DOI: 10.33994/kndise.2025.70.12
УДК 343.98

Правове регулювання притягнення до відповідальності за правопорушення, вчинені штучним інтелектом

Світлана Кухарева

Старша судова експертка відділу нормативно-правового забезпечення лабораторії організації наукової, методичної діяльності, нормативного забезпечення, міжнародного співробітництва та підготовки експертів Київського науково-дослідного інституту судових експертиз Міністерства юстиції України

e-mail: svitlana.kukhareva@kndise.gov.ua

Дмитро Кальной

Завідувач відділу нормативно-правового забезпечення лабораторії організації наукової, методичної діяльності, нормативного забезпечення, міжнародного співробітництва та підготовки експертів Київського науково-дослідного інституту судових експертиз Міністерства юстиції України

e-mail: d.kalnoy@kndise.gov.ua

Антон Камінський

Молодший науковий співробітник відділу нормативно-правового забезпечення лабораторії організації наукової, методичної діяльності, нормативного забезпечення, міжнародного співробітництва та підготовки експертів Київського науково-дослідного інституту судових експертиз Міністерства юстиції України

e-mail: anton.kaminskyi@kndise.gov.ua

У статті висвітлено наукові дискусії щодо видів покарання за кримінальні правопорушення, вчинені штучним інтелектом. Автори окреслюють нормативно-правову базу притягнення до відповідальності за такі правопорушення. Наведено визначення та види штучного інтелекту залежно від сфери його використання. Висвітлено нові способи використання новітніх технологій штучного інтелекту для вчинення правопорушень у сучасних реаліях. Проаналізовано проблемні аспекти визначення суб'єктів відповідальності за правопорушення, вчинені за допомогою штучного інтелекту. Розглянуто

можливості закріплення відповідальності за такі правопорушення на законодавчому національному та міжнародному рівні. Зокрема, розглянуто три моделі кримінальної відповідальності залежно від різних ситуацій (штучний інтелект як інструмент для вчинення злочину; модель більш просунутої версії штучного інтелекту; модель прямої відповідальності штучного інтелекту, яка означає, що на нього із деякими незначними змінами або коригуваннями повинні поширюватися ті самі кримінальні закони, що і на людей). Також проаналізовано передбачені українським законодавством види покарань, які можуть бути застосовані до штучного інтелекту. Автори акцентували увагу на деяких положеннях першого у світі закону, що регулює розробку та використання штучного інтелекту,— Закону Європейського Союзу про штучний інтелект (AI Act), прийнятого Європейським парламентом.

Ключові слова: штучний інтелект; новітні технології; правопорушення; відповідальність; покарання; правове регулювання.

Постановка проблеми. Сьогодні ми живемо в період стрімкого розвитку новітніх технологій. Століттями людськість прагнула автоматизувати та спростити свої завдання: досягти поставленої мети з меншими витратами та швидшими темпами. Ці намагання продовжуються і донині задля оптимізації роботи з великими обсягами інформації. За останні двадцять років штучний інтелект (далі — *ШІ*) пройшов шлях від наукової абстракції до повсякденного застосування [1]. Наразі системи ШІ інтегруються майже в усі сфери діяльності людини. Однак, із розвитком новітніх технологій з'являються нові виклики на різних рівнях суспільного життя, зокрема й на правовому. Система правового регулювання повинна бути адаптована до нових реалій, водночас важливо визначити, хто нестиме відповідальність у разі правопорушення: розробник, користувач або ШІ.

Аналіз останніх досліджень і публікацій. Питанням правового регулювання використання ШІ приділяють значну увагу як зарубіжні, так і вітчизняні науковці та практики. Зокрема, С. Рассел і П. Норвіг визначили типи штучного інтелекту відповідно до їх застосування, своєю чергою Г. Халлеві виокремив моделі кримінальної відповідальності ШІ; Ч. Яні та С. П. Ратор проаналізували види покарання ШІ та навели паралель із корпоративною кримінальною відповідальністю. Цим питанням була також приділена увага М. Карчевського, А. Кисельова, Ж. Удовенко, С. Ойеделе, Б. Джеймса та ін. Проте варто зазначити, що проблема притягнення до відповідальності за правопорушення, вчинені ШІ, на сьогодні є доволі дискусійною та потребує подальших досліджень.

Мета дослідження. Висвітлення наукових дискусій щодо притягнення до відповідальності за правопорушення, вчинені ШІ, аналізування актуальних питань правового регулювання притягнення до відповідальності ШІ та можливостей закріплення такої відповідальності в Україні.

Викладення основного матеріалу. ШІ — це сукупність алгоритмів, розроблених із метою створення пристроїв, які мають можливості, подібні до людських. Тип технології, який починає бути присутнім у повсякденному житті в найпоширеніших додатках, таких як асистенти мобільних телефонів *Siri* та *Alexa*, програмах розпізнавання облич, або таких, що використовують аргентинський уряд у системах на кшталт *ANSES* (Національна адміністрація соціального забезпечення) та *AFIP* (Федеральна адміністрація державних доходів) [2, 3].

Науковці у сфері комп'ютерних наук С. Рассел і П. Норвіг визначили такі типи ШІ відповідно до їх застосування [4]:

— системи, які «думають» як люди (наприклад, штучні нейронні мережі);

— системи, які діють як люди (наприклад, роботи);

— системи, які навчаються та генерують нові знання (наприклад, експертні системи).

Разом із технологічним розвитком зростає кількість правопорушень у цій сфері та змінюються способи їх вчинення залежно від типу ШІ. Правопорушення, спричинені ШІ, функціонально вчиняють машини, водночас майже неможливо ідентифікувати особу, яка за цим стоїть [5]. Наприклад, сьогодні, якщо хтось наносить смертельні поранення ножем, злочинцем буде вважатися людина, яка застосувала ніж, а не сам ніж, оскільки ніж у цьому випадку є лише знаряддям вчинення злочину. Однак ШІ може відрізнятися від традиційних машин або інструментів у деяких важливих аспектах, що ставить під питання пряме застосування кримінального права. Зокрема, ШІ демонструє високий рівень автономності, тобто може ухвалювати рішення самостійно, без контролю з боку людини; миттєво отримувати дані з численних джерел; визначати цілі; оцінювати результати за певними критеріями і коригувати свою поведінку відповідно до обставин, щоб підвищити шанси на успіх. Якщо правопорушення скоєно людиною, то вона нестиме за нього кримінальну відповідальність, але якщо його вчинить ШІ, то без втручання людини на сьогодні ніхто не може бути притягнутий до відповідальності. Така ситуація є критичною, адже дедалі більша кількість правопорушень залишаються безкарними у цивілізованому суспільстві.

Варто зазначити, що досить складно притягнути до відповідальності одну особу за правопорушення, пов'язані зі ШІ: *по-перше,*

системи ШІ розробляють у результаті співпраці значної кількості людей протягом багатьох років; *по-друге,* ШІ накопичує досвід, збираючи дані з мільярдів різнорідних джерел. Розроблений для суспільно корисної діяльності, ШІ може використати ці дані для того, щоб зашкодити суспільству. Таку ситуацію достовірно не може передбачити жодна людина, тому важко визначити розробника, який має бути притягнутий до відповідальності.

У зв'язку зі зростанням кількості правопорушень, вчинених за допомогою або самою системою ШІ, кримінальне законодавство вочевидь потребує змін. Найважливішим питанням кримінального права є питання притягнення до кримінальної відповідальності певної особи (у цьому випадку — фізичної або юридичної особи чи ШІ). Для цього необхідна сукупність об'єктивних і суб'єктивних ознак, що дають змогу кваліфікувати суспільно-небезпечне діяння як конкретне кримінальне правопорушення. Кожен склад кримінального правопорушення обов'язково містить такі елементи: об'єкт кримінального правопорушення, об'єктивну сторону, суб'єкт та суб'єктивну сторону. Відсутність хоча б одного з цих елементів свідчить про відсутність у діянні особи складу кримінального правопорушення, що виключає кримінальну відповідальність. Кримінальну відповідальність також застосовують у випадках недбалості, коли особа могла і мала б передбачити наслідки й уникнути певної дії (бездіяльності). Але чи можна розглядати ШІ як суб'єкт правопорушення? Пропонуємо розглянути три моделі кримінальної відповідальності ШІ в різних ситуаціях, запропоновані ізраїльським професором кримінального права Г. Халлеві [7].

ШІ як знаряддя вчинення злочину

У цій моделі ШІ розглядають лише як машину, інструмент, і тому він не може бути суб'єктом правопорушення, адже не має необхідних розумових здібностей. Передбачається, що за будь-яким правопорушенням, скоєним ШІ, завжди стоїть людина, яка повинна нести відповідальність. Виникає питання: хто має бути визнаний винним у випадку зі ШІ? Це може бути розробник ШІ, користувач або керівник. Розробник може запрограмувати або спроектувати ШІ спеціально для вчинення певного злочину. Іншим порушником може бути користувач, який може використовувати ШІ, розроблений з іншою метою, для вчинення правопорушень. Наприклад, якщо ШІ, розроблений для виконання команд, використовують для злочинної діяльності, то справжнім порушником, який повинен нести кримінальну відповідальність, є його власник або користувач. Так само, якщо керівник через недбалість або зі злочинних намірів дозволяє ШІ здійснювати діяльність, яка є протиправною за своєю природою, він може і повинен бути притягнутий до відповідальності.

Тут об'єктивною стороною є діяння ШІ, а суб'єктом — розробник, користувач, власник або керівник. У цій моделі ШІ подібний до інструменту або тварини, яку використовують для вчинення злочину. Злодій може використовувати інструмент, щоб відкрити шафку і вкрасти цінності, або господар може використовувати свого собаку, щоб напасти на когось — у цих випадках інструмент або собака не є суб'єктами злочину.

Ця модель є можливою для базового рівня ШІ, за якого він не має високої когнітивної здатності. Сучасний ШІ може ухвалити рішення про вчинення правопорушення на основі власних накопичених знань, навчання та досвіду. За такого сценарію несправедливо притягати користувача, розробника або власника до відповідальності за правопорушення, скоєне ШІ.

Модель більш розвиненої версії ШІ

Нерідко ШІ, розроблений для виявлення вірусів, шкідливих і шпигунських програм, сам стає такою програмою і надсилає віруси в інші системи, використовуючи своє базове програмування. У цьому випадку ШІ створюється розробником для іншої мети, тому він дізнається про правопорушення лише після того, як воно скоєне за допомогою тієї самої програми. У цій моделі спостерігається суттєве залучення розробника або користувача, але відсутній намір вчинення злочину. Наприклад, ШІ-робот сприйняв людину, яка зайшла полагодити його, як загрозу своїм налаштуванням і вбив її. Цей робот не був розроблений для вбивства людей, проте робітник був убитий у результаті дій ШІ, який самостійно змінив мету програмування. У таких випадках перша модель не може бути застосована, оскільки в цій ситуації користувач або розробник не мали наміру вчинити злочин, але проявили недбалість, адже мали передбачити, що такий злочин є ймовірним наслідком певних дій. Отже, така особа може бути притягнута до відповідальності за правопорушення, якщо воно є природним і ймовірним наслідком її дій (бездіяльності). Недбалість може бути двох типів: 1) розробник або користувач не передбачав можливості настання суспільно небезпечних наслідків своєї дії (бездіяльності), хоча повинен був і міг їх передбачити; 2) якщо розробник або користувач передбачав можливість настання суспільно небезпечних наслідків своєї дії (бездіяльності), але легковажно розраховував на їх відвернення. Також може статися ситуація, коли розробник або користувач розробив чи використав ШІ навмисно для вчинення одного виду правопорушення, але ШІ помилково або через використання програмного забезпечення в інший спосіб вчинив інше на додаток до запланованого або замість нього. Наприклад, якщо ШІ, розроблений для крадіжки речей із будинків, під час вчинення злочину вбив того, хто чинив йому опір, це є ймовірним наслідком його дій і мало

бути передбачено розробником або користувачем. У таких випадках вони повинні нести відповідальність за фактично скоєне правопорушення, навіть якщо воно не було заплановане. У наведеному прикладі розробник (користувач) мають бути притягнуті до відповідальності за крадіжку, якщо вона була вчинена згідно з початковим планом, а також за вбивство, яке не було заплановане.

Модель прямої відповідальності ШІ

Для притягнення будь-якої особи до кримінальної відповідальності наявність складу правопорушення є обов'язковою. Якщо ШІ відповідає цим умовам, то відсутні жодні підстави не притягати його до прямої відповідальності за вчинене правопорушення. Справжній виклик полягає в тому, щоб довести, що ШІ мав намір вчинити правопорушення. Людина отримує дані від різних органів чуття (таких як очі, вуха, язик, ніс і шкіра), а потім обробляє їх у мозку, результатом чого є вчинення певних дій або бездіяльність. Просунуті технології ШІ виконують ту саму роботу: вони збирають дані з різних джерел, вчяться на них, обробляють, аналізують і ухвалюють рішення про свої подальші дії. Чому ж тоді ШІ має звільнятися від кримінальної відповідальності? ШІ та людина можуть бути спільними злочинцями, і, відповідно, обидва можуть бути покарані. Отже, за третьою моделлю до ШІ слід застосовувати ті самі кримінальні закони, як до людини, із деякими незначними змінами або коригуваннями.

Основними видами покарання в Україні відповідно до ст. 51 Кримінального кодексу України [8] є штраф; позбавлення військового, спеціального звання, рангу, чину або кваліфікаційного класу; позбавлення права обіймати певні посади або займатися певною діяльністю; громадські роботи; виправні роботи; службові обмеження для військовослужбовців; конфіскація майна; пробаційний нагляд; арешт; обмеження волі; тримання в дисциплінарному батальйоні військовослужбовців; позбавлення волі на певний строк; довічне позбавлення волі. Деякі з цих видів можуть бути застосовані до ШІ, щоб позбавити його здатності або запобігти вчиненню правопорушень у майбутньому. Наприклад, видалення програмного забезпечення, яке керує ШІ, або конфіскація цінного і дорогого ШІ, заборона його використання або знищення. До того ж власники ШІ можуть бути оштрафовані на значні суми або ув'язнені з метою стримування. Розробників або власників можуть попросити виплатити компенсацію постраждалим особам. Особиста свобода ШІ може бути обмежена шляхом призупинення його використання на певний період часу. У сучасних умовах набирають обертів громадські роботи. Тому ШІ, який використовувався для отримання прибутку, може бути використаний для громадських потреб. Ще однією формою покарання є штраф, метою якого є позбавлення особи частини її майна для

створення ефекту стримування. Фізичні та юридичні особи можуть мати активи та банківські рахунки (на відміну від ШІ), тому пропонується зробити невелику поправку під час накладення штрафу на ШІ (на нього може бути накладений примус праці з виплатами на благо суспільства).

13 березня 2024 р. Європейський парламент ухвалив перший у світі акт, який регулює розробку та використання штучного інтелекту — Закон Європейського Союзу (далі — *ЄС*) про штучний інтелект (англ. *AI Act*). У ньому закликали до обов'язкового страхування систем ШІ задля забезпечення можливості сплати ним достатньої грошової компенсації постраждалим. Члени Європарламенту також зазначили, що системи ШІ, визначені як системи високого ризику, тобто які можуть спричиняти значну шкоду здоров'ю, безпеці та основним правам осіб в ЄС, мають бути обмежені, такі обмеження мають також зводити до мінімуму міжнародну торгівлю ШІ. Відповідно до цілей гармонізації законодавства ЄС щодо сприяння вільному переміщенню продуктів на внутрішньому ринку та забезпечення того, щоб на нього потрапляли лише безпечні продукти, важливо, щоб ризики, які можуть бути спричинені системами ШІ, були належним чином попереджені та мінімізовані. Наприклад, роботи, що стають дедалі більш автономними, призначені як для виробництва, так і для особистого застосування, повинні бути здатні безпечно працювати і виконувати свої функції в складних умовах. Аналогічно у секторі охорони здоров'я новітні системи ШІ, що сприяють роботі медичних працівників, повинні бути надійними і точними [9].

Уважають, що якщо винний ШІ буде покараний, це не утримає інші моделі ШІ від скоєння подібних правопорушень, оскільки він не піддається контролю, що суперечить меті стримування, яке може бути двох видів [5]:

— спеціальне стримування орієнтоване на злочинця, який зазнає покарання. Він буде утримуватися від вчинення злочинів у майбутньому. Базові наявні моделі ШІ не розроблені таким чином, щоб відчувати покарання, але майбутні ШІ, збираючи дані з різних джерел, здатні самостійно вчитися на минулому досвіді. Покарання ШІ подаватиме приклад і теоретично може мати стримувальний ефект;

— загальний стримувальний ефект покарання полягає в тому, що воно є прикладом для інших потенційних злочинців. Воно може не стримувати ШІ безпосередньо, але створить загальний ефект, відлякуючи інших потенційних злочинців від вчинення правопорушень із використанням ШІ. Це може бути стримувальним чинником також для інших розробників ШІ, користувачів тощо, адже розробка ШІ вимагає величезних витрат, часу і зусиль.

Ще однією проблемою є те, що за правопорушенням, пов'язаним зі ШІ, може стояти особа, яка перебуває в темній мережі, тобто є повністю анонімною. Відомі випадки, коли хакери заразили ШІ вірусом і залишилися не ідентифікованими, або сам ШІ створив якийсь вірус [11]. Це є дуже небезпечним, оскільки нинішня система кримінального правосуддя не визнає ШІ суб'єктом правопорушення, а коли жодна людина не може бути притягнута до відповідальності, ці злочини залишаться безкарними. Натомість, якщо за автономні дії ШІ каратимуть розробників, то це стане величезною перешкодою для нових досліджень і спричинить побоювання щодо нових розробках ШІ, що зупинить стрімкий технологічний розвиток.

Насамкінець ці три моделі не є взаємовиключними, вони мають рекомендаційний характер щодо того, у яких випадках яку з них слід використовувати. Гармонізація цих моделей може створити неминучу пастку для порушників, незалежно від того, чи це фізична або юридична особа, чи ШІ.

Висновки. Внесення змін до законів для притягнення ШІ до кримінальної відповідальності є дійсно дуже складним завданням. Необхідно провести глибоке дослідження всіх обставин, оскільки щойно ці закони набудуть чинності, вони матимуть незворотні наслідки. ШІ з кожним днем стає складнішим і автономнішим, тому притягнення будь-якої людини до кримінальної відповідальності за правопорушення, скоєні ШІ, не завжди є доцільним. Проте поки ШІ перебуває на стадії зародження, не так багато злочинів він вчиняє сам, здебільшого він є підконтрольним людині. На цьому етапі доцільно внести зміни до чинного законодавства, розширити сферу застосування кримінальних і цивільних покарань, запровадити сувору політику ліцензування та реєстрації ШІ тощо для його стримування від вчинення правопорушень, або, принаймні, стане стримувальним чинником для власників, розробників і користувачів ШІ. Водночас розглядати кримінальну відповідальність безпосередньо ШІ не є передчасним, оскільки науковці безперервно працюють над створенням просунутого ШІ, здатного самостійно ухвалювати вольові рішення. Своєю чергою, це посилить відчуття безпеки в суспільстві та віру в систему кримінального правосуддя. Люди переконаються, що держава дотримується політики нульової толерантності до правопорушень, навіть якщо вони скоєні ШІ. І навпаки, якщо ШІ залишатиметься безкарним, це створить атмосферу страху, що з кожним днем він ставатиме могутнішим і неконтрольованим.

Перелік посилань	**References**
1 Карчевський М. В. Штучний інтелект у діяльності правоохоронних органів: світовий дискурс та	Karchevskyi, M. V. (2023). Artificial Intelligence in Law Enforcement: Global Discourse and Opportunities

можливості для України. Матеріали IX (XXII) Львівського форуму кримінальної юстиції (Львів, 26—27.10.2023). Львів, 2023. С. 121. URL: https://www.lvduvs.edu.ua/uk/library/materialy-naukovykh-onferentsii.html (дата звернення: 04.04.2024).

for Ukraine. Materials of the IX (XXII) Lviv Criminal Justice Forum (Lviv, 26-27.10.2023). Lviv. URL: https://www.lvduvs.edu.ua/uk/library/materialy-naukovykh-onferentsii.html (access date: 04.04.2024) [in Ukrainian].

2. Administración Nacional de la Seguridad Social. URL: https://www.argentina.gob.ar/anses (access date: 04.04.2024).

3. La Administración Federal de Ingresos Públicos (AFIP). URL: https://www.afip.gob.ar/landing/default.asp (access date: 04.04.2024).

4. Russell, S. J., Norvig, P. (2022). Artificial Intelligence: A Modern Approach. URL: http://lib.ysu.am/disciplines_bk/efdd4d1d4c2087fe1cbe03d9ced67f34.pdf (access date: 04.04.2024).

5. Jani, Ch., Rathor, S. P. (2024). A Legal Framework for Determining The Criminal Liability And Punishment For Artificial Intelligence. *Tuijin Jishu/Journal of Propulsion Technology*. Vol. 45. No. 1. URL: https://www.propulsiontechjournal.com/index.php/journal/article/view/4056/2760 (access date: 04.04.2024).

6. Hart, H. L. A. (2008). Punishment and Responsibility. Essays in the Philosophy of Law. Oxford University Press. URL: http://ndl.ethernet.edu.et/bitstream/123456789/77294/1/21%20pdf.pdf (access date: 04.04.2024).

7. Hallevy, G. (2010). The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control. *Akron Intellectual Property Journal*. Vol. 4. Iss. 2. Art. 1. URL: https://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/1 (access date: 04.04.2024).

8. Кримінальний кодекс України від 05.04.2001 № 2341-III (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 04.04.2024).

Criminal Code of Ukraine dated April 5, 2001 No. 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (access date: 04.04.2024) [in Ukrainian].

9. European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021). URL: https://www.europarl.europa.eu/doceo/document/TA-9-2024-03-13_EN.html (access date: 04.04.2024).

10. Oyedele, S. (2023). The Impact of AI on Law Enforcement. Criminology and Criminal Justice / Linkedin. URL: https://www.linkedin.com/pulse/impact-ai-law-enforcement-criminology-criminal-justice-saheed-oyedele-a9sle (access date: 04.04.2024).

11. Swami, B. (2023). Hackers are using artificial intelligence to create sophisticated attacks and malware / Linkedin. URL: https://www.linkedin.com/pulse/hackers-using-artificial-intelligence-create-attacks-malware-bhattar (access date: 04.04.2024).

12. Barrat, J. (2013). Our Final Invention: Artificial Intelligence and the End of the Human Era. URL: https://reactormag.com/our-final-invention-excerpt/ (access date: 04.04.2024).
13. Карчевський М. В. Право роботів, або робот з правами. URL: www.ukrainepravo.com/scientific-thought/naukova-dumka/pravo-robotiv-abo-robot-z-pravami (дата звернення: 04.04.2024). Karchevskyi, M. V. Robot law, or a robot with rights. URL: www.ukrainepravo.com/scientific-thought/naukova-dumka/pravo-robotiv-abo-robot-z-pravami (access date: 04.04.2024) [in Ukrainian].
14. Удовенко Ж. В., Басиста І. В. Використання штучного інтелекту у кримінальному провадженні: ілюзія чи реальність. *Штучний інтелект у правовій практиці: межі та можливості* : зб. тез Всеукр. круглого столу (Львів, 15.03.2024). Львів, 2024. С. 188—197. URL: https://ekmair.ukma.edu.ua/handle/123456789/31443 (дата звернення: 04.04.2024). Udovenko, Zh. V., Basysta, I. V. (2024). The use of artificial intelligence in criminal proceedings: illusion or reality. *Artificial Intelligence in Legal Practice: Limits and Opportunities:* Collection of abstracts of the All-Ukrainian Round Table (Lviv, 15.03.2024). Lviv. URL: https://ekmair.ukma.edu.ua/handle/123456789/31443 (access date: 04.04.2024) [in Ukrainian].

Legal regulation of liability for offenses committed by Artificial Intelligence

Svitlana Kukhareva, Dmytro Kalnoi, Anton Kaminskyi

This article shows scientific discussions on the ways of punishment for the criminal offences committed by artificial intelligent. The author outlines the regulatory framework for bringing to justice for such offences. The definition and types of AI depending on its use are specified in the article. New ways of using latest technologies of AI for the commission of offenses in today`s reality are highlighted. The problematic aspects of identification of the subjects responsible for the offences committed by AI are analyzed. Possibilities of legalization of liability for such offenses at the legislative national and international level, are considered. In particular, three models of criminal liability depending on different situations defined by the Israel professor are examined, such as: AI as a tool for committing a crime, a model of a more advanced version of AI, the model of direct responsibility of AI that means that AI should be subject to the same criminal laws as humans, with some minor changes or adjustments. Also, the forms of punishment due to the Ukrainian legislation that might be applied to AI are analyzed. The author emphasizes some provisions of the world's first act regulating the development and use of artificial intelligence - the EU Artificial Intelligence Act (AI Act) adopted by The European Parliament.

Keywords: *artificial intelligence; latest technologies; offenses; liability; punishment; legal regulation.*

⇒ Кухарева, С., Кальной, Д., Камінський, А. (2025). Правове регулювання притягнення до відповідальності за правопорушення, вчинені штучним інтелектом. *Криміналістика і судова експертиза.* Вип. 70. С. 155—164. DOI: 10.33994/kndise.2025.70.12.