

УДК 343.22

DOI: <https://doi.org/10.21564/2311-9640.2023.20.292386>

**М. В. Шепітько,**

докт. юрид. наук, проф.,  
професор кафедри кримінального права  
Національного юридичного  
університету імені Ярослава Мудрого,  
провідний науковий співробітник  
НДІ вивчення проблем злочинності  
імені академіка В. В. Сташиса

### **ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ, ВИКОРИСТАННЯ ТА ВІДПОВІДАЛЬНОСТІ ШТУЧНОГО ІНТЕЛЕКТУ В ЄС ТА УКРАЇНІ**

*Розвиток штучного інтелекту та його значна роль в економічних та соціальних відносинах, воєнні та кіберзагрози, які ним породжуються вказують на актуальність дослідження даної проблеми. Україна як жертва російської широкомасштабної воєнної агресії в 2022 р. є зацікавленою у регулюванні даної сфери з метою нейтралізації загроз в воєнному та кіберпросторах.*

*Дослідження впровадження, використання та відповідальності штучного інтелекту в Європейському Союзі може надати вектори кримінальної відповідальності фізичних (операторів), юридичних осіб (заводів і постачальників), а також держав, які реалізують їх у мирний або воєнний час із злочинною (терористичною) метою. Важливим у цьому дослідженні стає питання можливого впровадження штучного інтелекту як інструменту діяльності органів кримінальної юстиції. Європейська комісія, враховуючи зростання застосування ШІ в Європейському Союзі, сформулювала в 2018 р. його визначення. Україна також в 2020 р. прийняла Концепцію розвитку штучного інтелекту. Однак очевидним стає факт гармонізації законодавства ЄС та України в цій сфері.*

*Робота Європейської комісії щодо штучного інтелекту втілюється в Стратегію штучного інтелекту для Європи на 2018 р. (2018 AI Strategy for Europe), білу книгу щодо штучного інтелекту на 2020 р. (White Paper on AI) і нещодавно оновлений скоординований план щодо штучного інтелекту. Також триває підготовка закону про штучний інтелект (Artificial Intelligence Act).*

*Аналіз нормативної бази та позицій щодо впровадження, використання та відповідальності штучного інтелекту вказують на такі тенденції: 1) використання штучного інтелекту в Європейському Союзі стає регульованою сферою, що формує права, обов'язки та відповідальність учасників; 2) застосування штучного інтелекту в органах кримінальної юстиції зазнає суттєвих обмежень та заборон; 3) відповідальність за застосування штучного інтелекту та за небезпечні наслідки, які ним*

можуть бути спричинені, покладається на фізичних та юридичних осіб, а також держав, в чийх інтересах він застосовується.

**Ключові слова:** кримінальна відповідальність, кримінальна політика, кримінальна юстиція, інформаційна безпека, цифрова безпека, штучний інтелект.

Українська національна група Міжнародної асоціації карного права (далі – МАКП) прийняла участь в науковому циклі (2019–2024), що завершується Конгресом «Штучний інтелект та кримінальна юстиція» 26–28 червня 2024 р. в Парижі (Франція). МАКП наполягає, що «кримінальне право – у найширшому сенсі – більше не може ігнорувати штучний інтелект (далі – ШІ) та пов’язані з ним проблеми. Глибокі роздуми про те, чи, якою мірою та за яких умов сумісне використання систем ШІ в кримінальному судочинстві з основними принципами наших систем, більше не можна відкладати»<sup>1</sup>.

Враховуючи розвиток ШІ, зростаючу роль в економічних та соціальних відносинах, воєнні та кіберзагрози, актуальність дослідження даної проблеми тільки зросла<sup>2</sup>. В Україні, яка стала жертвою російської широкомасштабної воєнної агресії в 2022 р., дана проблема є однією з найбільш актуальних через використання елементів штучного інтелекту з метою нейтралізації загроз в воєнному та кіберпросторах. Тому звіти, сформовані Українською національною групою МАКП в 2022 р.<sup>3</sup>, відіграли важливу роль у формуванні кримінальної політики в сфері застосування ШІ та будуть відображені в Резолюції на Конгресі МАКП 2024 р. в Парижі.

Такі підходи до вирішення цієї проблеми можуть надати вектори кримінальної відповідальності фізичних (операторів), юридичних осіб

---

<sup>1</sup> Сайт Міжнародної асоціації карного права. URL: <https://www.penal.org/en/information>.

<sup>2</sup> Див.: RIDP – Revue Internationale de Droit Pénal. Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice. Vol. 92. January 2022.

<sup>3</sup> Див. напр.: Shepitko M., Senatorova O., Zadoia K., Ponomarenko Yu. International Criminal Law Perspectives on Artificial Intelligence in Ukraine: between the War and Legal Reformation. *Вісник Асоціації кримінального права України*. 2022. No 2(18). С. 35–51; Karchevskiy M., Radutniy O. Artificial Intelligence in Ukrainian Traditional Categories of Criminal Law. *Вісник Асоціації кримінального права України*. 2023. No 1(19). С. 1–25.

(заводів і постачальників), а також держав, які реалізують їх у мирний або воєнний час із злочинною (терористичною) метою. Також постає питання самої можливості впровадження ШІ як інструментів діяльності органів кримінальної юстиції.

Слід зазначити, що ще у 2018 р. Європейська комісія, враховуючи зростання застосування ШІ в Європейському Союзі, сформулювала його визначення: *«ШІ відноситься до систем, розроблених людьми, які, отримавши складну мету, діє у фізичному або цифровому світі, сприймаючи своє оточення, інтерпретуючи зібрані структуровані або неструктуровані дані, обґрунтовуючи знання, отримані з цих даних, і вирішуючи, найкращі дії (відповідно до попередньо визначених параметрів) для досягнення поставленої мети. Системи ШІ також можуть бути розроблені таким чином, щоб навчитися адаптувати свою поведінку, аналізуючи, як їхні попередні дії впливають на середовище. Як наукова дисципліна ШІ включає кілька підходів і методів, таких як машинне навчання (конкретними прикладами якого є глибоке навчання та навчання з підкріпленням), машинне мислення (що включає планування, календарне планування, відтворення знань та пояснення, пошук і оптимізацію) і робототехніка (яка включає контроль, сприйняття, датчики та виконавчі механізми, а також інтеграцію всіх інших методів у кіберфізичні системи)»<sup>4</sup>.*

12 лютого 2019 р. Європейський Парламент прийняв резолюцію про всеосяжну європейську промислову політику в галузі штучного інтелекту та робототехніки (2018/2088(INI)). У цій резолюції він зазначив, що «вітає ініціативу Комісії зі створення Групи експертів з відповідальності та нових технологій з метою надання ЄС досвіду в галузі застосування Директиви про відповідальність за продукцію (16) до традиційних продуктів, нових технологій та нових проблем суспільства (формування Директиви про

---

<sup>4</sup> High-Level Expert Group on Artificial Intelligence. A definition of AI: Main capabilities and scientific disciplines. European Commission. Brussels, 2018. P. 7.

відповідальність за продукцію) та надання допомоги ЄС у розробці принципів, які можуть бути керівними принципами для можливої адаптації застосовного законодавства на рівні ЄС та національного рівня, що стосується нових технологій (формування нових технологій); проте шкодує, що в ході цього законодавчого органу не було висунуто жодної законодавчої пропозиції, що затримує оновлення правил відповідальності на рівні ЄС та загрожує правовій визначеності у всьому ЄС у цій галузі як для торговців, так і для споживачів; зазначає, що *інженери ШІ або компанії, які їх наймають, повинні нести відповідальність за соціальний, екологічний та медичний вплив, який системи ШІ або робототехніка можуть вплинути на сьогодення та майбутні покоління* (п. 131–133)<sup>5</sup>.

Такий підхід Європейського Парламенту демонструє заклик до відповідального використання ШІ в Європі та необхідності регулювання даної сфери в найближчому майбутньому. Слід відзначити, що європейські органи влади здійснили велику роботу в регулюванні ШІ, яка найближчим часом, з врахуванням європейського вектору розвитку, стане актуальною і в Україні.

Так, робота Європейської комісії щодо штучного інтелекту втілилася в Стратегію ШІ для Європи на 2018 р. (2018 AI Strategy for Europe), білу книгу щодо ШІ на 2020 р. (White Paper on AI) і нещодавно оновлений скоординований план щодо ШІ. У квітні 2021 р. Комісія оприлюднила законодавчу пропозицію щодо закону про ШІ (Artificial Intelligence Act). Пропозиція передбачає класифікацію систем ШІ на основі ризиків. Системи ШІ для правосуддя та правоохоронних органів вважаються «підвищеними ризиками» і повинні відповідати суворим вимогам (оцінка відповідності, прозорість, людський нагляд). Рада також визнала конкретні вимоги до фундаментальних прав, які виникають у зв'язку з використанням штучного

---

<sup>5</sup> Сайт Європейського Парламенту. URL: [https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081\\_EN.html?redirect](https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.html?redirect).

інтелекту в правоохоронних органах, наголошуючи при цьому на потенціалі штучного інтелекту покращити запобігання злочинам, розслідування та судове переслідування. У своїх висновках щодо внутрішньої безпеки від грудня 2020 р. Рада поставила мету, згідно з якою до 2025 р. правоохоронні органи повинні мати можливість використовувати технології ШІ у своїй повсякденній роботі «за умови дотримання чітких гарантій». Щодо штучного інтелекту в секторі юстиції Рада виступає за необхідність прийняття рішень людьми та наголошує на необхідності ефективних засобів правового захисту для забезпечення права на справедливий суд, презумпції невинуватості та права на захист<sup>6</sup>.

У проєкті нового закону про ШІ (Artificail Intelligence Act), який на сьогодні обговорюється, Європейський Парламент планує змінити регулювання даної сфери, в тому числі визначити заборонені практики. Так, розділ II (ст. 5) запропонованого проєкту закону чітко забороняє шкідливі практики ШІ, які вважаються явною загрозою безпеці, засобам існування та правам людей через «неприйнятний ризик», який вони створюють. Відповідно, буде заборонено розміщувати на ринку, вводити в послуги або використовувати в ЄС:

- усі системи, які використовують шкідливі маніпулятивні «підсвідомі» техніки;
- усі системи, які використовують певні вразливі групи (фізичні або психічні вади);
- усі системи, що використовуються органами державної влади або від їх імені для цілей соціального оцінювання;
- системи віддаленої біометричної ідентифікації в реальному часі в загальнодоступних місцях для цілей правоохоронних органів, за винятком обмеженої кількості випадків».

---

<sup>6</sup> Voronova S. Artificial intelligence in criminal law. European Parliament. Plenary – October I 2021. URL: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/698039/EPRS\\_ATA\(2021\)698039\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/698039/EPRS_ATA(2021)698039_EN.pdf).

Надалі в ст. 6 названого проєкту закону про ШІ згадуються системи ШІ «високого ризику», які «створюють негативний вплив на безпеку людей або їхні основні права. Проєкт закону розрізняє дві категорії систем ШІ «високого ризику»:

1) системи, які використовуються як компонент безпеки продукту або підпадають під дію законодавства ЄС про гармонізацію здоров'я та безпеки (наприклад, іграшки, авіація, автомобілі, медичні пристрої, ліфти).

2) системи, розгорнуті у восьми конкретних сферах, визначених у Додатку III, які Комісія може оновлювати за необхідності шляхом делегованих актів (ст. 7):

- біометрична ідентифікація та категоризація фізичних осіб;
- управління та експлуатація критичної інфраструктури;
- освіта та професійна підготовка;
- працевлаштування, управління працівниками та доступ до самозайнятості;
- доступ і користування основними приватними та державними послугами та перевагами;
- правозастосування;
- управління міграцією, притулком та прикордонним контролем;
- відправлення правосуддя та демократичні процеси»<sup>7</sup>.

Сам факт підготовки такого проєкту закону вказує на те, що сфера впровадження та застосування ШІ в Європейському Союзі стає жорстко регульованою та такою, що забороняє або суттєво обмежує застосування ШІ, включаючи сферу кримінальної юстиції. Слід звернути увагу, що

---

<sup>7</sup> Artificial Intelligence act. European Parliament. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS\\_BRI\(2021\)698792\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf).

європейська позиція зводиться до особистої відповідальності інженерів ШІ та юридичних осіб, які їх наймають<sup>8</sup>.

Відповідно до застосування ШІ у воєнний час, Європейський Парламент наголосив, що «автономне прийняття рішень не повинно звільняти людей від відповідальності і що люди повинні нести кінцеву відповідальність за процеси прийняття рішень, щоб можна було визначити людину, відповідальну за прийняття рішення; ...при використанні ШІ у військовому контексті держави-члени, сторони конфлікту та окремі особи повинні у будь-який час виконувати свої зобов'язання відповідно до застосовного міжнародного права та брати на себе відповідальність за дії, що впливають із використання таких систем; ...за будь-яких обставин очікувані, випадкові чи небажані дії та наслідки систем, що ґрунтуються на ШІ, повинні розглядатися як відповідальність держав-членів, сторін конфлікту та окремих осіб» (пп. 8–10)<sup>9</sup>.

В резолюції Європейського Парламенту «ШІ в кримінальному праві та його застосування в поліції та судовій владі в кримінальних цілях» вказується на серйозні побоювання щодо самої можливості використання або неправильного використання систем ШІ. Зокрема, зазначається, що «багато алгоритмічних технологій ідентифікації, які зараз використовуються, непропорційно неправильно ідентифікують і неправильно класифікують і, отже, завдають шкоди особам за ознакою раси, особам, які належать до певних етнічних спільнот, ЛГБТІ, дітям і людям похилого віку, а також жінкам... Слід докласти значних зусиль, щоб уникнути автоматизованої дискримінації та упередженості, і вони закликали до того, щоб гарантії проти

---

<sup>8</sup> Саме тому позиції інтригуючі позиції окремих дослідників щодо можливості визнання ШІ як суб'єкта кримінального правопорушення поки, що не отримують свого підтвердження в тенденціях регулювання ШІ та встановлення відповідальності за його застосування в окремих сферах. Див. напр., Радутний О. Е. Штучний інтелект як суб'єкт злочину. *Інформація та право*. 4(23)/2017. С. 106–115. URL: [https://ippi.org.ua/sites/default/files/14\\_5.pdf](https://ippi.org.ua/sites/default/files/14_5.pdf).

<sup>9</sup> European Parliament resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI)). European Parliament. URL: [https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html).

зловживання технологіями штучного інтелекту правоохоронними та судовими органами також регулювалися однаково по всьому Союзу... Члени закликали дотримуватися принципу обережності в усіх застосуваннях ШІ в правоохоронних органах і наголосили, що *в судових і правоохоронних органах рішення, яке має юридичну чи подібну силу, завжди має прийматися людиною, яка може нести відповідальність за рішення...* Парламент закликав *назавжди заборонити використання автоматизованого аналізу та/або розпізнавання в загальнодоступних місцях інших людських особливостей, таких як хода, відбитки пальців, ДНК, голос та інші біометричні та поведінкові сигнали. Він також закликав заборонити використання приватних баз даних розпізнавання облич (таких як система Clearview AI)...* Члени закликали до мораторію на розгортання правоохоронних систем розпізнавання облич для цілей ідентифікації, якщо вони не використовуються лише для ідентифікації жертв злочинів, доки технічні стандарти не будуть вважатися такими, що повністю поважають основні права»<sup>10</sup>.

Цей заклик Європейського Парламенту поступово знайшов своє відображення і в проєкті закону щодо ШІ, де вже пропонується «заборонити використання систем біометричної ідентифікації в ЄС як для використання в режимі реального часу, так і для *ex-post* використання (за винятком випадків серйозних злочинів і досудового уповноваження на *ex-post* використання), а не лише для використання в режимі реального часу, як запропоновано Комісією. Крім того, Парламент хоче заборонити всі системи біометричної категоризації з використанням чутливих характеристик (наприклад, стать, раса, етнічна приналежність, статус громадянства, релігія, політична орієнтація); інтелектуальні поліцейські системи (на основі профілювання, місцезнаходження або минулої злочинної поведінки); системи розпізнавання

---

<sup>10</sup> Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters 2020/2016(INI). European Parliament. URL: <https://oeil.secure.europarl.europa.eu/oeil/popups/printficheglobal.pdf?id=710029&l=en>.



емоцій (використовуються в правоохоронних органах, прикордонній службі, на робочому місці та в навчальних закладах); і системи ШІ, які використовують невідбиркове збирання біометричних даних із соціальних мереж або записів із камер відеоспостереження для створення баз даних розпізнавання облич»<sup>11</sup>.

Аналіз нормативної бази та позицій щодо впровадження, використання та відповідальності ШІ вказують на наступні тенденції: 1) використання ШІ в Європейському Союзі стає регульованою сферою, що формує права, обов'язки та відповідальність учасників; 2) застосування ШІ в органах кримінальної юстиції зазнає суттєвих обмежень та заборон; 3) відповідальність, в тому числі кримінальна, за застосування ШІ та за небезпечні наслідки, які ним можуть бути спричинені, покладається на фізичних та юридичних осіб, а також держав, в чиїх інтересах застосовується ШІ.

Україна знаходиться тільки на початкових спробах регулювання застосування ШІ. Розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. була схвалена Концепція розвитку штучного інтелекту в Україні. У цій концепції надається визначення ШІ: *«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»*. Очевидним стає те, що дане визначення не дає розуміння ШІ, його ролі в науці та технологіях. Також визначення ШІ, надане у вказаній

---

<sup>11</sup> Artificial Intelligence act. European Parliament. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS\\_BRI\(2021\)698792\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf).

концепції, не відповідає визначенню ШІ, яке надається в Європейському Союзі.

Цікавим також є те, що концепція не вказує шляхи регулювання сфер, в яких може бути застосований ШІ, а формулює завдання, які можуть бути вирішені за допомогою ШІ в сферах освіти і професійного навчання, науки, економіки, кібербезпеки, інформаційної безпеки, оборони, публічного управління, правового регулювання та етики, а також правосуддя. Разом із цим в даній концепції не підіймалися питання обмежень та заборон на використання ШІ в Україні, а також принципів відповідальності за застосування ШІ та наслідки, які системи ШІ можуть спричинити.

У даній Концепції розвитку ШІ в Україні в сфері правосуддя слід забезпечити виконання таких завдань:

- подальший розвиток вже існуючих технології у сфері правосуддя (Єдина судова інформаційно-телекомунікаційна система, Електронний суд, Єдиний реєстр досудових розслідувань тощо);
- впровадження консультативних програм на основі ШІ, які відкриють доступ до юридичної консультації широким верствам населення;
- попередження суспільно небезпечних явищ шляхом аналізу наявних даних за допомогою ШІ;
- визначення необхідних заходів ресоціалізації засуджених шляхом проведення аналізу наявних даних за допомогою технологій ШІ;
- винесення судових рішень у справах незначної складності (за взаємною згодою сторін) на основі результатів аналізу, здійсненого з використанням технологій ШІ, стану дотримання законодавства та судової практики.

Аналіз сформованих в Україні завдань навіть в одній сфері правосуддя демонструє відсутність єдиного погляду в Україні та ЄС на регулювання ШІ. В ситуації коли в ЄС наголошується на особистому прийнятті рішень в сфері

правосуддя, в Україні проголошується постановлення судових рішень у справах «незначної складності». Так само, розвиток існуючих технологій в сфері правосуддя в Україні ймовірно включає окремі елементи ШІ, однак за своєю суттю такими не можуть вважатися. Разом із цим проблеми використання ШІ під час збирання даних та аналізу ознак людини оперативними органами, органами кримінальної юстиції, судово-експертними інституціями взагалі ігнорується. Тому перспективною та необхідною видається гармонізація законодавства України та Європейського Союзу з метою наближення європейських стандартів, забезпечення прав особи, унеможливлення їх порушення та дискримінації за будь-якою ознакою.

Також перспективним стає регулювання проблем кримінальної відповідальності за застосування ШІ (за умови заборони його застосування) та за небезпечні наслідки (які ним можуть бути спричинені). На нашу думку, це питання має бути врегульоване в чинному КК України або в перспективі в новому КК України<sup>12</sup> (в Загальній та Особливій частинах) через встановлення кримінальної відповідальності фізичних та юридичних осіб, які здійснили таку розробку системи ШІ. Також логічним стане встановлення кримінальної відповідальності за порушення заборони на використання ШІ в окремих сферах, що призводить до тяжких наслідків.

#### Список використаних джерел

1. Проект нового Кримінального кодексу України. URL: <https://newcriminalcode.org.ua/criminal-code>.
2. Радутний О. Е. Штучний інтелект як суб'єкт злочину. *Інформація та право*. 2017. 4(23). С. 106–115. URL: [https://ippi.org.ua/sites/default/files/14\\_5.pdf](https://ippi.org.ua/sites/default/files/14_5.pdf).
3. Сайт Європейського Парламенту. URL: [https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081\\_EN.html?redirect](https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.html?redirect).

---

<sup>12</sup> Див.: проект нового Кримінального кодексу України. URL: <https://newcriminalcode.org.ua/criminal-code>.

4. Сайт Міжнародної асоціації карного права. URL: <https://www.penal.org/en/information>.
5. Artificial Intelligence act. European Parliament. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS\\_BRI\(2021\)698792\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf).
6. Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters 2020/2016(INI). European Parliament. URL: <https://oeil.secure.europarl.europa.eu/oeil/popups/printficheglobal.pdf?id=710029&l=en>.
7. European Parliament resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI)). European Parliament. URL: [https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html).
8. High-Level Expert Group on Artificial Intelligence. A definition of AI: Main capabilities and scientific disciplines. European Commission. Brussels, 2018. P. 7.
9. Karchevskiy M., Radutniy O. Artificial Intelligence in Ukrainian Traditional Categories of Criminal Law. *Вісник Асоціації кримінального права України*. 2023. No 1(19). С. 1–25.
10. RIDP – Revue Internationale de Droit Pénal. Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice, Vol. 92. January 2022.
11. Shepitko M., Senatorova O., Zadoia K., Ponomarenko Yu. International Criminal Law Perspectives on Artificial Intelligence in Ukraine: between the War and Legal Reformation. *Вісник Асоціації кримінального права України*. 2022. No 2(18). С. 35–51.
12. Voronova S. Artificial intelligence in criminal law. European Parliament. Plenary – October I 2021. URL: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/698039/EPRS\\_ATA\(2021\)698039\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/698039/EPRS_ATA(2021)698039_EN.pdf).

#### REFERENCES

1. Proiekt novoho Kryminalnogo kodeksu Ukrainy. URL: <https://newcriminalcode.org.ua/criminal-code> [in Ukrainian].
2. Radutnyi, O. E. (2017) Shtuchnyi intelekt yak subiekt zlochynu. *Informatsiia ta pravo*, 4(23), 106–115. URL: [https://ippi.org.ua/sites/default/files/14\\_5.pdf](https://ippi.org.ua/sites/default/files/14_5.pdf) [in Ukrainian].
3. Sait Yevropeiskoho Parlamentu. URL: [https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081\\_EN.html?redirect](https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.html?redirect) [in Ukrainian].
4. Sait Mizhnarodnoi asotsiatsii karnoho prava. URL: <https://www.penal.org/en/information> [in Ukrainian].

5. Artificial Intelligence act. European Parliament. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS\\_BRI\(2021\)698792\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf) [in English].
6. Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters 2020/2016(INI). European Parliament. URL: <https://oeil.secure.europarl.europa.eu/oeil/popups/printficheglobal.pdf?id=710029&l=en> [in English].
7. European Parliament resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI)). European Parliament. URL: [https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html) [in English].
8. High-Level Expert Group on Artificial Intelligence (2018). A definition of AI: Main capabilities and scientific disciplines. European Commission. Brussels. P. 7. [in English].
9. Karchevskiy, M., & Radutniy, O. (2023) Artificial Intelligence in Ukrainian Traditional Categories of Criminal Law. *Visnyk Asotsiatsii kryminalnoho prava Ukrainy*, 1(19), 1–25 [in English].
10. RIDP (2022) – Revue Internationale de Droit Pénal. Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice, Vol. 92. January 2022 [in English].
11. Shepitko, M., Senatorova, O., Zadoia, K., & Ponomarenko, Yu. (2022) International Criminal Law Perspectives on Artificial Intelligence in Ukraine: between the War and Legal Reformation. *Visnyk Asotsiatsii kryminalnoho prava Ukrainy*, 2(18), 35–51 [in English].
12. Voronova, S. (2021) Artificial intelligence in criminal law. European Parliament. Plenary – October I 2021. URL: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/698039/EPRS\\_ATA\(2021\)698039\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/698039/EPRS_ATA(2021)698039_EN.pdf) [in English].

***Shepitko M. V. Prospects for the introduction, usage and responsibility of artificial intelligence in the EU and Ukraine***

*The development of artificial intelligence and its significant role in economic and social relations, military and cyber threats generated by it indicate the urgency of researching this problem. Ukraine, as a victim of russian large-scale military aggression in 2022, is interested in regulating this area in order to neutralize threats in military and cyberspace.*

*The study of the introduction, usage and responsibility of artificial intelligence in the European Union can provide vectors of criminal responsibility of individuals, legal entities, as well as states that implement them in peacetime or wartime with a criminal (terrorist) purpose. An important issue in this study is the*

*possible implementation of artificial intelligence as a tool for criminal justice agencies. The European Commission, taking into account the growing use of artificial intelligence in the European Union, formulated its definition in 2018. In 2020, Ukraine also adopted the Concept of the Development of Artificial Intelligence. However, the fact of harmonization of the legislation of the EU and Ukraine in this area becomes obvious.*

*The European Commission's work on artificial intelligence is reflected in the 2018 AI Strategy for Europe, the 2020 White Paper on AI and the recently updated Coordinated Plan on Artificial Intelligence. The preparation of the Artificial Intelligence Act is also underway.*

*Analysis of the regulatory framework and positions regarding the implementation, usage and responsibility of artificial intelligence indicate the following trends: 1) the use of artificial intelligence in the European Union is becoming a regulated area that shapes the rights, duties and responsibilities of participants; 2) the usage of artificial intelligence in criminal justice agencies is subject to significant restrictions and prohibitions; 3) responsibility for the use of artificial intelligence and for the dangerous consequences that may be caused by it rests with individuals and legal entities, as well as states, in whose interests it is used.*

**Key words:** *criminal liability, criminal policy, criminal justice, information security, digital security, artificial intelligence.*