РОЗДІЛ І
ПОНЯТТЯ, ІСТОРІЯ ВИНИКНЕННЯ ТА ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

1.1. Поняття, історія виникнення та складові штучного інтелекту

Штучний інтелект – молода дисципліна шістдесяти років, яка являє собою сукупність наук, теорій і технік (включаючи математичну логіку, статистику, ймовірності, обчислювальну нейробіологію, інформатику), яка має на меті імітувати когнітивні здібності людини. Сучасні комп'ютерно-програмні технології, зокрема технології ШІ, день за днем продовжують стрімко й досить активно розвиватися. Найбільш перспективними і при цьому найбільш неоднозначними технологіями, які вже застосовуються в багатьох сферах суспільних відносин, є технології ШІ. Взагалі виникнення проблеми створення інтелектуальних систем обумовлено з однієї сторони розвитком досліджень в напряму ШІ, з іншого боку – швидким розвитком обчислювальної техніки, інформаційно-комунікаційних технологій, і постійно зростаючими потребами їх різноманітних застосувань. Тому створення ШІ, який дорівнює інтелекту людини або перевищує його, є доволі реальною та такою, що може бути досягнута у найближчому майбутньому.

У періоді розвитку ШІ можна виділити чотири етапи. Це – період від заснування і до 1974 року, який часто називають «золотою добою» ШІ. У цей час були зроблені перші значні відкриття у цій галузі, що мали суттєвий евристичний потенціал. На тодішніх комп'ютерах науковцям вдалося застосовувати технологію для доведення геометричних теорем або розрахунків алгебраїчних виразів. Також були зроблені перші кроки щодо синтезу *природної мови* та її обробки.

У 80-х роках XX століття відбувається другий важливий етап розвитку ШІ, пов'язаний із *експертними системами* – це такі системи, які моделюють поведінку людини-експерта у певній галузі. Завдяки цьому підходу створювалися так звані *бази знань*

З 90-х років XX століття і по сьогоднішній день виокремлюється ще один етап, пов'язаний із виникненням теорії *інтелектуальних агентів*, а також сегмента *Big Data – великі дан*і, і так зване *глибоке навчання – Deep Learning*[7].

[7] Виклики штучного інтелекту («Збруч»). URL: https://ucu.edu.ua/news/vyklyky-shtuchnogo-intelektu-zbruch/.

У наш час людство освоює третю («цифрова революція» – повсюдний перехід у виробництві до застосування інформаційно-комунікаційних технологій) і четверту (масове впровадження кіберфізичних систем у виробництво) промислові революції.

В Україні історія розвитку базових засад інформаційного суспільства та інтелектуальних систем пов'язана з діяльністю всесвітньо відомої школи кібернетики, розроблення на початку 90-х років минулого століття концепції та програми інформатизації, створення різноманітних інформаційно-комунікаційних технологій і загальнодержавних електронних інформаційно-аналітичних систем різного рівня та призначення[8].

У науково-довідкових виданнях визначення ШІ з'явилося в 1979 році в Словнику з кібернетики під редакцією академіка В.М. Глушкова, в якому надано таке визначення: *штучний інтелект* – це:

1) штучна система, що імітує рішення людиною складних завдань в процесі його життєдіяльності;

2) напрямок наукових досліджень, які супроводжують і обумовлюють створення систем ШІ, побудованих на базі засобів обчислювальної техніки і призначених для сприйняття, обробки і зберігання інформації, а також формування рішень щодо доцільної поведінки в ситуаціях, що моделюють стан світу природи і суспільства. Дослідження в галузі ШІ знаходяться на стику психології, лінгвістики, філософії, соціології, математики та обчислювальної техніки.

Штучний інтелект (з англ.: Artificial Intelligence) – це унікальний продукт технічного прогресу, що дає змогу машинам вчитися, використовуючи людський і власний досвід, пристосовуватися до нових умов в рамках свого застосування, виконувати різнопланові завдання, які тривалий час були під силу лише людині, прогнозувати події й оптимізувати ресурси різного характеру.

Під ним розуміється здатність автоматичних систем брати на себе функції людини, вибирати і приймати оптимальні рішення на основі раніше отриманого життєвого досвіду і аналізу зовнішніх впливів. Будь-який інтелект спирається на діяльність. У свою чергу, діяльність мозку – це мислення. Інтелект і мислення пов'язані багатьма цілями і завданнями: розпізнавання ситуацій, логічний аналіз, планування поведінки. Характерними особливостями інтелекту є здатність до навчання, узагальнення, накопичення досвіду, адаптація до умов, що змінюються в процесі вирішення завдань. Висока продуктивність нових технологій значною мірою залежить від використання в них засобів ШІ[9].

На сьогоднішній день переважають такі напрями дослідженні в сфері використання ШІ, як:

1. *Робота з великими даними (BigData).*

[8]Стратегія розвитку інформаційного суспільства в Україні: схвалено розпорядженням Кабінету Міністрів України від 15 травня 2013 р. № 386-р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#n8.

[9]Глушков В. М. Історія розвитку Штучного інтелекту в ІК. URL: https://web.archive.org/web/20131203002125/http://www.iprinet.kiev.ua/gf/serg1.htm

Великі дані та ШІ – це дві найпопулярніші та найкорисніші технології сьогодні. ШІ існує вже більше десяти років, тоді як BigData з'явився лише кілька років тому. Комп'ютери можна використовувати для зберігання мільйонів записів великих обсягів структурованих, а також неструктурованих даних у великих масштабах, але можливість аналізу цих даних забезпечується за допомогою Великих даних. Це дані для яких не підходять стандартні способи зберігання і обробки через їх величезного обсягу і / або різноманітності.

Під великими даними потрібно розуміти як велику кількість інформації, яку необхідно проаналізувати, щоб прийти до якогось корисного висновку. Аналіз великих даних називається складним процесом вивчення великих даних для виявлення деяких прихованих кореляційних зв'язків у даних.

Робота з великими даними будується на основі чотирьох правил (з англ. V'sof BigData: Volume, Velocity, Variety, Veracity):

Обсяг (Volume): обсяг даних, які можуть збирати компанії, дійсно величезний, і тому їх розмір стає критичним фактором в аналітиці.

Швидкість (Velocity): висока швидкість, з якою генерується інформація. Практично все, що відбувається навколо нас (пошукові запити, соціальні мережі і т. ін.). Виробляє нові дані, багато з яких можуть бути використані в бізнес-рішеннях.

Різноманітність (Variety): генерується інформація неоднорідна і може бути представлена в різних форматах, таких, наприклад, як відео, текст, бази даних, числова інформація, сенсорні дані і т. д. Розуміння типу великих даних є ключовим фактором для розкриття їх цінностей.

Достовірність (Veracity): достовірність відноситься до якості аналізованих даних. Дані високу вірогідність містять багато записів, які цінні для аналізу і які вносять значний вклад в загальні результати. З іншого боку дані з низькою вірогідністю містять високий відсоток безглуздої інформації, яка називається шумом.

Термін «Великі дані» включає в себе великий різнорідний набір даних (відкриті дані, власні(персональні)) дані.

Відкриті дані.

Цей термін стосується загальнодоступності структурованих баз даних шляхом завантаження. Ці дані можуть бути повторно використані в немонетарному порядку на умовах конкретної ліцензії, яка, може вказувати або забороняти певні цілі повторного використання.

Відкриті дані не слід плутати із загальнодоступною інформацією, доступною на веб-сайтах, всю базу даних якої неможливо завантажити (наприклад, бази даних судової практики). Він не замінює обов'язкову публікацію певних адміністративних або судових заходів або рішень, вже прийнятих певними законами чи нормативними актами.

Персональні дані.

Персональні дані – це будь-яку інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»), саме так визначається Загальним регламентом захисту даних (GDPR/Регламент), який був

прийнятий у травні 2018 року і є одним із основних законів у сфері захисту приватності людини за останні роки та замінив рамкову Директиву про захист персональних даних 95/46/ЄС від 1995 року.

Так, у вказаному вище регламенті надається тлумачення визначенню «будь яка інформація», під яким розуміється будь-які відомості про людину, що відображають її фізичну, фізіологічну, генетичну, економічну, соціальну або культурну ідентичність. Вони діляться на дві категорії: загальні та особливі (чутливі).

До загальних персональних даних відносять:

1. прізвище та ім'я по-батькові;
2. місце народження;
3. громадянство;
4. сімейний стан;
5. банківські дані;
6. особистий підпис;
7. адреса проживання;
8. онлайн ідентифікатор;
9. диплом про освіту.

До особливих (чутливих) персональних даних відносять:

1. расове, етнічне та національне походження;
2. політичні, релігійні та світоглядні переконання;
3. стан здоров'я (медичні дані);
4. статеве життя;
5. біометричні, генетичні дані[10].

Персональні дані можуть бути виражені у формі:

а) цифр (ідентифікаційний код, номер телефону);

б) фото (зображення людини);

в) відео;

г) звуку (голос).

Також до персональних даних належать онлайн ідентифікатори: IP-адреси, коди і т. д[11].

Важливе значення має і управління швидкістю передачі даних, оскільки аналіз великих даних поширюється на такі галузі, як машинне навчання та ШІ, де аналітичні процеси автоматично знаходять закономірності в зібраних даних і використовують їх для отримання знань.

Машинне навчання (Machine Learning).

Машинне навчання (МН) – це використання математичних моделей даних, щоб полегшити навчання комп'ютеру без прямих інструкцій. Це трактується як

[10]Council of Europe and Artificial Intelligence. URL:https://www.coe.int/en/web/artificial-intelligence/home.

[11]Захист персональних даних за правилами GDPR. Експертний центр з прав людину. URL: https://ecpl.com.ua/news/zakhyst-personal-nykh-danykh-za-pravylamy-gdpr/.

Kalliopi Spyridaki.General Data Protection Regulation: From burden to opportunity. URL: https://www.sas.com/en_us/insights/articles/data-management/general-data-protection-regulation-from-burden-to-opportunity.html.

підмножина ШІ. Алгоритми МН дозволяють задавати шаблони у наборі даних. Потім ці шаблони використовуються для побудови моделі даних, яка дозволяє робити прогнози. Точність результатів МН з часом покращується, а обсяг даних збільшується – як і у людей.

МН як підгалузь ШІ дозволяє системам розуміти своє оточення, планувати дії, реагувати на перешкоди та надавати консультації. Процес навчання автоматизований та вдосконалений на основі досвіду роботи машин протягом усього процесу. Дані хорошої якості подаються на машини, і різні алгоритми використовуються для побудови моделей МН для навчання машин на цих даних. Вибір алгоритму залежить від типу наявних даних та виду діяльності, який потрібно автоматизувати[12].

За допомогою МН можливо автоматизувати рутинні завдання. Це також допомагає в автоматизації та швидкому створенні моделей для аналізу даних. Ці моделі є точними та масштабованими та функціонують із меншим часом обробки. МН дозволяє системі самостійно розпізнавати незалежно повторювані шаблони та об'єкти на основі робочих даних та інтелектуальних алгоритмів і робити прогнози, отримані під час навчання на великих наборах даних (BigData). Потім, отримані знання можна застосувати до невідомих та не відсортованих даних. Це дозволяє виявляти джерела помилок, планувати та оптимізувати процеси та робити прогнози. Тобто, вся основа МН – це дані. Система навчається та робить аналіз, використовуючи дані, які їй надано. Машини, як і люди, можуть робити помилки, покладаючись на дезінформацію, неправдиву інформацію або неточну інформацію. З цієї причини хороший збір даних є вирішальною роллю хорошого застосування МН.

Терміни МН та ШІ часто обговорюються разом, а іноді використовуються як взаємозамінні, але вони не означають одне і те ж. Важливою відмінністю є те, що, хоча всі системи МН є ШІ, не всі ШІ є МН. МН фокусується на побудові систем, які можуть вивчати або покращувати свою ефективність на основі даних, які вони обробляють. МН передбачає спостереження та вивчення даних або досвіду для виявлення закономірностей та створення системи міркувань на основі отриманих результатів[13].

Завдяки технологіям ШІ та МН правоохоронні органи можуть фільтрувати свої пошуки для пошуку конкретних характеристик; наприклад, чоловік у червоній сорочці. Тоді система буде шукати саме чоловіка в червоній сорочці. Щойно чоловіка ідентифікують, працівник поліції може відредагувати або видалити всю непричетну або невідповідну інформацію, залишивши на екрані лише чоловіка в червоній сорочці.

Глибоке навчання (Deep Learning) – підгалузь машинного навчання. Воно є спеціалізованою формою МН, яке дозволяє відповідати за допомогою нейронних мереж. Глибоке навчання визначає точність автоматично, дозволяючи

[12] Great Learning What is Machine Learning? How Machine Learning Works and future of it? Jan 19, 2022. URL:https://www.mygreatlearning.com/blog/what-is-machine-learning/.

[13]Marina Chatterjee. Data Science vs Machine Learning and Artificial Intelligence. Jan 11, 2020. URL: https://www.mygreatlearning.com/blog/difference-data-science-machine-learning-ai/

класифікувати інформацію способом, характерним для людського мозку, та використовується в деяких рішеннях ШІ, що імітують людину.

Здебільшого використовує деякі методи нейронних мереж, які можуть імітувати людське прийняття рішень.

Нейронні Мережі – це підмножина Machine Learning, мережі із здатністю самостійного навчання. Вони застосовуються не як технологія чи інструмент або засіб, а як систему яка здатність вчитися і використовувати вивчене.

Нейронні мережі – влаштовані за образом і подобою людського мозку. Тобто намагаються відтворити окремі аспекти влаштування нейромереж у мозку людини та використовують BigData, DataScience як матеріал, на якому вони навчаються.

Глибоке навчання вартісне і вимагає величезних масивів даних для навчання. Це пояснюється тим, що існує величезна кількість параметрів, які необхідно налаштувати для алгоритмів навчання, щоб уникнути помилкової поведінки.

Розвиток ШІ забезпечує потужні умови для побудови розумної поліцейської роботи, яка сприяє розширенню функцій сучасної поліцейської діяльності, сприянню реформуванню поліцейських механізмів та покращенню рівня вдосконаленого управління поліцією. Як потужний двигун для інновацій та розвитку, ШІ сприяє підвищенню рівня інформатизації, інтелекту та модернізації роботи з громадської безпеки.

1.2. Правове регулювання використання технологій штучного інтелекту в Європейському Союзі

Практичні заходи щодо розробки правових стандартів в сфері становлення правового регулювання вживаються і в Європейському Союзі. Потреба у врегулюванні застосування ШІ пов'язується, перш за все,з необхідністю захисту персональних даних осіб та інших прав людини, мінімізацію ризиків зловживання цією технологією. Також правове врегулювання використання ШІ необхідне для забезпечення стимулювання соціально ефективного використання технологій ШІ у різноманітних сферах, серед яких можна відмітити наступні:

- наукова, виробнича,господарська та інші види діяльності;
- «змішана юстиція» та «юстиція штучного інтелекту», тобто застосування технологій ШІ в правосудді;
- правоохоронна діяльність та кібербезпека;
- дотримання авторських права на твори, виноходи, програмні продукти тощо, створені технологіями ШІ;
- відповідальності за протиправне використання технологій ШІ.

Підходи до регулювання штучного інтелекту	
США	Відкритість та ефективність ринку
Європейський Союз	Дотримання прав людини
Китай	Стабільний розвиток економіки

Розвиток робототехніки та технологій ШІ й пов'язані з цим проблеми правового й етичного характеру обумовили прийняття Європейським Парламентом 16 лютого 2017 року Резолюції 2015/2103(INL) щодо цивільно-правового регулювання робототехніки з пропозиціями для Європейської Комісії.

Велика увага в Резолюції присвячувалася саме питанням цивільно-правової відповідальності за негативні наслідки використання робототехніки та технологій ШІ. Слід звернути увагу, що в документі зазначалося, що: «*…згідно із чинною правовою базою, роботи (а з ними і технології штучного інтелекту – не можуть бути притягненими до відповідальності за дії..., що спричинили шкоду третім сторонам»* та, що *«на цьому етапі відповідальність повинна покладатися на людину»* (п. т 56).

Найбільш конкретні пропозиції в Резолюції розглядалися щодо створення системи контролю в сфері розробки та використання робототехніки й технологій ШІ. Так, в п. 16) Резолюції 2015/2103(INL) міститься заклик до Єврокомісії розглянути можливість створення Агенції Європейського Союзу з робототехніки та ШІ, яка б здійснювала «*технічну, етичну та регуляторну експертну діяльність*» у відповідній сфері[14].

8 квітня 2019 року Експертною групою високого рівня з питань ШІ (AI HLEG)[15] були надані та представлені етичні вказівки щодо надійного ШІ. Відповідно до Керівних принципів, надійний ШІ повинен бути:

1. законний – з дотриманням усіх чинних законів та норм;
2. етичний – дотримання етичних принципів та цінностей;
3. надійний – як з технічної точки зору, враховуючи соціальне середовище.

Рекомендації висувають із семи ключових вимог, яким повинні відповідати системи ШІ, щоб їх можна було визнати надійними. Спеціальний перелік оцінок має на меті допомогти перевірити застосування кожної з ключових вимог:

- аналіз та нагляд за діяльністю людини: системи ШІ повинні розширювати можливості людей, дозволяючи їм приймати обґрунтовані рішення та сприяючи їх основним правам. У той же час слід забезпечити належні механізми нагляду, що може бути досягнуто за допомогою підходів «людина в циклі», «людина на циклі» та «людина-командир»;
- технічна надійність і безпека: системи ШІ повинні бути стійкими та безпечними. Вони повинні бути в безпеці, забезпечуючи резервний план у випадку, якщо щось піде не так, а також бути точними, надійними та відтворюваними. Це єдиний спосіб забезпечити мінімізацію та запобігання ненавмисній шкоді;
- конфіденційність та управління даними: крім забезпечення повної поваги до конфіденційності та захисту даних, також повинні бути забезпечені адекватні механізми управління даними, враховуючи якість та цілісність даних, та забезпечуючи законний доступ до даних;
- прозорість: дані, система та бізнес-моделі ШІ повинні бути прозорими. Механізми простежуваності можуть допомогти досягти цього. Більше того, системи ШІ та їх рішення слід пояснювати у спосіб, адаптований до зацікавлених сторін. Люди повинні усвідомлювати, що вони взаємодіють із системою ШІ, і повинні бути проінформовані про можливості та обмеження системи;
- різноманітності, недискримінації та справедливості: необхідно уникати несправедливих упереджень, оскільки це може мати багато негативних наслідків.
- соціальне та екологічне благополуччя: системи ШІ повинні приносити користь усім людям, включаючи майбутні покоління.

[14]European Parliament resolution of 16 February 2017 with recommendations to the Commissionon Civi lLaw Ruleson Robotics (2015/2103(INL)) // EuropeanParliamentOfficialweb-site. Cit. 07.11.2017. URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN

[15]AI HLEG – це незалежна експертна група, створена Європейською Комісією в червні 2018 року

- підзвітність: слід запровадити механізми, що забезпечують відповідальність та підзвітність систем ШІ та їх результатів. Аудит, який дозволяє оцінювати алгоритми, дані та процеси проектування, відіграє тут ключову роль, особливо у критичних програмах. Більше того, слід забезпечити належне доступне відшкодування.

Згодом, восени 2019 року було створено Спеціальний комітет з питань штучного інтелекту (CAHAI) – міжурядовий комітет, заснований Комітетом міністрів Ради Європи задля становлення правових рамок, які стосуються розробки, розвитку та застосування ШІ з урахуванням стандартів Ради Європи в області прав людини, демократії та верховенства права. До складу Комітету входять представники 47 держав-членів[16].

Для побудови надійних моделей в основі систем, що базуються на ШІ, якісні дані є ключовим фактором для отримання най достовірніших висновків.

Європейська Комісія пропонує правила, щоб зробити системи ШІ, що використовуються в Європейському Союзі безпечними, прозорими, етичними, неупередженими та керованими людьми. Системи, що використовують ШІ, класифікуються за рівнем ризику:

Неприйнятний ризик: системи ШІ, які вважаються явною загрозою безпеці, існуванню та правам громадян, будуть заборонені. Наприклад, системи або додатки, які використовують ШІ для маніпулювання поведінкою людини, щоб обійти свободу волі користувачів (наприклад, іграшки із вбудованим голосовим помічником, що заохочує неповнолітніх до небезпечної поведінки) та державні системи оцінки для громадян.

Високий ризик: системи ШІ, визнані високим ризиком, включають технологію ШІ, що використовується в:

- критична інфраструктура (наприклад, на транспорті), яка може загрожувати життю та здоров'ю громадян;
- професійну освіту чи навчання, що може визначати доступ особи до професійної освіти та навчання (наприклад, іспит на іспити);
- елементи безпеки продукції (наприклад, використання ШІ в хірургії з роботом);
- працевлаштування, управління працівниками та доступ до само зайнятості (наприклад, програмне забезпечення для сортування резюме для процедур набору);
- основні приватні та державні послуги (наприклад, оцінка кредитоспроможності, що може перешкодити громадянам робити певні інвестиції);

[16]Штучний інтелект та його вплив на молодь. URL: https://cid.center/59380583/#:~:text=%D0%97%20%D0%BD%D0%BE%D0%B2%D0%BE%D0%B3%D0%BE%20%E2%80%93%20%D0%B2%D0%BE%D1%81%D0%B5%D0%BD%D0%B8%202019%20%D1%80%D0%BE%D0%BA%D1%83,%D0%A0%D0%B0%D0%B4%D0%B8%20%D0%84%D0%B2%D1%80%D0%BE%D0%BF%D0%B8%20%D0%B2%20%D0%BE%D0%B1%D0%BB%D0%B0%D1%81%D1%82%D1%96%20%D0%BF%D1%80%D0%B0%D0%B2

- правоохоронні органи, що може суперечити основним правам громадян (наприклад, оцінка надійності доказів);
- управління міграцією, притулком та прикордонним контролем (наприклад, підтвердження проїзних документів);
- здійснення правосуддя та демократичні процеси (наприклад, застосування закону до певної сукупності фактів).

Системи ШІ з високим ризиком повинні відповідати суворим вимогам, перш ніж їх можна буде розміщувати на ринку:

- відповідні системи оцінки та пом'якшення ризиків;
- висока якість наборів даних, що живлять систему з метою мінімізації ризику та дискримінаційних наслідків;
- запис діяльності для забезпечення простежуваності результатів;
- детальна документація, що містить всю інформацію про систему та її призначення, щоб органи влади могли оцінити її відповідність;
- чітка та відповідна інформація для користувача;
- відповідні заходи спостереження за людьми для мінімізації ризиків;
- високий рівень надійності, безпеки та точності.

Зокрема, усі типи дистанційної біометричної ідентифікації вважаються системами високого ризику, які підлягають суворим вимогам та нагляду з боку як розробників, так і користувачів. Їх використання в реальному часі для цілей правопорядку в місцях, доступних для громадськості, в принципі заборонено. Винятки з цього правила суворо визначені та регламентовані (це стосується, наприклад, коли використання таких технологій є абсолютно необхідним для пошуку зниклої дитини, запобігання конкретній та безпосередній терористичній загрозі або для виявлення, пошуку, ідентифікації або притягнення до відповідальності винний або підозрюваний у вчиненні кримінальному правопорушенні). Таке використання вимагає дозволу суду або іншого незалежного органу та має бути належним чином обмежене з точки зору часу, географічного охоплення та пошуку баз даних.

Обмежений ризик: тобто системи ШІ, на які поширюються конкретні зобов'язання щодо прозорості: користуючись системами ШІ, такими як чат-боти, користувачі повинні знати, що вони взаємодіють з машиною, щоб вони могли прийняти обґрунтоване рішення продовжувати або припиняти взаємодію.

Мінімальний ризик: законодавча пропозиція дозволяє вільно використовувати такі програми, як ШІ відеоігри або спам-фільтри. Переважна більшість систем ШІ належать до цієї категорії. Проект регламенту не передбачає жодних втручань щодо цієї категорії використання, оскільки такі системи ШІ не становлять загрози для прав чи безпеки громадян або ризик є мінімальним[17].

Чинне законодавство Європейського Союзу про безпеку та відповідність продукції на сьогодні може застосовуватися до продуктів, але не до послуг. Відтак – і не до послуг, що базуються на технологіях ШІ (транспортні послуги,

[17]Komisja Europejska. Przedstawicielstwo w Polsce. URL: https://ec.europa.eu/poland/news/210421_digital_europe_pl

охорона здоров'я і т. п.). Тому відповідальність за всі компоненти, в тому числі ШІ, покладається на виробника продукту, що виходить на ринок.

Після виведення системи ШІ на ринок державні органи відповідають за нагляд за ринком, користувачі забезпечують людський нагляд та моніторинг, а постачальники застосовують систему пост-ринкового моніторингу. Постачальники та користувачі також повідомлятимуть розробника технологій ШІ про серйозні випадки та несправності.

Крок 1	**Крок 2**	**Крок 3**	**Крок 4**	
Розробляється система ШІ з високим ризиком	Він повинен пройти оцінку відповідності та відповідати вимогам щодо ШІ. Для деяких систем необхідна участь нотифікованого органу.	Реєстрація автономних систем ШІ в базі даних Європейського Союзу	Необхідно підписати декларацію про відповідність для даної системи ШІ, яка також повинна мати маркування Європейського Союзу. Система може бути розміщена на ринку	*Якщо в життєвому циклі системи ШІ відбуваються суттєві зміни, поверніться до кроку 2.*

Правила для постачальників систем штучного інтелекту з високим ризиком.

У Резолюції 2015/2103 (INL) Європейського парламенту від 16 лютого 2017 року з рекомендаціями Європейської комісії щодо цивільно-правового регулювання робототехніки (далі – Резолюція 2015/2103 (INL)) наголошено на неможливості притягнення ШІ до відповідальності за дії, що спричинили шкоду третім сторонам. Так, відповідно до п. «ad» Резолюції 2015/2103 (INL) відповідальність за завдання шкоди може бути покладено на одного з так званих агентів (англійською – humanagent), а саме: на виробника, оператора, власника або користувача ШІ. При цьому під час установлення обсягу відповідальності з боку «агента» одним із головних аспектів визначено факт доведення можливості передбачення негативних наслідків і запобігання їм.

Резолюція 2015/2103 (INL) не є загальнообов'язковим актом і має лише рекомендаційний характер. Водночас, зважаючи на обраний євроінтеграційний курс України, з великою ймовірність можна розраховувати, що подальше вдосконалення національного законодавства щодо правового регулювання ШІ разом із процедурою визначення відповідальності за помилки, що призвели до негативних наслідків, ґрунтуватиметься саме на вже сформованих стандартах ЄС[18].

У країнах Європейського Союзу докладається максимум зусиль щоб населення, державні служби, розуміли норми закону, що регулюють обробку даних, кібербезпеку та електронну комунікацію, знали практичні аспекти впровадження та ризики, щодо не дотримання законодавства в сфері обробки

[18]Doskonałość i zaufanie do sztucznej inteligencji. Komisja Europejska. Przedstawicielstwo w Polsce. URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_pl

персональних даних. Під час обробки даних необхідно враховувати категорію персональних даних, та застосовувати відповідні рівні безпеки. Процедура обробки даних повинна бути детально регламентована. Співробітники поліції повинні бути проінструктовані та пройти навчання щодо заходів безпеки та недоторканності приватного життя людини. Адже довіра до більшості організацій буде продовжувати зростати, коли дані надійно захищатимуться суворими вимогами щодо аудиту та обґрунтування пошуку. Правоохоронні органи повинні підтримувати бездоганні стандарти безпеки, контролю доступу, аудиту та обґрунтування доступу до даних.

1.3. Нормативно-правове регулювання використання технологій штучного інтелекту Національною поліцією України

Нормативно-правовим підґрунтям використання Національною поліцією України інформаційних технологій, до яких зокрема, відносяться технології ШІ, з метою запобігання та протидії правопорушенням, є система нормативно-правових актів, які визначають допустимість, порядок і умови використання цих технологій у правоохоронній діяльності.

Названу систему можна умовно поділити на дві категорії:

– перша категорія, які містить нормативно-правові акти, які встановлюють загальні вимоги до систем інформаційних технологій, до яких відносяться зокрема технології ШІ, та регулюють обіг інформації, зокрема у Національній поліції України.

До цієї категорії відносяться Закон України «Про інформацію»[19], що регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Закон України «Про захист персональних даних»[20], що регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних.

Закон України «Про доступ до публічної інформації»[21], який визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес.

[19]Про інформацію: Закон України від 02 жовтня 1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

[20]Про захист персональних даних громадян: Закон України від 01 червня 2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

[21]Про доступ до публічної інформації: Закон України від 13 січня 2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

Закон України «Про захист інформації в інформаційно-комунікаційних системах»[22], що регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

Необхідно зауважити, що 2 грудня 2021 року розпорядженням Кабінету Міністрів України № 1556-р. схвалено Концепцію розвитку штучного інтелекту в Україні[23], завдяки якій визначення поняття «штучний інтелект» на законодавчому рівні відкриє доступ новітнім технологіям до нових сфер в тому числі в правоохоронної діяльності. У цій Концепції термін ШІ визначається як 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. Одним із пріоритетних напрямів реалізації положень Концепції розвитку ШІ має бути формування стратегій розвитку, регулювання та стандартизації ШІ. Концепцією визначаються мета, принципи та завдання розвитку технологій ШІ в Україні як одного з пріоритетних напрямів у сфері науково-технологічних досліджень.

– друга категорія визначає підстави та напрями інформаційного забезпечення Національної поліції України, формування та використання інформаційних ресурсів різного характеру, використання інформаційних технологій, тобто й технологій ШІ, у протидії правопорушенням.

До таких законодавчих актів відносяться закони України «Про Національну поліцію»[24], «Про оперативно-розшукову діяльність»[25], Кримінальний процесуальний кодекс (далі – КПК) України та інші нормативно-правові акти.

Стаття 23 Закон України «Про Національну поліцію»[26] надає працівникам поліції низку повноважень, визначимо деякі з них, де можуть бути використані технології ШІ, зокрема: здійснює превентивну та профілактичну діяльність, спрямовану на запобігання вчиненню правопорушень (п. 1); виявляє причини та умови, що сприяють вчиненню кримінальних та адміністративних правопорушень, вживає у межах своєї компетенції заходів для їх усунення (п. 2); вживає заходів з метою виявлення кримінальних, адміністративних правопорушень; припиняє виявлені кримінальні та адміністративні

[22]Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05 липня 1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

[23]Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.

[24]Про Національну поліцію: Закон України від 02 липня 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

[25]Про оперативно-розшукову діяльність: Закон України від 18.02.1992 р. № 2135-XII. URL: http://zakon2.rada.gov.ua/laws/show/2135-12

[26]Про Національну поліцію: Закон України від 02 липня 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

правопорушення (п. 3); вживає заходів, спрямованих на усунення загроз життю та здоров'ю фізичних осіб і публічній безпеці, що виникли внаслідок учинення кримінального, адміністративного правопорушення (п. 4); розшукує осіб, які переховуються від органів досудового розслідування, слідчого судді, суду, ухиляються від виконання кримінального покарання, пропали безвісти, та інших осіб у випадках, визначених законом (п. 7); вживає заходів для забезпечення публічної безпеки і порядку на вулицях, площах, у парках, скверах, на стадіонах, вокзалах, в аеропортах, морських та річкових портах, інших публічних місцях (п. 10); регулює дорожній рух та здійснює контроль за дотриманням Правил дорожнього руху його учасниками та за правомірністю експлуатації транспортних засобів на вулично-дорожній мережі (п. 11); здійснює охорону об'єктів права державної власності у випадках та порядку, визначених законом та іншими нормативно-правовими актами, а також бере участь у здійсненні державної охорони (п. 19); здійснює на договірних засадах охорону фізичних осіб та об'єктів права приватної і комунальної власності (п. 20); виявляє транспортні засоби особистого користування, тимчасово ввезені на митну територію України громадянами більш як на 30 діб та не зареєстровані в Україні у встановлені законодавством строки (п. 29); вживає заходів для виявлення неправомірного керування транспортними засобами, щодо яких порушено обмеження, встановлені Митним кодексом України, а саме: порушено строки їх тимчасового ввезення та/або переміщення в митному режимі транзиту; транспортні засоби використовуються для цілей підприємницької діяльності та/або отримання доходів в Україні; транспортні засоби передано у володіння, користування або розпорядження особам, які не ввозили їх на митну територію України або не поміщували в митний режим транзиту, а також заходів для виявлення неправомірного розкомплектування таких транспортних засобів (п. 30). Таким чином, перерахований перелік засвідчує про наявність достатніх підстав та напрямів правоохоронної діяльності, за якими технології ШІ можуть бути використані Національною поліцією.

Так, відповідно до частини 2 статті 25 Закону України «Про Національну поліцію»[27], поліція у межах інформаційно-аналітичної діяльності: формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади; здійснює інформаційно-пошукову та інформаційно-аналітичну роботу; здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями».

Також стаття 27 вищеназваного Закону[28] передбачає можливість поліції мати безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади з неухильним дотриманням Закону України «Про

[27]Про Національну поліцію: Закон України від 02 липня 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

[28]Про Національну поліцію: Закон України від 02 липня 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

захист персональних даних»[29]. Інформація про доступ до бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про поліцейського, який отримав доступ, та про обсяг даних, доступ до яких було отримано. Кожна дія поліцейського щодо отримання інформації з інформаційних ресурсів, передбаченихстаттями 26, 27цього Закону[30], фіксується у спеціальному електронному архіві, ведення якого покладається на службу інформаційних технологій МВС України. В електронному архіві фіксуються прізвища, ім'я, по батькові та номер спеціального жетона поліцейського, вид отриманої інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації поліцейського, який отримував інформацію з реєстрів.

Використання технологій ШІ під час запобігання правопорушенням. Аналіз положень статей 25 та 27 Закону України «Про Національну поліцію»[31] дає підстави, що вони не в повній мірі надають можливість використовувати інструменти ШІ для збору та в подальшому обробки інформації. Зокрема, названі норми не передбачають можливість отримувати дані з відеокамер без згоди їх власників, що належать органам місцевого самоврядування, підприємств, організацій, установ не державної форми власності, а також від фізичних осіб. У статті 27 не уточнюється та не надається тлумачення терміну «оперативний доступ» до інформації та інформаційних ресурсів інших органів державної влади, а саме як він повинен здійснюватися поліцією.

У статті 25 Закону України «Про Національну поліцію»[32] не передбачено порядок отримання інформації від інших юридичних осіб, які не належать до органів влади, а також від фізичних осіб. Для прикладу, концепція «Безпечне місто» передбачає використання комплекс програмно-апаратних засобів та організаційних заходів для забезпечення відеоохорони та технічної безпеки, а також для управління в єдиному інформаційному просторі об'єктами житлово-комунального господарства та іншими розподіленими об'єктами, за допомогою єдиної системи відеоспостереження з розсердженим контролем доступу користувачів. Для забезпечення виконання функцій забезпечення публічної безпеки і порядку, безпеки дорожнього руху, захисту власності тощо Національною поліцією України передбачається використання апаратних комплексів систем відеоспостереження, які фіксують, що відбувається в місцях загального доступу: на стадіонах, всередині й зовні публічних і/або приватних приміщень, транспортних магістралей, в аеропортах, вокзалах та ін.

Проте, в Україні безліч апаратних комплексів систем відеоспостереження перебувають саме на балансі муніципальних органів, об'єднань власників

[29]Про захист персональних даних громадян: Закон України від 01 червня 2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

[30]Про Національну поліцію: Закон України від 02 липня 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

[31]Про Національну поліцію: Закон України від 02 липня 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

[32]Про Національну поліцію: Закон України від 02 липня 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

житлових та нежитлових приміщень, комунальних підприємств тощо. Загальновідомо, що органи місцевого самоврядування, як організаційно самостійний елемент системи місцевого самоврядування та комунальні підприємства до органів державної влади не належать. Як наслідок, ускладнюється доступ та втрачається оперативність аналізу правоохоронними органами інформаційного відеопотоку, який надходить з вказаних вище камер відеоспостереження у режимі реального часу, а це, у свою чергу, негативно впливає на результативність запобігання та протидії правопорушенням.

На сьогодні існують різні алгоритми обміну та порядку доступу поліції до інформаційних серверів та систем відеоспостереження, що не належать органам державної влади, як правило це меморандуми, різні форми угод та договорів. У деяких випадках порядок доступу поліцейських до відеоданих встановлюється актами органів місцевого самоврядування, в інших – взагалі не регламентується. Тому, законодавчо визначений доступ до пристроїв відеоспостереження та обробки інформації у роботі Національної поліції України має величезне значення у запобіганні та розкритті правопорушень, а також встановлення осіб, які їх вчинили тощо.

У Законі України «Про оперативно-розшукову діяльність»[33] закріплені основоположні правові норми, які регламентують допустимість проведення ОРД, дотримання прав і свобод людини, взаємодії з органами управління і населенням, а також здійснено законодавче регламентування всієї ОРД, унаслідок чого матеріали, отримані у процесі її здійснення, мають значення даних, отриманих у передбаченому законом порядку. Стаття 6 Закон України «Про оперативно-розшукову діяльність» визначає підстави для проведення оперативно-розшукових заходів, при цьому у статті 7 цього Закону зазначається, що підрозділи, які здійснюють оперативно-розшукову діяльність, зобов'язані у межах своїх повноважень відповідно до законів, що становлять правову основу оперативно-розшукової діяльності, вживати необхідних оперативно-розшукових заходів щодо попередження, своєчасного виявлення і припинення кримінальних правопорушень та викриття причин і умов, які сприяють вчиненню кримінальних правопорушень, здійснювати профілактику правопорушень. У разі виявлення ознак кримінального правопорушення оперативний підрозділ, який здійснює оперативно-розшукову діяльність, зобов’язаний невідкладно направити зібрані матеріали, в яких зафіксовані фактичні дані про протиправні діяння окремих осіб та груп, за вчинення яких передбачена відповідальність Кримінальним кодексом України, до відповідного органу досудового розслідування для початку та здійснення досудового розслідування в порядку, передбаченому КПК України. Таким чином вказані норми можуть слугувати підставами для використання підрозділами Національної поліції України, які здійснюють оперативно-розшукову діяльність, технологій ШІ й в ОРД.

[33]Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 р. № 2135-XII. URL: http://zakon2.rada.gov.ua/laws/show/2135-12.

У статті 8 Закону України «Про оперативно-розшукову діяльність»[34]для отримання інформації законодавець наділяє підрозділи, які здійснюють оперативно-розшукову діяльність, виключними правами, до яких, зокрема, відповідно до пп. 6, 7, 9, 11, 12, 15, 18, 21 можливе використання технологій ШІ, а саме належить право: збирати відомості про протиправну діяльність осіб, щодо яких провадиться перевірка; негласно виявляти та фіксувати сліди тяжкого або особливо тяжкого кримінального правопорушення; здійснювати аудіо-, відеоконтроль особи, зняття інформації з електронних комунікаційних мереж, електронних інформаційних мереж згідно з положеннями статей 260, 263-265 КПК України[35]; здійснювати спостереження за особою, річчю або місцем, а також аудіо-, відеоконтроль місця згідно з положеннями статей 269, 270 КПК України; здійснювати установлення місцезнаходження радіоелектронного засобу згідно з положеннями статті 268 КПК України; отримувати від юридичних чи фізичних осіб безкоштовно або за винагороду інформацію про кримінальні правопорушення, що готуються або вчинені, та про загрозу безпеці суспільства і держави; створювати і застосовувати автоматизовані інформаційні системи; безпосередньо проводити або ініціювати проведення кримінального аналізу.

КПК України[36] дозволяє слідчим НП України використовувати технології та інструменти ШТ у кримінальних провадженнях під час досудового розслідування, зокрема під час провадження наступних НСРД:

– аудіо-, відеоконтроль особи (ст. 260 КПК України) полягає в негласній (без відома особи) фіксації та обробці із використанням технічних засобів розмови цієї особи або інших звуків, рухів, дій, пов'язаних з її діяльністю або місцем перебування тощо;

– зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України)полягає в негласному проведенні із застосуванням відповідних технічних засобів спостереження, відбору та фіксації змісту інформації, яка передається особою, а також одержанні, перетворенні і фіксації різних видів сигналів, що передаються каналами зв'язку (знаки, сигнали, письмовий текст, зображення, звуки, повідомлення будь-якого виду);

– зняття інформації з електронних інформаційних систем (ст. 264 КПК України) полягає в пошуку, виявленні і фіксації відомостей, що містяться в електронній інформаційній системі або їх частин (електронно-обчислювальних машинах (комп'ютер), автоматичних системах, комп'ютерній мережі), доступ до електронної інформаційної системи або її частин;

– установлення місцезнаходження радіоелектронного засобу(ст. 268 КПК України) полягає в застосуванні технічного обладнання для локалізації місцезнаходження радіоелектронного засобу, у тому числі мобільного терміналу,

[34]Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 р. № 2135-XII. URL: http://zakon2.rada.gov.ua/laws/show/2135-12.

[35]Кримінальний процесуальний кодекс України від 13 квітня 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

[36]Кримінальний процесуальний кодекс України від 13 квітня 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

систем зв'язку та інших радіовипромінювальних пристроїв, активованих у мережах операторів рухомого (мобільного) зв'язку, без розкриття змісту повідомлень, що передаються, якщо в результаті його проведення можна встановити обставини, які мають значення для кримінального провадження;

– спостереження за річчю або місцем у публічно доступних місцях (ст. 269 КПК України) полягає у візуальному спостереженні за певною річчю або певним місцем слідчим чи уповноваженою особою для фіксації її переміщення, контактів з нею певних осіб, подій у певному місці для перевірки відомостей під час досудового розслідування тяжкого або особливо тяжкого злочину або застосуванні з цією метою спеціальних технічних засобів для спостереження;

– аудіо-, відеоконтроль місця (ст. 270 КПК України) полягає у застосуванні технічного обладнання у публічно доступному місці з метою фіксації відомостей (розмов, поведінки осіб, інших подій), які мають значення для кримінального провадження, без відома присутніх у ньому осіб.

Що стосується підзаконних актів, які регламентують використання інформаційних технологій в Національній поліції України, то на сьогодні наказом МВС України від 03 серпня 2017 р. № 676 затверджено Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»[37], яким визначено основні завдання, призначення, суб'єкти та структуру інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України», а також умови її функціонування. Аналіз вказаного положення засвідчує, що у ньому відсутні норми, які б повністю дали можливість урегулювати використання Національною поліцією України технологій ШІ, зокрема: загальні стандарти або правила використання технологій ШІ, способи реалізації рішень, які виробляються завдяки технологій ШІ, недопущення порушення фундаментальних прав людини, пов'язаних з використанням технологій ШІ в роботі правоохоронних органів.

Таким чином на сьогодні виникла необхідність розробити нові або внести зміни у вже існуючи відомчі та міжвідомчі нормативні акти, які повинні регулювати використання технологій ШІ під час:

– впровадження геоінформаційних систем для просторового розміщення об'єктів з використанням карт або планів, можливості використання інформаційно-телекомунікаційні системи МВС України та Національної поліції України з метою здійснення аналітики та кримінального аналізу правопорушень;

– створення спеціалізованих інформаційних інтелектуальних систем оперативно-розшукового призначення з метою забезпечення проведення оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування;

– впровадження інтелектуальних систем відеоспостереження з метою розпізнавання та класифікація об'єктів відеоспостереження та відстеження їх шляху переміщення;

[37]Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»: наказ Міністерства внутрішніх справ України від 03 серпня 2017 р. № 676. URL: https://zakon.rada.gov.ua/laws/show/z1059–17

– використання окремих видів транспортних засобів, у т. ч., що рухаються по поверхні води або під нею, безпілотних повітряних суден тощо;

– охорони об'єктів різних форм власності;

– встановлення місцеперебування осіб, які переховуються від органів досудового розслідування, слідчого судді, суду, ухиляються від виконання кримінального покарання, зникли безвісти, інших осіб у випадках, визначених законом;

– визначення правового статусу технологій ШІ в криминальному процесуальному законодавстві України, у тому числі при проведенні експертно-криміналістичних експертиз та досліджень, зокрема від час розслідування кримінальних правопорушень, які вчиненні з використанням технологій ШІ.

Крім того, потребує прийняття відомчих нормативно-правових актів МВС України та Національної поліції України, які б:

– визначали загальні стандарти (правила й обмеження) використання технологій ШІ в Національній поліції України;

– порядок використання інструментів отримання інформації підрозділами та територіальними органами Національної поліції при використанні технологій ШІ, у першу чергу під час застосування відеокамер здатних розпізнавати обличчя, що не належать органам державної влади;

– способи реалізації поліцейським чи іншою уповноваженою особою підрозділу чи територіального органу Національної поліції України рішень прийнятих системами ШІ;

− нейтралізація ризиків порушення фундаментальних прав людини, пов'язаних з використанням технологій ШІ в роботі Національної поліції України.