УДК 343:004.8
DOI: https://doi.org/10.24144/2307-3322.2026.94.3.14

«АЛГОРИТМ-ЗЛОЧИНЕЦЬ» АБО ПРО ПЕРСПЕКТИВИ КРИМІНАЛІЗАЦІЇ ЗЛОВЖИВАНЬ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Каменський Д.В.,
доктор юридичних наук, професор,
професор кафедри кримінального права та кримінології
Національної академії Служби безпеки України
ORCID: 0000-0002-3610-2514
e-mail: dm.kamensky@gmail.com

Каменський Д.В. «Алгоритм-злочинець» або про перспективи криміналізації зловживань з використанням штучного інтелекту.

У статті розглянуті сучасні виклики кримінально-правового регулювання, пов'язані з використанням технологій штучного інтелекту (ШІ). Автор аналізує вплив стрімкого розвитку систем ШІ на трансформацію традиційних уявлень про суб'єкта кримінального правопорушення, про форми суспільно небезпечної поведінки та механізми притягнення до кримінальної відповідальності. Особливу увагу приділено проблемі визначення суб'єкта правопорушення в умовах складної взаємодії розробників, виробників, користувачів та інших залучених до створення та використання ШІ осіб.

У роботі висловлено позицію про те, що класичні елементи складу злочину, зокрема діяння (actus reus), вина (mens rea) та причинний зв'язок між діянням і наслідками, не завжди можуть бути коректно застосовані до діянь, вчинених із використанням автономних алгоритмічних систем. Проаналізовано сучасні підходи до вирішення цієї проблеми, включаючи концепцію «електронної особи», а також альтернативні моделі розподілу відповідальності між учасниками процесу створення, навчання та використання ШІ. Водночас зроблено застереження, що на сучасному етапі розвитку технологій надання ШІ статусу самостійного суб'єкта кримінальної відповідальності є передчасним.

Окрему увагу приділено аналізу європейського підходу до регулювання ШІ, зокрема положенням Акта ЄС про штучний інтелект, який визначає, поміж іншого, заборонені практики використання відповідних технологій. Проаналізовано ст. 5 Акта, яка забороняє зокрема використання ШІ для маніпуляції поведінкою людей, експлуатації їх вразливостей, соціального рейтингування, профілювання злочинності, масового збору біометричних даних, розпізнавання емоцій, дискримінаційної біометричної категоризації та широкого застосування біометричної ідентифікації. Показано, що криміналізація зловживань із використанням ШІ перебуває на початковій стадії формування як у ЄС, так і у США, де відсутній комплексний кримінально-правовий акт у цій сфері.

У висновках роботи наголошується на необхідності обережної адаптації чинного кримінального законодавства до нових технологічних реалій, зокрема шляхом розроблення спеціальних заборон, удосконалення механізмів розслідування правопорушень у сфері ШІ та забезпечення оптимального балансу між інноваційним розвитком технологій та захистом суспільних інтересів.

Ключові слова: штучний інтелект, суб'єкт кримінального правопорушення, кримінальна відповідальність, вина, «електронна особа».

Kamensky D.V. «Criminal algorithm», or on the prospects of criminalizing offenses involving artificial intelligence.

The article examines contemporary challenges in criminal law regulation arising from the use of artificial intelligence (AI) technologies. The author analyzes the impact of the rapid development of AI systems on the transformation of traditional understandings of the subject of a criminal offense, the forms of socially dangerous behavior, and the mechanisms of criminal liability. Particular attention is paid to the problem of identifying the offender in the context of complex interactions among developers, manufacturers, users, and other actors involved in the creation and use of AI.

The paper argues that the classical elements of a crime – namely, conduct (*actus reus*), fault (*mens rea*), and the causal link between conduct and consequences – cannot always be properly applied to acts committed with the use of autonomous algorithmic systems. The author reviews current approaches to addressing this issue, including the concept of an "electronic person," as well as alternative models for distributing liability among participants in the development and deployment of AI. At the same time, it is emphasized that, at the current stage of technological development, granting AI the status of an independent subject of criminal liability would be premature.

Special attention is paid to the analysis of the European approach to AI regulation, in particular the provisions of the EU Act on Artificial Intelligence, which defines, among other things, prohibited practices in the use of relevant technologies. The analysis includes Article 5 of the Act, which prohibits, in particular, the use of AI for the manipulation of human behavior, exploitation of their vulnerabilities, social ranking, criminal profiling, mass collection of biometric data, recognition of emotions, discriminatory biometric categorization and widespread use of biometric identification. It is shown that the criminalization of abuses of AI is at the initial stage of formation in both the EU and the USA, where there is no comprehensive criminal law act in this area.

The conclusions stress the need for cautious adaptation of existing criminal legislation to new technological realities, including the development of specific prohibitions, improvements to investigative mechanisms for AI-related offenses, and the maintenance of an appropriate balance between technological innovation and the protection of societal interests.

Key words: artificial intelligence, subject of a criminal offense, criminal liability, fault, "electronic person".

Постановка проблеми. «Це не моя вина – це алгоритм!» – висловлювання на кшталт цього можна почути в сучасному дедалі більш диджиталізованому світі, в якому нові технології нерідко випереджають не лише питання безпеки для користувачів, а й навіть базове правове регулювання. Справді, хоча використання шкідливого алгоритму може означати, що штучний інтелект (ШІ) спричинив небажану подію, яка зашкодила охоронюваним законом інтересам, питання юридичної відповідальності наразі й здебільшого залишається без відповіді. У таких випадках правильне визначення суб'єкта правопорушення стає надзвичайно важливим завданням.

Сьогодні фахівці та широкий загал виходять з того, що стрімкий розвиток різноманітних систем і технологій ШІ істотно впливає на соціальні, економічні та правові відносини в суспільстві. Алгоритми машинного навчання, автономні системи прийняття рішень, генеративні моделі та інші форми штучного інтелекту дедалі ширше використовуються у сфері фінансів, транспорту, медицини, державного управління, безпеки й навіть юриспруденції. Водночас їх масове використання породжує нові правові виклики та загрози, не останньою чергою в сфері кримінального права, де постає актуальне питання визначення нових форм суспільно небезпечної поведінки, вчиненої за участю або з використанням таких технологій.

Творчим поштовхом до написання цієї роботи стала нещодавно опублікована стаття моєї американської колеги, професорки кримінального права Університету Стетсона Еллен Подгор з провокативною назвою «Smart Crime» («Розумна злочинність») [1]. У своєму безперечно актуальному та ретельно проведеному дослідженні авторка аналізує численні виклики, які створює стрімкий розвиток ШІ для сучасної системи кримінального права США та інших держав. Е. Подгор застерігає: подальше очікуване зростання автономності систем штучного інтелекту супроводжується небезпечною відсутністю адекватної кримінально-правової моделі, здатної ефективно запобігати новим проявам протиправної поведінки, пов'язані з використанням таких технологій. Авторка проводить історичну паралель із розвитком законодавства про комп'ютерні злочини у США, зокрема із запровадженням федерального акта «Computer Fraud and Abuse Act». Вона застерігає: в минулому спроби застосовувати до нових технологій традиційні кримінально-правові заборони часто виявлялися неефективними. Водночас класична для англо-американського кримінального права конструкція злочину, з його вихідними ознаками діяння та вини – *actus reus*, *mens rea,* а також причинного зв'язку – не завжди придатна для правової оцінки діянь, у яких задіяні не фізичні чи юридичні особи, а власне автономні алгоритмічні системи. У зв'язку з цим згадана авторка обґрунтовує потребу саме в проактивному формуванні спеціального кримінально-правового регулювання у сфері використання технологій штучного інтелекту, яке, з одного боку, не повинно перешкоджати технологічному прогресу, а з іншого

– повинно забезпечувати надійний захист суспільства від протиправного зловживання технологіями ШІ чи його окремими компонентами.

Автор вбачає **мету статті** в аналізі випадків шкідливого (суспільно-небезпечного) використання технології ШІ через призму його перспективного кримінально-правового регулювання, у визначенні основних кримінально-правових ризиків, пов'язаних із використанням систем ШІ, а також в оцінці можливих напрямів розвитку кримінального законодавства у відповідь на сучасні виклики технологічного розвитку машинних систем.

Стан опрацювання проблематики. Проблематика кримінальної відповідальності штучного інтелекту дедалі більш активно розвивається у сучасній доктрині кримінального права та в суміжних міждисциплінарних дослідженнях. В українській науці окремі матеріальні та процесуальні аспекти цієї тематики розглядаються у працях О. Радутного, С. Денисова, М. Карчевського, А. Підуудбної, К. Ярового. У США вагомий внесок у дослідження кримінально-правових викликів, пов'язаних із застосуванням штучного інтелекту, здійснили E. Podgor, M. Diamantis, R. Abbott, D. Citron, W. Eichner та деякі інші. У європейській правовій науці ця проблематика активно розробляється в працях S. Quattrocolo, K. Ligeti, S. Gless, P. De Hert, V. Mitsilegas, G. Sartor, K. Burdziak, I. Ambrus тощо. Широка географія сучасних досліджень підтверджує глобальний характер цієї нової проблематики та необхідність вироблення нових, і бажано узгоджених, підходів до кримінально-правового регулювання ШІ.

Під час написання цієї роботи інструменти штучного інтелекту (ChatGPT) використовувались виключно для перекладу деяких зарубіжних наукових джерел, а також для оформлення й упорядкування списку використаних джерел.

Виклад основного матеріалу. У кримінально-правовій доктрині виникає низка складних, наразі не розв'язаних питань на кшталт: чи може штучний інтелект визнаватись самостійним суб'єктом кримінальної відповідальності; яким чином розподіляється відповідальність між розробниками, власниками, користувачами та операторами систем штучного інтелекту; також чи потребує кримінальне законодавство спеціальних норм, спрямованих на регулювання таких технологій? Наразі в різних правових системах пропонуються різні підходи до вирішення цих питань – від збереження традиційної концепції відповідальності людини до формування нових моделей технологічної відповідальності.

Напевне має рацію М.В. Карчевський, коли пише: сучасні моделі штучного інтелекту, зокрема великі мовні моделі (LLM), демонструють значні досягнення у сфері обробки природної мови, розпізнавання образів, генерації контенту та інших напрямах. Водночас, попри здатність відтворювати окремі риси людської поведінки, вони залишаються всього лише інструментами, створеними для виконання конкретних завдань [2]. Відповідно, активні фахові дискусії наразі точаться навколо питань про сфери застосування таких систем, про мінімізацію потенційних ризиків заподіяння шкоди та встановлення меж їх допустимого використання.

До слова, в сучасних збройних конфліктах ШІ дедалі частіше використовується не лише як технологія озброєння, а й як інструмент інформаційного впливу та маніпуляцій зі свідомістю аудиторії (так званий "deep fake"). Як приклад, в одній з нещодавніх публікацій газети «New York Times» повідомлялось про масове поширення під час війни на Близькому Сході фальшивих відео та зображень, створених за допомогою технологій ШІ. За даними журналістського розслідування, лише протягом двох тижнів було виявлено понад 110 унікальних AI-генерованих матеріалів, які імітували бойові дії, руйнування міст в країнах Перської затоки, атаки на військові об'єкти або сцени людських втрат, хоча насправді такі події не відбувалися. Ці матеріали отримали мільйонні перегляди в соціальних мережах та месенджерах, формуючи викривлене уявлення серед аудиторії про перебіг війни [3]. Подібні приклади демонструють, що технології ШІ можуть використовуватися як інструмент інформаційної війни, пропаганди та масштабних маніпуляцій громадською думкою. Для кримінального права це створює нові виклики, пов'язані з необхідністю точної кримінально-правової оцінки діянь, пов'язаних із поширенням дезінформації, створенням deepfake-контенту, втручанням в інформаційну безпеку держави та використанням ШІ як засобу вчинення злочинів, передусім шахрайського, корисливого спрямування.

Власне термін «штучний інтелект» (англ. – Artificial Intelligence, скор. – AI) був запропонований в науковий обіг ще в 1956 р. під час конференції в Дартмутському коледжі, організованої професором цього коледжу Джоном Маккарті. У своїй промові на тому заході професор Маккарті зазначив, що учасники конференції повинні були виходити з припущення про те, що будь-яка

складова людського навчання чи будь-яка інша особливість інтелекту в принципі може бути настільки точно описана, що можливо створити машину для її імітації [4]. Концепція ШІ із самого початку була зосереджена на пошуку способів зробити машини (комп'ютери) більш здатними до усвідомленого пізнання та обробки масивів інформації, максимально точно імітувати людську свідомість та інтелект. Хоча технології машинного навчання існували ще до формального визнання ШІ як окремого напряму досліджень, саме запровадження цього терміна в науковий, а згодом і суспільний обіг стимулювало новий етап розвитку технологій, пов'язаних з використанням та аналізом даних.

Водночас потрібно застерегти, що єдиного, універсально визнаного визначення штучного інтелекту наразі не існує, що в принципі є виправданим.

Американський інститут права (англ. American Law Institute)[1] визначає алгоритм (як базовий структурний елемент функціонування систем ШІ) таким чином: це набір покрокових інструкцій або правил, призначених для вирішення проблеми або виконання певного завдання. Подібно до будь-якого рецепта, алгоритм приймає вхідні дані (інгредієнти), обробляє їх за допомогою визначеної послідовності дій та видає вихідний результат (так би мовити, готову страву). Алгоритм – це широке поняття, що має надзвичайно важливе значення в інформатиці. Комп'ютерний алгоритм реалізується за допомогою програмного забезпечення, написаного на певних мовах програмування, які можуть виконувати комп'ютери [5].

Вітчизняний вчений О. Радутний пише, що ШІ характеризується низкою ключових рис. По-перше, він здатний здійснювати комплексну обробку великих масивів даних, отриманих із різних джерел; по-друге, володіє можливістю самонавчання, що включає накопичення досвіду, узагальнення інформації та виявлення прихованих зв'язків, а також синтезування висновків; по-третє, здатний до планування; і, по-четверте, може здійснювати певні «роздуми». Причому у відповідь на інтелектуальні запити чи аналіз з боку розробників система здатна спрямовувати додаткові ресурси на власне осмислення. Відтак штучний інтелект потенційно набуває рис, подібних до людських: він може усвідомлювати фактичні обставини, оцінювати суспільну небезпечність своїх дій, що реалізуються як у цифровому середовищі, так і через роботизовані системи у матеріальному світі, а також здійснювати вибір між альтернативними моделями поведінки й контролювати власні дії чи бездіяльність. Це, зокрема, підтверджується сучасними практиками застосування ШІ у хірургії, робототехніці чи керуванні безпілотними апаратами [6, с. 109].

Водночас, у доктрині вітчизняного кримінального права (слідом за кримінальним законом) аксіоматичною є позиція, відповідно до якої суб'єктом кримінального правопорушення може бути виключно фізична особа. Основним аргументом на користь цього є відсутність у ШІ свободи волі, оскільки він функціонує в межах заздалегідь закладених у нього алгоритмів. Проте з огляду на подальше зростання автономності таких систем цей аргумент поступово втрачає свою беззаперечність. Таким чином, відносно нова концепція «електронної особи» залишається принаймні дискусійною.

Надання ШІ статусу «електронної особи» як суб'єкта правовідносин не є концептуально чужим для сучасних правових систем деяких держав, передусім США, з огляду на вже усталене визнання юридичних осіб, які також мають умовно «віртуальний» характер. Традиційно вважалося, що юридична особа діє виключно через фізичних осіб, які, власне, можуть підлягати кримінальній відповідальності. Однак у США, а згодом і деяких інших юрисдикціях, юридичні особи (корпорації) згодом трансформувались у цілком самостійних суб'єктів злочинів із притаманними ознаками вини та протиправного діяння.

Це може виступати підґрунтям для поступового розширення підходів до суб'єктності у кримінальному праві та створювати новий простір для подальших дискусій щодо правового (і кримінально-правового) статусу ШІ.

Зі свого боку, уже згадувана мною Е. Подгор також ретельно розмірковує над питанням про можливість кримінально-правової «суб'єктивізації» ШІ як окремого різновиду «електронної особи». Вона вважає, що при визначенні «особи», яка вчинила діяння, необхідно враховувати три допоміжні питання: 1) хто саме вчинив дію; 2) чи був цей суб'єкт людиною; 3) чи може «нелюдський» суб'єкт вчинити *actus reus*?

[1] Це провідна незалежна науково-правова організація США, заснована у 1923 р., яка об'єднує суддів, науковців та практикуючих юристів. Основна мета полягає у регулярному вдосконаленні національного права, уніфікації правових підходів, підвищенні якості правосуддя.

Встановлення того, хто саме вчинив діяння, є значно складнішим, аніж у типовій справі про загальнокримінальний злочин, де правопорушником є особа, яка безпосередньо завдала фізичної шкоди потерпілому, або, наприклад, особа, що здійснила крадіжку чи ввела команду у випадку комп'ютерного злому. Натомість галузі ШІ потенційними суб'єктами можуть виступати розробник алгоритму, науковці, які створили модель ШІ, виробник системи, продавець або користувач алгоритму, а також інші особи [1, с. 40–41].

Уже сьогодні стає очевидним, що зростання автономності ШІ-систем ставить під сумнів ефективність усталених форм кримінальної відповідальності. Наразі відповідальність покладається переважно на розробників, виробників або власників таких систем, однак у майбутньому може виникнути потреба у формуванні нових моделей правосуб'єктності та відповідальності.

Концепція автономної «електронної особи» тлумачиться як потенційний механізм вирішення проблеми відповідальності. Водночас сучасні цифрові технології поки що не досягли такого рівня, який би обґрунтовував надання ШІ-системам статусу, аналогічного фізичній особі. А тому більш реалістичним підходом, на думку деяких фахівців, видається створення окремої правової категорії для автономних систем із визначеними правами та обов'язками [7, с. 22].

Передбачається, що такий статус може в майбутньому надаватися лише системам із високим рівнем автономії, здатним до самостійного ухвалення рішень і повноцінної взаємодії з людьми. Разом із тим, для більшості спеціалізованих технічних систем (наприклад, роботизованих транспортних засобів) надання правосуб'єктності не є доцільним, оскільки відповідальність і надалі може покладатися на розробників та осіб, які їх використовують.

Ситуація суттєво ускладняється в умовах розвитку загального штучного інтелекту (Artificial General Intelligence або AGI), коли система уже здатна діяти самостійно, на свій розсуд, без прямого людського втручання й контролю. У таких випадках визначення наявності діяння та добровільності його вчинення стає особливо проблематичним. Постає питання, чи має значення тип штучного інтелекту (звичайний ШІ, агентний ШІ чи AGI) для оцінки обсягу людської відповідальності, яка може змінюватися залежно від рівня автономності системи.

Наразі класична теорія кримінального права, як у державах континентального, так і у державах прецедентного права, навіть у випадках притягнення до відповідальності людини або юридичної особи, поки що навіть концептуально не визнає алгоритм самостійним суб'єктом злочинного діяння. Водночас варто очікувати посилення фахових дискусій у цьому напрямі, що актуалізує проведення порівняльно-правових досліджень [8, с. 108–112].

У контексті євроінтеграційного поступу України варто звернути увагу на положення Акта ЄС про штучний інтелект (далі – Акт про ШІ) [9][1]. Головною метою цього об'ємного за змістом документа, ухваленого 13 червня 2024 р., стало покращення функціонування внутрішнього ринку шляхом встановлення єдиної правової бази, зокрема для розробки, розміщення на ринку, введення в експлуатацію та використання систем штучного інтелекту (систем ШІ) у ЄС відповідно до цінностей Союзу, для сприяння впровадженню людиноцентричного та надійного штучного інтелекту (ШІ), забезпечуючи при цьому високий рівень захисту здоров'я, безпеки, основних прав, закріплених у Хартії основних прав Європейського Союзу («Хартія»), включаючи демократію, верховенство права та охорону навколишнього середовища, для захисту від шкідливого впливу систем ШІ в Союзі та для підтримки інновацій.

Окрім великої кількості положень, присвячених організаційно-правовим, економічним, екологічним та іншим засадам розвитку ШІ-технологій на теренах Євросоюзу, ст. 5 документа безпосередньо адресує питання заборонених практики – тобто сфер застосування ШІ, на які поширюється пряма заборона.

Отже, ст. 5 «Заборонені ШІ-практики» безпосередньо забороняє наступні форми (способи) використання технологій ШІ:

(а) виведення на ринок, введення в експлуатацію або використання системи ШІ, яка застосовує підсвідомі техніки поза межами усвідомлення особи або навмисно маніпулятивні чи оманливі техніки з метою або з наслідком істотного викривлення поведінки особи чи групи осіб шляхом

[1] Повна назва цього документа - Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту та вносить зміни до Регламентів (ЄС) № 300/2008, (ЄС) № 167/2013, (ЄС) № 168/2013, (ЄС) 2018/858, (ЄС) 2018/1139 та (ЄС) 2019/2144 та Директив 2014/90/ЄС, (ЄС) 2016/797 та (ЄС) 2020/1828 (Акт про штучний інтелект).

суттєвого порушення їх здатності приймати обґрунтоване рішення, внаслідок чого вони приймають рішення, яке вони за інших умов не прийняли б, і яке спричиняє або з розумною ймовірністю може спричинити значну шкоду цій особі, іншій особі або групі осіб;

(b) виведення на ринок, введення в експлуатацію або використання системи ШІ, яка експлуатує будь-які вразливості фізичної особи або певної групи осіб, пов'язані з їхнім віком, інвалідністю або конкретним соціальним чи економічним становищем, з метою або з наслідком істотного викривлення поведінки цієї особи або особи з такої групи таким чином, що це спричиняє або з розумною ймовірністю може спричинити значну шкоду цій особі або іншій особі;

(c) виведення на ринок, введення в експлуатацію або використання систем ШІ для оцінювання або класифікації фізичних осіб чи груп осіб протягом певного періоду часу на основі їхньої соціальної поведінки або відомих, виведених чи прогнозованих персональних або особистісних характеристик, якщо такий соціальний рейтинг призводить до одного або обох із таких наслідків:

(i) шкідливого або несприятливого ставлення до певних фізичних осіб або груп осіб у соціальних контекстах, не пов'язаних із тими, в яких дані були спочатку згенеровані або зібрані;

(ii) шкідливого або несприятливого ставлення до певних фізичних осіб або груп осіб, яке є невиправданим або непропорційним їхній соціальній поведінці або її тяжкості;

(d) виведення на ринок, введення в експлуатацію для цієї конкретної мети або використання системи ШІ для здійснення оцінки ризиків щодо фізичних осіб з метою оцінювання або прогнозування ризику вчинення фізичною особою кримінального правопорушення, якщо це здійснюється виключно на основі профілювання фізичної особи або оцінки її особистісних рис і характеристик; ця заборона не застосовується до систем ШІ, що використовуються для підтримки людської оцінки участі особи у злочинній діяльності, яка вже базується на об'єктивних і верифікованих фактах, безпосередньо пов'язаних із такою протиправною діяльністю;

(e) виведення на ринок, введення в експлуатацію для цієї конкретної мети або використання систем ШІ, які створюють або розширюють бази даних розпізнавання обличь шляхом невибіркового збирання зображень обличь з інтернету або записів відеоспостереження;

(f) виведення на ринок, введення в експлуатацію для цієї конкретної мети або використання систем ШІ для визначення емоцій фізичної особи у сферах праці та освіти, за винятком випадків, коли використання системи ШІ призначене для медичних або безпекових цілей;

(g) виведення на ринок, введення в експлуатацію для цієї конкретної мети або використання систем біометричної категоризації, які класифікують фізичних осіб на основі їхніх біометричних даних з метою визначення або виведення їхньої раси, політичних поглядів, членства у профспілках, релігійних або філософських переконань, статевого життя чи сексуальної орієнтації; ця заборона не охоплює маркування або фільтрацію законно отриманих біометричних наборів даних, таких як зображення, на основі біометричних даних або категоризацію біометричних даних у сфері правоохоронної діяльності;

(h) використання систем «реального часу» щодо віддаленої біометричної ідентифікації у публічно доступних місцях з метою правоохоронної діяльності, якщо тільки і в тій мірі, в якій таке використання є строго необхідним для досягнення однієї з таких цілей:

(i) цільового пошуку конкретних жертв викрадення, торгівлі людьми або сексуальної експлуатації, а також пошуку зниклих осіб;

(ii) запобігання конкретній, значній і неминучій загрозі життю або фізичній безпеці фізичних осіб або реальній і наявній чи передбачуваній загрозі терористичного нападу;

(iii) встановлення місцезнаходження або ідентифікація особи, яка підозрюється у вчиненні кримінального правопорушення, з метою проведення кримінального розслідування або кримінального переслідування чи виконання кримінального покарання за правопорушення, зазначені в Додатку II, і які караються у відповідній державі-члені позбавленням волі або заходом затримання на максимальний строк не менше чотирьох років [10]. Ідеться зокрема про такі правопорушення: тероризм, торгівля людьми, сексуальна експлуатація дітей та дитяча порнографія, незаконний обіг наркотичних засобів або психотропних речовин, незаконний обіг зброї, боєприпасів або вибухових речовин, вбивство, тяжкі тілесні ушкодження, незаконна торгівля органами або тканинами людини, незаконний обіг ядерних або радіоактивних матеріалів, викрадення людей, незаконне позбавлення волі або захоплення заручників, злочини, що підпадають під юрисдикцію Міжнародного кримінального суду, незаконне захоплення повітряних суден або суден, згвалтування, злочини проти довкілля, організоване або збройне пограбування, саботаж.

Як можна побачити з наведеного переліку заборонених (і поки що не криміналізованих на національному рівні) способів використання ШІ, тут ідеться здебільшого про окремі випадки «на перехресті» технологій та людської діяльності – зокрема заборони на використання шахрайських практик за допомогою ШІ, цифрові форми «стеження» за людьми та їхньою поведінкою, а також різні форми створення профайлів користувачів під загрозою можливої дискримінації за окремим ознаками. Звертає на себе увагу універсальний текстуальний зворот «виведення на ринок, введення в експлуатацію або використання систем ШІ». Таке формулювання не є оригінальним, воно активно застосовується також в інших Директивах ЄС і підкреслює власне комерційно-функціональний характер відповідних заборон – забороняється саме виводити на ринок (варто розуміти – передусім з метою одержання доходу), а також продовжувати використовувати раніше виведену на ринок технологію ШІ.

Також варто прогнозувати, що з подальшим стрімким розвитком технологій ШІ перелік заборонених кримінальним законом діянь істотно збільшуватиметься.

Наразі вид юридичної відповідальності, види та розміри санкцій за порушення цих заборон не конкретизовані в Акті про ШІ. Натомість можна прогнозувати, що ці питання будуть згодом конкретизовані як в загальноєвропейському, так і в національному законодавстві держав-членів ЄС.

Аналіз інших юрисдикцій на предмет можливої криміналізації зловживань із ШІ також демонструє, що це питання наразі перебуває лише на рудиментарних стадіях публічних і фахових обговорень. Так, у США, незважаючи на наявність уже чималої кількості наукових праць та експертних досліджень щодо проблем, пов'язаних із правовим регулюванням ШІ, як безпосередньо у сфері кримінального права, так і поза нею, досі не запроваджено комплексного федерального акта, який прямо був би спрямований на всі форми зловживання ШІ [10, с. 682–685]. Запропоновані законодавчі ініціативи у сфері ШІ мають, як правило, фрагментарний характер і зосереджені лише на окремих питаннях, таких як захист прав дітей або авторське право. Водночас спостерігається відсутність комплексного підходу до різних кримінально-правових аспектів застосування та зловживання ШІ, що вже наявні або тільки-но мають з'явитися у майбутньому.

До того ж, наголошує Е. Подгор, «рамковий» кримінальний закон про ШІ, побудований на класичних елементах *actus reus*, *mens rea* та причинного зв'язку, навряд чи може з'явитися найближчим часом. Причиною цього є те, що автономна поведінка ШІ не вписується чітко у ці традиційні категорії. Наприклад, задається питанням американська дослідниця, коли алгоритм вчиняє добровільну дію? Чи варто шукати ознаку вини в діях розробника, програміста, користувача чи корпорації, яка могла придбати відповідний алгоритм для власних цілей [1, с. 8]? Водночас, незважаючи на наявні правові прогалини, спостерігається певний прогрес у створенні кримінально-правової архітектури ШІ. Навіть на міжнародному рівні багато хто утримується від закликів до прийняття спеціальних кримінально-правових норм, присвячених ШІ-зловживанням, натомість вдаючись до підходу використання уже наявних кримінально-правових заборон для переслідування неправомірного використання ШІ.

Висновки. Узагальнюючи проведений у цій статті аналіз, варто зазначити, що порушення і зловживання, пов'язані з використанням ШІ, характеризуються складністю та множинністю потенційно відповідальних суб'єктів. Покладення відповідальності виключно на користувача ШІ-системи у разі настання шкоди не завжди є справедливим або обґрунтованим, тоді як у певних випадках відповідальність може нести виробник чи розробник відповідних систем у разі встановлення недбалої форми вини. Це свідчить про багаторівневий характер таких правопорушень і водночас ускладнює процес визначення суб'єкта кримінальної відповідальності порівняно з традиційними ситуаціями.

Попри відсутність універсальної правової моделі притягнення до відповідальності за протиправні діяння, вчинені з використанням таких систем, чинні правові механізми демонструють достатню гнучкість для реагування на такі виклики. У зв'язку з цим, вважаю, що запровадження концепції «електронної особи» для потенційної криміналізації поведінки ШІ видається передчасним, оскільки наявна нормативна база загалом здатна охопити можливі випадки зловживань у найближчій перспективі.

ШІ створює ситуацію *sui generis* для потенційного реформування кримінального права. Його стрімкий розвиток, конкуренція між питаннями безпеки та перспективами розвитку інновацій, а також невідповідність традиційним кримінально-правовим категоріям зумовлюють необхідність спеціального законодавчого регулювання, яке не може бути забезпечене загальними нормами. Очевидно, що ефективне кримінально-правове регулювання неможливе без глибокого розуміння

як сучасних можливостей ШІ, так і перспектив його подальшого розвитку. Водночас законодавець (і не лише вітчизняний) повинен забезпечити баланс між вимогами безпеки та необхідністю підтримки інноваційного розвитку, що може передбачати інструменти прозорості, механізми викривачів, а також ліцензування ШІ-систем.

Незалежно від обраної моделі регулювання – чи то через спеціалізований державний орган, агентське наглядове регулювання або регламентацію через міжнародні інституції, формування кримінально-правових підходів повинно здійснюватися із залученням широкого кола стейкхолдерів, включаючи державу в особі відповідних органів влади (передусім законодавчих та правоохоронних), науковців та представників приватний сектор. Такий діалог в режимі *de lege ferenda* стає затребуваним в умовах стрімкого технологічного розвитку.

Під час написання цього дослідження автор мав можливість розкрити лише декілька актуальних аспектів комплексної науково-прикладної проблематики про місце ШІ в механізмі кримінально-правового регулювання сучасних суспільних відносин. Варто додати власне припущення про те, що одночасно з активним розвитком технологій ШІ також виникатиме дедалі більше питань про юридичну природу та наслідки суспільно небезпечних діянь (наразі не визнаних кримінально протиправними), що вчиняються з використанням ШІ – бодай поки що не власне алгоритмами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Podgor E.S. Smart crime. *Stetson University College of Law Research Paper*. 2026. URL: https://ssrn.com/abstract=6296118 (дата звернення: 16.03.2026). DOI: http://dx.doi.org/10.2139 / ssrn.6296118.
2. Карчевський М.В., Карчевська О.В. Структурний вимір правового регулювання штучного інтелекту. *Український політико-правовий дискурс.* 2024. DOI: https://doi.org/10.5281/zenodo.15782211.
3. The New York Times. A.I.-generated disinformation about the Iran war floods social media. URL: https://www.nytimes.com/interactive/2026/03/14/business/media/iran-disinfo-artificial-intelligence.html (accessed: 16.03.2026).
4. McCarthy J., Minsky M. L., Rochester N., Shannon C. E. A proposal for the Dartmouth summer research project on artificial intelligence. 1956. URL: https://home.dartmouth.edu/ about/ artificial-intelligence-ai-coined-dartmouth (accessed: 16.03.2026).
5. American Law Institute. Civil liability for artificial intelligence. URL: https://www.ali.org/system/files/project-documents-2025-09/Civil%20Liability%20for%20AI%20-%20PD1%20-%20booked.pdf (accessed: 26.03.2026).
6. Радутний О. Е. Штучний інтелект як суб'єкт злочину. *Інформація і право.* 2017. № 4(23). С. 106–115. DOI: https://doi.org/10.37750/2616-6798.2017.4(23).273130.
7. Nanos A. Criminal liability of artificial intelligence. *Charles University in Prague Faculty of Law Research Paper.* 2023. No. 2023/III/3. URL: https://papers.ssrn.com/sol3/ papers.cfm?abstract_id=4623126 (дата звернення: 22.03.2026).
8. Каменський Д.В. Методологічні особливості порівняльних кримінально-правових досліджень: здобутки української та американської доктрини. *Науковий вісник Міжнародного гуманітарного університету.* 2020. № 44. С. 108–112. DOI: https://doi.org/10.32841/2307-1745.2020.44.23.
9. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. 2024. URL: https://eur-lex.europa.eu (дата звернення: 24.03.2026).
10. Lima D. Could AI agents be held criminally liable? Artificial intelligence and the challenges for criminal law. *South Carolina Law Review.* 2018. Vol. 69, No. 3. P. 677–696.

Дата першого надходження рукопису до видання: 26.03.2026
Дата прийняття до друку рукопису після рецензування: 23.04.2026
Дата публікації: 10.05.2026