інформації мають вирішальне значення.

Галюцинування ШІ може проявлятися у:

У контексті кримінального провадження, проблема "галюцинування" ШІ становить значну процесуальну загрозу і може проявлятися у:

- створенні неіснуючих судових "прецедентів" або викривленні практики Верховного Суду (наприклад, при аналізі складних юридичних питань ШІ може посилатися на неіснуючі постанови Пленуму ВС);
- некоректному цитуванні законодавчих норм, зокрема при роботі з КПК України, коли система може змішувати чинні норми з тими, що втратили силу внаслідок численних змін і доповнень;
- неправильній інтерпретації фактів справи, особливо при аналізі складних причинно-наслідкових зв’язків у матеріалах кримінального провадження;
- помилковому аналізі процесуальних документів, що може призвести до хибних висновків про дотримання або порушення процесуальних строків, порядку проведення слідчих дій тощо.

Для мінімізації ризиків, пов'язаних з «галюцинуванням» ШІ, необхідно:

- використовувати ШІ як допоміжний інструмент, а не як заміну професійного юридичного аналізу;
- перевіряти всю інформацію, згенеровану ШІ, з першоджерелами;
- застосовувати кілька незалежних моделей ШІ для перехресної перевірки інформації;
- постійно оновлювати моделі ШІ відповідно до змін у законодавстві та судовій практиці.

Наразі, ШІ може виконувати лише допоміжну функцію [3], як-то аналіз окремих процесуальних документів, письмових та електронних доказів, висновків експертів. Для мінімізації так званого ефекту “галюцинування”, необхідно надавати максимально точний контекст: чинні нормативно правові документи, зразки процесуальних документів, детально і точно поставлені завдання та звісно контекст, який надає мовній моделі ШІ більш точно виконати поставлене завдання.

Слід вказати, що розмір так званого “контекстного вікна” у безкоштовних або початкових Pro-версіях є недостанім для виконання більшості поставлених задач.

З практичної точки зору, для обробки об’ємних матеріалів кримінального провадження (що часто включають сотні сторінок доказів, протоколів, експертних висновків того) необхідно застосовувати спеціальні методи, які дозволяють штучному інтелекту працювати з великими обсягами тексту:

- **Налаштування моделей під конкретні завдання** (Fine-tuning) – адаптація системи штучного інтелекту до специфічного юридичного контексту, що значно підвищує точність аналізу процесуальних документів
- **Технологія доповненого пошуку** (RAG) – дозволяє системі автоматично звертатися до бази правових документів (кодексів, постанов Верховного Суду тощо) для перевірки своїх висновків
- **Спеціалізовані архітектури для обробки великих текстів** – технічні рішення, які дозволяють системі аналізувати одночасно весь обсяг матеріалів справи, що критично важливо для виявлення суперечностей у доказах

Другий підхід, який посилить можливості щодо використання у контексті кримінального судочинства[4]:

- **Створення тематичних баз даних** — організація документів за категоріями (докази, процесуальні документи, свідчення)
- **Двостадійний аналіз** — спочатку резюмування всіх документів, потім глибший аналіз ключових частин
- **Паралельний аналіз** — паралельна обробка різних частин справи з подальшим зіставленням результатів
- **Гібридний підхід** — використання ШІ для первинного аналізу та пошуку протиріч, з подальшим людським аналізом

Ми бачимо, що повноцінне впровадження ШІ для виконання завдань у кримінальних провадженнях потребує значних інвестицій у посилення

технічних можливостей та навчання користувачів спеціалізованим методам співпраці з моделями ШІ.

Наведені вище проблеми демонструють, що використання штучного інтелекту в українському кримінальному провадженні наразі супроводжується серйозними викликами, пов'язаними з проблемою "галюцинування" ШІ (генерації недостовірної інформації), технічними обмеженнями щодо розміру контекстного вікна та відсутністю належної нормативно-правової бази; для подолання цих перешкод необхідне впровадження локальних моделей ШІ з покращеними системами захисту даних, використання спеціальних технологій розширення контекстного вікна (Fine-tuning, RAG, моделі Transformer-XL), створення тематичних баз даних для навчання систем ШІ та розробка відповідної методологічної бази, що дозволить використовувати штучний інтелект як допоміжний інструмент у аналітичних задачах кримінального провадження при безумовному дотриманні принципів справедливого судочинства та захисту прав людини.

Список використаних джерел:

1. Google Cloud. "Responsible AI practices". URL: https://cloud.google.com/responsible-ai.
2. Anthropic. "Claude's Approach to Safety and Security". URL: https://www.anthropic.com/safety.
3. Блізнюк В. В. Можливості використання штучного інтелекту у кримінальному провадженні в Україні. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право»*. 2023. № 36. С. 180–189. https://doi.org/10.26565/2075-1834-2023-36-22.
4. Nguyen, P. T. (2023). The Use of Artificial Intelligence in Criminal Investigation and Trials in Europe and Some Countries: Experience for Vietnam. *Vietnamese Journal of Legal Sciences*. Vol. 8 (1). P. 55–77. DOI: 10.2478/vjls-2023-0003.

Терлецький А. В.,
викладач кафедри адміністративно-правових дисциплін,
доктор філософії
(Одеський державний університет внутрішніх справ)

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ВІЙНИ: МОЖЛИВОСТІ ТА РИЗИКИ

Стрімкий розвиток технологій штучного інтелекту (ШІ) відкриває широкі можливості для його застосування у різних сферах суспільного життя, зокрема у військовій та правовій практиці. В умовах повномасштабної війни, яку Російська Федерація розв’язала проти України, ШІ став не лише інструментом оборони, але й загрозою, яка використовується ворогом у гібридній війні.

З одного боку, штучний інтелект сприяє покращенню системи розвідки, автоматизації аналізу великих масивів даних, забезпеченню кібербезпеки та швидшому ухваленню рішень у критичних ситуаціях. Він також допомагає

виявляти ворожу інформацію в інформаційному просторі та протидіяти дезінформації.

З іншого боку, агресор активно використовує можливості ШІ для створення діпфейків, маніпуляції громадською думкою, а також для здійснення інформаційно-психологічних операцій (ІПСО). Відомими стали випадки поширення фальшивих відеозвернень від Президента України Володимира Зеленського, у яких ворог намагався деморалізувати українське суспільство.

Окрім того, спостерігається збільшення телефонних шахрайств із підміною голосу за допомогою ШІ, що використовується для отримання конфіденційної інформації або введення в оману українських громадян [1].

Так, на прикладі соціальної мережі Facebook розглянемо питання застосування ними штучного інтелекту. З виникненням соціальної мережі та реєстрації з метою використання величезної кількості користувачів, виникла проблематика «відсіювання» позитивного контенту від негативного (наприклад: шахрайство; пропаганда; дитяча порнографія, тощо…). Використання людської сили для фільтрації публікованого матеріалу була неефективною так як перевірка кожного публікованого контенту займає велику частину часу, що унеможливлює швидке публікування контенту для користувача, на початку розвитку Facebook програмно використовували фільтрації по ключовим словам (наприклад заборона на публікування слів насильницького характеру: вбий його; бий іноземців, тощо…), проте це частково вирішувало проблематику, так як негативні користувачі публікували малюнки з негативним контентом або замінювали певні букви на символи (наприклад замість «вбий його» – використовували «3bий YогO»), що унеможливлювало фільтрацію такого контенту якісно та вчасно. У 2021 році Facebook ввела новітню технологію штучного інтелекту для відсіювання непотрібної інформації для користувачів та перегляд рекомендацій за зацікавленості кожної особи окремо, для цього були введенні модерні системи штучного інтелекту які за налаштуванням адміністратора (працівники Facebook) та адміністратори певних спільнот (Наприклад спільнота «Україна – не росія») могли налаштовувати публікації коментарів та малюнки з метою відсіювання недоброзичливого контенту, а адміністратори Facebook застосовувати по замовчуванню фільтр який не дозволяє публікувати коментарі які мають негативний характер (Наприклад: матюкливі слова; розв’язування недоброзичливості щодо інших національностей, тощо…), адміністратор спільноти налаштовує окремий фільтр для неможливості публікування у своїй спільноті непотрібного та неправдивого контенту [2].

Таким чином, запровадження штучного інтелекту у Facebook стало ефективним рішенням для фільтрації контенту, що дозволило значно зменшити кількість шахрайських, пропагандистських та небезпечних матеріалів. Завдяки автоматизованим алгоритмам стало можливим не лише швидко ідентифікувати заборонений контент, але й адаптувати механізми модерації під конкретні потреби спільнот. Однак, попри значні досягнення у цій сфері, залишається

виклик щодо вдосконалення ШІ для боротьби з новими методами, які використовують порушники правил, особливо під час війни.

Також, штучний інтелект активно використовується Українськими спеціальними службами і для воєнних цілей, під час де окупації захоплених територій російською федерацією, на цих територіях часто залишаються організовані злочинні групи яких встановити особливо важко, для цього використовуються системи відео фіксації в які програмно влаштовані системи штучного інтелекту (Наприклад технології від компанії Clearview AI) та можуть ефективно та швидко виявити самозванця з подальшою метою його покарання відповідно до чинного законодавства України [3].

Отже, штучний інтелект відіграє ключову роль у сучасних умовах війни, допомагаючи як у фільтрації інформації, так і в ідентифікації загроз. Його використання значно підвищує ефективність безпеки, виявлення шахрайських дій та розпізнавання ворожих агентів. Використання штучного інтелекту несе не лише позитивні можливості, а й серйозні загрози, особливо в умовах воєнного стану, де використовується ШІ ворогом для маніпуляцій, поширення дезінформації та кібератак. Російська Федерація активно застосовує штучний інтелект у гібридній війні проти України, використовуючи його як інструмент інформаційного впливу, маніпуляцій та дестабілізації суспільства. Одним із ключових напрямів є створення та поширення пропагандистського контенту, що має на меті викривлення реальності, формування негативного емоційного фону серед українців, а також підрив довіри до державних інституцій та партнерів України. На відміну від платформ, які впроваджують жорсткі механізми модерації та фільтрації контенту на основі штучного інтелекту, таких як Facebook, де запроваджено суворі алгоритми виявлення дезінформації та маніпуляцій, інші соціальні мережі, зокрема TikTok, мають значно м'якші підходи до контролю за поширюваним контентом. Цим активно користуються російські пропагандисти та спецслужби. Вони застосовують штучний інтелект для створення відео, що підсилюють певні наративи, маніпулюють алгоритмами просування контенту та сприяють масовому поширенню дезінформації. Алгоритми TikTok орієнтовані на максимальне залучення аудиторії та вірусне розповсюдження контенту, що дає змогу пропагандистам швидко та ефективно поширювати фейки. Наприклад, з використанням нейромереж створюються відеоролики, в яких штучний інтелект імітує голоси українських лідерів, підроблює їхні заяви або фабрикує кадри нібито реальних подій. Це створює значну загрозу інформаційній безпеці, адже навіть обізнані користувачі можуть піддатися маніпуляціям, якщо контент виглядає переконливо. Окрім того, штучний інтелект використовується ворогом для аналізу поведінки українських користувачів у соцмережах. На основі зібраних даних складаються психологічні профілі, що дозволяють використовувати маніпулятивні матеріали та впливати на конкретні групи населення. Такі технології дозволяють проводити точковий інформаційний вплив, розпалювати паніку, сіяти недовіру та сприяти соціальній дестабілізації [4].

Таким чином, Росія використовує штучний інтелект не лише у військових діях, а й у кібервійні та пропагандистських кампаніях. Його застосування в неконтрольованих інформаційних просторах, таких як TikTok, створює серйозні виклики для України, вимагаючи комплексного підходу до протидії дезінформації та забезпечення кібербезпеки. Застосування штучного інтелекту в умовах війни має двоїстий характер: з одного боку, він є потужним інструментом для підвищення ефективності оборонних, розвідувальних і кібербезпекових заходів, а з іншого – створює серйозні загрози, коли використовується ворогом для ведення гібридної війни. Україна активно застосовує ШІ для виявлення ворожих агентів, автоматизації розвідки та інформаційної безпеки, що значно підсилює її обороноздатність. Водночас Російська Федерація використовує штучний інтелект для інформаційно-психологічних операцій, маніпулювання громадською думкою та проведення кібератак. Діпфейки, телефонні шахрайства з підміною голосу, фабрикація новин та алгоритмічне поширення пропагандистського контенту через неконтрольовані платформи, такі як TikTok, становлять серйозну загрозу національній безпеці України.

В умовах сучасних викликів критично важливо розробити ефективні механізми протидії ворожим інформаційним атакам, зокрема шляхом впровадження власних систем штучного інтелекту для виявлення та блокування дезінформації, посилення співпраці з міжнародними технологічними компаніями та підвищення цифрової грамотності громадян. Лише комплексний підхід дозволить Україні використати можливості штучного інтелекту для зміцнення безпеки та мінімізувати ризики, які несе його застосування ворогом.

Список використаних джерел:

1. Facebook видалив дипфейк-відео із Володимиром Зеленським. URL:https://tsn.ua/svit/facebook-vidaliv-dipfeyk-video-iz-volodimirom-zelenskim-20116. Html

2. We've built *new admin tools and experiences* to help you manage your community, moderate conversations and reinforce culture. URL: https://www.facebook. com/community/whats-new/new-tools-features-nurture-community/.

3. Штучний інтелект може бути ключем до перемоги України у війні – західні експерти. URL: https://www.radiosvoboda.org/a/ukrayina-shtuchnyy-intelekt-viyna/32785722.html.

4. Фабрика фейків. Як руйнує Україну «аполітичний» TikTok і чому фахівці вважають його небезпечнішим за анонімні телеграм-канали URL: https://nv.ua/ukr/ukraine/events/tiktok-chim-nebezpechniy-yak-vikoristovuye-rosiya-ta-do-chogo-shi-do-shpiguvannya-za-ukrajinoyu-50415505.html.

Тополевський Р. Б.,
доцент кафедри теорії, історії та
конституційного права
ННІ права та правоохоронної діяльності,
кандидат юридичних наук, доцент
(Львівський державний університет внутрішніх справ)

ФІЛОСОФСЬКО-ПРАВОВІ ЗАСАДИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ: ОСОБЛИВОСТІ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ

Розвиток штучного інтелекту (ШІ) є фундаментом сучасних тенденцій технологічного прогресу. Спроби впровадження ШІ в усі сфери суспільного життя неодмінно викликає потребу в юридичному осмисленні цієї проблематики, в тому числі щодо відповідальності за шкоду, спричинену внаслідок використання ШІ.

Філософсько-правовий аналіз проблеми відповідальності за шкоду, спричинену внаслідок використання ШІ ставить питання про те, хто виступає суб'єктом, який діє, а також про те, хто виступає суб'єктом, який має нести відповідальність. Так само як питання про те, чи вони співпадають?

Чинне право базується на оцінці дій фізичних осіб, які мають волю, мотив та спроможні усвідомлювати наслідки своїх дій або притягненні до відповідальності юридичних осіб, представники або працівники яких спричинили відповідну матеріальну шкоду. Проблемою, однак є те, що системи ШІ, засновані на алгоритмах машинного навчання, можуть приймати рішення не лише без прямого втручання людини, але й таким чином, що відповідна людина з якою взаємодіє ШІ не може передбачити результати такого рішення. І, відповідно, нам потрібно провести переосмислення щодо того, якою мірою існуючі підходи до юридичної відповідальності залишаються чинними у справах щодо ШІ.

Відповідно, нам слід спробувати відповісти на низку питань: 1) хто має нести юридичну відповідальність? 2) чи можна розглядати сам ШІ суб'єктом відповідальності? 3) яким чином юридична відповідальність розподіляється між розробниками ШІ, операторами ШІ та користувачами ШІ? 4) як можливе формування механізмів попередження та компенсації шкоди, спричиненої внаслідок використання ШІ?

Окремі питання виникають в рамках галузевих юридичних наук. Так, у кримінальному праві, зокрема постає питання, чи ШІ є об'єктом кримінальної відповідальності чи знаряддям злочину. В цивільному праві, зокрема, постає питання про розподіл відповідальності між особами, причетними до прийняття автономних рішень з боку ШІ. В адміністративному праві – яким чином необхідно врегулювати взаємодію ШІ та органів влади, якою мірою органи влади можуть застосовувати ШІ.

Разом із тим, без вирішення засадничих філософсько-правових проблем щодо ШІ навряд чи буде можливо рухатися далі. Йдеться, перш за все, про питання суб'єктності ШІ, правового статусу автономних систем, етичних меж їх застосування та ризиків, пов'язаних із передачею ключових рішень алгоритмам, однак не обмежуються ними. Таким чином, існує необхідність здійснити комплексний філософсько-правовий підхід до ШІ. Так, на онтологічному рівні слід з'ясувати як ШІ існує у правовій реальності, яке його

місце і взаємозв'язки як правового явища. На гносеологічному рівні потрібно з'ясувати, якою мірою ми можемо бути обізнаними щодо способів прийняття ШІ рішень, які матимуть правове значення. На антропологічному рівні вартує з'ясувати питання про те, яким чином використання ШІ може зачіпати права людини. На прагматичному рівні дослідження необхідно з'ясувати безпосередньо розподіл відповідальності між різними суб'єктами, залученими до створення, контролю та використання ШІ.

Традиційно, ШІ можна розглядати лише як інструмент, знаряддя подібне до комп'ютерних програм або механізмів. Відповідно, контроль та відповідальність покладатиметься на розробників, які створили відповідне програмне рішення, власників (які володіють ШІ або серверами, на яких розміщений ШІ та надають відповідні послуги), операторів (які використовують ШІ у своїй діяльності) та кінцевих користувачів (які отримують вигоду або несуть ризики). Цей підхід рішення ШІ не є самостійними, а є результатом певних дій фізичних та юридичних осіб.

Все ще залишається під питанням можливість концепції «електронної особи»[1, para.59f], яка передбачає формування нового суб'єкта права, який матиме спеціальну правосуб'єктність, використовуючи правову фікцію, подібну до концепції юридичної особи. Однак з розвитком і ускладненням ШІ можна прогнозувати повернення до одного з варіантів такого підходу, в тому числі за аналогією з правовим статусом тварин. В той же час питання майнової відповідальності може бути вирішене за допомогою системи обов'язкового страхування заподіяння шкоди з боку ШІ.

Вивчення цих питань є не лише академічним викликом, а й нагальною необхідністю для формування правового середовища, що відповідатиме реаліям цифрової епохи. Саме тому аналіз філософсько-правових засад застосування ШІ та особливостей юридичної відповідальності є критично важливим як для наукової спільноти, так і для практичних розробників нормативних актів у сфері права та технологій.

Разом із тим, підсумовуючи, можемо зазначити наступне:

1. Сучасна правова система не готова до повного визнання ШІ як суб'єкта юридичної відповідальності, ШІ залишається об'єктом права

2. Необхідне поєднання кримінальної, адміністративної та цивільно-правової відповідальності для притягнення фізичних та юридичних осіб, які спричинили правопорушення або шкоду, в тому числі, внаслідок розроблення та контролю ШІ.

3. Разом із тим, регулювання ШІ не може охоплюватися лише юридичними нормами, а потребує розроблення відповідних етичних норм та технічних правил та стандартів.

4. З урахуванням міжнародного досвіду, існує необхідність розробити в Україні комплексну модель притягнення до відповідальності за шкоду, спричинену внаслідок використання ШІ, в тому числі із залученням спеціальних правових механізмів, наприклад системи страхування від шкоди, заподіяної внаслідок використання ШІ.

5. Збереження контролю людини за використанням рішень, запропонованих ШІ залишається суттєвим елементом системи запобігання можливої шкоди.

Список використаних джерел:

1. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Official Journal of the European Union. 18.7.2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0051.

Троцький О. О.,
здобувач ступеня доктора філософії з права
(Державний університет інфраструктури та технологій)

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ ОБОРОННИХ ЗАКУПІВЕЛЬ В УМОВАХ ВІЙНИ: МОЖЛИВОСТІ ТА РИЗИКИ

В умовах воєнного стану державні інституції та механізми забезпечення функціонування державної системи зазнають суттєвих трансформацій, зумовлених необхідністю оперативного реагування на актуальні загрози. Особливого значення набуває сфера оборонної промисловості та оборонних закупівель, оскільки ці напрями зокрема впливають на забезпечення національної безпеки та обороноздатності держави. Зазначені процеси супроводжуються високою динамічністю і варіативністю, що обумовлені змінами глобальної геополітичної ситуації, ситуацією на лінії бойового зіткнення та внутрішньодержавними викликами, що постають перед країною в умовах збройного протистояння. Відтак ці процеси потребують гнучких правових механізмів, належного нормативного регулювання, здатного забезпечити ефективність та прозорість відповідних процедур.

Для налагодження та систематизації процесу оборонних закупівель вже сьогодні ми можемо спостерігати за залученням цифрових технологій, зокрема штучного інтелекту (ШІ). Це відкриває нові можливості для оптимізації складних бюрократичних процесів, забезпечуючи високу ефективність та оперативність задля своєчасного забезпечення виконання державного оборонного замовлення. Водночас, впровадження ШІ супроводжується значними ризиками, зокрема у сфері безпеки чутливої інформації та даних, що становлять державну таємницю.

Дана робота покликана аналізувати переваги та потенційні загрози, що можуть виникнути в процесі інтеграції ШІ у сферу оборонних закупівель.

Штучний інтелект дозволяє автоматизувати окремі процеси в механізмі закупівель та забезпечити їх прозорість на всіх етапах від надходження комерційних пропозицій потенційних контрагентів до служби державного замовника й до відвантажень необхідної номенклатури безпосередньо у підрозділі, який буде її застосовувати. Оперативність і злагодженість цих процесів є надзвичайно важливими в умовах ведення активних бойових дій,

коли постачання озброєння та техніки має відбуватись без жодних затримок, і навіть незначні прострочення зобов'язань можуть призвести до критичних наслідків на лінії бойового зіткнення (ЛБЗ).

За прикладом успішного застосування сучасних цифрових технологій для створення ефективної системи функціонування окремих процесів в оборонній сфері, ми можемо звернутися до інноваційної IT-системи DOT-Chain – від Державного оператора тилу, яка покликана автоматизувати управління тиловими потребами Збройних Сил України. Завдання системи полягає у спрощенні складних процесів, збільшенні проінформованості та підсиленні підтримки як збройних сил, так і постачальників.

Система DOT-Chain здатна значно скоротити час на постачання, вона відстежує статуси документів, а накладні завантажуються автоматично. Державний оператор тилу може швидко оплатити заявки, використовуючи електронні підписи сторін. Міноборони, отримуючи дані з системи, зможе оперативно коригувати потреби військових. Вона допомагає відслідковувати проблеми з постачанням і приймати рішення в реальному часі [1].

Застосування інформаційних алгоритмів зокрема дозволяє прогнозувати коливання вартості на необхідну продукцію військового призначення, аналізувати економічні та навіть геополітичні фактори, що формують або можуть впливати на ринок. Це дозволяє ефективніше працювати над детальним плануванням бюджетних витрат й управлінням фінансовими ризиками, забезпечуючи оптимальний розподіл в умовах обмежених ресурсів.

Варто зазначити, що особливості здійснення оборонних закупівель під час дії правового режиму воєнного стану визначає Постанова Кабінету Міністрів України № 1275. Відповідно до якої державні замовники закуповують більшість товарів, робіт і послуг без застосування конкурентних процедур, визначених Законами України «Про оборонні закупівлі» та «Про публічні закупівлі», укладаючи натомість прямі договори [2].

Алгоритми ШІ також здатні виявити у тендерах і майбутніх контрактах аномальні патерни, які стосуються корупційної складової. Це дозволяє знизити реальні та потенційні ризики корупційних зловживань та підвищити рівень прозорості й безпосередньої відповідальності учасників процесу закупівель. Такий контроль своєю чергою зміцнює і довіру до державних інституцій. Виявлення потенційно підозрілих схем дає змогу зменшити простір для маніпулювання результатами тендерів та забезпечити справедливу конкуренцію.

Ще однією перевагою застосування ШІ у сфері оборонних закупівель є можливість автоматизації, виявлення та попередження основних комплаєнс-ризиків. Співпраця з терористичними організаціями, знаходження потенційного контрагента у санкційних списках, наявність прострочених зобов'язань у постачанні продукції оборонного призначення, судові тяжби й фінансове становище постачальників. Ці складні та багаторівневі процеси перевірки та верифікації можливо автоматизувати із залученням алгоритмів, що

пришвидшує процеси, які в підсумку вплинуть на оперативність ухвалення рішень.

Варто вказати, на сьогодні в Україні відсутня повноцінна нормативно-правова база, що регулює використання ШІ у державних закупівлях, зокрема в оборонному секторі, що складає загрозу для обороноздатності та створює правові прогалини. Відсутність чітких правил і стандартів для інтеграції ШІ може призвести до зловживань як на етапі розробки програмного забезпечення, так і на етапі виконання оборонних державних замовлень. І задля вирішення проблематики передусім необхідно розробити відповідні регуляторні механізми, що забезпечать достатню правомірність, прозорість та ефективність використання технологій в оборонній сфері.

Крім того, слід враховувати, що залежність від технологій може створювати й нові ризики. Зростаюча автоматизація процесів закупівель знижує ймовірність людських помилок, однак надмірна залежність від ШІ може стати проблемою у разі технічних зламів, які можуть виникати у випадках кібератак чи внутрішнього збою алгоритмів. Технічні несправності щонайменше можуть призвести до серйозних порушень у виконанні державних оборонних замовлень й затримок у постачаннях. Що більше, становити загрозу національній безпеці. Людський фактор залишатиметься важливим у процесах прийняття рішень й контролю за застосуванням ШІ, що вимагає безперебійної підготовки фахівців та створення ефективної системи контролю.

Впровадження ШІ у сферу оборонних закупівель створює значні можливості для оптимізації процесів, покращення прозорості та зниження корупційних ризиків. Однак, разом з потенційними перевагами, необхідно враховувати і значні ризики, пов'язані з безпекою даних, правовими аспектами та технічними обмеженнями. Для успішної інтеграції ШІ у оборонних закупівлях необхідно розробити відповідну нормативно-правову базу, удосконалювати системи кібербезпеки та забезпечити баланс між технологічною ефективністю та людським контролем.

Список використаних джерел:

1. Офіційний сайт Міністерства оборони України. URL: https://mod.gov.ua/explanation/yak-koristuvatisya-novoyu-sistemoyu-dot-chain-ta-v-chomu-yiyi-korist

2. Постанова Кабінету Міністрів України «Деякі питання здійснення оборонних закупівель на період дії правового режиму воєнного стану» від 11 листопада 2022 р. № 1275 Директиви 2009/81/ЄС. URL: https://zakononline.com.ua/documents/show/510216756944.

Удовенко Ж. В.,
доцент кафедри кримінального та
кримінального процесуального права,
доктор юридичних наук, доцент
*(Національний університет
«Києво-Могилянська академія»)*

Галаган В. І.,
завідувач кафедри кримінального
та кримінального процесуального права,
доктор юридичних наук, професор,
(Національний університет
«Києво-Могилянська академія»)

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ, ЯКІ ОБРОБЛЯЮТЬСЯ СИСТЕМАМИ ШТУЧНОГО ІНТЕЛЕКТУ: ОКРЕМІ АСПЕКТИ

Питання застосування інтелектуальних систем у сфері кримінального провадження є відносно новим та недостатньо дослідженим. Незважаючи на значний інтерес з боку науковців та практичних працівників, досі не існує єдиного бачення щодо багатьох аспектів використання штучного інтелекту (ШІ) в цій сфері.

Основним документом, який був розроблений у 2018 році Радою Європи, є Європейська етична хартія щодо використання ШІ в судовій системі та її середовищі, яка закріплює 5 фундаментальних принципів використання ШІ:

1. Принцип поваги до фундаментальних прав: дотримання правила, що розробка та впровадження інструментів і послуг ШІ мають бути сумісними з основними/фундаментальними правами, більшість з яких перелічені та закріплені в Європейській конвенції з прав людини та в Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних.

2. Принцип недискримінації.

3. Принцип якості та безпеки: для обробки судових рішень і отриманих даних слід використовувати сертифіковані джерела та нематеріальні дані з моделями, розробленими міждисциплінарним способом, у безпечному технологічному середовищі.

4. Принцип прозорості, неупередженості та чесності.

5. Принцип «під контролем користувача»: слід виключити директивний підхід і забезпечити такі умови, щоб користувачі були поінформованими щодо своїх прав та всіх дій, які пов'язані з ними (обробка персональних даних) та мали можливість контролювати зроблений вибір [1, с. 7].

Водночас існує багато міжнародних ініціатив, спрямованих на сприяння розвитку та впровадження ШІ в кримінальному провадженні. Однією з таких ініціатив є план дій «Цифровізація для кращого правосуддя» на 2022-2025 роки, розроблений Європейською комісією Ради Європи з ефективності правосуддя (CEPEJ) [2]. Цей план дій є важливим кроком на шляху до створення єдиного правового простору в Європі, де цифрові технології використовують для підвищення ефективності та якості правосуддя. Він передбачає співпрацю між державами-членами Ради Європи з метою обміну досвідом та кращими практиками у сфері цифровізації правосуддя.

Наразі традиційні методи кримінального провадження подеколи виявляються недостатньо ефективними. Злочинність набуває нових форм, тож для правоохоронних органів з'являються нові виклики, що потребують сучасних технологічних рішень. ШІ є однією з таких технологій, яка може допомогти правоохоронним органам та судам у боротьбі зі злочинністю. Водночас, серед ключових питань, що потребують подальшого вивчення, можна виділити такі: Чи може ШІ бути суб'єктом права, тобто мати права та обов'язки? Якщо так, то яким чином це має бути врегульовано законодавчо? Хто несе відповідальність за рішення, прийняті за допомогою ШІ? Чи може бути покладена відповідальність на розробників програмного забезпечення, слідчих, суддів, які використовують такі системи, або ж на сам ШІ? Ці та інші питання, пов'язані з його використанням в кримінальному провадженні, потребують глибокого та всебічного вивчення з метою забезпечення його законності, справедливості та ефективності.

Поняття ШІ є широким та складним. Раніше нами вже був проведений розлогий огляд цієї проблематики, який мав на меті з'ясувати поняття ШІ; як змінюються правоохоронна та правнича сфери з огляду на поширення та все більшу доступність ШІ; у чому полягає роль держави, як регулятора та реалізації відповідної функції; яких правил мають дотримуватися розробники та користувачі; які аспекти використання ШІ вже доступні для правничої сфери та як може допомогти ШІ із прийняттям рішень (залишаючи, при цьому, саме за людиною провідну роль у їх постановленні та у виборі за наявних альтернатив) у перебігу кримінального провадження та які перспективи нас очікують [3, с.19-38]. Законодавче визначення цього поняття саме як «система» є, на наш погляд, досить вдалим. Штучний інтелект – потужний інструмент, але його використання потребує мудрості та відповідальності. Зокрема, наразі існує проблема «чорних скриньок» в ШІ [4], тобто непрозорості роботи системи, що може порушувати принцип транспарентності. Тож **спосіб, у який ШІ приймає рішення, має бути прозорим і доступним для розуміння людиною**.

Перш, ніж вдатися до активного застосування ШІ, особливо у правничій та правоохоронній царинах, важливо встановити чіткі межі й правила, а що не найостанніше – відповідальність за шкоду. Такі чутливі аспекти, як непорушність сфери людської приватності, дотримання прав людини тощо мають превалювати у цьому механізмі [5].

Продовжуючи дискурс, хочемо звернути увагу на етичні питання, пов'язані з використанням ШІ в кримінальному провадженні, зокрема питання захисту персональних даних. Забезпечення належного захисту персональних даних, що обробляються системами ШІ, є критично важливим завданням, особливо в умовах зростаючої цифрової трансформації та поширення технологій ШІ. На це вказує і звіт Уповноваженого з прав людини за 2023 рік про те, що нагально потребує оновлення законодавства про захист персональних даних [6]. Це підкреслив і Єгор Чернєв, народний депутат України, Заступник голови Комітету Верховної Ради України з питань національної безпеки, оборони та розвідки, вказавши, що українське

законодавство у сфері захисту персональних даних не оновлювалось вже понад 10 років. В умовах війни та суттєвого впливу інтернету на життя людей це питання стало актуальним як ніколи, що дозволить захистити права людей та виконати умови щодо європейської інтеграції України [7].

Стрімкий розвиток технологій, особливо ШІ, ставить перед суспільством нові виклики. Їхнє використання в різних сферах життя, зокрема і в кримінальному провадженні, вимагає чіткого правового регулювання, щоб гарантувати захист прав і свобод людини. Законність, справедливість, прозорість – ось три кити етичного використання ШІ в кримінальному провадженні.

Ця тема є надзвичайно актуальною для юридичної науки з кількох причин. Зокрема, існуюче законодавство часто не встигає за темпами розвитку технологій, оскільки з'являються нові способи збирання, обробки та використання персональних даних, що потребують правового регулювання. Необхідно знайти баланс між сприянням розвитку технологій та забезпеченням захисту прав і свобод людини. Занадто жорстке регулювання може стримати інновації, тоді як його відсутність може призвести до порушення прав людини.

У Дорожній карті з регулювання ШІ зазначено, що окремий об'єкт суспільних відносин, до якого ШІ має відношення, має охоплюватися своїм галузевим законодавством [8]. Реформування законодавства має бути комплексним та відповідати вимогам цифрової епохи. Уряд України пропонує регуляцію ШІ шляхом застосування тієї чи іншої галузі права, тобто удосконалення наявного законодавства, а не створення нового [4].

Ось деякі ключові аспекти та заходи, які необхідно враховувати для з**абезпечення належного захисту персональних даних, які обробляються системами ШІ:**

1. Законодавче та нормативне регулювання:

- імплементація загального регламенту про захист даних (GDPR) як одного із найвідоміших та найвпливовіших міжнародних документів у сфері захисту персональних даних, який встановлює жорсткі вимоги до обробки персональних даних, зокрема використання ШІ [9];
- кожна країна повинна мати власне законодавство, яке відповідає міжнародним стандартам та враховує особливості використання ШІ в різних сферах;
- окремі області, такі як охорона здоров'я, фінанси або освіта, можуть мати власні закони та регулювання, які стосуються обробки персональних даних за допомогою ШІ.

2. Принципи захисту персональних даних:

- обробка персональних даних повинна здійснюватися на законних підставах, бути справедливою та прозорою для суб'єктів таких даних;
- персональні дані повинні збиратися та оброблятися лише для чітко визначених та законних цілей;
- обсяг персональних даних, які обробляються, повинен бути мінімальним та відповідати заявленим цілям;

- персональні дані повинні бути точними та актуальними;
- персональні дані повинні зберігатися протягом обмеженого часу, який відповідає цілям їх обробки;
- персональні дані повинні бути захищені від несанкціонованого доступу, використання або розголошення.

3. Технічні та організаційні заходи:

- перед початком обробки персональних даних за допомогою ШІ необхідно провести оцінку ризиків для прав та свобод суб'єктів цих даних;
- використання методів мінімізації даних, таких як анонімізація або псевдонімізація, для зменшення обсягу персональних даних, які обробляють;
- встановлення суворого контролю доступу до персональних даних, включаючи використання шифрування;
- впровадження заходів для запобігання витоку персональних даних, таких як моніторинг безпеки, аудит та реагування на інциденти;
- проведення навчання для працівників, які працюють з системами ШІ, щодо принципів захисту персональних даних та вимог законодавства з цього питання.

4. Етичні аспекти:

- забезпечення прозорості використання ШІ в обробці персональних даних, включаючи інформування суб'єктів даних про те, як використовують їхні дані;
- встановлення чіткої відповідальності за прийняті рішення, які базуються на результатах роботи систем ШІ;
- забезпечення неупередженості алгоритмів ШІ та запобігання дискримінації за будь-якими ознаками;
- дотримання конфіденційності персональних даних та захист їх від несанкціонованого доступу.

Отже, використання ШІ в кримінальному провадженні є перспективним напрямом, який може значно підвищити ефективність та якість роботи правоохоронних органів. Проте, важливо враховувати етичні, юридичні та технічні аспекти, а також забезпечити прозорість та підконтрольність використання таких технологій. Лише за умови зваженого та відповідального підходу можливо досягти в кримінальному провадженні позитивних результатів та уникнути негативних наслідків. Для цього необхідно розробити чітке законодавче регулювання використання ШІ в кримінальному провадженні (як варіант – етичний кодекс використання ШІ), удосконалити наявне законодавство, зокрема Закон України «Про захист персональних даних», доповнивши його положеннями про ШІ як «третю сторону» в контексті обробки персональних даних; уточнити критерії порядку доступу третіх осіб до персональних даних; створити систему контролю за використанням ШІ, яка б гарантувала захист прав людини та забезпечувала відповідальність за прийняті рішення, зокрема повноцінний незалежний наглядовий орган за дотриманням законодавства про захист персональних даних; проводити навчання та підвищення кваліфікації працівників правоохоронних органів та суддів щодо

використання ШІ тощо. Важливо пам'ятати, що ШІ – це лише інструмент, який може допомогти у боротьбі зі злочинністю та забезпеченні правопорядку. Головне завдання держави та суспільства – забезпечити, щоб цей інструмент було використано на благо людини, не порушуючи її права та свободи, зокрема, з**абезпечуючи належний захист персональних даних з метою досягнення завдань кримінального провадження.**

Список використаних джерел:

1. European Commission for the Efficiency of Justice. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. *Council of Europe*. URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.
2. European Commission for the Efficiency of Justice. 2022 – 2025 CEPEJ Action plan: «Digitalisation for a better justice». *Council of Europe*. URL: https://rm.coe.int/cepej-2021-12-en-cepej-action-plan-2022-2025-digitalisation-justice/1680a4cf2c.
3. Басиста І. В., Удовенко Ж. В., Кулинич М. А. Огляд тенденцій щодо штучного інтелекту та його перспективність для процесуальних рішень у перебігу кримінального провадження. *Науковий вісник Ужгородського Національного Університету*. Серія право. 2024. Вип. 81, т. 3. С. 19–38. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/03/81_part3.pdf.
4. Остіян Є. З. Штучний інтелект та персональні дані: захист приватності в цифровому середовищі1 *Науковий вісник Ужгородського Національного Університету*, Серія «Право». 2024. Вип. 85, ч. 3. С. 47–53.
5. Удовенко Ж. В., Басиста І. В. Застосування штучного інтелекту у кримінальному провадженні: ілюзія чи реальність. *Штучний інтелект у правовій практиці :* матеріали круглого столу (Київ, 15 берез. 2024 р.). Львів : Львівський державний університет внутрішніх справ, 2024. С. 188–197.
6. Звіт Уповноваженого з прав людини за 2023 рік. URL: https://ombudsman.gov.ua/storage/app/media/uploaded-files/%D0%A9%D0%BE%D1%80%D1%96%D1%87%D0%BD%D0%B0_%D0%B4%D0%BE%D0%BF%D0%BE%D0%B2%D1%96%D0%B4%D1%8C_%D0%A3%D0%BF%D0%BE%D0%B2%D0%BD%D0%BE%D0%B2%D0%B0%D0%B6%D0%B5%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B7%D0%B0_2023_%D1%80%D1%96%D0%BA.pdf.
7. Захист персональних даних українців на часі – обговорення висновку ради Європи щодо проєкту Закону «Про захист персональних даних» № 8153 від 25.10.2022. URL: https://www.coe.int/uk/web/kyiv/-/protection-of-ukrainians-personal-data-is-on-time-an-expert-discussion-of-the-opinion-provided-by-the-council-of-europe-on-the-draft-law-no.-8153-of-25.10.2022-on-personal-data-protection-.
8. Регулювання штучного інтелекту в Україні: Мінцифри презентує Білу книгу. *Урядовий портал*. 2024. 30 с. URL: https://www.kmu.gov.ua/ news/rehuliuvannia-shtuchnoho-intelektuv-ukraini-mintsyfry-prezentuie-bilu-knyhu.
9. Загальний регламент про захист даних (GDPR). URL: https://gdpr-text.com/uk/.

Хілобок Д. Р.,
курсант факультету підготовки фахівців
для органів досудового розслідування
Національної поліції України
(Одеський державний університет внутрішніх справ)
Жуковський С. В.,

старший викладач кафедри тактико-спеціальної
та спеціальної фізичної підготовки
факультету підготовки фахівців
для підрозділів превентивної діяльності
(Одеський державний університет внутрішніх справ)

КОНФІДЕНЦІЙНІСТЬ ТА ПРИВАТНІСТЬ В СУЧАСНОМУ КІБЕРПРОСТОРІ

Чарлз Персі Сноу вказав на одну аксіому сучасності: «Технологія... це дивна річ, яка, з одного боку, приносить вам великі дари, а з іншого боку, завдає удару в спину».

У світі де-факто все стало пов'язаним, люди все більше залежними, та все це дуже легко стає вразливим та легкодоступним для будь-яких злочинців та навіть звичайних користувачів кіберпростору.

Одне із тлумачень «privacy», це «право бути наданим самому собі». Кожна людина має право на свій «власний куточок» у просторі, захищений від зазіхань із боку інших осіб [1]. Конфіденційність, можливо розуміти як суто приватність виключна особиста (приватна) інформація.

Інтернет світ – це в деякому понятті «квартира з відчиненими дверима… і вікнами», хоча існує певна ілюзія що в такому просторі, все є достатньо приватним й конфіденційним.

Протягом трьох з половиною століть у нашому світі панувала Вестфальська система міжнародних відносин [2]. Це означало, що незалежні національні держави мали бути суверенними в межах своїх територій, і жодна зовнішня влада не мала права втручатися у внутрішні справи іншої країни.

Вестфальська система зберігалась завдяки таким чинникам, як існування: 1) кордонів; 2) армій; 3) пропускних пунктів.

Для одночасного обмеження імміграції та еміграції здійснювалося державне регулювання відповідними службами. Крім того, щоб контролювати потік товарів через національні кордони, створювалися митні та інспекційні структури. Проте, яким би даром передбачення не були наділені ті, хто підписали Вестфальський договір у 1648 році, жоден з них не передбачав появи Snapchat1-у або TikTok-у та інших соціальних мереж..

Хоча фізичні кордони все ще мають значення для фізичного простору, таке розмежування в онлайновому світі набагато менш чітке і не є визначене. Біти та байти вільно перетікають з однієї країни до іншої без будь-яких прикордонників, без імміграційного контролю або митних декларацій, що мали б уповільнити їхнє проходження.

Для транснаціональної злочинності в онлайновому світі не існує традиційних бар'єрів, з якими стикалися колишні покоління злодіїв, і це дозволяє людям із сумнівною репутацією вільно входити у будь-яку ділянку віртуального простору, особливо що стосується приватної та конфіденційної безпеки.

Що стосується інформаційної приватності та конфіденційності, то вони завжди займали особливе місце у стосунках між людьми в кіберпросторі.

Основою є забезпечення захисту відомостей про людину від нецільового та несанкціонованого отримання/використання її персональних даних.

Виділяють наступні елементи права на інформаційну приватність: 1) право на самотність; 2) право на інтимність; 3) право на анонімність; 4) право контролювати інформацію про себе, а також 5) право «бути забутим» [3].

У законодавстві це передбачає наявність пріоритетних гарантій забезпечення умов приватности для будь-яких дій стосовно персональних даних, які повинні бути: 1) отриманими законним способом; 2) збиратися з відома й згоди особи, у кількості мінімально необхідній для певної мети; 3) бути точними й захищеними від несанкціонованого доступу; 4) використовуватися тільки з метою, заради якої вони були отримані; 5) надаватися третім особам тільки за згодою особи, про яку вони зібрані.

Усі ці норми права закріплені чинним національним та міжнародним законодавством, і де-юре мають захищатися як органами публічної влади, так і міжнародною спільнотою взагалі.

Однак важливо враховувати той факт, що норми можуть працювати, але за умови, що люди самі не починають «зливати» інформацію про себе в соціальні мережі й стають легкодоступними мішенями для шахраїв. Що під цим треба розуміти? Це великий комплекс дій особистості, який містить деякі дії, наприклад: оновлення статусу, розміщення цікавих роликів про себе чи друзів, зміна фотографій та геолокації, розміщення політичних, релігійних або інших поглядів, фото і відеоінформацію про родинні зв'язки та друзів або інформацію про місце проживання (що дуже важливо для злодіїв).

Таким чином, законодавство не має можливості забезпечити будь-який вид захисту приватних даних, якщо люди самі, «за власним бажанням» оприлюднюють в публічному просторі відомості щодо себе. Хоча й самі програмні продукти (застосунки і сайти), які знаходяться під керуванням державних органів, не мають відповідного рівня захисту від втручання сторонніх осіб.

Тому завданням не законодавства, а людей, є те, що необхідно ретельно ставитися до вибору відомостей, які викладаються в мережу, про приватні та конфіденційні дані особи, бо інформацію щодо вас можливо використовувати будь-яким чином і це може нашкодити не тільки морально та психологічно, а також фізично.

Список використаних джерел :

1. Privacy & Human Rights. Privacy International and Electronic Privacy Information Center, 1999. URL: www.epic.org.

2. Philip C. Cutler A. Critical reflections on the Westphalian assumptions of international law and organization: a crisis of legitimacy. Review of International Studies. 27.02.2001. P. 133–150.

3. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія за ред. В.М. Брижка, В.Г. Пилипчука. Київ. 2017. 226 с.

Цигульський С. М.,
заступник начальника
відділу організації наукової діяльності,
кандидат історичних наук
(Дніпровський державний університет внутрішніх справ)

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ПОНЯТТЯ ШТУЧНОГО ІНТЕЛЕКТУ

Наразі в Україні через повномасштабне вторгнення росіян головна увага суспільства прикута до проблем відсічі такій агресії, але у світі однією із основних тенденцій є впровадження штучного інтелекту у всі сфери життя, що викликає жваві дискусії серед дослідників стосовно його переваг і небезпек. В Україні у сфері освіти переваги та недоліки використання штучного інтелекту «відчули на собі» учасники освітнього процесу, особливо в питаннях академічної доброчесності. Не секрет, що здобувачі вищої освіти активно використовують можливості штучного інтелекту для того, щоб згенерувати унікальний текст задля виконання завдань, пов'язаних із відповідними освітніми програмами, натомість структурні підрозділи університетів, на яких покладене завдання із забезпечення академічної доброчесності (перевірка курсових проєктів тощо на наявність академічного плагіату із використанням антиплагіатних програм) зазнали проблеми, коли антиплагіатні системи не можуть виявити ознаки використання штучного інтелекту. Здобувачі вищої освіти не можуть отримати увесь необхідний обсяг освітніх послуг, оскільки програми штучного інтелекту виконують за них значний спектр завдань, виконання яких передбачає отримання певних компетентностей для здобувача.

Ефективне регулювання певних суспільних відносин, у нашому випадку у сфері використання штучного інтелекту, залежить від багатьох факторів, серед яких і наявність нормативно-правових актів, норми яких регулюють конкретні суспільні відносини. Базисом є понятійно-категоріальний апарат і розуміння змісту поняття певного явища. Для регулювання таких суспільних відносин важливо розуміти, який зміст законодавець вкладає в поняття штучного інтелекту, яке нормативне визначення такого поняття.

У 2024 р. Європарламент прийняв Закон про штучний інтелект як перший у світі нормативний акт, що комплексно регулюватиме суспільні відносини, пов'язані зі штучним інтелектом. Цей закон також схвалила Рада ЄС «Artificial Intelligence Act». У документі класифікується штучний інтелект за рівнем ризику завдання шкоди («неприйнятний», «високий», «обмежений» і «мінімальний»). У статті 3 Закону наведене визначення системи штучного інтелекту, що означає програмне забезпечення і може, для заданого набору визначених людиною цілей, генерувати результати, такі як: контент, прогнози, рекомендації або рішення, що можуть впливати на фізичне та віртуальне середовище [1, с. 16; 5].

Стосовно українського законодавства О. Кузьменко, В. Чорна та С. Островський зауважують, що питання правового регулювання діяльності штучного інтелекту вимагає комплексного підходу, який має забезпечувати захист прав людини та суспільних інтересів. Розробка і провадження ефективного правового механізму постає ключовим завданням для законодавців та юристів, а також міжнародного співтовариства. Правове регулювання штучного інтелекту, на думку дослідників, є критично важливим для забезпечення безпечного та етичного його використання [4, с. 177].

В Україні нормативне визначення штучного інтелекту міститься в Концепції розвитку штучного інтелекту в Україні: «штучний інтелект – 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» [2]. На нашу думку, таке важливе явище має бути закріплене на законодавчому рівні, а не на рівні підзаконного акту. С. Корнєєва зазначає з цього приводу, що серед дослідників, які вивчають питання правового регулювання застосування штучного інтелекту, існують дві основні концепції: «Одна група науковців пропонують розроблення нових нормативно-правових актів в рамках існуючих галузей права… Інший підхід передбачає розробку абсолютно нової галузі права, яка покликана регулювати використання ШІ, відповідальність за розробку та використання таких технологій» [3, с. 55].

Отже, ми вважаємо, що чинне питання нормативного регулювання суспільних відносин у сфері штучного інтелекту вимагає законодавчого закріплення. Акцентуємо увагу на тому, що окремо у сфері вищої освіти потребує нормативного регулювання процедура застосування штучного інтелекту в освіті та наукових дослідженнях, у законодавстві щодо академічної доброчесності. Необхідно встановити чіткі межі застосування штучного інтелекту у зазначених напрямах задля того, щоб не нашкодити якості надання освітніх послуг, не порушувати норми академічної доброчесності. Водночас підкреслимо, що необхідно визначити ті форми використання штучного інтелекту, які сприятимуть навчанню здобувачів та науковим дослідженням.

Список використаних джерел:

1. Гелецька І. О., Шовдра М. М. Визначення поняття «штучного інтелекту» та його місце у системі цивільного законодавства України. *Галицькі студії*: *юридичні науки*. 2024. Вип. 6. С. 13–19.

2. Концепція розвитку штучного інтелекту в Україні : схвалено розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.

3. Корнєєва С. Р. Теоретичні підходи до визначення поняття та правового регулювання штучного інтелекту. *Науковий вісник Ужгородського національного університету*. *Серія : Право.* 2021. Вип. 66. С. 50–55.

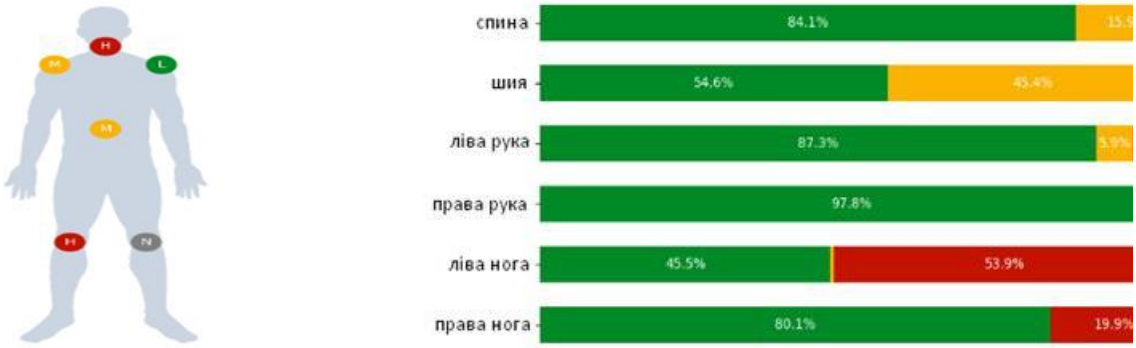
4. Кузьменко О., Чорна В., Островський С. Правове регулювання запровадження та використання штучного інтелекту. *Київський часопис права*. 2024. № 1. С. 173–177.
5. Artificial intelligence act. a9-0188/2023. Url: https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808_EN.pdf.

Цимбал Б. М.,
професор кафедри охорони праці
та екологічної безпеки,
доктор наук з державного управління, доцент
(Національний університет цивільного захисту України)
Свіржевський П. В.,
здобувач навчально-наукового інституту
управління та безпеки населення
(Національний університет цивільного захисту України)

ДОСЛІДЖЕННЯ ЕРГОНОМІЧНИХ РИЗИКІВ САПЕРІВ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

SoterTask – інноваційний інструмент, що використовує відеоаналіз для проведення ергономічної оцінки завдань. SoterTask – це сучасна розробка, яка працює на основі штучного інтелекту й не потребує спеціального обладнання чи датчиків. Головна перевага – автоматизація процесу оцінки: замість традиційного спостереження алгоритми аналізують рухи людини, що дає змогу отримати об'єктивні та точні результати [1].

За допомогою даного інструменту були досліджені ергономічні ризики саперів під час розмінування на відкритій місцевості. Під час дослідження було встановлено, що група ризику визначена як середня, а максимальний бал REBA становить 8, що свідчить про високий рівень небезпеки. Загальний ризик за показниками Soter також оцінюється як середній.



а б

Рисунок 1. Ергономічна оцінка ризиків під час розмінування:
а – група ризику за частинами тіла та б – розподіл часу за ризиком положення тіла

Розподіл ризиків за частинами тіла показує, що шия та ліва нога мають високий рівень ризику. Спина та ліва рука зазнають середнього ризику, тоді як права рука має низький ризик, а права нога – відсутність ризику (рис. 1).

Першою небезпекою є тривале згинання та присідання саперів. Вони часто виконують згинальні рухи та присідання під час огляду землі, що створює значне навантаження на поперек та колінні суглоби (рис. 2.а). Тривале

перебування в такій позі може викликати порушення опорно-рухового апарату, включаючи біль у попереку та можливі травми колін. Рівень ризику оцінюється як високий (части критичний). Для мінімізації навантаження доцільно використовувати оглядові пристрої з довгими ручками, що дозволяють уникати частого згинання. Також важливо навчати саперів правильній техніці згинання та передбачити регулярні перерви для зменшення навантаження.

а б

Рисунок 2. Результати оцінки ергономічних ризиків саперів:
а – розмінування; б – підрив

Наступною небезпекою є повторювані рухи руками. Робота передбачає часте використання металошукачів та інших інструментів, що спричиняє безперервні рухи руками відповідно до рис. 2.б. Це може призвести до перевантаження м’язів плечей, ліктів та зап’ясть, особливо для лівої руки, яка відноситься до групи середнього ризику. Рівень ризику оцінюється як серйозний (частий, граничний). Для зниження ризику необхідно використовувати ергономічні інструменти, що зменшують потребу у повторюваних рухах. Додатково слід впровадити чергування завдань між членами команди, щоб рівномірно розподілити фізичне навантаження. Важливим також є навчання правильним методам роботи з інструментами.

Третьою небезпекою є ходьба по нерівній місцевості. Переміщення по нерівному рельєфу створює ризик спотикання, послизнення та падіння. Це може призвести до травм, таких як розтягнення зв’язок, переломи або інші ушкодження опорно-рухового апарату, зокрема ніг. Рівень ризику оцінюється як середній (іноді незначний).

Для зниження небезпеки слід використовувати відповідне взуття з хорошою підтримкою щиколоток і нековзкою підошвою. Додатково рекомендується проводити регулярні оцінки місцевості, позначати небезпечні ділянки та навчати саперів техніці безпечного пересування по складній місцевості.

Було проведене ще одне дослідження з оцінкою роботи саперів у лісній місцевості. Дослідження показує, що група ризику визначена як середня, а максимальний бал REBA становить 8, що свідчить про високий рівень небезпеки. Загальний ризик за показниками Soter також оцінюється як середній.

Розподіл ризиків за частинами тіла показує, що шия має високий рівень ризику. Спина та права рука зазнають середнього ризику, тоді як ліва рука, права нога та ліва нога відповідно мають низький рівень небезпеки.

Небезпекою є тривале нахиляння та стояння на колінах (рис. 3.а). Сапер часто нахиляється та стає на коліна під час огляду землі, що створює значне навантаження на поперек та коліна. Тривале перебування в такій позі може викликати порушення опорно-рухового апарату, включаючи біль у попереку та можливі травми колін. Рівень ризику оцінюється як високий (частий, критичний). Для мінімізації навантаження рекомендується використовувати оглядові пристрої з довгими ручками, що дозволяють уникати частого згинання та стояння на колінах. Також варто навчати саперів правильної механіки тіла та передбачити регулярні перерви для зменшення напруження.

Наступною небезпекою є повторювані рухи руками. Часте використання портативних пристроїв створює ризик перенапруження м'язів рук, особливо правої, яка має середній рівень ризику. Це може призвести до професійних захворювань, таких як тендиніт або синдром зап'ястного каналу. Рівень ризику оцінюється як серйозний (частий, граничний). Для зниження навантаження рекомендується використовувати ергономічні пристрої, що зменшують потребу в повторюваних рухах. Також варто впровадити ротацію робочих місць для розподілу фізичного навантаження та забезпечити навчання ергономічним технікам. Додатково слід заохочувати регулярні вправи на розтяжку.

Третьою небезпекою є напруження шиї від постійного погляду вниз. Сапер часто дивиться вниз, оглядаючи землю, що спричиняє значне навантаження на м'язи шиї. Тривале згинання шиї може спричинити хронічний біль та порушення опорно-рухового апарату відповідно до рис. 3.б.

а б

Рисунок 3. Результати оцінки ергономічних ризиків саперів:
а – робота з металошукачем; б – саперною лопаткою

Рівень ризику оцінюється як серйозний (часті, граничні). Для мінімізації цього ризику рекомендується використовувати інструменти з регульованими ручками, що дозволяють підтримувати більш нейтральне положення шиї. Також важливо навчати саперів ергономічним методам підтримки правильної постави та заохочувати регулярні перерви для розслаблення м'язів.

Список використаних джерел:
1. This AI Vision Processing Technology Assesses Task in Minutes. *Home EHS Today*. URL: https://www.ehstoday.com/sponsored/article/21174205/this-ai-vision-processing-technology-assesses-tasks-in-minutes-on-the-go (дата звернення: 25.02.2025).

Цицик О. І.,
кандидатка юридичних наук,
доцентка кафедри адміністративного-правових дисциплін
ННІ права та правоохоронної діяльності
(Львівський державний університет внутрішніх справ)

ОСНОВНІ ЗАСАДИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ДІЯЛЬНОСТІ ТА ФУНКЦІОНУВАННІ ТЕРИТОРІАЛЬНОЇ ГРОМАДИ

Важливим для сучасного ефективного розвитку будь-якого суспільства і для держави зокрема виявилося створення штучного інтелекту. Це одна із останніх розробок технічної революції, яка увійшла майже у всі сфери життєдіяльності людини. Інноваційні технології до яких належить штучний інтелект значно підвищують ефективність будь-якої діяльності як людини так і системних утворень держави, також й таких як територіальна громада й безпосередньо такої діяльності, яка стосується її управління.

Проте, як будь-яке нове явище - штучний інтелект не позбавлений певних неточностей та недоліків. Тому, наша увага буде зосереджена на позитивних та негативних чинниках в процесі використання основних засад штучного інтелекту в діяльності територіальних громад.

В першу чергу розглядаючи засади функціонування штучного інтелекту потрібно наголосити на тому, що використання такого виду цифрових технологій передбачає певну стратегію та практику його найефективнішого виростання в управлінні територіальних громад.

Як зазначає А. Мацерук, щодо участі громади в діяльності держави, що вона є важливою складовою у прийнятті рішень та визначенні пріоритетів для її соціально-економічного розвитку та держави, зокрема, а також вбачає громаду як складний структурний організм зі множинними процесами її функціонування, що вимагає постійної унормованості та оптимізації механізмів її позитивного розвитку [1, с. 114–115].

І для такого ефективного функціонування та реальної дієвості територіальної громади в нагоді стають сучасні методи управлянні, які використовують новітні інформаційні технології для покращення своєї життєспроможності. Безперечно, що штучний інтелект володіє якісно новими методами, які допоможуть урегулювати та покращити управління громадами, що в свою чергу сприятиме швидкому та ефективному процесу вирішення конфліктів та спірних питань, які так чи інакше виникають в процесі існування територіальної громади.

Нами виділено декілька основних засадничих аспектів використання ШІ під час керування та функціонування територіальної громади. Розглядаючи штучний інтелект як систему, яка містить сукупність інформаційних технологій, здійснює обробку інформації на основі якої самостійно (за рахунок оптимізації отриманої чи самостійно створеної під час свої робити обробки значної доступної інформації) створює та приймає нові рішення у вирішенні проблем та питань. Така особливість штучного інтелекту дає можливість швидко та якісно отримати потрібне рішення за рахунок обробки та підбору найефективнішої інформації для прийняття відповідного найоптимальнішого рішення. Проте є в цьому аспекті, на нашу думку, і певна ключова вимога, яка полягає в тому, щоб під час прийняття таких рішень обов'язково мають бути враховані та дотриманні права та свободи людини, забезпечено гарантованість верховенства права та дотримання демократичних принципів.

Важливу роль штучний інтелект також може відігравати й під час поставлення цілей та завдань для тієї чи іншої територіальної громади [2, с. 2], адже здійснивши розрахунок (за допомогою інформації) потенційних можливостей (економічних, соціальних, екологічних, культурних тощо) громади (а в кожної громади він різний) ми можемо вибудувати дієву та структурезовану модель функціонування територіальної громади, яка принесе максимальну користь як на соціально-економічному рівні її розвитку, так і в цілому на державно-правовому.

Цифровізація, яка зараз ефективно впроваджується та відбувається в Україні - реальний дієвий приклад використання інформаційних технологій в розвитку доступності громадян до реалізації своїх чисельних прав та можливосте, та у використанні й наданні різних електронних послуг (адміністративних, управлінських, економічних, податкових, соціальних тощо). Про ефективність та доступність такого цифрового впровадження свідчать, навіть наші громадяни, які вимушено опинилися за кордоном у зв'язку із війною.

Також, наприклад, на всіх офіційних українських сайтах територіальних громад активно популяризується та пропонується інформація щодо ознайомлення зі ШІ та його використанням у різних сферах: робота ШІ з відкритими даними «Мовні моделі», основи штучного інтелекту (зокрема для ветеранів з інвалідністю), відео курси та уроки для молоді «Майбутні лідери ШІ» та багато інших [3]. На нашу думку, це свідчить про те, що територіальні громади нашої держави йдуть в ногу з часом та опановують новітні технологічні можливості, які однозначно покращують їхню діяльність.

Також, на нашу думку, базові основи на яких ґрунтується штучний інтелект полягають в тому, що він не знецінює людські можливості, а навпаки користуючись всіма інформаційними знаннями, які створила людини може запропонувати ту чи іншу модель вирішення чи врегулювання правовідносин. Проте ключовим в такій використовуваній цифровій моделі залишається прийняття рішення, яке завжди залишається за суб'єктом його прийняття, тобто за людиною.

Безперечно, засадничі основи використання штучного інтелекту базуються на принципі швидкості та зручності щодо отримання потрібної інформації на основі якої, особа сама створює рішення чи бере вже створену штучним інтелектом модель вирішення потрібного питання.

Дуже актуальним та однозначно не дослідженими в ШІ залишається питання наділенності його свідомістю. У більшості штучний інтелект лише узагальнює величезну базу інформації, до якої він має доступ, проте самосвідомістю не володіє, що є полем для подальших дискусій та його вивчення.

Штучний інтелект має великий потенціал для розвитку будь-якого явища, зокрема й для територіальної громади та її функціонування й дієвості. Проте потрібно пам'ятати, що ШІ не замінює людського розуму та взаємостосунків між людьми, що так важливо у побудові функціоналу територіальних громад, при цьому також потрібно розуміти та сприймати результати надані штучним інтелектом критично та раціонально здійснювати їхнє оцінювання.

Список використаних джерел:

1. Мацерук А. Застосування штучного інтелекту в контексті сталого розвитку громад. *Вісник Хмельницького національного університету*. 2024. № 2. С. 114–120.

2. Панчишин Т. В., Вдовин М. Л. Компоненти сталого розвитку територіальних громад та регіонів в умовах суспільно-політичних викликів. *Економіка і суспільство*. 2023. Вип. 50. С. 1–10. URL: https://economyandsociety.in.ua/index.php/journal/article/view/2379/2300.

3. Штучний інтелект. Дія. Цифрова освіта. URL: https://osvita.diia.gov.ua/courses/artificial-intelligenc.

Цуркан І. О.,
курсант 2 курсу навчально-наукового інституту № 4
(Харківський національний університет внутрішніх справ)
Манжай О. В.,
завідувач кафедри протидії кіберзлочинності,
кандидат юридичних наук, професор
(Харківський національний університет внутрішніх справ)
https://orcid.org/0000-0001-5435-5921

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

У сучасному цифровому світі кіберзлочинність стала однією з найсерйозніших загроз безпеці націй, підприємств та інших спільнот. З розвитком технологій кіберзлочинці використовують дедалі складніші методи для здійснення атак, що ускладнює їх виявлення та розслідування. Разом із тим, під час виконання оперативно-службових завдань працівниками поліції нерідко виникає потреба у визначенні місця, де було зроблено певні фотознімки, а

також у встановленні особи, яка їх створила. Звичайний пошук в інтернеті часто не дає бажаного результату, проте сучасні розробки на основі ШІ пропонують ефективні інструменти для вирішення таких завдань. Отже, доцільно проаналізувати роботу чотирьох подібних програмних рішень, щоб оцінити їхню ефективність у боротьбі з кіберзлочинністю та забезпеченні правопорядку.

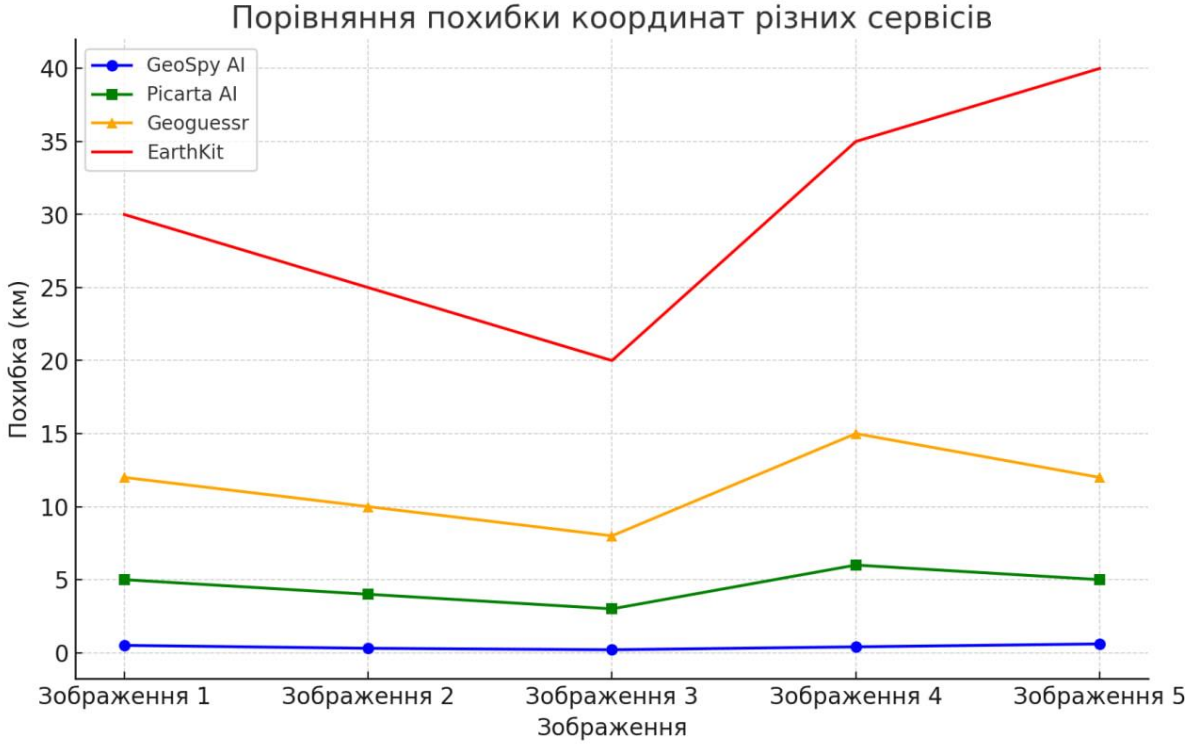
У нашому дослідженні були використані: GeoSpy AI [1], Picarta AI [2], Geoguessr [**Ошибка! Источник ссылки не найден.**], EarthKit [4].

Зображення	Сервіс	Визначена координата	Похибка (км)	Точність (%)
1	GeoSpy AI	48.8566°N, 2.3522°E	0,5	99
	Picarta AI	48.85°N, 2.35°E	5,1	90
	Geoguessr	48.80°N, 2.30°E	12	80
	EarthKit	48.60°N, 2.00°E	29,4	60
2	GeoSpy AI	40.7128°N, 74.0060°W	0,3	99.5
	Picarta AI	40.70°N, 74.00°W	4,1	92
	Geoguessr	40.65°N, 73.95°W	9,7	85
	EarthKit	40.50°N, 73.80°W	22,6	65
3	GeoSpy AI	35.6895°N, 139.6917°E	0,2	99.8
	Picarta AI	35.68°N, 139.69°E	3	95
	Geoguessr	35.60°N, 139.60°E	8,4	85
	EarthKit	35.50°N, 139.50°E	20,2	70
4	GeoSpy AI	51.5074°N, 0.1278°W	0,4	99.2
	Picarta AI	51.50°N, 0.12°W	5,8	88
	Geoguessr	51.40°N, 0.10°W	15	78
	EarthKit	51.20°N, 0.05°W	36,6	55
5	GeoSpy AI	34.0522°N, 118.2437°W	0.6	98.5
	Picarta AI	34.05°N, 118.24°W	5	90
	Geoguessr	34.00°N, 118.20°W	11,9	80
	EarthKit	33.80°N, 118.00°W	41,7	50

На основі отриманих результатів тестування різних сервісів геолокації за зображенням можна зробити детальний аналіз їхньої ефективності. GeoSpy AI показує найкращі результати за точністю визначення координат, ідентифікуючи зображення місцевості в районі Coalinga, Каліфорнія, з мінімальним відхиленням. Його алгоритм точно розпізнає тип місцевості, враховуючи природні особливості та інфраструктурні об'єкти. Picarta AI також знаходить

правильну область, однак дає кілька варіантів локації з різною точністю, що зменшує його ефективність у порівнянні з GeoSpy AI. Geoguessr визначає загальний регіон, однак допускає більшу похибку в координатах, припускаючи, що зображення було зроблене поблизу Bakersfield. EarthKit хоча і правильно ідентифікує Каліфорнію, але його припущення менш точні, оскільки він вказує значно ширшу область.

GeoSpy AI вигідно відрізняється точністю координат, здатністю ідентифікувати конкретні міста та місцевості, а також розширеним аналізом характеристик місцевості, таких як рослинність, структура ґрунту і наявність специфічних об'єктів (наприклад, нафтових насосів). Це дозволяє робити точніші припущення навіть у випадку зображень з обмеженими географічними підказками.



Графік демонструє рівень похибки у визначенні координат для чотирьох сервісів: GeoSpy AI, Picarta AI, Geoguessr та EarthKit. GeoSpy AI стабільно забезпечує найменшу похибку, яка не перевищує 1 км на всіх п'яти зображеннях. Це означає, що сервіс працює з найвищою точністю, аналізуючи особливості місцевості, знаки, дорожню розмітку та інші візуальні елементи. Picarta AI має дещо вищу похибку в межах 3-6 км, що свідчить про обмежену здатність деталізованого аналізу. Geoguessr демонструє ще більшу похибку, яка коливається від 8 до 15 км, що вказує на значну неточність у визначенні локацій. Найгірший результат має EarthKit, де похибка досягає 40 км, роблячи цей сервіс непридатним для точного геолокаційного аналізу. Обираючи GeoSpy AI, ми гарантуємо мінімальну похибку, швидкість обробки та надійність визначення координат, що робить його беззаперечним лідером серед представлених сервісів.

GeoSpy AI може стати потужним інструментом для розслідування кіберзлочинів завдяки своїм можливостям у геолокаційному аналізі зображень

[5]. Використовуючи алгоритми штучного інтелекту, цей сервіс дозволяє визначати місцезнаходження за фото, що може допомогти у відстеженні злочинців, розпізнаванні місць злочину або аналізі доказів.

Одним із ключових застосувань є виявлення місця зйомки зображень, які використовуються у шахрайських схемах або незаконному контенті [6]. Наприклад, якщо злочинці завантажують фото в даркнет або соціальні мережі, аналіз середовища, архітектури, дорожніх знаків і навіть природних особливостей може допомогти встановити географічне розташування. Це може бути корисним для правоохоронних органів у виявленні місць, пов'язаних із незаконною діяльністю [7].

Також цей сервіс може бути ефективним у виявленні нелегальних операцій, пов'язаних із торгівлею людьми чи контрабандою. Виявлення схожих локацій на основі аналізу великої кількості зображень допомагає побудувати зв'язки між злочинними угрупованнями та визначити маршрути їхнього пересування.

Використання штучного інтелекту в розслідуванні кіберзлочинів значно підвищує ефективність роботи правоохоронних органів і аналітиків. GeoSpy AI демонструє високу точність аналізу зображень і дозволяє ідентифікувати місця подій із великою деталізацією. Його здатність розкривати шахрайські схеми та аналізувати метадані робить його незамінним інструментом у сфері кібербезпеки. Завдяки передовим алгоритмам і доступності, GeoSpy AI є найкращим вибором для глибокого аналізу геолокаційних даних у контексті розслідування кіберзлочинів [8].

Список використаних джерел:

1. GeoSpy AI. URL: https://geospy.ai/ (дата звернення: 10.03.2025).
2. Picarta AI. URL: https://picarta.ai/ (дата звернення: 10.03.2025).
3. GeoGuessr GPT. URL: https://chatgpt.com/g/g-brlHi7t2R-geoguessr-gpt (дата звернення: 10.03.2025).
4. EarthKit. URL: https://earthkit.app/ (дата звернення: 10.03.2025).
5. GeoSpy AI у криміналістиці. URL: https://cybercrime.org (дата звернення: 10.03.2025).
6. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. URL: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/?utm_source=chatgpt.com (дата звернення: 10.03.2025).
7. Що таке ШІ для кібербезпеки. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-ai-for-cybersecurity?utm_source=chatgpt.com (дата звернення: 10.03.2025).
8. Вплив штучного інтелекту на сферу кібербезпеки. URL: https://softico.ua/uk/news/vpliv-shtuchnogo-intelektu-na-sferu-kiberbezpeki/?utm_source=chatgpt.com (дата звернення: 10.03.2025).

Шаповалова К. І.,
заступниця начальника відділу
зв'язків з громадськістю Управління патрульної поліції
у Львівській області, капітан поліції
(Департамент патрульної поліції)

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ЕЛЕМЕНТ АДМІНІСТРАТИВНОГО КОНТРОЛЮ: НОВІТНІ МЕХАНІЗМИ ДОТРИМАННЯ ПРАВ ЛЮДИНИ В ПОЛІЦІЇ

У сучасному світі технології розвиваються з неймовірною швидкістю, і штучний інтелект (ШІ) стає невід'ємною частиною нашого життя, проникає в усі сфери діяльності, змінюючи їх на краще. Однак, разом із новими можливостями, ШІ приносить і певні виклики. Відомий історик та філософ Ювал Ной Харарі зазначає: «Ми повинні розуміти, що штучний інтелект є першою технологією в історії, яка може самостійно приймати рішення… Нам потрібно переконатися, що ШІ приймає правильні рішення щодо нашого життя» [1]. Це означає, що впровадження ШІ потребує відповідального підходу та чіткого регулювання. 1 серпня 2024 року набув чинності Закон Європейського Союзу про ШІ (EU AI Act), який спрямований на сприяння відповідальному використанню та розвитку штучного інтелекту в ЄС [2]. Україні теж необхідно законодавчо врегулювати механізм використання ШІ у всіх сферах діяльності суспільства, зокрема, для того щоб забезпечити прозорість і дотримання прав людини. Серед усіх сфер суспільного життя, де можливе використання ШІ, його впровадження в діяльність правоохоронних органів має особливий потенціал для підвищення ефективності, забезпечення прозорості та дотримання прав людини. Оскільки держава має не лише гарантувати дотримання прав людини, закріплюючи це на законодавчому рівні, але й розробляти ефективні механізми дотримання цих прав.

Одним із яскравих прикладів використання штучного інтелекту в роботі поліцейських стала система Soze, яку створили в Австралії та почали використовувати у Великобританії. Її тестування показало, що цей аналізатор поліцейських даних здатен виконати 81 рік детективної роботи всього за 30 годин. Він здатний одночасно аналізувати відеозаписи, фінансові транзакції, соціальні мережі, електронні листи та інші документи, та на основі цього аналізу виявляти неочевидні закономірності та потенційні сліди, які могли бути пропущені під час традиційного аналізу доказів, які робить людина. Тестування Soze показало, що система може переглянути матеріали у 27 складних справах лише за 30 годин, тоді як для звичайного слідчого на це потрібно було б потратити понад 80 років. Використання інструментів розпізнавання обличь – це іще одна технологія, яка допомагає у роботі поліції. Поліція Лондона активно використовує технології розпізнавання обличь в режимі реального часу (LFR – Live Facial Recognition). Якщо в Лондоні та окремих штатах в США використовують інструменти розпізнавання для виявлення злочинців, то в

Південній Кореї пішли дані – там нещодавно запустили систему «Dejaview», яка може аналізувати дані камер відеоспостереження та виявляти злочини до їх скоєння та навіть запобігати їм. Технології штучного інтелекту в поліції можуть стати потужним інструментом для підвищення безпеки та ефективності роботи правоохоронних органів. Проте їхнє використання потребує ретельного моніторингу та регулювання. В першу чергу, задля того, аби уникнути зловживань і забезпечити дотримання прав людини [3].

Отже, використання ШІ відкриває нові горизонти для забезпечення правопорядку та дотримання прав людини. Сьогодні Міністерство внутрішніх справ України (далі – МВС) і Національна поліція України (далі – НПУ) активно працюють над інтеграцією сучасних технологій у свою діяльність з метою забезпечення безпеки громадян та дотримання прав людини. Впровадження ШІ в діяльність поліції сприятиме підвищенню прозорості, ефективності та довіри громадян до правоохоронних органів. Автоматизовані системи можуть аналізувати відеоматеріали з метою виявлення неправомірних дій, розглядати скарги громадян, прогнозувати потенційні ризики та запобігати можливим правопорушенням. Саме тому, доцільно розглянути ШІ як елемент адміністративного контролю в діяльності управління дотримання прав людини Департаменту головної інспекції та дотримання прав людини Національної поліції України (далі – УДПЛ). Технології ШІ дозволять впроваджувати в діяльність УДПЛ новітні механізми дотримання прав людини у поліції.

Одними із ключових завдань УДПЛ є моніторинг, превенція та реагування на випадки порушень прав і свобод людини під час надання поліцейських послуг. Проте, традиційні методи контролю часто неефективні через суб'єктивність, корупційні ризики та обмеженість людських ресурсів. Тому, технології ШІ можна використовувати для аналітики та моніторингу, зокрема, аналізу відеоматеріалів, аудіозаписів та звернень громадян, у тому числі, в реальному часі, для статистичного аналізу звернень громадян, службових розслідувань, судових рішень, навіть для документального оформлення матеріалів розгляду звернень і матеріалів службових розслідувань, а також, для прогнозування можливих правопорушень.

Вище ми зазначали про те, що у деяких країнах AI-система вже аналізує тисячі годин відеозаписів боді-камер і автоматично ідентифікує ситуації, які потребують перевірки. Тому, під час перевірки скарг громадян щодо можливих неправомірних дій працівників поліції, під час проведення службових розслідувань або моніторингу законності затримань неправомірні дії поліції, ШІ може аналізувати відеоматеріали з боді-камер та камер спостереження, автоматично ідентифікувати агресивну поведінку поліцейських або затриманих, виявляти випадки неправомірного застосування сили, аналізувати моделі поведінки для виявлення системних проблем у роботі поліції.

Інструменти ШІ можливо застосовувати для автоматизованого аналізу скарг громадян, зокрема, автоматичної класифікації скарг за рівнем серйозності, виявляти повторювані проблеми у діяльності окремих підрозділів поліції, створювати інтелектуальні профілі правопорушень для покращення

службових перевірок. Вже зараз AI-чат-боти приймають звернення громадян, автоматично аналізують їх і передають відповідним підрозділам поліції. Цілком можливо, що в майбутньому, інструменти ШІ будуть інтегровані в ІПНП НПУ.

Технології ШІ доцільно використовувати і в системі Custody Records, яку запроваджено для контролю за дотримання прав людини під час затримань за допомогою фіксації всіх подій, що відбуваються із затриманими. AI-система може в режимі реального часу аналізувати відео з камер спостереження у відділеннях поліції і виявляти випадки неправомірного застосування сили або порушення процедур утримання, ідентифікувати ознаки психологічного чи фізичного тиску під час допитів. AI може автоматично сповіщати керівництво про порушення регламентованого часу затримання, відсутність відеофіксації у момент проведення процесуальних дій, випадки можливої дискримінації або неналежного поводження. Використовуючи профайлінг, AI може оцінювати ризики на підставі поведінки осіб.

Водночас, сьогодні невирішеними залишаються питання конфіденційності і приватності даних, а також законодавчого врегулювання прозорості використання інструментів ШІ. Відкритим залишається питання: чи можна покласти юридичну відповідальність за помилкові рішення на алгоритми? Очевидно, що необхідно розробити модель відповідальності між людиною та ШІ за прийняті рішення, і впровадити AI-омбудсмена для оцінки рішень ШІ.

Впровадження ШІ в діяльність УДПЛ, зокрема, як елемент адміністративного контролю, відкриває нові можливості у сфері дотримання прав людини, оскільки дозволить використовувати новітні механізми попередження та реагування на правопорушення, а також розгляду матеріалів щодо можливих неправомірних дій працівників поліції. Використання ШІ у правоохоронній діяльності може стати інструментом, що дозволить зменшити ризики свавільного застосування сили та дискримінаційних практик. Проте ефективність цього механізму залежатиме від прозорого адміністрування, кібербезпеки та етичних стандартів, що мають стати основою цифрової трансформації поліції України. Технології змінюють правоохоронну систему. Важливо, щоб ці зміни відбувалися на користь суспільства!

Список використаних джерел:

1. Харарі Ю. Н. Нове покоління штучного інтелекту не просто поширює контент, створений людьми. Він може створювати контент сам. *Dev.ua.* 2023. URL: https://dev.ua/news/kharari-1682406158 (дата звернення: 23.02.2025).

2. Офіс Омбудсмана України. Права людини в епоху штучного інтелекту: виклики та правове регулювання. *Офіційний сайт Уповноваженого Верховної Ради України з прав людини*. 2024. URL: https://ombudsman.gov.ua/news_details/prava-lyudini-v-epohu-shtuchnogo-intelektu-vikliki-ta-pravove-regulyuvannya (дата звернення: 23.02.2025).

3. Алгоритми правосуддя: як поліцейські та слідчі використовують штучний інтелект. *Dsnews.ua*. URL: https://www.dsnews.ua/ukr/society/algoritmi-pravosuddya-yak-policeyski-ta-slidchi-vikoristovuyut-shtuchniy-intelekt-30112024-512565?utm_source=chatgpt.com (дата звернення: 23.02.2025).

Шевчук В. М.,
завідувач кафедри криміналістики,
доктор юридичних наук, професор,
(Національний юридичний університет імені Ярослава Мудрого)
головний науковий співробітник
(НДІ вивчення проблем злочинності
імені академіка В. В. Сташиса НАПрН України,
м. Харків)

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

У сучасних реаліях воєнного стану в Україні використання штучного інтелекту у роботі правоохоронних органів є актуальними та затребуваними практикою. Насьогодні застосування та впровадження технологій штучного інтелекту у правоохоронну діяльність багато в чому обумовлено необхідністю протистояти злочинному світу, який дедалі бере на озброєння найсучасніші інноваційні технології. Злочинці достатньо активно використовують останні досягнення четвертої промислової революції: технології блокчейну, дрони, робототехніку, штучний інтелект [1, с. 12–46]. Тому в сучасних умовах війни органи правопорядку активно використовують технології штучного інтелекту за різними напрямками, які суттєво підвищують ефективність цієї роботи, оптимізують вирішення завдань протидії злочинності.

Штучний інтелект у правоохоронній діяльності, як важливий інструмент підвищення ефективності роботи органів правопорядку, має перспективи використння та впровадження за такими напрямами: 1) інформаційно-аналітичне забезпечення правоохоронної діяльності; 2) інформаційно-довідкове забезпечення правоохоронної діяльності; 3) створення спеціалізованих інформаційних інтелектуальних систем оперативно-розшукового призначення; 4) формування та розвиток інтелектуальних систем відеоспостереження; 5) охорона об’єктів; 6) створення відомчих спеціалізованих інтелектуальних інформаційних систем; 7) впровадження інтелектуальних інформаційних освітніх систем; 8) запровадження інформаційно-телекомунікаційної системи досудового.

На сьогодні застосування та впровадження технологій штучного інтелекту у правоохоронну діяльність є перспективними темами криміналістичних досліджень, які мають розглядатися комплексно та системно. На наш погляд, основними напрямами таких наукових пошуків в реаліях сьогодення складають наступні.

Розпізнавання обличчя. Аналіз міжнародного і вітчизняного досвіду свідчить про те, що правоохоронці вже досить давно використовують програмні комплекси, які дозволяють автоматично розпізнавати обличчя [2, с. 139–148], порівнюючи із системами відеоспостереження та інформацією яка

вже є у базі. При цьому висока точність розпізнання досягається завдяки застосуванню технологій індексу за біометричними параметрами обличчя. Правоохоронці зазначають, що майже 30 % кримінальних правопорушень виявлено та розкрито завдяки таким відеокамерам. Такі технології розпізнають обличчя трупів окупантів та знаходять їх в соцмережах. Міністерство оборони України активно використовує технологію розпізнавання обличчя «Clearview AI», щоб розпізнавати російських нападників, боротися з дезінформацією, ідентифікувати загиблих та воєнних злочинців-окупантів. У воєнних реаліях повномасштабної військової агресії РФ на території України інструменти цифрової криміналістики значно допомагають у виявленні, розкритті та розслідуванні воєнних злочинів [3, с. 105–115].

Забезпечення безпеки на дорогах. Фіксація даних щодо правопорушень на дорогах реалізується за допомогою комплексів автоматичної фіксації, а саме спеціальних технічних засобів, укомплектованих функціями фото- і відеозапису, що надає можливість в автоматичному режимі здійснювати виявлення та документування в базах даних фактичних подій, які містять ознаки адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху [4, с. 55–60]. Установлення стаціонарних технічних засобів здійснюється на аварійно-небезпечних місцях та місцях концентрації дорожньо-транспортних пригод, автомобільних доріг загального користування, державного та місцевого значення, вулиць і доріг у містах та інших населених пунктах за погодженням із відповідним уповноваженим підрозділом Національної поліції [5].

Використання безпілотників. Сьогодні в реаліях військового часу в Україні найширша сфера застосування БПЛА. За їх допомогою здійснюється протидія незаконному оббіг вогнепальної зброї та боєприпасів, наркозлочинності в сучасних умовах. Також безпілотники можуть виявляти незаконні рубки лісу, знаходити лісові пожежі, фіксувати незаконний видобуток корисних копалин, допомагати шукати заблукалих в лісі, горах, виявляти ділянки, засіяні коноплями. Національна поліція України проводить роботу по формуванню спецгруп аеророзвідки у кожному регіоні країни.

Попередження та профілактика кримінальних правопорушень. Одним із поширених способів використання штучного інтелекту для профілактики вчинення кримінальних правопорушень є задіяння так званих інтелектуальних систем безпеки з різноманітними датчиками збору інформації, насамперед, відеокамерами високої роздільної здатності. Модернізовані камери зі штучним інтелектом можуть розпізнавати людей, автомобілі, зброю і навіть підозрілу поведінку. Зокрема, технологічна компанія Coban Technologies анонсувала запуск модернізованої версії камер з штучним інтелектом для поліцейських автомобілів. Coban Technologies має намір перетворити свій проект на цілу платформу, що дозволить іншим розробникам вдосконалювати камеру, наприклад, за допомогою спеціального додатку, що розпізнає зброю. Існуюча версія смарт-камери розпізнає об’єкти лише на записаному нею відеопотоці. Розробники повідомляють, що в перспективі буде створена камера, яка

аналізуватиме поведінку людей безпосередньо на вулицях в режимі онлайн [6].

Прогнозування кримінальних правопорушень. Останнім часом дослідження фахівців у царині наукових знань новітніх цифрових технологій показують, що штучний інтелект із застосуванням системи сучасних методів може успішно використовуватись для прогнозування злочинності. Зокрема, інноваційні цифрові технології дозволяють запобігати вчиненню кримінального правопорушення з боку конкретної особи, тобто на стадії формування злочинної мотивації, готування або замаху на його вчинення. Це стало реальністю завдяки моделюванню майбутньої поведінки окремих осіб на підставі особливостей їх соціально-демографічної та кримінально-правової характеристики. Сприяє підвищенню ефективності роботи поліції та прогнозування кримінальних правопорушень також метод картографування злочинності, за допомогою якого формуються прогнози щодо місцевої злочинності та індивідуальної злочинної поведінки. Отже, завдяки технологій штучного інтелекту можуть створюватися обґрунтовані прогнози щодо темпоральних, територіальних і якісних показників злочинності.

Отже, в сучасних умовах війни активно застосовуються технології штучного інтелекту у правоохоронній діяльності за різними напрямами, які суттєво підвищують ефективність такої діяльності, оптимізують вирішення завдань боротьби зі злочинністю.

Список використаних джерел:

1. Matulienė, S., Shevchuk, V., & Baltrūnienė, J. (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.

2. Kryvoruchko, O., Bebeshko, B., Khorolska, K., Desiatko, A., & Kotenko, N. (2020). Artificial intelligence face recognition for authentication. *Технічні науки та технології*, (2(20), 139–148.

3. Шевчук В. М. Можливості та перспективи використання технологій штучного інтелекту в розслідуванні кримінальних правопорушень. *Інноваційні методи, засоби та технології в криміналістиці та судовій експертизі :* наук.-практ. посіб. / НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків : Право, 2023. С. 105–115.

4. Мисливий В. А. Штучний інтелект як фактор запобігання дорожньо-транспортної злочинності. *Використання технологій штучного інтелекту у протидії злочинності :* матеріали науково-практичного онлайн-семінару (м. Харків, 5 листопада 2020 р.). Харків : Право, 2020. С. 55–60.

5. Вінницька поліція презентувала перший в Україні інноваційний безпековий IT-проєкт, який впроваджуватиме у свою діяльність. *Національна поліція України*. URL: https://www.npu.gov.ua/news/vinnitska-politsiya-prezentuvala-pershiy-v-ukraini-innovatsiyniy-bezpekoviy-it-proekt-yakiy-vprovadzhuvatime-u-svoyu-diyalnist (дата звернення: 10.03.2025).

6. «Розумні» камери допоможуть поліцейським визначати злочинців. URL: https://www.ukrinform.ua/rubric- technology/ 2331687-rozumni-kameri-dopomozut-policejskim-viznacati-zlocinciv.html(дата звернення: 10.03.2025).

Шипіло Д.,
аспірант кафедри адміністративного права і процесу
(Дніпровськоий державний університет внутрішніх справ)

АДМІНІСТРАТИВНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ПОРЯДКУ ПЕРЕМІЩЕННЯ ТОВАРІВ В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

У період воєнних дій та правового режиму воєнного стану роль митних органів та суду у застосуванні адміністративної відповідальності за порушення порядку переміщення товарів через кордон стає особливим. Митні органи – це перші контрольні посилання, що забезпечують своєчасне виявлення та фіксацію злочинних дій, які можуть вплинути на економічну безпеку держави. У цей період ризик контрабанди та незаконний обіг важливих стратегічних товарів або намагається обійти Закон, що вимагає координації та дії. Крім того, в умовах війни вони не лише стикаються з захистом державних економічних інтересів, але й необхідністю забезпечення швидкого переміщення гуманітарної допомоги.

Про актуальність даної проблеми та ролі митних органів в застосуванні адміністративної відповідальності за порушення порядку переміщення товарів свідчать, статистичні дані про збільшення кількості відповідних правопорушень. Державна митна служба України висвітлює на на сайті певні цифри, а саме, протягом січня-грудня 2023 року митниці виявили 11 935 порушень митних правил на суму 8,9 млрд грн. У порівнянні з 2022 роком, вартісний показник збільшився у 3 рази. Безпосередньо митницями розглянуто 3493 справи про порушення митних правил. Застосовано адміністративне стягнення у вигляді штрафу на суму 110 млн грн, з яких стягнуто до Держбюджету 80 млн гривень. На розгляд до суду митницями передано 6912 справ про порушення митних правил на суму 6,4 млрд гривень. За результатами розгляду справ судами накладено стягнень (конфіскація товарів та штрафи) на суму 2 млрд грн (конфіскація – 1,04 млрд грн, штрафи – 963 млн грн) [1].

Крім того, протягом січня-березня 2024 року співробітники Державної митної служби України виявили 2356 порушень митних правил на суму 4,8 млрд грн. Вартісний показник збільшився майже в 4 рази, порівняно з аналогічним періодом 2023 року. У 908 справах про порушення митних правил, у тому числі заведених у попередніх періодах, митницями застосовано адміністративне стягнення у вигляді штрафу на суму 19 млн грн, стягнуто штрафів на суму 23 млн грн. На розгляд до суду митницями передано 1116 справ про порушення митних правил на суму 1 млрд грн. У 1 263 справах, у тому числі заведених у попередні періоди, судом прийняті рішення про накладення стягнень у вигляді штрафу та конфіскації на загальну суму 363 млн грн (конфіскація – 146 млн грн, штрафи – 217 млн грн) [2].

Такі злочинні дії показують значні ризики для економічної безпеки держави, оскільки вони спричиняють значні втрати до державного бюджету

України, ускладнюють контроль обігу товарів. Крім того, незаконний імпорт заборонених товарів, таких як зброя, є серйозною загрозою для громадської безпеки.

В умовах воєнного стану, коли економіка країни зазнає значних змін, а митні процедури можуть спрощуватися або ускладнюватися, питання адміністративної відповідальності за порушення митних правил набуває особливої актуальності.

Основні особливості адміністративної відповідальності за порушення митних правил в умовах війни полягає в змінах у законодавстві. Урядом можуть вводитися тимчасові зміни до митного законодавства, що покликані спростити або ускладнити певні митні процедури, залежно від потреб країни в конкретний період. Це може вплинути на види та розміри адміністративних стягнень.

З метою запобігання незаконному ввезенню зброї, боєприпасів, товарів подвійного призначення та інших заборонених товарів, митний контроль може бути значно посилений контроль. Це означає, що ризик виявлення порушень і притягнення до відповідальності зростає.

З іншого боку, для підтримки економіки та спрощення процедур імпорту товарів, необхідних для забезпечення оборони та безпеки країни, можуть бути спрощені певні митні процедури, наприклад для переміщення гуманітарних товарів. Для забезпечення гуманітарної допомоги постраждалому населенню як правило передбачені спеціальні правила, які спрощують митне оформлення таких товарів. В умовах війни може спостерігатися зростання кількості порушень митних правил, пов'язаних з контрабандою, незаконним переміщенням товарів та валюти.

У деяких випадках можуть бути передбачені додаткові підстави для звільнення від адміністративної відповідальності, наприклад, для осіб, які вчинили правопорушення внаслідок форс-мажорних обставин.

Законодавство передбачає широкий спектр заходів відповідальності за порушення митних правил в умовах війни, серед яких: штрафи, конфіскація товарів, адміністративний арест та інші.

Особливості відповідальності за окремі порушення митних правил передбачають, що такі дії, якщо вони стали наслідком аварії, дії обставин непереборної сили чи протиправних дій третіх осіб (підтверджених відповідними документами), а також помилки у митній декларації, які не спричинили незаконного звільнення від сплати митних платежів чи їх зменшення, або порушення заходів тарифного чи нетарифного регулювання, за умови, що такі помилки не носять систематичного характеру, можуть мати специфічний порядок розгляду.

Особливого значення взаємодія між митними органами та судом набуває в умовах воєнних дій та правового режиму воєнного стану, коли порушення митних правил можуть становити серйозну загрозу економічній і національній безпеці держави. У цей період митні органи виконують додаткову функцію щодо запобігання контрабанді та незаконному обігу стратегічних ресурсів, а

суди гарантують, що застосування адміністративної відповідальності залишається в межах закону та правопорядку. Саме тому, акцентується увага на чіткості і обґрунтованості зібраної митними органами доказової бази, яка підтверджує факт правопорушення, для швидкого та якісного розгляду матеріалів судом [4].

Шляхами підвищення ефективності є удосконалення митного законодавства, спрощення та уніфікація норм, підвищення їхньої чіткості. Посилення відповідальності посадових осіб, застосування більш жорстких заходів відповідальності до посадових осіб, винних у порушенні митних правил. Впровадження нових технологій, використання сучасних інформаційних технологій для контролю за переміщенням товарів. Співпраця з іншими правоохоронними органами, обмін інформацією та координація дій з іншими правоохоронними органами для боротьби з контрабандою та іншими видами незаконної діяльності, проведення інформаційних кампаній з метою підвищення обізнаності громадян про митне законодавство.

Адміністративна відповідальність за порушення митних правил є важливим інструментом державного регулювання зовнішньоекономічної діяльності. Однак, для досягнення максимальної ефективності необхідно постійно вдосконалювати механізми її застосування та усувати існуючі проблеми.

Таким чином, комплексна та ефективна співпраця митних органів і судів є запорукою дотримання законності, захисту державних інтересів та забезпечення економічної стабільності країни, особливо у складних умовах сучасних викликів.

Список використаних джерел:

1. За 2023 рік митниці Держмитслужби виявили порушень митних правил на суму 8,9 млрд грн. URL: https://customs.gov.ua/news/zagalne-20/post/za-2023-rik-mitnitsi-derzhmitsluzhbi-viiavili-porushen-mitnikh-pravil-na-sumu-89-mlrd-grn-1444 (дата звернення: 24.12.2024).

2. За І квартал 2024 року митниці Держмитслужби виявили порушень митних правил на 4,8 млрд грн. URL: https://customs.gov.ua/news/zagalne-20/post/za-i-kvartal-2024-roku-mitnitsi-derzhmitsluzhbi-viiavili-porushen-mitnikh-pravil-na-48-mlrd-grn-1557 (дата звернення: 24.12.2024).

3. Митний кодекс України від 13.03.2012 № 4495-VI. URL: https://zakon.rada.gov.ua/laws/show/4495-17#Text (дата звернення: 24.12.2024).

4. Кодекс України про адміністративні правопорушення : Закон України від 07.12.1984 № 8073-X. *Відомості Верховної Ради УРСР*. 1984. № 51. С. 1122.

Юрчук О. В.,
начальниця відділу правового аналізу
та моніторингу інвестиційної діяльності
управління з питань економічної політики
(Львівська обласна рада)
асистентка кафедри медичного права ФПДО
*(Львівський національний медичний університет імені
Данила Галицького)*

ЕТИЧНІ ТА ПРАВОВІ АСПЕКТИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В МЕДИЦИНІ

У грудні 2020 року Кабінет Міністрів України затвердив Концепцію розвитку штучного інтелекту в Україні, у якій визначені мета, принципи та завдання розвитку таких технологій як одного з пріоритетних напрямів у сфері науково-технологічних досліджень і наведено визначення штучного інтелекту (ШІ): це 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 ухвалення рішень, алгоритми роботи з інформацією та визначати способи досягнення поставле- них завдань [3].

Розпорядженням Кабінету Міністрів України від 13.04.2024 за № 320-р схвалено Концепцію Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 р., згідно з якою використання технологій ШІ в пріоритетних галузях економіки дасть змогу підвищити ефективність ухвалення рішень шляхом автоматизованої обробки різноманітної інформації та виявлення нових інформаційних шаблонів і тенденцій [4].

Відповідно до Закону України «Основи законодавства України про охорону здоров’я» суспільство і держава забезпечують пріоритетність охорони здоров'я в діяльності держави, вдосконалення медичної допомоги і запровадження здорового способу життя [2]. Держава визначає правові, організаційні, економічні та соціальні засади охорони здоров'я в Україні, впливає на регулювання суспільних відносин у цій сфері з метою забезпечення гармонійного розвитку фізичних і духовних сил, високої працездатності і довголітнього активного життя громадян, усунення факторів, що шкідливо впливають на їх здоров’я, попередження і зниження захворюваності, інвалідності та смертності, поліпшення спадковості.

З огляду на викладене та враховуючи положення статті 49 Конституції України охорона здоров’я є пріоритетною сферою соціальної політики держави, оскільки безпосередньо впливає на якість життя, здоров'я та благополуччя нації [1].

Оцінюючи приватність та безпеку даних в сфері охорони здоров’я, можна ствердно зробити висновок, що застосування ШІ в медицині становить фундаментальний виклик. Центральним аспектом є те, що ШІ для своєї ефективної роботи потребує доступу до великих масивів даних, зокрема, чутливих медичних відомостей пацієнтів. Ці дані часто включають особисті ідентифікаційні деталі, історію хвороб, генетичну інформацію, що робить їх привабливою мішенню для кібератак.

Один із яскравих прикладів втрати даних стався у 2016 році, коли медичний центр UCLA Health в США зазнав витоку даних, що стосувався особистої інформації близько 4.5 мільйонів пацієнтів [5]. Цей інцидент підняв питання про необхідність посилення заходів безпеки даних і виявив потенційні юридичні наслідки, у тому числі судові позови від постраждалих пацієнтів.

На моє переконання, ключ до забезпечення конфіденційності полягає в імплементації строгих протоколів безпеки, таких як шифрування даних, використання безпечних протоколів передачі інформації та постійний моніторинг доступу до даних. Різноманітні регуляторні рамки, як GDPR в Європейському Союзі та HIPAA в США, також ставлять жорсткі вимоги до збереження та обробки медичної інформації, надаючи пацієнтам контроль над їхніми даними і встановлюючи значні штрафи за порушення. Практика показує, що постійне оновлення захисту даних є необхідністю у відповідь на постійно розвиваючі загрози. Інституції, які залучені до збору та обробки медичних даних, мають регулярно проводити аудити безпеки та тренінги для персоналу, з метою підвищення обізнаності та компетентності в області кібербезпеки.

Разом з тим, вважаю, що захист приватності в медицині є не просто юридичним обов'язком, але й етичною необхідністю, що забезпечує довіру пацієнтів і сприяє ефективній медичній практиці. Це особливо важливо в контексті інтеграції штучного інтелекту в сферу, де є значний відсоток випадків для зловживань та помилок. Таким чином, балансування між інноваціями та конфіденційністю стає ключовим викликом сучасної медичної етики та практики.

Отже, приватність та безпека даних є одними з найголовніших викликів при використанні штучного інтелекту в медицині. Ефективний захист цих даних вимагає розробки та впровадження строгих правових рамок. Потрібно законодавче зміцнення вимог до шифрування, аудиту доступу та збереження медичних даних, подібно до загального регламенту захисту даних (GDPR) в Європейському Союзі. Встановлення чітких форм відповідальності для організацій, які порушують ці протоколи, включно з суттєвими штрафами та вимогами до відшкодування, може стати дієвим детермінантом.

Питання відповідальності за помилки, допущені алгоритмами ШІ, демонструє складність юридичних і етичних аспектів у використанні ШІ в медицині. Визначення того, хто саме несе відповідальність у разі виникнення помилок – чи то лікарі, розробники програмного забезпечення, чи виробники медичного обладнання – є предметом жвавих дискусій і правового регулювання.

Реальний кейс, який ілюструє цю проблему, стався з системою ШІ Watson for Oncology, розробленою IBM [6]. Ця система була призначена для надання рекомендацій щодо лікування раку на основі медичних даних пацієнтів. Однак у декількох випадках система давала помилкові рекомендації, що могло призвести до серйозних наслідків для здоров'я пацієнтів. Це порушило питання про те, хто відповідає за ці помилки: чи це IBM як розробник і постачальник системи, чи заклад охорони здоров’я, працівники якого використовували ці рекомендації при призначенні лікування.

Такі інциденти підкреслюють необхідність розробки чітких юридичних рамок та стандартів, які б регулювали використання медичних технологій на основі ШІ. На даний момент в багатьох країнах, включно зі США та країнами Європейського Союзу, юридичне регулювання ШІ в медицині залишається у розробці, але основні принципи включають підвищення прозорості процесів ШІ, покращення контролю за даними і роз'яснення відповідальності всіх заінтересованих сторін.

Одним із варіантів рішення може стати модель спільної відповідальності, де розробники і постачальники ШІ систем несуть відповідальність за програмне забезпечення та його оновлення, в той час як медичні заклади і лікарі відповідають за правильне та обачне використання цих систем в лікувальній практиці. Крім того, юристи акцентують увагу на необхідності страхування професійної відповідальності та залучення страхових компаній у покриття ризиків, пов'язаних із застосуванням ШІ. Вважаю, що страхування в цій сфері допоможе не тільки зменшити юридичні ризики для лікарів і закладів охорони здоров’я, але й сприятиме зміцненню довіри пацієнтів до використання інноваційних медичних технологій, забезпечуючи захист їхніх інтересів у разі помилкових медичних рішень.

В контексті відповідальності за помилки, допущені штучним інтелектом (ШІ) в медичній практиці, вважаю за необхідне ретельно розробити правові рамки, які б визначали, хто відповідає за різні типи помилок. Так, якщо помилка виникає через невірно введені дані медичним працівником, відповідальність повинна лягати на заклад охорони здоров’я. Якщо помилка відбувається через технічну недосконаліть самої ШІ системи, наприклад, через помилки у програмному забезпеченні або апаратних компонентах, відповідальність мають нести розробники та виробники цих систем. У таких випадках необхідно встановити чіткі умови з гарантій обладнання та програмного забезпечення.

Отже, для кожного з цих видів помилок необхідно запровадити страхування відповідальності, що дозволить покривати збитки, заподіяні пацієнтам, незалежно від джерела помилки. Таке страхування не тільки захищає пацієнтів, але й стимулює розробників та медичні установи до високих стандартів безпеки і точності.

Таким чином, застосування ШІ у медицині викликає серйозні етичні та юридичні питання, які вимагають подальшого ретельного вивчення та регулювання.

Список використаних джерел:

1. Конституція України (Відомості Верховної Ради України (ВВР), 1996, No 30, ст. 141). URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.
2. Основи законодавства України про охорону здоров'я : Закон України. *Відомості Верховної Ради України (ВВР).* 1993. № 4, ст. 19. URL: https://zakon.rada.gov.ua/laws/show/2801-12#Text.
3. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text.
4. Про схвалення Концепції Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року : Розпорядження Кабінету Міністрів України від 13.04.2024 № 320-р. URL: https://zakon.rada.gov.ua/laws/show/320-2024-р#.
5. Times Now News. UCLA medical school faces allegations of lowered standards amid affirmative action controversy. *Times Now News*. 2023. URL: https://www.timesnownews.com/world/us/us-news/ucla-medical-school-faces-allegations-of-lowered-standards-amid-affirmative-action-controversy-article-110475690.
6. Levitan, N. Confronting the Criticisms Facing Watson for Oncology. *The ASCO Post*. 2021. URL: https://www.ascopost.com.

Яковенко Ю. В.,
викладач
(Національний юридичний університет
ім. Ярослава Мудрого)

ШТУЧНИЙ ІНТЕЛЕКТ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: ПЕРСПЕКТИВИ АВТОМАТИЗАЦІЇ В КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Штучний інтелект (ШІ) в правоохоронній діяльності відкриває нові горизонти для автоматизації процесів та підвищення ефективності боротьби зі злочинністю. Водночас, його застосування піднімає низку дискусійних питань, зокрема в контексті національної безпеки.

Одним із ключових напрямків використання ШІ в правоохоронній діяльності є автоматизація процесів обробки документів у досудовому розслідуванні та процедури кримінального аналізу. Зокрема, на прикладі міжнародного досвіду, можна зазначити, що ШІ дозволяє значно прискорити обробку великих обсягів інформації, що надходить під час розслідування кримінальних справ, однак за для дотримання прав людини міжнародним законодавством забезпечується дотримання принципу особистої приватності осіб. Як зазначають М. Бєлова і Д. Бєлов, впровадження ШІ дозволяє зменшити кількість помилок, які можуть виникати через людський фактор, та забезпечити більш точний аналіз доказів [2].

В Україні інтеграція технологій ШІ у правоохоронну діяльність також відкриває нові можливості. Зокрема, Т. Гудзь та А. Синжерян акцентують увагу на тому, що штучний інтелект може сприяти ефективному моніторингу ситуацій в реальному часі, що особливо важливо в умовах складних кримінальних ситуацій та під час кризових подій, таких як воєнний стан [3, с. 55]. За допомогою ШІ можна швидше виявляти закономірності в поведінці злочинців, передбачати їхні подальшу поведінку та підвищувати загальну оперативність правоохоронних органів.

Штучний інтелект може бути використаний для автоматизованої оцінки ризиків, пов'язаних із конкретними злочинними діяннями або правопорушниками. Зокрема, системи, засновані на алгоритмах машинного навчання, здатні аналізувати великі масиви інформації для ідентифікації територій із підвищеним рівнем криміногенної обстановки, що дозволяє оптимізувати превентивні заходи.

Однак, незважаючи на численні переваги, застосування ШІ в правоохоронній діяльності, обов'язково, потрібно розуміти ризики його використання. Серед основних ризиків, які можуть виникнути під час застосування ШІ це порушення прав людини та виток персональних даних. Впровадження автоматизованих систем, які займаються збором і обробкою даних про осіб, може призвести до порушення конфіденційності. Як зазначає О. П. Андрущенко, важливо, щоб система ШІ, яка застосовується для боротьби зі злочинністю, була прозорою і підлягала громадському контролю [1, с. 189].

Водночас питання відповідальності за помилки, допущені штучним інтелектом, залишаються відкритими. Випадкові помилки в обробці даних або в рішенні ШІ можуть призвести до порушень прав осіб. Як зазначають автори, важливою є розробка чітких правових норм, що визначають межі використання ШІ в правооохоронній діяльності, зокрема механізм перевірки та контролю рішень, прийнятих на основі даних, зібраних штучним інтелектом [4].

У контексті національної безпеки впровадження ШІ може мати як позитивний, так і негативний вплив. З одного боку, використання технологій ШІ може сприяти підвищенню ефективності у розкритті кримінальних правопорушень та збору доказів, оскільки за його допомогою можливо здійснювати швидкий пошук та аналіз доказів отриманих з онлайн- ресурсів та соціальних мереж.

З іншого боку, невиправдане розширення застосування ШІ без належного правового регулювання може призвести до загрози несанкціонованого спостереження за громадянами, втручання в особисте життя, чим порушувати їх права та свободи. Насамперед, це стосується збору, зберігання та аналізу персональних даних без належного контролю. Автоматизовані системи можуть збирати інформацію про пересування людей, їхні контакти, поведінкові моделі, це створює ризик збору особистих даних осіб, які можуть не мати відношення до кримінальних або адміністративних правопорушень. Наприклад, дослідження міжнародного досвіду застосування автоматизованих систем розпізнавання обличчя показали, що вони часто помиляються при ідентифікації

представників певних етнічних або соціальних груп, що може призводити до помилкових звинувачень або переслідувань [2].

Для уникнення можливості зловживання владою, межі використання штучного інтелекту, на стадії досудового розслідування, повинно бути чітко регламентовано законодавством. Оскільки без належних механізмів його використання у правоохоронній сфері, під приводом боротьби зі злочинністю, можуть з'явитись форми цифрового утиску громадян, що поставить під питання принцип демократії держави та правові основи громадянського суспільства.

У сьогоднішніх реаліях України, не менш важливим фактором є загроза кібератак. Будь-яка автоматизована система, що працює на основі ШІ, може стати об'єктом хакерського втручання, особливо якщо вона пов'язана з державними реєстрами даних чи критичною інфраструктурою. У разі отримання несанкціонованого доступу до таких систем, кіберзочинці можуть використовувати отриману інформацію для її витоку, передачі третім особам або маніпулювати нею для вербування, цікавих їм особистостей, шляхом компрометації. Як зазначають дослідники, особливо небезпечно, коли штучний інтелект використовується для автоматизованих рішень у судовій системі, оскільки навіть незначна маніпуляція алгоритмом може мати катастрофічні наслідки для підозрюваних [4].

Для уникнення негативного впливу використання штучного інтелекту у правоохоронній діяльності: по-перше необхідно на законодавчому рівні визначити чіткі межі його застосування та процедури, по-друге встановити відповідальність суб'єктів, які можуть використовувати ШІ у своїй професійній діяльності, за використання штучного інтелекту у непередбачених законом випадках, в-третє впровадження систем багаторівневого захисту автоматизованих програм, реєстрів та баз даних, які побудовані на основі штучного інтелекту. Крім того, необхідно розуміти, що ШІ не замінить інтуїцію, досвід, емоційний інтелект людини та він є допоміжним інструментом у професійній діяльності.

Список використаних джерел:

1. Андрущенко О. П. Вплив штучного інтелекту на захист прав людини: проблеми, прогнози та перспективи боротьби зі злочинністю. *Питання боротьби зі злочинністю*. 2024. Т. 1, № 47. С. 186–193.
2. Бєлова М., Бєлов Д. Імплементація штучного інтелекту в досудове розслідування кримінальних справ: міжнародний досвід. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2023. № 2. С. 448–453. URL: https://app-journal.in.ua/wp-content/uploads/2023/05/80.pdf (дата звернення: 03.03.2025).
3. Гудзь Т. І., Синжерян А. А. Інтеграція технології штучного інтелекту у діяльність національної поліції України: Перспективи та виклики. *Українська поліцеїстика: теорія, законодавство, практика*. 2024. № 3. С. 53–59.
4. Северин О., Шапошник М., Кисельов А. Використання інформаційно-телекомунікаційних засобів у кримінальному аналізі під час воєнного стану: Особливості та можливості. *Universum*. 2023. № 5. С. 102–106. URL: https://archive.liga.science/index.php/universum/article/view/769/778 (дата звернення: 03.03.2025).

Н А У К О В Е В И Д А Н Н Я

ШТУЧНИЙ ІНТЕЛЕКТ У ПРАВОВІЙ ПРАКТИЦІ: МЕЖІ ТА МОЖЛИВОСТІ

Збірник тез
круглого столу

14 березня 2025 року

Упорядник – **О. О. Барабаш**