

УДК 342.7:004.8

ІРХА Ю.Б., кандидат юридичних наук, доцент, заслужений юрист України, завідувач наукової лабораторії права національної та міжнародної безпеки Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України»
ORCID: <https://orcid.org/0000-0002-6442-0974>

ЗАГРОЗИ ПРАВАМ І СВОБОДАМ ЛЮДИНИ В ЕПОХУ ШТУЧНОГО ІНТЕЛЕКТУ

DOI: [https://doi.org/10.37750/2616-6798.2025.4\(55\).346356](https://doi.org/10.37750/2616-6798.2025.4(55).346356)

Анотація. У статті здійснено комплексний аналіз впливу технологій штучного інтелекту на систему захисту прав і свобод людини. Автором проаналізовано міжнародні підходи до визначення сутності штучного інтелекту та констатовано формування нової технологічної реальності, де людський інтелект втрачає монополію на прийняття складних рішень. Ним акцентовано увагу на тому, що незважаючи на очевидні переваги систем штучного інтелекту для економіки та науки, їх безконтрольне поширення, особливо в умовах юридичної невизначеності, створює екзистенційні загрози демократії.

У роботі виокремлено ключові загрози правам і свободам людини в епоху штучного інтелекту, серед яких: тотальний цифровий нагляд, алгоритмічна дискримінація, маніпулювання суспільною свідомістю через дезінформацію та дінфейки, ерозія приватності та загроза втрати людської автономії. Детально розглянуто вразливість конкретних конституційних прав і свобод людини.

За результатами дослідження обґрунтовано неможливість подальшого перебування України в стані декларативного (“м’якого”) регулювання сфери штучного інтелекту. Автором сформульовано перелік пріоритетних кроків для законодавчого врегулювання галузі. Запропоновані заходи спрямовані на гармонізацію українського законодавства з європейськими стандартами та забезпечення балансу між технологічним розвитком і захистом фундаментальних прав і свобод людини.

Ключові слова: штучний інтелект, права і свободи людини, загрози правам і свободам людини, інформаційна безпека, національна безпека, правове регулювання, державна політика.

Summary. This article provides a comprehensive analysis of how artificial intelligence tech affects the system for protecting human rights and freedoms. The author looks at international approaches to defining what artificial intelligence is and notes that a new tech reality is forming where human intelligence is losing its monopoly on making tough decisions. He emphasizes that despite the obvious advantages of artificial intelligence systems for the economy and science, their uncontrolled spread, especially in conditions of legal uncertainty, creates existential threats to democracy.

The paper highlights key threats to human rights and freedoms in the age of artificial intelligence, including total digital surveillance, algorithmic discrimination, manipulation of public consciousness through disinformation and deepfakes, erosion of privacy, and the threat of loss of human autonomy. The vulnerability of specific constitutional human rights and freedoms is examined in detail.

The results of the study justify the impossibility of Ukraine's remaining into the status of declarative (“soft”) regulation of the field of artificial intelligence. The author has formulated a list of priority steps for legislative regulation of the industry. The proposed measures are aimed at

harmonizing Ukrainian legislation with European standards and ensuring a balance between technological development and the protection of fundamental human rights and freedoms.

Keywords: *artificial intelligence, human rights and freedoms, threats to human rights and freedoms, information security, national security, legal regulation, public policy.*

*Світ ловив мене, та не спіймав
Г. Сковорода*

Постановка проблеми. Стрімкий розвиток технологій поступово сформував нову реальність, де людський інтелект більше не є унікальним у своїй здатності до складної мови, абстрактного мислення та творчості. Розроблення різноманітних технологій штучного інтелекту (далі – ШІ) з можливостями, які постійно удосконалюються і перевершують людські, докорінно змінило життя багатьох, хто прямо чи опосередковано ними користується.

Здатність небіологічного інтелекту, так званого цифрового розуму, швидко обробляти, систематизувати, аналізувати та зберігати великі обсяги даних; виявляти приховані закономірності; робити короткострокові та довгострокові прогнози; створювати нову інформацію; автономно діяти та взаємодіяти з реальним та цифровим середовищем для досягнення поставленої мети; набувати власного досвіду; самостійно вчитися та удосконалюватися – суттєво прискорила розвиток науки і техніки та відкрила величезні можливості для реалізації кожним своїх прав, свобод та здібностей.

ШІ інтенсивно інтегрується у ключові сфери суспільного життя, трансформуючи усталені процеси та створюючи підґрунтя для якісних змін. Він знаходить широке застосування в управлінській, медичній, банківській, правоохоронній, воєнній, освітній, науковій та інших сферах. Серед основних позитивних результатів впровадження ШІ варто виділити такі:

- зниження частки участі людини в рутинних та небезпечних операціях;
- підвищення ефективності функціонування складних технологічних механізмів та бізнес-процесів;
- оптимізація використання ресурсів на побутовому, виробничому та державному рівнях;
- оптимізація управління ризиками;
- підвищення рівня безпеки для людини, суспільства, держави і довкілля;
- прискорення доступу до інформації, її пошуку та обробки для прийняття обґрунтованих рішень;
- розширення можливостей для наукових досліджень та прискорення впровадження нових технологій;
- створення нових інструментів для творчості та генерації контенту тощо.

Очевидно, що з появою ШІ людство отримало надпотужний інструмент для прогресу, однак його потенціал і спроможності дедалі більше викликають побоювань за демократичне майбутнє людства. Ці побоювання викликані не лише гіпотетичними трагічними сценаріями майбутнього, а й цілком реальними загрозами правам і свободам людини. Відтак, всебічне вивчення цих загроз є необхідною передумовою для створення дієвих механізмів захисту, які спрямують розвиток ШІ у безпечне русло.

Результати аналізу наукових публікацій. Широкомасштабне та безконтрольне поширення різноманітних технологій ШІ, їх надмірне та інколи сліпе впровадження у життя кожної людини викликають обґрунтовану стурбованість у науковій спільноті. Вчені у галузі юриспруденції, психології, соціології, філософії, медіа та комп'ютерних

наук одностайні в думці, що ці процеси формують безпрецедентні загрози для усталених соціальних та правових інститутів.

В Україні правові аспекти функціонування ШІ досліджували такі вчені, як О.А. Баранов, І.М. Берназюк, В.М. Брижко, С.Є. Булавіна, А.О. Гачкевич, Т.О. Давидова, О.П. Дзьобань, М.В. Дубняк, А.А. Завадський, М.В. Карчевський, О.І. Косілова, О.В. Кузьменко, Н.С. Марценко, В.А. Мисливий, Н. Пацурія, Н.А. Савінова, Х.К. Солодовнікова, В.М. Фурашев та інші.

Науковці однозначно визнають позитивні аспекти використання та застосування ШІ, але одночасно з цим багато хто з них звертає увагу на проблемні аспекти та негативні наслідки, які породжує стрімкий розвиток ШІ. У зв'язку з цим, існує необхідність поглибленого вивчення загроз ШІ правам і свободам людини, а також визначення ефективності існуючих механізмів захисту прав і свобод людини в умовах, коли рішення, що впливають на долю значної кількості індивідів та людства загалом, все частіше приймаються алгоритмами.

Мета статті полягає в системному аналізі ключових загроз правам і свободам людини, що виникають унаслідок розвитку та впровадження технологій ШІ, а також у розробці науково обґрунтованих рекомендацій щодо вдосконалення вітчизняного законодавства для ефективної протидії цим загрозам.

Виклад основного матеріалу. З кожним днем ШІ проникає дедалі більше у професійне, духовне та повсякденне життя людей, тому на міжнародному та національному рівнях істотно активізувалися дискусії та зусилля щодо створення етичних стандартів та правових механізмів для його регулювання. Це здійснюється з метою збалансування стрімких інновацій у сфері ШІ з потребою гарантувати безпеку людей, захистити їх фундаментальні права і свободи, запобігти можливим зловживанням технологіями, а також підвищити рівень довіри до них.

Основою для розробки вказаних норм є чітке визначення самого об'єкта регулювання. Саме тому провідні міжнародні організації зосередили зусилля на формулюванні єдиного підходу до розуміння того, що слід вважати ШІ.

Під егідою Організації Об'єднаних Націй з питань освіти, науки і культури (ЮНЕСКО) у 2021 році була прийнята Рекомендація щодо етики штучного інтелекту, в якій під системами ШІ запропоновано розуміти системи, що мають здатність обробляти дані та інформацію у спосіб, який нагадує інтелектуальну поведінку, і зазвичай включає аспекти міркування, навчання, сприйняття, прогнозування, планування або контролю. У документі наголошено, що системи ШІ – це технології обробки інформації, що інтегрують моделі та алгоритми, які забезпечують здатність навчатися та виконувати когнітивні завдання, що призводять до таких результатів, як прогнозування та прийняття рішень у фізичних та віртуальних середовищах [1].

Рада Організації економічного співробітництва та розвитку у Рекомендації щодо штучного інтелекту визначила, що система ШІ – це машино-орієнтована система, яка для явних або неявних цілей, на основі отриманих даних, робить висновки про те, як генерувати результати, зокрема прогнози, контент, рекомендації або рішення, які можуть впливати на фізичне або віртуальне середовище [2].

На теренах Європейського союзу у 2024 році було ухвалено закон “Про штучний інтелект”, в якому Європейський Парламент і Рада Європейського Союзу розуміють систему ШІ як машинну систему, розроблену для роботи з різним рівнем автономності, яка може демонструвати адаптивність після розгортання і яка, для явних або неявних цілей, виводить з отриманих нею вхідних даних, як генерувати такі вихідні дані, як-от

прогнози, контент, рекомендації чи рішення, що можуть впливати на фізичне або віртуальне середовище [3].

У Рамковій Конвенції Ради Європи зі штучного інтелекту, прав людини, демократії та верховенства права вказано, що система ШІ – це машинна система, яка з явними або неявними цілями визначає на основі вхідних даних, які вона отримує, як генерувати вихідні дані, такі як прогнози, контент, рекомендації або рішення, що можуть впливати на фізичне або віртуальне середовище. Крім того, наголошено, що різні системи ШІ відрізняються за рівнем автономності та адаптивності після розгортання [4].

Таким чином, на міжнародному рівні простежується чітка тенденція до гармонізації підходів до розуміння ШІ. Безперечно, внаслідок науково-технічного прогресу сутність та можливості ШІ будуть розвиватися, що потребуватиме періодичного оновлення його дефініції. Однак така пильна увага міжнародних інституцій до ШІ викликана не лише його вражаючими можливостями. Попри явні переваги, які отримують користувачі прогресивних моделей ШІ у бізнесі, управлінні, творчості та науці, ця технологія подібно до місяця має і свою “темну сторону”. Про неї розробники, власники, розповсюджувачі та оператори різних систем ШІ мало говорять, замовчують або взагалі не знають. Їхній приватний інтерес, а часом і проста недбалість та відсутність обачності, значно переважає турботу про аналіз і прогнозування ризиків, які ці технології становлять для людини, суспільства та держави.

У Щорічні оцінці загроз розвідувального співтовариства США за 2024 рік зазначено, що швидкий розвиток технологій став однією із транснаціональних загроз для США. У поєднанні із загрозами від державних суб’єктів це створює складні та каскадні ризики для американської національної безпеки. Фахівці з розвідки наголошують, що нові технології в галузі ШІ розробляються і поширюються такими темпами, що компаніям і урядам стає дедалі складніше формувати норми щодо громадянських свобод, приватності та етики. Конвергенція цих нових технологій, ймовірно, створить прорив, який може призвести до швидкого розвитку асиметричних загроз для американських інтересів. Генеративний ШІ – це засіб для відкриття і розробки нових технологій і передових процесів системного рівня, які можуть посилити технологічну, економічну і, ширше, стратегічну конкурентоспроможність країни. Досягнення в галузі ШІ та нові моделі машинного навчання переводять ШІ в індустріальну епоху з потенційно величезними економічними наслідками як для переможців, так і для переможених, а також непередбачуваними наслідками – від нестримного поширення фейків і дезінформації до розробки комп’ютерних вірусів, згенерованих ШІ, або нових видів хімічної зброї.

Американські фахівці звертають увагу на те, що Китай використовує ШІ для “розумних міст”, масового спостереження, охорони здоров’я, пошуку ліків та інтелектуальних збройових платформ. Китайські фірми, що розробляють ШІ, вже є світовими лідерами в галузі розпізнавання голосу та зображень, відеоаналітики та технологій масового спостереження. Натомість росія використовує ШІ для створення глибоких фейків і розвиває можливості для обману експертів. Прогнозується, що люди в зонах бойових дій і нестабільних політичних умовах можуть стати одними з найцінніших мішеней для такого зловмисного впливу [5, с. 30].

У 2019 році Генеральний директор Salesforce Марк Беніюфф виступаючи на Всесвітньому економічному форумі в Давосі заявив, що ШІ стає “новим правом людини”, і доступ до нього знадобиться кожному. Він вважає, що “ті, хто володіє ШІ, будуть розумнішими, здоровішими, багатшими, а їхні засоби ведення війни будуть значно досконалішими”. Разом з тим, ті, хто не має доступу до ШІ, “будуть слабшими,

біднішими, менш освіченими і більш хворобливими”. Марк Беніофф звернув увагу на те, що “ІІІ – це технологія, яку ніхто з нас ніколи не бачив, і ніхто з нас не може точно сказати, куди вона рухається. Проте, ми знаємо одне – технологія ніколи не буває хорошою чи поганою. Важливо те, що ми робимо з нею” [6].

Компанія “Cisco”, яка займає передові місця у сфері мережевих технологій, офіційно повідомила, що ІІІ має величезний потенціал для поліпшення якості життя людей, підвищення ефективності та продуктивності бізнесу, а також розширення можливостей суспільства у вирішенні глобальних проблем. Однак швидкий розвиток технологій ІІІ вимагає пильної уваги до питань безпеки, надійності, прозорості, справедливості, етики та рівності. Ці питання можуть стати загрозою для основних прав людини, особливо коли наслідки нових технологій неможливо передбачити. Темпи розвитку ІІІ та численні невідомі наслідки – як позитивні, так і негативні – для окремих осіб та громад у всьому світі вимагають від бізнесу зобов’язань щодо проактивного дотримання прав людини при проектуванні, розробці та використанні ІІІ [7].

О.В. Турута і О.П. Турута наголошують, що ІІІ відрізняється від людського: він не втомлюється, не піддається впливу емоцій та здатний обробляти величезні масиви інформації за короткий час. Саме ці переваги роблять ІІІ-рішення ефективними в ряді галузей. Впровадження технологій ІІІ в різні сфери життя здатне якісно змінити їх і підвищити результативність будь-якої роботи. Багато функцій, які, зазвичай, виконувалися людьми, стають все більш автоматизованими. Водночас, швидкий розвиток технологій ІІІ потребує пильної уваги до питань безпеки, надійності, прозорості, справедливості, етики та рівності (неупередженості). Ці проблеми можуть нести ризики для основних прав людини, особливо коли неможливо передбачити наслідки застосування такої нової технології. У міру того, як ІІІ продовжує проникати в наше повсякденне життя, його схильність до порушення прав людини стає дедалі серйознішою. Багато проблем, що виникають при дослідженні в цій галузі, не є новими, але вони значно погіршуються масштабом, поширенням і реальним впливом, який має ІІІ. Через це потенціал ІІІ як допомагати, так і шкодити людям набагато більший, ніж у технологій, що з’явилися раніше [8, с. 50].

Центральною проблемою технологій ІІІ є відсутність ефективних правових, інституційних та програмно-технічних механізмів контролю за їх розповсюдженням і функціонуванням. Це відбувається тому, що темпи технологічного розвитку значно випереджають здатність суспільства та державних інститутів вчасно на них реагувати. Ситуацію ускладнює також факт надзвичайної складності та непрозорості роботи багатьох систем ІІІ, що створює так званий ефект “чорної скриньки”, за якого навіть самі розробники не можуть до кінця пояснити, як саме нейромережа прийшла до певного висновку чи рішення.

Передові системи ІІІ здатні формувати у користувачів залежність від себе, маніпулювати ними, втручатися у їх права і свободи, здійснювати тотальний нагляд за їхньою поведінкою у публічних місцях та цифровому середовищі, а також поглиблювати соціальну нерівність, приймати непрозорі та непідзвітні рішення, розмивати межу між реальністю та фейком. Такий негативний вплив ІІІ може здійснюватися як автоматично, так і за прямою вказівкою своїх розробників чи операторів. На додаток, у найближчі роки існує висока ймовірність того, що ІІІ зможе вийти за межі початкових параметрів та директив і самостійно визначити власні пріоритети, цілі та цінності, які не збігатимуться з людськими. Цей момент докорінно змінить хід людської історії, розпочавши епоху з абсолютно непередбачуваним майбутнім.

Нобелівський лауреат Джефрі Хінтон, якого називають “хрещеним батьком штучного інтелекту”, заявив, що його турбує потенціал ШІ ліквідувати робочі місця та створити світ, де багато хто більше не зможе знати, що є правдою. Вчений вказав на приголомшливі темпи розвитку ШІ, які набагато перевищують те, що він та інші фахівці очікували. На його переконання, якщо ШІ стане набагато розумнішим за людей, він буде дуже добре ними маніпулювати, адже цьому він навчиться у них. За його твердженнями, у природі існує дуже мало прикладів того, як більш розумна істота контролюється менш розумною [9].

За твердженнями українських експертів, на відміну від звичайних обчислювальних систем, у випадку ШІ спостерігається ефект непередбачуваності (частково – нетривіальності) результатів його “роздумів”, що в загальному випадку є однією з ознак творчості та інноваційної діяльності, яка притаманна людині. З іншого боку, відсутність прозорих методів перевірки запропонованих ШІ висновків та рекомендацій утворює джерело невизначеності щодо їх вірності і практичної цінності [10, с. 7].

Журналісти британської газети “The Guardian” занепокоєні тим, що системи ШІ можуть перехитрити людину, адже зі зростанням їх складності зростає і їхня здатність до обману. Їх турбує те, що науковці Массачусетського технологічного інституту виявили численні випадки, коли системи ШІ обманювали опонентів, блефували і прикидалися людьми. Одна система навіть змінила свою поведінку під час імітації тестів на безпеку, що підвищило ймовірність того, що аудитори були втягнуті в оманливе відчуття захищеності. Так, під час одного дослідження ШІ знайшов спосіб обійти тест, що мав на меті усунути системи, які еволюціонували для швидкого розмноження. Щоб вижити, ШІ в цифровій симуляції тимчасово припинив активність (“прикинувся мертвим”), а після завершення тестування відновив її. Це яскраво демонструє, наскільки технічно складно уникнути появи непередбачуваної та небажаної поведінки в таких системах [11].

У 2023 році засновник SpaceX Ілон Маск, співзасновник Apple Стів Возняк та інші відомі фахівці та вчені у сфері новітніх технологій підписали відкритий лист про призупинення розвитку ШІ. На їхнє переконання, лабораторії ШІ вступили в неконтрольовану гонку з розробки та впровадження все більш потужних цифрових розумів, які ніхто – навіть їхні творці – не може зрозуміти, передбачити або надійно контролювати. Вони застерegli світ від небезпечної гонитви за дедалі більш непередбачуваними моделями “чорної скриньки” з новітніми можливостями.

Автори листа вважають, що дослідження та розробки в галузі ШІ повинні бути переорієнтовані на те, щоб зробити сучасні високотехнологічні системи більш точними, безпечними, зрозумілими, прозорими, стійкими, збалансованими, надійними та лояльними. Підписанти пропонували встановити щонайменше піврічний мораторій на розробку програм ШІ, які є потужнішими за ChatGPT-4, задля формування універсальних протоколів безпеки для прогресивного проектування та розробки ШІ. Ці протоколи мали б гарантувати, що системи, які їх дотримуються, є безпечними поза розумними сумнівами [12].

Сьогодні новітні технології ШІ використовуються не тільки для покращення нашого життя, вони все частіше стають зброєю у руках зловмисників. Їх активно використовують у злочинній діяльності, тероризмі, розвідувально-підривній діяльності, шпигунстві та для ведення бойових дій різного масштабу. Такі високотехнологічні загрози спрямовані безпосередньо проти демократії, верховенства права та фундаментальних прав і свобод людини, створюючи нові виклики для національної та глобальної безпеки. Особливе занепокоєння викликає той факт, що транснаціональні

корпорації, які є розробниками та рушіями технологічного прогресу, самі можуть бути причетними до неправомірного використання власних інновацій. Маючи величезні ресурси та доступ до передових розробок, такі компанії отримують потужні інструменти впливу на соціальні, економічні, політичні та міжнародні процеси у всьому світі.

Кейт Кроуфорд з Microsoft Research попередила, що оскільки ШІ стає дедалі потужнішим, людям потрібно переконатися, що авторитарні режими не використовують його для централізації влади та атак на певні групи населення. Дослідниця звертає увагу на реальну можливість використання радикальними рухами технологій ШІ у боротьбі за владу [13].

Науковці зі Сполучених Штатів Америки вважають, що існує багато ризиків, пов'язаних з тим, що системи ШІ систематично викликають помилкові переконання. Основними джерелами неправдивої інформації від ШІ сьогодні є неточні чат-боти та навмисно створені “deepfakes”, але існує й третє джерело – навчений обман. Вчені б'ють на сполох, адже зловмисне використання технології навченого обману в системах ШІ прискорить процес формування помилкових переконань у користувачів-людей. При втраті контролю автономні системи ШІ можуть використовувати обман для досягнення власних цілей. Вважається, що коли ШІ навчиться “професійно” обманювати, він може бути використаний для неправомірних цілей.

По-перше, використання ШІ може призвести до збільшення кількості випадків шахрайства. Системи ШІ з можливостями обману можуть бути індивідуалізовані під конкретні цілі та, за необхідності, легко масштабовані.

По-друге, ШІ може стати зброєю на виборах. Просунутий штучний інтелект потенційно може генерувати та поширювати фейкові новини, провокаційні дописи в соціальних мережах та відео з використанням технології deepfake, які будуть адаптовані до індивідуальних потреб виборців. Окрім впливу на вибори, генеративний ШІ може видавати себе за виборців і намагатися впливати безпосередньо на політиків.

По-третє, ШІ може бути використаний для вербування терористів. На сьогодні у країнах не існує чіткої юридичної відповідальності за створення чат-ботів, що пропагують тероризм, вихваляють та ідеалізують терористичні організації. Це приводить до негативних наслідків. Так, у 2021 році у Великій Британії Джасвант Сінгх Чайл намагався вбити королеву, частково завдяки заохоченню з боку чат-бота зі ШІ. Існує інформація, що окремі терористичні угруповання вже почали вивчати можливості використання генеративного ШІ для пропаганди терористичних ідеологій. Вважається, що ШІ може сприяти терористичним кампаніям з дезінформації та радикалізації.

Іноземні науковці дійшли висновку, що в перспективі системи ШІ відіграватимуть дедалі більшу роль у житті людей, які ними користуються. Тенденції до навченого обману в цих системах можуть призвести до глибоких змін у структурі суспільства, створюючи потужні перешкоди, які заважатимуть формуванню чітких переконань, політичній стабільності та автономії [14].

Наведені думки експертів та приклади функціонування сучасних систем ШІ свідчать про формування нової технологічної реальності, де загрози правам і свободам людини набувають комплексного та багатовимірного характеру. Це вимагає від суспільства та держави швидкої адаптації та удосконалення механізмів захисту. Системний аналіз міжнародних правових документів та наукових праць вчених у сфері ШІ дозволяє виокремити ключові загрози для прав і свобод людини, що виникають внаслідок використання та застосування ШІ, а саме:

- 1) несанкціонований збір величезних масивів даних та інформації про фізичних та юридичних осіб, явища, події тощо;

- 2) безтермінове зберігання даних та інформації;
- 3) надмірна обізнаність про приватне і публічне життя людей;
- 4) контроль за економічною активністю, соціальною і політичною поведінкою людини;
- 5) використання персональних даних та іншої інформації для сортування та мікротаргетингу людей;
- 6) вплив та маніпулювання думками та діями людей;
- 7) проведення спеціальних інформаційних операцій та поведінкових експериментів над окремими людьми, їх групами, спільнотами;
- 8) виявлення та використання індивідуальних вразливостей людини;
- 9) відтворення, закріплення та посилення існуючих у суспільстві стереотипів;
- 10) формування у користувачів психоемоційної залежності від продуктів зі ШІ;
- 11) ерозія людської автономії та відповідальності;
- 12) скорочення робочих місць через автоматизацію виробничих процесів;
- 13) створення систем озброєння, що діють без людського контролю та здатних самостійно приймати рішення про життя та смерть «ворога»;
- 14) застосування методів профілювання для ідентифікації та цільового моніторингу осіб з метою прогнозування ймовірності їх злочинної діяльності;
- 15) ігнорування загальнолюдських цінностей та соціального, етичного, культурного й іншого контексту під час прийняття рішень;
- 16) формування значного технологічного, інформаційного, освітнього, наукового розриву між тими, хто користується ШІ та тими, хто ні.

Зазначені загрози не є ізольованими, вони взаємопов'язані, підсилюють одна одну та здатні створювати каскад порушень громадянських, політичних, економічних, соціальних, інформаційних прав і свобод людини. Поділяючи думку Ю.С. Разметаєвої про складність прогнозування, які саме права і свободи людини опиняються під ударом із кожною наступною інновацією, які неявні наслідки для них приносять самі технологічні інструменти або специфіка їх використання [15, с. 107], вважаємо за необхідне виокремити ті права і свободи, які на сьогодні є найбільш вразливими до негативного впливу ШІ.

1. Право на приватність.

Системи ШІ здатні здійснювати безпрецедентний за своїми масштабами збір, аналіз та використання персональних даних та іншої інформації, що дозволяє відстежувати кожен крок людини, виявляти її соціальні зв'язки, звички, політичні погляди, релігійні переконання, стан здоров'я, сексуальну орієнтацію, фінансове становище тощо, а також визначати її вразливості та психологічний профіль. Поступово це може призвести до втрати людиною своєї автономії, що дозволить державі, бізнесу, криміналітету, а також “цифровому розуму” здійснювати значний вплив на її життя.

2. Право на свободу.

Масове впровадження технологій розпізнавання облич і емоцій у публічних місцях, освітніх закладах, робочому місці, моніторингу активності в цифровому середовищі, а також систем соціального рейтингу формує у суспільстві атмосферу недовіри та страху. Усвідомлення постійного контролю спонукає людей до самоцензури та конформізму, оскільки будь-яке відхилення від соціальних чи офіційно встановлених норм поведінки може стати підставою для дискримінації, тиску чи переслідування. Побоюючись таких наслідків, вони починають уникати вираження непопулярних чи критичних поглядів, обмежують свою участь у громадському та політичному житті. Усе це підриває автономію особистості та знецінює свободу як таку.

3. Право на життя.

У військовій та правоохоронній сферах розробляються та розгортаються автономні системи зі ШІ, яким делегується можливість самостійно, без людського контролю, обирати та атакувати цілі (ворога, злочинця) із застосуванням летального озброєння. Делегування нейромережі, а не людині, повноважень приймати рішення про життя та смерть порушує істотні етичні та правові питання. Такі системи, на відміну від людини (військовослужбовця, правоохоронця), не здатні до складного морального судження, розуміння контексту, співчуття та застосування принципів законності, необхідності, пропорційності та розрізнення, що є обов'язковим у міжнародному гуманітарному праві та міжнародних стандартах правоохоронної діяльності. Крім того, виникає питання щодо відповідальних за дії цих систем. У випадку загибелі невинних людей, завдання їм травм або пошкодження їхнього майна внаслідок технічного збою, системної помилки чи неадекватної реакції алгоритму на нештатну ситуацію, неможливо визначити, хто саме несе юридичну відповідальність – програміст, виробник чи оператор, що активував систему.

4. Право на інформацію.

Алгоритми ШІ, що лежать в основі соціальних мереж та онлайн-платформ, часто використовують механізми персоналізації для створення так званих “інформаційних бульбашок” (інформаційної ізоляції), які є потужним каталізатором для “ехо-камери” (соціальної ізоляції). Аналізуючи поведінку користувача, системи ШІ здатні показувати йому лише той контент, що відповідає його існуючим поглядам, та водночас непомітно відфільтровує альтернативну інформацію. У такий спосіб для кожної людини формується індивідуальна цифрова реальність. Окремо варто звернути увагу на спроможності систем ШІ за лічені секунди створювати та масово поширювати упереджену інформацію, дезінформацію, сфабриковані відео- та аудіозаписи (“діпфейки”).

Наведене розмиває межі між правдою і вигадкою та порушує право кожного на вільне отримання актуальної, достовірної, об'єктивної, повної, перевіреної інформації. Внаслідок цього у людей знижується здатність до критичного мислення та формування власного незалежного світогляду, що робить її досить вразливою до маніпуляцій.

5. Політичні права і свободи

За допомогою генеративного ШІ в Інтернеті та соціальних мережах можна створювати інформаційні матеріали для дискредитації або формування ілюзії масової підтримки чи осуду органів публічної влади, державних чи громадських діячів, політичних чи громадських організацій, певних ідеологій, кандидатів на виборні посади. Крім того, на підставі аналізу великих масивів даних можна створювати психологічні портрети виборців і персоналізовано впливати на їх світогляд та волевиявлення. Усе це відкриває можливості для цілеспрямованого втручання у результати виборів та референдумів, фактично нівелюючи виборчі права громадян.

Через ШІ можна згенерувати масові звернення до органів публічної влади від імені “стурбованих” представників громадськості, створюючи хибне уявлення про громадську думку та примушуючи їх до ухвалення необхідних комусь рішень, фактично перетворює інститут звернень громадян (право на петицію) на фікцію.

Використання державою технологій ШІ для збору різноманітної інформації про людей в інтересах національної безпеки та правоохоронної діяльності може одночасно бути використано для контролю і придушення інакомислення та протестної активності в суспільстві. Така ситуація підриває основи демократії, оскільки призводить до згортання

плюралізму та обмеження громадянських прав: від свободи слова та віросповідання до права на мирні зібрання і доступ до інформації

6. Порушення презумпції невинуватості та права на доступ до правосуддя

Використання правоохоронними органами систем ШІ для прогнозування злочинів та їх рецидиву істотно змінює підходи до їх роботи. Замість того, щоб реагувати на вже скоєний злочин, правоохоронці починають більше діяти на основі ймовірності, що хтось може його скоїти. Внаслідок цього індивіда розглядають як потенційного правопорушника не на основі доказів його вини, а через його відповідність певному профілю правопорушника. Через це до нього можуть застосовуватися адміністративні, оперативно-розшукові, контррозвідувальні та кримінально-процесуальні заходи, пов'язані із втручанням у його права і свободи. Наведене суперечить презумпції невинуватості, яка є основою правової держави.

Судді використовують системи ШІ для аналізу та оцінки доказів, виявлення неочевидних зв'язків між ними та прихованих закономірностей у матеріалах справи, пошуку релевантних норм права і юридичних прецедентів. Надмірна залежність суддів від ШІ може призвести до зниження їх кваліфікації та ухвалення несправедливих і необ'єктивних рішень.

Прагнення до скорочення витрат на судову систему може призвести до надмірної автоматизації окремих судових процесів, особливо у справах, що вважаються “малозначними”. У випадках застосування системи ШІ у правосудді людина може бути позбавлена права бути вислуханою, а також права на справедливе судове рішення.

7. Право на рівність та недискримінацію

Алгоритми різноманітних систем ШІ можуть формуватися на даних, які відображають існуючі людські стереотипи (гендерні, расові, соціальні) чи містять дискримінаційні або несправедливі практики. Навчаючись на таких даних, ШІ сприймає цю упередженість як об'єктивну закономірність, що є проявом так званої “алгоритмічної упередженості”. Внаслідок цього його рішення та згенерована інформація можуть ставати проявом неправомірного розрізнення. Це явище отримало назву “алгоритмічна дискримінація”. ШІ здатний не лише відтворювати, але й автоматизувати, масштабувати та посилювати існуючу в суспільстві нерівність, створюючи нові форми дискримінації.

Крім того, нерівний доступ до технологій ШІ сам по собі стає потужним джерелом дискримінації. Розробка та впровадження передових систем ШІ вимагають величезних фінансових, освітніх, наукових та інших ресурсів, які сконцентровані в руках небагатьох технологічних гігантів та розвинених країн. Це створює “цифровий розрив”, в якому переваги від ШІ стають привілеєм для одних, тоді як інші залишаються не лише без доступу до цих благ, а й стають більш вразливими до їхніх негативних наслідків. Таким чином, виникає новий вид структурної нерівності, де цілі суспільства та країни ризикують опинитися на узбіччі технологічного прогресу.

8. Трудові права

Внаслідок значної автоматизації виробничих процесів за допомогою систем ШІ відбувається заміщення людей не лише з рутинних, а й з інтелектуальних та творчих професій. Це призводить до зростання структурного безробіття і знецінення людських навичок, залишаючи мільйони людей без засобів до існування та можливості реалізувати свій професійний та творчий потенціал. Водночас, загроза автоматизації використовується для послаблення позицій профспілок і тиску на працівників з метою погіршення умов праці та зниження їх заробітної плати. Окрім заміщення людей, системи ШІ можуть призводити до зниження їх кваліфікації, оскільки вони здатні перебрати на себе складні, творчі та

аналітичні частини роботи, а людині залишити лише примітивні, монотонні завдання. У зв'язку з цим рівень оплати праці таких осіб знижується.

У деяких технологічно розвинутих компаніях системи ШІ впроваджуються в механізми управління персоналом. Такі системи можуть непрозоро розподіляти завдання, оцінювати продуктивність і, навіть, ухвалювати рішення про преміювання чи звільнення без участі людини. Це позбавляє працівників відчуття власної цінності та суб'єктності, що веде до демотивації та професійного вигорання. До того ж, рекрутингові системи на базі ШІ, навчені на упереджених даних, можуть систематично відсіювати резюме кандидатів на підставі їх належності до певної соціальної групи.

ШІ надає роботодавцям безпрецедентні інструменти для тотального контролю за працівниками, порушуючи їх право на приватність та гідні умови праці. Відомі випадки, коли роботодавці використовували ШІ для аналізу робочої електронної пошти, моніторингу робочої активності, діяльності та емоцій людини на робочому місці тощо. Такий цифровий нагляд створює вороже робоче середовище, підвищує стрес та позбавляє працівників автономії.

9. Права і свободи дитини

Із самого малечку діти оточені смартфонами, “розумними” іграшками, соціальними мережами, комп'ютерними іграми, освітніми та іншими інтернет платформами в яких використовується ШІ. Застосунки та пристрої з ШІ масово збирають персональні дані дитини: її голос, зображення, місцезнаходження, інтереси та поведінку. Постійне цифрове спостереження, часто без повної згоди та розуміння батьків, є прямим порушенням права дитини на приватність.

Алгоритми ШІ, що лежать в основі багатьох технологічних продуктів, створені для максимального утримання уваги. Оскільки діти ще не мають розвиненого критичного мислення, вони є особливо вразливими до їхнього впливу. ШІ підбирає контент, що може викликати цифрову залежність, нав'язувати певні погляди, споживацькі звички або навіть небезпечні ідеї. Це обмежує свободу волі дитини та перешкоджає її здоровому розвитку.

Надмірна взаємодія із продуктами на базі ШІ може призвести до спрощеного розуміння складних людських стосунків. Віртуальне спілкування, кероване нейромережами, ризикує підмінити живе спілкування з однолітками та батьками, що може негативно позначатися не лише на психічному, а й на фізичному здоров'ї дитини, призвести до відриву від реального світу та труднощів у соціалізації.

Проведений аналіз демонструє, що ШІ чинить серйозний і дедалі зростаючий негативний вплив на права і свободи людини, змінюючи сам баланс сил між людиною, суспільством та державою. Очевидно, що правозахисні механізми, успадковані з аналогової епохи, виявляються непристосованими до цієї нової реальності та потребують модернізації. Відтак, головним завданням сучасності стає побудова надійної правової системи, адаптованої до загроз, які несе ШІ. Це вимагає не лише адаптації існуючих правових інститутів, а й створення нових правових та організаційних механізмів моніторингу та контролю за розробкою, поширенням, використанням і застосуванням ШІ в різних сферах.

В Асіломарських принципах роботи зі штучним інтелектом наголошено, що:

- передовий ШІ може спричинити глибокі зміни в історії життя на Землі, тому його впровадження та управління ним повинні плануватися з відповідною ретельністю та ресурсами;
- системи ШІ повинні бути безпечними та надійними протягом усього терміну їх експлуатації, а також піддаватися перевірці, де це доцільно та можливо;

- високоавтономні системи ШІ повинні бути розроблені таким чином, щоб їх цілі та поведінка були узгоджені з людськими цінностями протягом усього терміну їх експлуатації;
- системи ШІ повинні бути спроектовані та експлуатуватися таким чином, щоб бути сумісними з ідеалами людської гідності, прав, свобод та культурного різноманіття;
- люди повинні вибирати, яким чином і чи варто делегувати прийняття рішень системам ШІ для досягнення обраних людьми цілей;
- системи ШІ, розроблені для рекурсивного самовдосконалення або самовідтворення, що може призвести до швидкого підвищення їх якості або кількості, повинні підлягати суворим заходам безпеки та контролю [16].

Зазначені принципи є універсальними і слугують міжнародним орієнтиром для формування національних політик у сфері ШІ. Для України це завдання постає з особливою гостротою, адже до сьогодні у нас існують лише концептуальні документи, які визначають стратегії та наміри, а не загальнообов'язкові правила поведінки у сфері ШІ.

Відповідно до Концепції розвитку штучного інтелекту в Україні, схваленої розпорядженням Кабінету Міністрів України від 02.12.2020 № 1556, під ШІ розуміється 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 [17].

На переконання О.А. Баранова, ШІ – це система, яка складається із сукупності технологій, методів, способів, засобів та пристроїв, насамперед, комп'ютерних, що імітує (моделює) певну сукупність когнітивних функцій еквівалентних відповідним когнітивним функціям людини [18, с. 67].

Утім, попри наявність доктринального розуміння сутності штучного інтелекту та перших спроб його офіційного тлумачення Урядом України, подальша інституціоналізація цієї сфери фактично зупинилася. Всупереч глобальним тенденціям щодо правового регулювання ШІ та інших наскрізних технологій, вітчизняна правова система й досі демонструє інертність у питанні їх належної законодавчої регламентації.

Неможливо не погодитися з твердженнями О.Б. Бунчук, що право завжди “наздоганяє” людські відносини, які перебувають у стані безперестанного динамічного розвитку [19]. У своєму дослідженні О.С. Гиляка аргументовано стверджує, що сучасні технології поряд з розширенням можливостей для реалізації прав і свобод людини призвели до масового їх порушення. Жодна політична, соціальна чи правова інституції не встигають за цим переходом, і розуміння того, як захищати права і свободи людини, зазнає серйозних викликів. На сьогодні у світі існує еволюційний розрив між технічним прогресом та його правовим забезпеченням. Адаптація як національного, так і міжнародного права до досягнень науки і техніки часто буває надто повільною і, як наслідок, право не завжди в змозі адекватно врегульовувати ситуації, спричинені розвитком технологій [20, с. 17].

Ще у 2018 році Р.С. Стефанчук наголошував, що стан нормативно-правового забезпечення сфери інформаційних технологій в Україні має початковий рівень, який надає можливість лише доганяти розвинуті правові порядки, а не відігравати роль лідера. Адже фактично на сьогодні немає навіть натяків на формування єдиного, концептуально нового, системного, всеохоплюючого правового механізму, за допомогою якого можна було б комплексно забезпечити динаміку суспільних відносин, спричинену бурхливим розвитком

сфери інформаційних технологій. Ані науковці-правники, ані законотворці не готові до формування правової політики в цій сфері, визначення меж та умов комплексного нормативно-правового регулювання застосування сучасних інноваційних підходів, методологій і технологій [21, с. 38].

У червні 2024 року Міністерство цифрової трансформації України опублікувало аналітичний матеріал “Біла книга з регулювання ІІІ в Україні: бачення Мінцифри”, в якому пропонує здійснити поступове впровадження регулювання у сфері ІІІ: від позазаконодавчих інструментів та ініціатив протягом найближчих кількох років до прийняття спеціального закону зі ІІІ на фінальному етапі. Суть цього підходу полягає в розділенні шляху до впровадження обов’язкового регулювання на два етапи: підготовчий етап та етап впровадження закону-аналога Регламенту ЄС зі штучного інтелекту [22, с. 13]. Вважаємо, що запропоноване згаданим міністерством м’яке регулювання сфери ІІІ є запізнілим рішенням, яке несе ризики консервації стану юридичної невизначеності та робить людей і державу вразливими перед новітніми технологічними загрозами.

Станом на кінець 2025 року доводиться констатувати, що фундаментального зрушення в бік системності так і не відбулося, а розрив між технологічним прогресом та його нормативним забезпеченням в Україні лише поглибився. Замість створення цілісного цифрового кодексу чи узгодженого комплексу правових актів, законодавець пішов шляхом фрагментарних, точкових рішень, які не охоплюють глибини новітніх суспільних відносин. Фактично, українське правове поле у сфері ІІІ – це сукупність застарілих норм, законодавчих прогалин та новітніх декларацій. Такий стан справ призводить не тільки до численних порушень прав і свобод людини, але й створює реальні загрози національній безпеці, оскільки держава втрачає контроль над впливом алгоритмів на суспільну свідомість, процеси прийняття державних рішень, функціонування демократичних інститутів, критичну інфраструктуру тощо.

Висновки. На тлі бурхливого розвитку ІІІ світ надзвичайно швидко рухається до глобального цифрового суспільного ладу, який ніхто повністю не розуміє, але наслідки якого ми усі відчуваємо. Необхідно визнати – технології мали, мають і будуть мати істотний вплив на людей. Вони не тільки змінюють їх звички, уподобання, мислення та поведінку, але й ціннісні уявлення про добро, зло, справедливість, сенс життя, щастя, гідність, честь, обов’язок, відповідальність. На гірше чи на краще – залежить від того, чи зможемо ми вибудувати чіткі правові та етичні запобіжники, за яких технологічний прогрес слугуватиме утвердженню, а не нівелюванню людської сутності.

Очевидно, що традиційні механізми захисту прав і свобод людини, розроблені в доцифрову епоху, вже не здатні повною мірою реагувати на динаміку, непрозорість та масштаб загроз, що генеруються системами ІІІ. Людство повинно мати реальні важелі впливу на технології, які так глибоко формують його сьогодення та майбутнє. Зазначене повною мірою стосується і України, яка не може залишатися осторонь глобальних процесів цифрової трансформації.

В умовах російсько-української війни та стратегічного курсу на європейську та євроатлантичну інтеграцію наша держава не може дозволити собі й надалі залишатися в стані юридичної невизначеності у сфері регулювання ІІІ. Відтак, на рівні закону необхідно якнайшвидше визначити:

- правові та етичні засади функціонування ІІІ;
- допустимі сфери та межі застосування ІІІ, а також перелік заборонених практик;

- статус контрольованих середовищ для тестування систем ШІ (“regulatory sandboxes”), які дозволяють оцінити безпеку, юридичні наслідки функціонування цих технологій у реальних умовах, а також адаптувати законодавство до їх виходу на ринок;
- механізми обов’язкового державного та недержавного нагляду, тестування, сертифікації та аудиту у сфері ШІ, а також суб’єктів, уповноважених на здійснення оцінки відповідності та прийняття рішень щодо допуску таких систем до експлуатації;
- рівні та вимоги до взаємодії людини і ШІ залежно від ступеня ризику відповідної системи;
- вимоги до кібербезпеки, захисту інформації та даних, що використовуються для навчання ШІ;
- правила маркування контенту, створеного за допомогою ШІ;
- правовий режим об’єктів інтелектуальної власності, згенерованих ШІ;
- стандарти прозорості та пояснюваності рішень, що мають юридичні наслідки для людини;
- права, обов’язки та відповідальність розробників, виробників, користувачів ШІ;
- вимоги до використання систем ШІ в державному управлінні, правосудді, критичній інфраструктурі, охороні здоров’я, освіті, сфері праці та наданні адміністративних і соціальних послуг;
- особливості використання та застосування систем ШІ в органах сектору безпеки і оборони під час виконання бойових завдань, правоохоронних операцій, здійснення інформаційно-аналітичної, контррозвідувальної, оперативно-розшукової та розвідувальної діяльності;
- заходи щодо підвищення рівня цифрової грамотності та компетентності у сфері ШІ для різних категорій населення.

Вітчизняна правова система має ефективно “спіймати” ШІ у законодавчі рамки, унеможлививши його використання на шкоду людині, суспільству і державі. Тільки так ми зможемо захистити права і свободи та гарантувати умови, за яких людина не буде поглинута власними технологіями, а залишатиметься вільною особистістю, чия гідність і сутність цей цифровий світ ловив, та не спіймав.

Перелік використаних джерел

1. United Nations Educational, Scientific and Cultural Organization. Recommendation on the Ethics of Artificial Intelligence, adopted on 23 November 2021. URL: <https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence> (дата звернення: 15.11.2025).
2. Organisation for Economic Co-operation and Development. Recommendation of the Council on Artificial Intelligence, adopted on 3 May 2024. URL: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> (дата звернення: 15.11.2025).
3. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689 (дата звернення: 15.11.2025).
4. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, adopted on 5 September 2024. URL: <https://rm.coe.int/1680afae3c> (дата звернення: 20.11.2025).
5. Annual Threat Assessment of the U.S. Intelligence Community. Office of the Director of National Intelligence. February 5, 2024. 41 p. URL:

<https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf> (дата звернення: 20.11.2025).

6. Salesforce CEO Marc Benioff calls artificial intelligence a «new human right». *Business Insider*. January 24, 2019. URL: <https://www.businessinsider.com/salesforces-benioff-calls-artificial-intelligence-a-new-human-right-2019-1> (дата звернення: 21.11.2025).

7. Cisco Human Rights Position Statements. URL: <https://www.cisco.com/c/dam/assets/csr/pdf/Human-Rights-Position-Statements-2018.pdf> (дата звернення: 21.09.2025).

8. Турута О. В., Турута О. П. Штучний інтелект крізь призму фундаментальних прав людини. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2022. № 71. С. 49-54. DOI: <https://doi.org/10.24144/2307-3322.2022.71.7> (дата звернення: 20.11.2025).

9. Jennifer Korn. Why the «Godfather of AI» decided he had to ‘blow the whistle’ on the technology. URL: <https://edition.cnn.com/2023/05/02/tech/hinton-tapper-wozniak-ai-fears> (дата звернення: 20.11.2025).

10. Скіцько О., Складанний П., Ширшов Р., Гуменюк М., Ворохоб М. Загрози та ризики використання штучного інтелекту. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2023. № 2(22), С. 6–18. DOI: <https://doi.org/10.28925/2663-4023.2023.22.618>.

11. Hannah Devlin. Is AI lying to me? Scientists warn of growing capacity for deception. URL: <https://www.theguardian.com/technology/article/2024/may/10/is-ai-lying-to-me-scientists-warn-of-growing-capacity-for-deception> (дата звернення: 20.11.2025).

12. Pause Giant AI Experiments: An Open Letter. URL: https://futureoflife.org/wp-content/uploads/2023/05/FLI_Pause-Giant-AI-Experiments_An-Open-Letter.pdf (дата звернення: 20.11.2025).

13. Olivia Solon. Artificial intelligence is ripe for abuse, tech researcher warns: «a fascist's dream». URL: <https://www.theguardian.com/technology/2017/mar/13/artificial-intelligence-ai-abuses-fascism-donald-trump> (дата звернення: 20.11.2025).

14. Park P.S., Goldstein S., O'Gara A., Chen M., Hendrycks D. AI deception: A survey of examples, risks, and potential solutions. *Patterns*. 2024. May 10. Vol. 5(5). URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC11117051/>. DOI: doi: 10.1016/j.patter.2024.100988 (дата звернення: 20.11.2025).

15. Разметаєва Ю.С. Демократія, права людини та інтернет. *Право і суспільство*. 2020. № 1. С. 104–110. DOI: <https://doi.org/10.32842/2078-3736/2020.1-1.16>.

16. Asilomar AI Principles. URL: <https://futureoflife.org/open-letter/ai-principles/> (дата звернення: 20.11.2025).

17. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 р. № 1556. URL: <https://zakon.rada.gov.ua/go/1556-2020-%D1%80> (дата звернення: 20.11.2025).

18. Баранов О. Штучний інтелект і система права : монографія / О. Баранов ; ДНУ «Інститут інформації, безпеки і права Національної академії правових наук України». Київ; Одеса : Фенікс, 2025. 296 с.

19. Бунчук О.Б. Новітні людські права: прийняти не можна заборонити. *Сайт юридичного факультету Чернівецький національний університет ім. Ю. Федьковича*. URL: <https://law.chnu.edu.ua/novitni-liudski-prava-priyniaty-ne-mozhna-zaboronyty/> (дата звернення: 20.11.2025).

20. Гиляка О.С. Новітні технології та права людини: аналіз деяких критичних проблем цифрової ери. *Вісник Національної академії правових наук України*. 2023. Т. 30. № 2. С. 15–30. DOI: <https://doi.org/10.31359/1993-0909-2023-30-2-15>.

21. Стефанчук Р.О. Інформаційні технології та право: quo vadis? *Право України*. 2018. № 1. С. 30–50.

22. Біла книга з регулювання ІІІ в Україні: бачення Мінцифри. Київ : Мінцифри. 30 с. <https://storage.thedigital.gov.ua/files/d/9d/0bbc3a705c821a197bedfcdfe00899d9.pdf> (дата звернення: 20.11.2025).