

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»
ФАКУЛЬТЕТ ПРАВНИЧИХ НАУК**

Кафедра загально-теоретичного правознавства

МАГІСТЕРСЬКА РОБОТА

**на тему: *Використання штучного інтелекту в судочинстві та
правозастосовній діяльності: правові ризики та переваги***

Виконав:

Студент 2 року навчання

магістерської програми,

спеціальність “Право”

Батхін Олександр Юрійович

oleksandr.batkhin@ukma.edu.ua

Керівник магістерської роботи:

Богатчук Дар’я Петрівна, старший

викладач, к.ю.н.

Київ 2026

Декларація академічної доброчесності

Я, Батхін Олександр Юрійович, студент 2 року навчання магістерської програми за спеціальністю «Право» факультету правничих наук НаУКМА підтверджую наступне:

- написана мною магістерська робота на тему “Використання штучного інтелекту в судочинстві та правозастосовній діяльності: правові ризики та переваги” відповідає вимогам академічної доброчесності та не містить порушень, передбачених п. 3.1. Положення про академічну доброчесність здобувачів освіти у НаУКМА, зі змістом якого я ознайомлений;
- надана мною для перевірки електронна версія роботи є ідентичною її друкованій версії.

23.04.2026

Батхін О. Ю.

ЗМІСТ

ВСТУП.....	5
РОЗДІЛ 1	8
1.1. Поняття, сутність та класифікація систем штучного інтелекту в контексті правничої діяльності	8
1.2. Основні напрями та форми використання ІІІ в судочинстві та в іншій правозастосовній діяльності	17
1.3. Світові тенденції розвитку LegalTech та роль ІІІ в трансформації сучасної юриспруденції.....	23
РОЗДІЛ 2	31
2.1. Міжнародні стандарти та етичні принципи регулювання ІІІ: досвід ООН, ОЕСР та Ради Європи, тощо	31
2.2. Правове регулювання ІІІ в Європейському Союзі: аналіз EU AI Act та вплив сучасного законодавства ЄС на глобальні правові процеси.....	38
2.3. Сучасний стан та перспективи правового регулювання ІІІ в Україні в контексті європейської інтеграції.....	45
РОЗДІЛ 3	55
3.1. Основні правові ризики застосування ІІІ в правозастосовній діяльності.....	55
3.2. Аналіз причин та наслідків актуальних випадків неправомірного застосування систем ІІІ.....	62
3.3. Встановлення успішних практик і переваг використання ІІІ в правозастосовній діяльності та розробка ефективних запобіжників і механізмів контролю за діяльністю постачальників та користувачів систем ІІІ	70
ВИСНОВКИ.....	78
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	84

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

- **ВНЗ** - вищий навчальний заклад
- **ДСА** - Державна судова адміністрація України
- **ЕКПЛ** - Європейська конвенція з прав людини (також відома як Конвенція про захист прав людини і основоположних свобод)
- **ЄС** - Європейський Союз
- **ЄСІКС** - Єдина судова інформаційно-комунікаційна система
- **ЗУ** - Закон України
- **КМУ** - Кабінет Міністрів України
- **Мінцифри** - Міністерство цифрової трансформації України
- **НААУ** - Національна асоціація адвокатів України
- **ООН** - Організація Об'єднаних Націй
- **ОЕСР** - Організація економічного співробітництва та розвитку
- **РСУ** - Рада суддів України
- **США** - Сполучені Штати Америки
- **ШІ** - штучний інтелект
- **ЮНЕСКО** - Організація Об'єднаних Націй з питань освіти, науки і культури
- **ADR** - Alternative Dispute Resolution (альтернативне вирішення спорів)
- **AI** (Artificial Intelligence) - штучний інтелект (ШІ)
- **AI Act (EU AI Act)** - Регламент Європейського Парламенту і Ради про штучний інтелект
- **AIMS** - Artificial Intelligence Management System (система управління штучним інтелектом)
- **CEPEJ** - European Commission for the Efficiency of Justice (Європейська комісія з питань ефективності правосуддя)
- **COMPAS** - Correctional Offender Management Profiling for Alternative Sanctions (алгоритм оцінки ризиків рецидиву)
- **GDPR** - General Data Protection Regulation (Загальний регламент про захист даних ЄС)
- **GPAI** - Global Partnership on Artificial Intelligence (Глобальне партнерство зі

штучного інтелекту)

- **IBA** - International Bar Association (Міжнародна асоціація юристів)
- **IEC** - International Electrotechnical Commission (Міжнародна електротехнічна комісія)
- **ISO** - International Organization for Standardization (Міжнародна організація зі стандартизації)
- **IT** - Information Technology (інформаційні технології)
- **LegalTech** - юридичні технології (Legal Technology)
- **LLM** - Large Language Model (велика мовна модель)
- **NLP** - Natural Language Processing (обробка природної мови)
- **ODR** - Online Dispute Resolution (онлайн вирішення спорів)
- **SVM** - Support Vector Machines (метод опорних векторів)

ВСТУП

Актуальність теми дослідження. Актуальність дослідження правових ризиків та переваг використання штучного інтелекту (ШІ) в судочинстві та правозастосовній діяльності зумовлена масштабною цифровою трансформацією правової сфери та появою сфери LegalTech. Штучний інтелект еволюціонував зі статусу експериментальних розробок у стратегічний чинник, що докорінно змінює архітектуру надання юридичних послуг та здійснення правосуддя. Впровадження інтелектуальних систем обіцяє радикальне прискорення розгляду справ та уніфікацію правових позицій, проте водночас створює безпрецедентні виклики для фундаментальних прав людини, принципу прозорості та етичних засад юридичної професії.

Особливої гостроти це питання набуває в контексті ухвалення Регламенту ЄС про штучний інтелект (EU AI Act), який запроваджує жорстке імперативне регулювання та ризико-орієнтований підхід [27, ст. 1]. Для України, як кандидата на вступ до ЄС, критично важливою є гармонізація національного законодавства з європейськими стандартами для побудови безпечної екосистеми ШІ, здатної захистити людську гідність у відносинах з автономними системами [2, с. 5]. Неминучість інтеграції ШІ вимагає від правничої спільноти не просто автоматизації процесів, а створення надійних правових запобіжників проти «алгоритмічної упередженості» та дегуманізації правосуддя.

Об'єктом дослідження є штучний інтелект як комплексний алгоритмічний інструмент в системі суспільних відносин у сфері судочинства та правозастосування.

Предметом дослідження є правове регулювання, форми використання, а також правові ризики та переваги імплементації систем штучного інтелекту в судову та іншу правозастосовну діяльність.

Мета і завдання дослідження. Метою магістерської роботи є комплексний аналіз теоретико-правових засад, міжнародних стандартів та практичних аспектів використання штучного інтелекту в правовій сфері для розробки стратегічних напрямів удосконалення механізмів контролю та безпечної інтеграції цих технологій в правову систему України.

Для досягнення поставленої мети визначено наступні завдання:

1. З'ясувати поняття, сутність та класифікацію систем ШІ в контексті правничої діяльності.
2. Визначити основні напрями та форми використання ШІ в судочинстві та правозастосуванні.
3. Проаналізувати світові тенденції розвитку LegalTech та роль ШІ в трансформації юриспруденції.
4. Дослідити міжнародні стандарти та етичні принципи регулювання ШІ (ООН, ОЕСР, Рада Європи).
5. Здійснити аналіз Регламенту ЄС про штучний інтелект (EU AI Act) та його впливу на глобальні процеси.
6. Оцінити стан та перспективи формування нормативно-правового регулювання ШІ в Україні.
7. Ідентифікувати основні правові ризики застосування ШІ в правозастосовній діяльності.
8. Проаналізувати причини та наслідки актуальних випадків неправомірного застосування систем ШІ.
9. Встановити успішні практики та розробити ефективні запобіжники і механізми контролю за діяльністю постачальників та користувачів ШІ.

Ступінь наукової розробки. Теоретичну базу дослідження становлять праці вітчизняних та зарубіжних науковців. Правова сутність ШІ та концепція «електронної особи» розглядаються крізь призму робіт О. І. Харитоновой. Економічне підґрунтя LegalTech та теорія «Великого розриву» базуються на

дослідженнях професора Р. Пірса. Питання етики та ризиків у кримінальному судочинстві (система COMPAS) та цивілізаційні виклики ШІ досліджуються з урахуванням застережень Стівена Гокінга та доповідей спеціалізованих міжнародних інституцій.

Методи дослідження. У роботі застосовано комплекс загальнонаукових та спеціальних правових методів:

- Системний метод: використаний для аналізу регулювання ШІ як цілісної ієрархічної системи на глобальному, регіональному та національному рівнях.
- Порівняльно-правовий метод: застосований для зіставлення американської ринкової, сінгапурської державно-центрованої та британської («регуляторна пісочниця») моделей інтеграції ШІ.
- Формально-логічний метод (індукція та дедукція): використаний для виведення загальних правових ризиків на основі аналізу конкретних судових прецедентів.
- Герменевтичний метод: застосований для тлумачення положень EU AI Act, Етичної хартії CEREJ та положень Білої книги з регулювання ШІ в Україні.
- Метод правового моделювання: використаний для розробки пропозицій щодо створення Державного реєстру сертифікованих юридичних ШІ-систем та впровадження стандарту «human-in-the-loop» в українське процесуальне законодавство.

РОЗДІЛ 1.

ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ТА ТЕХНОЛОГІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРАВНИЧІЙ ДІЯЛЬНОСТІ

1.1. Поняття, сутність та класифікація систем штучного інтелекту в контексті правничої діяльності

За словами Стівена Гокінга, успіх у створенні штучного інтелекту стане найбільшою подією в історії людства, але він також може стати останньою, якщо людство не навчиться уникати його ризиків [50, с. 12]. Штучний інтелект безумовно стає всеосяжним явищем, що пронизує всі сфери життя, в тому числі юриспруденцію. Ця робота присвячена комплексному дослідженню фундаментального руху в правовій діяльності, а саме інтеграції систем штучного інтелекту в архітектуру правозастосування. Дослідження спрямоване на те, щоб крізь призму міжнародних стандартів, новітнього законодавства ЄС, напрацювань Української правничої спільноти та загальних етичних правил розкрити дуалістичну природу ШІ: як потужного інструменту підвищення ефективності правосуддя та, водночас, як джерела нових викликів для прав людини, принципу прозорості та етичних засад юридичної професії.

Перший розділ цієї роботи присвячено комплексному дослідженню теоретичного фундаменту та технологічного базису, на якому ґрунтується сучасне впровадження ШІ в правову систему. Такий початок аналізу зумовлений тим, що без чіткого розуміння онтології ШІ та його технічних можливостей неможливо побудувати адекватну модель правового регулювання та оцінити ризики, що виникають у процесі судочинства. В рамках розділу здійснене визначення понятійного апарату та виявлення ключових векторів трансформації юриспруденції під впливом LegalTech інновацій.

Для досягнення поставленої мети дослідження розділ структуровано за принципом «від загального до конкретного». У підрозділі 1.1 ми зосередимо увагу на формуванні понятійного базису, проаналізуємо сутність ШІ через призму

міжнародних стандартів та запропонуємо класифікацію систем за рівнем їхньої автономності та ризиковості. Це дозволить чітко ідентифікувати об'єкт дослідження та відмежувати інтелектуальні системи від традиційних інструментів автоматизації.

Далі, у підрозділі 1.2, на розгляд береться прикладний аспект: ми проаналізуємо конкретні форми та напрями використання ШІ безпосередньо в судовій та правозастосовній діяльності від предикативної аналітики до автоматизованого управління справами. Завершальним етапом першого розділу стане підрозділ 1.3, у якому здійснено огляд світових тенденцій розвитку LegalTech. Цей підхід дозволяє розглянути роль ШІ не просто як технічного засобу, а як одного з ключових чинників системної трансформації сучасної юриспруденції. Такий послідовний аналіз забезпечує цілісне розуміння того, як технологічні параметри ШІ диктують необхідність оновлення правових доктрин.

Штучний інтелект у правовій сфері не є статичним інструментом; його імплементація - це комплексний та системний процес, який охоплює не лише зміну змісту інтелектуальної діяльності юриста, а й трансформацію структури правової діяльності. Сутнісні зміни проявляються в тому, що рутинні процеси, такі як огляд безлічі судових рішень або порівняльний аналіз законодавства, схильні бути автоматизованими, і натомість зростає попит на високоінтелектуальну творчу працю юриста щодо інтерпретації висновків ШІ. Така трансформація призводить до того, що класична модель «стандартної» юридичної діяльності поступається місцем більш гнучким формам роботи, де алгоритми стають повноцінними учасниками інформаційної взаємодії. У цьому ключі цифровізація призвела не просто до зміни форми правової роботи, а до докорінної зміни її змісту. Саме у дискурсі цифровізації та прогресу, як неминучих постійних явищ системного впливу на правову сферу, ШІ виступає черговим рушієм, об'єктом та учасником цих процесів і подекуди займає в них ключову роль [51, с. 45].

Визначення поняття «штучний інтелект» у правничому дискурсі вимагає відходу від суто технічних описів у бік правової сутності явища. Системи ШІ слід розглядати як машинні системи, які працюють з різним рівнем автономності, можуть демонструвати адаптивність після розгортання та, для явних або неявних цілей,

робити висновки - зокрема, прогнози, рекомендації або прийняття рішень на основі вхідних даних (ШІ АКТ) [27, ст. 3]. Ключовою ознакою, що відрізняє ШІ від звичайного програмного забезпечення, є автономність, тобто здатність системи самостійно виводити результати без жорсткого керування кожним кроком з боку програміста або користувача. Як зазначає М. Гільдебрандт, саме ця автономність створює підґрунтя для виникнення нових «цифрових прав та обов'язків», таких як право особи знати, що рішення щодо неї було прийнято або підготовлено алгоритмом [51, с. 45].

Варто наголосити, що феномен ШІ в праві вже призвів до формування специфічних концепцій, як-от праця К. Юнг - «алгоритмічне управління» юридичними процесами [82, с. 510]. Це явище характеризується тим, що межі між безпосереднім людським рішенням та машинною рекомендацією починають стиратися. За таких умов виникає ризик випадків, в яких юрист або суддя, покладаючись на авторитет і швидкість системи ШІ, фактично втрачає власну професійну автономію. Відтак, правове розуміння ШІ має базуватися на принципі пріоритету людини в управлінні, і це гарантує що будь-яке автоматизоване рішення, яке має значущі правові наслідки, повинно підлягати перегляду та фінальному затвердженню людиною.

Сутність ШІ в контексті судочинства також тісно пов'язана із проблемою деперсоналізації правової діяльності. Якщо рішення готується алгоритмом на основі статистичних закономірностей, наявних у базах даних системи, виникає загроза втрати індивідуального підходу до кожної справи, що є серцем правосуддя. У таких обставинах людина може почати сприйматись системою не як суб'єкт права, а як сукупність цифрових значень у відповідному полі програмного забезпечення. Це зумовлює необхідність доповнення класичних принципів рівності та змагальності вимогою алгоритмічної прозорості - обов'язком розкривати покроковий аналітичний процес, за результатами якого ШІ прийшов до певного висновку [25, с. 112].

Також, розглядаючи теоретичні засади застосування ШІ, слід звернути увагу на розмиття традиційних суб'єктів у цифровому правовому середовищі. Поява «цифрових агентів» та платформ, що організовують правову роботу, створює

ситуацію, де ідентифікувати реального відповідального за помилку стає вкрай складно. Таким чином, діджиталізація та в тому числі масове застосування ШІ трансформують не лише технічний складник юриспруденції, але і її саму природу, вимагаючи створення регуляторних механізмів та принципів, які б не тільки врегулювали сферу, але й забезпечили фундаментальні гарантії прав особи у цифрову епоху [25, с. 94].

Продовжуючи аналіз сутнісних характеристик штучного інтелекту, необхідно перейти до його більш розгорнутої класифікації, оскільки саме розрізнення технологій за рівнем їхнього впливу на правопорядок дозволяє побудувати адекватну модель юридичної відповідальності. У науковій літературі та міжнародних документах виокремлюють декілька фундаментальних підходів до класифікації ШІ, кожен з яких має особливе значення для судочинства. Першим і найбільш поширеним критерієм є поділ за ступенем автономності та алгоритмічної складності, що дозволяє розрізняти системи, які лише автоматизують процеси, від тих, що здатні до самостійної генерації правових висновків [30, с. 18; 20, с. 52].

Зокрема, за рівнем функціональних спроможностей системи ШІ класифікують на «слабкий» (Narrow AI) та «сильний» (General AI) штучний інтелект [30, с. 18]. Слабкий ШІ, який є домінуючим у сучасній LegalTech індустрії, спроектований для вирішення вузькоспеціалізованих завдань, як-от класифікація позовних заяв, автоматичне виявлення суперечливих умов у договорах або прогнозування ймовірного результату апеляційної скарги. Натомість концепція «сильного» ШІ передбачає створення системи, здатної до усвідомлення контексту та прийняття рішень у будь-якій сфері на рівні людського розуму, що наразі залишається предметом теоретичних дискусій та етичних застережень у межах рекомендаціях міжнародних експертів [75, с. 142]. Важливим в даному питанні є те, що наразі тільки слабкий ШІ зустрічається в повсякденних випадках використання цих технологій юристами, і розуміння цього факту дозволяє краще розрізняти, з якими перевагами та ризиками слід працювати спеціалістам в рамках імплементації ШІ.

Окрім функціональної та ризик-орієнтованої класифікації, для повного розуміння природи ШІ у праві критичне значення має аналіз типів архітектур, на яких

базуються ці системи. Зокрема, у сучасних LegalTech рішеннях широко застосовуються нейронні мережі, що здатні імітувати когнітивні функції мозку для обробки природної мови (NLP) у текстах судових рішень [29, с. 115; 69, с. 2]. Для задач класифікації та юридичного прогнозування використовуються такі алгоритми, як Random Forest (ансамблі «випадкових дерев»), що забезпечують високу точність при аналізі великих масивів структурованих даних, а також метод опорних векторів (SVM), який є ефективним інструментом для розпізнавання патернів та автоматичного категоризування правових документів [57, с. 912]. Розуміння цих архітектурних відмінностей є важливим для правника, враховуючи різний рівень «пояснюваності» (explainability) різних систем та можливість верифікації логіки, за якою ІІІ дійшов певного висновку.

Особливе значення для правничої діяльності має класифікація, запропонована в межах ризико-орієнтованого підходу Європейського Союзу, де системи ІІІ поділяються за рівнем загрози фундаментальним правам людини. Відповідно до цієї логіки, виділяють системи з «неприйнятним ризиком», використання яких у судочинстві прямо забороняється, оскільки вони можуть призвести до маніпулювання поведінкою учасників процесу або соціального скорингу та закономірно несправедливих результатів судочинства [27, ст. 5]. Системи «високого ризику», до яких зазвичай відносять інструменти для оцінки доказів або прогнозування порушень, підлягають суворому нагляду, обов'язковій сертифікації та аудиту алгоритмічної прозорості [27, ст. 6].

Водночас, європейський законодавець виокремлює системи з «обмеженим ризиком», до яких висуваються специфічні вимоги щодо прозорості: користувачі мають бути поінформовані про те, що вони взаємодіють із ІІІ (наприклад, юридичні чат-боти), аби забезпечити можливість прийняття ними усвідомлених рішень [27, ст. 52]. Більшість систем ІІІ, що використовуються в адміністративній роботі правників, підпадають під категорію з «мінімальним» або «незначним ризиком», що включає такі інструменти як спам-фільтри або інтелектуальні системи форматування документів; використання таких технологій дозволяється без спеціальних

нормативних обмежень, оскільки вони не становлять загрози безпеці чи правам громадян [27, ст. 69].

Окреме регуляторне значення мають моделі ШІ загального призначення (General-purpose AI models), зокрема потужні генеративні системи, які можуть бути інтегровані в різні сфери правничої діяльності. Для таких моделей встановлюються обов'язки щодо розкриття технічної документації, дотримання авторського права при навчанні та надання детальних звітів про архітектуру моделі, що є критично важливим для забезпечення системної безпеки цифрового простору ЄС [27, ст. 53].

Важливо також розглянути класифікацію за сферами застосування у правозастосовній діяльності, де виділяють три основні групи систем:

1. Системи підтримки прийняття рішень (Decision Support Systems), що допомагають юристу у структуруванні матеріалів справи;
2. Системи автоматизації рутинних завдань (Administrative AI), які оптимізують документообіг; та
3. Системи передбачуваного правосуддя (Predictive Justice Systems), що аналізують минулі рішення для моделювання майбутніх результатів [57, с. 925].

Кожна з цих груп має різний ступінь впливу на принципи незалежності, прозорості та справедливості у суддівстві та іншій правовій діяльності, але по суті всі ці системи ШІ можуть так чи інакше призводити до змін у оцінці ситуацій, прийнятті рішень або помилок у обробці даних, що може мати негативні наслідки для судового процесу [18, розд. 1].

Окремим критерієм класифікації є взаємодія системи з користувачем, де виділяють системи "human-in-the-loop" (людина в циклі), "human-on-the-loop" (людина над циклом) та "human-out-of-the-loop" (людина поза циклом). У правовому контексті допустимими вважаються лише перші два типи, оскільки вони гарантують, що остаточне правове рішення приймається людиною, яка несе за нього юридичну відповідальність. Відсутність людини в процесі прийняття юридично значущого рішення (human-out-of-the-loop) на сьогодні вважається порушенням стандартів справедливого суду та етичних норм, закладених у документах ОЕСР [64, с. 8].

На завершення огляду класифікації слід зазначити, що швидкість технологічного розвитку вимагає від законодавця гнучкого підходу, де правові дефініції не повинні бути прив'язані до конкретних мов програмування чи апаратних рішень. Замість цього класифікація має базуватися на функціональному впливі технології на суспільні відносини, що дозволить забезпечити тривалу актуальність нормативних актів у динамічному цифровому середовищі. Таким чином, розуміння різноманітності систем ШІ є необхідною передумовою для формування ефективних механізмів контролю, про які йтиметься у наступних розділах роботи [25, с. 50].

Послідовним продовженням дослідження правової сутності штучного інтелекту є аналіз його правового статусу, що в сучасній цивілістичній доктрині становить предмет гострих дискусій. Питання про те, чи є ШІ лише об'єктом права, чи він може набувати певних ознак суб'єктності, має як теоретичне, так і прикладне значення для судочинства. Розширення сфери застосування ШІ в правозастосовній діяльності неминуче веде до розмивання класичних уявлень про учасників правовідносин [22, с. 38]. Якщо алгоритм здатний автономно генерувати юридично значущі рішення, неминуче виникає потреба у визначенні відповідальності за наслідки таких рішень, що корелює з концепцією «електронної особи» (e-person), яка активно обговорюється експертами, зокрема експертами у Європейському Парламенті [43, с. 14].

У контексті правничої діяльності сутність ШІ розкривається через його здатність виступати в ролі цифрового посередника. У такому форматі система не володіє повною правосуб'єктністю, проте наділяється певним набором прав та обов'язків у межах конкретного процесу, наприклад, обов'язком дотримання конфіденційності даних або забезпеченням недискримінаційного підходу. Такий підхід дозволяє уникнути юридичного вакууму, коли шкода, заподіяна алгоритмом, не може бути персоніфікована через складність ланцюга постачання (розробник - власник - користувач). Відтак, сутність ШІ в праві слід трактувати як квазісуб'єкту, де система діє від імені та в інтересах людини, але за власною внутрішньою логікою обробки даних [25, с. 40].

Додаткову увагу в межах класифікації та визначення правового статусу ШІ слід приділити генеративному штучному інтелекту (Generative AI), який став справжнім викликом для сучасної юриспруденції у 2023-2024 роках [26, с. 112]. На відміну від класичних дискримінаційних проблем моделей ШІ, що лише класифікують дані, генеративні системи, зокрема великі мовні моделі (Large Language Models) здатні створювати нові тексти юридичного характеру - позови, висновки, проекти законів. Це зумовлює виокремлення такого критерію класифікації, як рівень унікальності вихідних даних, адже це має прямий вплив на питання авторського права та достовірності доказів у суді. Використання генеративного ШІ без належного людського контролю створює ризик появи галюцинацій у вигляді вигаданих фактів або неіснуючих прецедентів, що вже призводило до дисциплінарних стягнень адвокатів у світовій практиці [60, с. 3].

Підсумовуючи аналіз поняття та сутності ШІ, варто зазначити, що в контексті трансформації сучасної юриспруденції ШІ виступає не просто як технологічний додаток, а як каталізатор переходу до нової реальності правничої діяльності, так званого «Права 4.0» [38, с. 24]. Це стан правової системи, де алгоритмічна логіка інтегрується в саму структуру нормотворення та правозастосування. Таким чином, класифікація систем ШІ за рівнем ризику, автономності та функціонального призначення дозволяє законодавцю розрізняти та адаптувати підходи до їхнього регулювання: від стимулювання інновацій у сфері адміністративної підтримки до жорстких обмежень у сфері прийняття судових рішень.

У висновку, аналіз даних, наведених в рамках першого підрозділу роботи, наводять на думку, що штучний інтелект у правничій діяльності - це складна машинна система, що здатна до різного рівня автономності в рамках генерації юридично значущих результатів (висновків, рішень) на основі вхідних даних [27, с. 3]. Її сутність полягає у переході від автоматизації до інтелектуалізації права, де ключовим викликом залишається збереження контролю з боку людини та усунення всіх можливих ризиків від неминучого масового використання цих та дотичних технологій. Класифікація цих систем є динамічним процесом, що має базуватися на

принципах прозорості, безпеки та поваги до фундаментальних прав людини, закріплених у міжнародних стандартах.

Сформований у цьому підрозділі теоретичний базис та понятійний апарат стають основою для подальшого аналізу практичних аспектів цього питання. У наступному підрозділі ми детально розглянемо, як саме ці класифіковані системи впроваджуються безпосередньо в судочинство та які конкретні форми вони приймають у роботі сучасного правника. Здійснений аналіз поняття, сутності та класифікації систем штучного інтелекту в контексті правничої діяльності дозволяє сформулювати низку проміжних висновків.

По-перше, штучний інтелект у юриспруденції слід розглядати як комплексну автономну систему, що виходить за межі звичайної автоматизації, оскільки вона здатна до адаптивного навчання та генерації нових юридично значущих даних на основі аналізу великих масивів інформації. Така природа ШІ вимагає впровадження принципу «алгоритмічної прозорості» як обов'язкової умови його легітимного використання у правовому полі.

По-друге, запропонована класифікація систем ШІ за рівнем ризику та ступенем автономності підтверджує, що найбільший потенціал для правозастосування мають системи підтримки прийняття рішень («human-in-the-loop»), які зберігають за людиною-правником функцію фінальної верифікації та правової оцінки [64, с. 8].

По-третє, теоретичне обґрунтування сутності ШІ як «цифрового асистента» з елементами квазісуб'єктності створює підґрунтя для подальшого вивчення форм його практичної імплементації. Отримані результати підтверджують, що здійснене в даному підрозділі виокремлення понятійного апарату є фундаментом для переходу до аналізу конкретних напрямів використання ШІ в судочинстві, що і стане предметом розгляду у наступному підрозділі.

1.2. Основні напрями та форми використання ШІ в судочинстві та в іншій правозастосовній діяльності

Переходячи від загальнотеоретичних визначень до аналізу більш прикладних аспектів, слід визнати, що інтеграція штучного інтелекту в правозастосовну практику вже не є футуристичним прогнозом, а натомість сталою реальністю функціонування сучасних правових систем. Основним вектором цього процесу інтеграції є цифрова трансформація судочинства, де ШІ виступає як інструмент оптимізації процесуальних дій та підвищення ефективності управління судовими процесами. У цьому контексті різні форми застосування ШІ юристами можна розрізнити за рівнем їхнього впливу на процес прийняття юридичного рішення: від автоматизації технічного документообігу до складних систем аналітичної підтримки.

Першим і найбільш розповсюдженим напрямом є автоматизована обробка правової інформації (Automated Processing of Legal Information), що включає в себе аналіз позовних заяв та інших процесуальних документів або актуального законодавства. Сучасні алгоритми природної мови (NLP) дозволяють системі не просто «читати» текст, а й виокремлювати ключові юридичні факти, класифікувати позовні вимоги та автоматично перевіряти дотримання формальних вимог процесуального законодавства щодо форми та змісту звернень до суду [29, с. 201; 1, с. 8]. Таке застосування систем ШІ значно скорочує навантаження на апарат суду на етапі реєстрації справ, мінімізуючи вплив людського фактору та ймовірність технічних помилок.

Іншою важливою формою є інтелектуальний автоматизований розподіл справ та управління судовим календарем. Якщо традиційні системи розподілу базуються на випадковому виборі, то вдосконалені ШІ-моделі здатні враховувати складність справи, спеціалізацію судді, його поточне навантаження та навіть прогнозований час розгляду подібних кейсів у минулому. Така форма використання ШІ сприяє забезпеченню права на розгляд справи впродовж розумного строку, оскільки дозволяє більш раціонально розподіляти обмежені часові ресурси судової системи.

Іншим важливим напрямом є впровадження систем «розумного пошуку» та аналізу судової практики. На відміну від класичних пошукових систем, що працюють за ключовими словами, ШІ-інструменти (наприклад, системи типу ROSS Intelligence або українські аналоги в межах LegalTech) використовують семантичний аналіз для пошуку не просто схожих слів, а ідентичних правових ситуацій та ліній аргументації [6, с. 1; 57, с. 920]. Це дозволяє правникам майже миттєво знаходити релевантні випадки та правові позиції суду, що покращує навігацію судовою практикою. Така форма підтримки є критично важливою в умовах постійного зростання масиву нормативно-правових актів та судових рішень та є одним з прикладів зростаючого тренду на збільшення зручності пошуку релевантних даних в юридичному бізнесі та LegalTech.

Окремо слід виділити використання ШІ у сфері спрощених проваджень та малозначних справ. У деяких юрисдикціях (наприклад, досвід Естонії з спробами розробки «суддей-роботів» для дрібних позовів) ШІ залучається для підготовки проектів рішень у справах, де фактичні обставини є вкрай прямолінійними, а правова кваліфікація не викликає сумнівів [76, с. 145]. У таких випадках алгоритм аналізує надані цифрові докази та формує проект судового наказу, який згодом верифікується людиною-суддею. Це демонструє перехід від ШІ як пошукового інструменту до ШІ як асистента, що бере безпосередню участь у підготовці актів правозастосування.

Також, в рамках аналізу цього питання слід зазначити, що цифровізація через ШІ в судочинстві створює передумови для формування «цифрового правосуддя», де доступ до суду забезпечується через інтелектуальні інтерфейси. Однак, впровадження таких форм вимагає чіткого дотримання балансу між технологічною ефективністю та збереженням процесуальних гарантій учасників справи. Особливо актуальним це питання є в контексті глобального тренду цифровізації та необхідності покращення рівня цифрової грамотності в країні та в світі. Саме детальний розгляд складніших форм, таких як предиктивне правосуддя та оцінка ризиків, стане наступним кроком у предметному аналізі в рамках цього підрозділу.

Одним із найбільш технологічно складних та водночас етично чутливих напрямів є впровадження систем предиктивного правосуддя (Predictive Justice). Ця

форма використання цифрових технологій полягає у застосуванні алгоритмів машинного навчання для прогнозування ймовірних результатів судового розгляду на основі аналізу великих масивів ретроспективних даних [57, с. 925; 12, с. 115]. На відміну від простого пошуку прецедентів, предиктивні моделі здатні виявляти приховані закономірності у поведінці конкретних суддів, оцінювати шанси на задоволення позову в певній юрисдикції та навіть вибудовувати оптимальну стратегію захисту для кожного окремого набору обставин. Для адвокатури такі інструменти стають привабливими при оцінці ризиків та доцільності ініціювання судового спору, що сприяє розвантаженню системи через стимулювання досудового врегулювання конфліктів.

Особливе місце у правозастосовній діяльності посідають системи оцінки ризиків (Risk Assessment Tools), які найактивніше застосовуються у кримінальному судочинстві США та деяких країн ЄС. Найвідомішим прикладом є система COMPAS, яка аналізує дані про особу обвинуваченого для визначення ймовірності вчинення ним повторного злочину [59, с. 5; 68, с. 2]. У цій формі ІІІ виступає як допоміжний інструмент для судді при вирішенні питань про обрання запобіжного заходу або визначення міри покарання. Проте саме тут виникає гостра правова дискусія: наскільки етично покладати долю людини на математичну модель, яка може містити «вбудовані» соціальні упередження, та як забезпечити право особи на оспорування логіки алгоритму, що є закритим корпоративною або судовою таємницею.

Ще одним перспективним напрямком є використання ІІІ в альтернативних способах вирішення спорів (ADR), зокрема в онлайн-медіації (ODR) [56, с. 88]. Цифрові платформи здатні виконувати роль медіатора-асистента, який аналізує позиції сторін, виявляє точки дотику та пропонує варіанти компромісу, що базуються на об'єктивних даних та аналогічних успішних кейсах. Така форма правозастосування в теорії дозволяє значно знизити рівень конфліктності та забезпечити дещо більш швидкий доступ до справедливості у цивільних та господарських спорах, де емоційна складова є мінімальною.

У сфері публічного управління та правозастосовної діяльності контролюючих органів використання ІІІ може бути втілено через системи «розумного нагляду»

(Smart Oversight). Податкові та митні органи використовують такі алгоритми для виявлення аномалій у звітності, що можуть свідчити про порушення у, наприклад, поданні даних податкових та митних декларацій [27, ст. 13; 47, с. 52]. У цьому випадку ШІ може як частково автоматизувати перевірку даних податківців, а й здійснювати дещо превентивну функцію, виокремлюючи об'єкти високого ризику для подальшої перевірки людиною-інспектором, що робить державний контроль більш точковим та ефективним.

Крім того, варто виділити напрям використання ШІ для забезпечення лінгвістичної доступності правосуддя. У багатомовних юрисдикціях або у справах за участю іноземців системи синхронного ШІ-перекладу забезпечують миттєву трансформацію усного та письмового мовлення, гарантуючи право особи на розуміння суті обвинувачення та перебігу процесу. Це також є незамінною складовою ведення юридичного бізнесу, що вимагає консультацій з іноземними клієнтами. Це форма використання ШІ, яка прямо спрямована на зменшення бар'єрів між різними учасниками судового процесу та юридичного бізнесу.

Завершуючи огляд основних форм використання ШІ, слід підкреслити, що їхня класифікація та інтенсивність використання безпосередньо залежать від ступеня цифровізації конкретної правової системи. Попри значні переваги у швидкості та об'єктивності обробки даних, кожна з наведених форм містить у собі потенційні загрози для класичних правових процедур. Детальний аналіз цих загроз через призму трансформації юридичної професії та глобальних LegalTech трендів буде здійснено у заключному розділі цієї роботи.

Важливим та водночас дискусійним напрямом застосування інтелектуальних систем є сфера правоохоронної діяльності, де ШІ набуває форми предиктивної поліцейської діяльності (Predictive Policing) [67, с. 45; 32, с. 20]. Ця технологія базується на алгоритмічному аналізі історичних даних про злочинність, географічних параметрів та соціально-демографічних показників для прогнозування ймовірних місць вчинення правопорушень («hot spots») або ідентифікації осіб, які з високою вірогідністю можуть бути залучені до кримінальної активності. Використання таких систем, як PredPol або HunchLab, дозволяє правоохоронним органам раціонально

розподіляти патрульні ресурси, проте в контексті правозастосування це створює ризик «презумпції винуватості» щодо окремих районів чи соціальних груп, що вимагає суворого судового контролю за законністю підстав для превентивних заходів [67, с. 48].

У діяльності органів прокуратури та слідства ІІІ інструменти можуть застосовуватись для криміналістики та цифрового аналізу доказів. Сучасні системи здатні здійснювати автоматичне розпізнавання облич, аналізувати метадані мільйонів транзакцій для виявлення схем відмивання коштів та проводити семантичний аудит зашифрованих комунікацій. Така форма застосування ІІІ дозволяє виявляти складні корупційні та економічні злочини, які неможливо ідентифікувати традиційними методами. Однак, використання результатів роботи ІІІ як доказів у суді ставить питання про процесуальну чистоту алгоритму та можливість сторони захисту піддати експертизі алгоритм прийняття рішень, на основі якого було здійснено той чи інший висновок.

Окремим вектором розвитку є використання ІІІ для забезпечення прозорості та антикорупційного моніторингу в самій юридичній системі. Спеціальні модулі, інтегровані в державні реєстри, здатні у короткі часові проміжки відстежувати аномалії в реєстраційних діях, автоматично сигналізуючи про можливі зловживання. Це створює умови для формування цифрового моніторингу над діяльністю суб'єктів владних повноважень, де алгоритм виступає безстороннім аудитором відповідних реєстрів.

Підбиваючи підсумок аналізу основних напрямів використання ІІІ, слід констатувати, що ми спостерігаємо перехід від ери «права в книгах» до «права в коді». Впровадження інтелектуальних систем у судочинство та правозастосування забезпечує низку незаперечних переваг: радикальне прискорення розгляду справ, уніфікацію правових позицій та зручність багатьох бюрократичних або ресурсовитратних процесів. Разом з тим, кожна з розглянутих форм використання ІІІ від електронного суду до предиктивної аналітики несе в собі ризик дегуманізації права та загрозу порушення багатьох основоположних принципів правової системи.

Узагальнення результатів дослідження основних напрямів та практичних форм імплементації штучного інтелекту дозволяє стверджувати, що сучасна правозастосовна діяльність перебуває у стані системного цифрового зламу. Технологія ШІ еволюціонувала від пасивного інструментарію до активного учасника юридичного процесу, що зумовлює необхідність переосмислення класичних процесуальних інститутів. Систематизація існуючих практик свідчить про те, що впровадження ШІ відбувається за ієрархічним принципом: від горизонтальної автоматизації допоміжних функцій (інтелектуальний документообіг, реєстрація та автоматизований розподіл справ) до вертикальної інтелектуалізації складних правових операцій, таких як предиктивна аналітика, семантичний аудит доказів та алгоритмічна оцінка ризиків рецидивів.

Важливо зазначити, що перехід до предиктивних моделей у кримінальному судочинстві (зокрема систем на кшталт COMPAS) висвітлює фундаментальну проблему, а саме конфлікт між математичною ефективністю алгоритму та презумпцією невинуватості [83, с. 630]. Міжнародний досвід доводить, що закритість алгоритмічної логіки через проблему «чорної скриньки» (black box) створює загрозу системної дискримінації та порушення права на вмотивоване судове рішення, оскільки сторони позбавлені можливості змістовно оспорити шлях, яким ШІ прийшов до певного висновку [66, с. 55].

Обґрунтованим вбачається висновок, що найбільш життєздатною моделлю використання ШІ в судочинстві на сучасному етапі є концепція «доповненого інтелекту» (Augmented Intelligence) [77, с. 110]. Вона базується на розподілі функцій: алгоритм бере на себе обробку надвеликих масивів даних (Big Data) та виявлення прихованих закономірностей, тоді як остаточне правове рішення, що потребує морально-етичної оцінки, зважування цінностей та врахування унікальних обставин кожної справи, залишається виключною прерогативою людини. Така архітектура правозастосування дозволяє зберегти людиноцентричний характер правосуддя та запобігти його дегуманізації, одночасно використовуючи весь потенціал LegalTech інновацій для подолання криз перевантаженості судових систем.

Додатково слід зауважити, що інтенсивність впровадження розглянутих форм використання ШІ прямо корелює з рівнем технологічної зрілості національної правової системи та готовністю професійної спільноти до трансформації етичних стандартів діяльності. Вивчення цих практичних аспектів формує необхідний аналітичний базис для переходу до дослідження та впровадження глобальних LegalTech трендів. Це дозволить у подальшому аналізі цього питання концептуалізувати роль штучного інтелекту як не тільки сервісної технології, а й сталого асистента в екосистемі права, що дещо змінює саму форму юридичної діяльності.

1.3. Світові тенденції розвитку LegalTech та роль ШІ в трансформації сучасної юриспруденції

Аналіз сучасного стану глобальної правової системи дозволяє констатувати, що правова діяльність перебуває в епіцентрі безпрецедентної технологічної трансформації, яка отримала назву LegalTech. Це явище не обмежується лише впровадженням окремих програмних продуктів, а являє собою комплексну інституціоналізацію високих технологій, що докорінно змінюють архітектуру надання юридичних послуг та здійснення правосуддя. На сучасному етапі штучний інтелект еволюціонував із категорії експериментальних розробок у статус стратегічного чинника, що визначає конкурентоспроможність бізнесу та сучасність національних правоохоронних систем у світовому масштабі. Глобальні тренди свідчать, що ігнорування алгоритмічних інструментів стає неможливим для консервативної юридичної спільноти, оскільки швидкість та точність обробки правової інформації машинами вже перевищує людські можливості у специфічних нішах, а вплив тренду розділяє людство, в тому числі юристів, за рівнем використання цих технологій на сучасних та тих, що відстають від тренду.

Метою цього підрозділу є концептуалізація ролі ШІ не просто як сервісної технології, а і потужного драйвера цифрової трансформації сучасної юриспруденції. Для цього необхідно розглянути динаміку розвитку світового ринку LegalTech крізь

призму сучасних трендів, проаналізувати стратегічний досвід провідних держав, які вже інтегрували ІІІ у свої правові доктрини, та оцінити зміну самого профілю юридичної професії під впливом генеративних моделей. Такий підхід дозволить виявити закономірності, за якими цифрова економіка та технологічні тренди диктують нові правила функціонування правової сфери, де класичне розуміння юриспруденції поєднується з аналітичним підходом до управління даними.

Дослідження світових тенденцій розвитку юриспруденції неможливе без аналізу економічного підґрунтя, яке стимулює технологічне переозброєння галузі. У сучасній науковій думці утвердилося розуміння того, що правова сфера перестала бути ізольованим інститутом і перетворилася на динамічний ринок LegalTech послуг, де ключовим активом стають не лише знання відповідних даних, а й алгоритми їх обробки. Концептуальним ядром цієї трансформації стала теорія «Великого розриву» (The Great Disruption), висунута професорами Дж. МакГіннісом та Р. Пірсом, які обґрунтували, що штучний інтелект не просто оптимізує роботу правника, а таким чином знижує вартість юридичних транзакцій, руйнуючи традиційну монополію юридичних фірм на складну інтелектуальну працю [62, с. 3045; 77, с. 50]. Суть цього розриву полягає в тому, що інтелектуальні системи здатні виконувати завдання з аналізу документів та пошуку правових позицій у рази швидше за людину, що робить класичну модель оплати по годинам економічно не ефективною та не конкурентною [77, с. 115].

Економічна динаміка цього процесу підтверджується безпрецедентним припливом венчурного капіталу в сектор LegalTech. Згідно з аналітичними звітами, за останні роки обсяг світових інвестицій у юридичні стартапи на базі ІІІ демонструє стабільне зростання, досягаючи мільярдних показників, що свідчить про глобальну зміну довіри інвесторів від традиційного консалтингу до технологічних платформ [26, с. 180]. Це призводить до виникнення явища, охарактеризованого в роботах Р. Сасскінда, яке дослідники називають «демократизацією права», процесу, за якого високі технології роблять якісну юридичну допомогу доступною для суб'єктів, що раніше були відрізані від неї через високу вартість послуг топ-юристів [77, с. 120]. Таким чином, ІІІ може у майбутньому використовуватись не лише як технічний

засіб, а як інструмент для надання базової консультативної допомоги в окремих випадках (наприклад на спеціалізованих сайтах державних послуг). Водночас із цим, завжди важливо враховувати при таких випадках використання ШІ, що без належної актуалізації вхідних даних та прозорої роботи алгоритму, такі консультації можуть бути не такими ефективними, як консультація з живим спеціалістом, а подекуди навіть шкідливими у разі надання некоректних відповідей.

Важливо підкреслити, що «Великий розрив» торкається не лише технічних аспектів, а й фундаментальної архітектури юридичного бізнесу [62, с. 3052]. Спостерігається поступовий відхід від моделі «великої піраміди» юридичних фірм, де велика кількість молодших юристів виконує рутинну роботу під наглядом партнерів. Штучний інтелект фактично зрізає основу цієї піраміди, оскільки функції з проведення Legal Due Diligence, аналізу договірних ризиків та структурування стандартних угод тепер до певної міри делегуються алгоритмам. Це зумовлює виникнення нових форм професійної взаємодії, де, за концепцією Р. Сасскінда, юридичні послуги трансформуються у юридичні продукти (commoditization of law), які продаються за фіксованою ціною через цифрові інтерфейси [77, с. 125].

Трансформація ринку під впливом ШІ також веде до консолідації юридичних даних як стратегічного ресурсу. Глобальні тренди вказують на те, що найбільші гравці ринку від міжнародних юридичних компаній до державних судових систем починають розглядати масиви судових рішень та нормативних актів як «сировину» для навчання власних великих мовних моделей. У цьому контексті роль ШІ полягає у виявленні прихованих кореляцій між правовими нормами та фактичними наслідками їх застосування, що раніше було недоступне для людського аналізу [69, с. 16].

На завершення аналізу економічного виміру тенденцій, слід зазначити, що концепція "The Great Disruption" ставить під загрозу існування традиційних етичних кодексів професії, які базувалися на персоналізованому характері відносин «клієнт - юрист». Світовий ринок вимагає нових стандартів відповідальності за помилки алгоритмів ШІ, що стимулює розвиток страхування від кібер-ризиків у юридичній діяльності та розробку сертифікаційних вимог для правового програмного

забезпечення [62, с. 3052]. Отже, динаміка розвитку LegalTech підтверджує, що штучний інтелект став головним фактором перерозподілу впливу на глобальному юридичному ринку, вимагаючи від правників не лише знання права, а й глибокого розуміння економічних та технологічних процесів цифрової епохи.

Вивчення глобального ландшафту трансформації юриспруденції дозволяє виокремити декілька моделей державної політики щодо інтеграції ШІ. Перша модель, репрезентована Сполученими Штатами Америки, характеризується децентралізованим, ринковим підходом, де основний імпульс інноваціям дає приватний сектор (BigTech та потужні LegalTech корпорації), а судова система виступає реципієнтом готових рішень. У США ШІ-стратегії в правовій сфері зосереджені на предиктивній аналітиці та автоматизації процедур "e-discovery" (електронного розкриття доказів), що дозволяє сторонам процесу опрацьовувати терабайти даних у цивільних та корпоративних спорах [29, с. 250]. Проте саме американський досвід висвітлив критичну потребу в етичному регулюванні, оскільки використання алгоритмів для оцінки ризиків у кримінальних справах (наприклад, система COMPAS) викликало широку дискусію щодо алгоритмічної упередженості та порушення рівності [68, с. 4].

Принципово іншу, державну-орієнтовану модель, демонструє Сінгапур. У межах національної стратегії "Smart Nation" уряд Сінгапуру створив унікальну екосистему, де Академія права Сінгапуру (Singapore Academy of Law) виступає як центральний хаб для розробки та валідації юридичних технологій. Сінгапурський підхід базується на створенні довіри до ШІ через державну сертифікацію алгоритмів та активне впровадження генеративного ШІ для автоматизації підготовки судових документів. Звіт "Generative AI Report" Сінгапурської академії права наголошує на важливості "освіченого використання" технологій, де держава бере на себе роль медіатора між розробниками та юридичною спільнотою, забезпечуючи відповідність ШІ-інструментів стандартам професійної етики [74, с. 15].

Велика Британія пропонує третю модель, яку можна назвати «регуляторною пісочницею» (regulatory sandbox). Британська стратегія розвитку правових технологій фокусується на створенні гнучкого правового режиму, який дозволяє стартапам

тестувати ІІІ-рішення в контрольованому середовищі під наглядом Регулятора юридичних послуг (Legal Services Board) [78, с. 12]. Особлива увага тут приділяється концепції «Відкритого права» (Open Law), що передбачає відкриття державних реєстрів та масивів судових рішень для машинного аналізу, що стимулює розвиток систем предиктивного правосуддя та інтелектуальних систем медіації. Британський досвід доводить, що залучення ІІІ до вирішення малозначних спорів через онлайн-платформи (наприклад, Civil Money Claims) значно підвищує рівень задоволеності громадян роботою судової системи [76, с. 210].

Спільним для всіх провідних юрисдикцій є перехід до стратегічного планування, де ІІІ розглядається як засіб подолання кризи доступності правосуддя. У країнах ОЕСР спостерігається тенденція до створення спеціалізованих етичних комісій при верховних судах, які здійснюють аудит ІІІ-систем перед їх впровадженням у процесуальну діяльність [37, с. 5; 64, с. 10]. Це свідчить про те, що світова практика відходить від спонтанної цифровізації до усвідомленого керування ризиками, де кожна держава намагається знайти баланс між технологічним прогресом та збереженням фундаментальних правових гарантій. Світовий досвід також підкреслює, що успіх трансформації залежить не стільки від потужності аналітичних систем, скільки від здатності юридичної професії адаптувати свої стандарти до нових реалій, про що детальніше йтиметься у наступній частині.

Еволюція технологій штучного інтелекту зумовлює не просто зміну інструментарію, а фундаментальну реконцептуалізацію ролі правника в сучасній цифровій екосистемі. Традиційна модель юриста як «охоронця знань», чия цінність базувалася на унікальному доступі до складних текстів та їх інтерпретації, остаточно поступається місцем моделі «T-shaped lawyer» [77, с. 140]. Дана концепція передбачає, що сучасний фахівець повинен володіти не лише глибокою експертизою в галузі права (вертикальна лінія букви Т), а й широким спектром суміжних компетенцій від аналізу великих масивів даних та розуміння архітектури алгоритмів до навичок управління технологічними проектами (горизонтальна лінія). Світові тенденції чітко вказують на те, що професійна цінність зміщується з процесу механічного «пошуку та компіляції інформації» до стратегічного дизайну правових

рішень, де ШІ виконує роль аналітичного фундаменту, а людина виконує роль етичного та стратегічного фільтра.

Поява та стрімке поширення генеративного штучного інтелекту (зокрема великих мовних моделей, таких як GPT-4) стали каталізатором виникнення принципово нових професійних ролей, які раніше не існували в юридичному дискурсі. Ключовою фігурою в сучасних юридичних департаментах та судах стає «Legal Engineer» (юридичний інженер), тобто фахівець, який володіє як юридичною освітою, так і навичками програмування або системного аналізу [77, с. 145]. Його функція полягає у налаштуванні ШІ-систем під конкретні потреби юридичної практики та забезпеченні технічної відповідності автоматизованих рішень нормам та духу закону. За даними Міжнародної асоціації юристів (ІВА), саме юридичні інженери стають архітекторами нової цифрової юстиції, забезпечуючи оцінку та погодження висновків ШІ та запобігаючи впливу системних помилок алгоритмів на рішення професійних діячів [49, с. 8]. Паралельно з цим зростає попит на «аналітиків юридичних даних» (Legal Data Scientists), які здатні інтерпретувати результати предиктивних моделей та виявляти приховані судові ризики чи корупційні аномалії, що не піддаються людському аналізу [29, с. 300].

Особливий вплив на повсякденну діяльність адвокатів, прокурорів та суддів має впровадження інструментів для автоматизації складного юридичного письма. Згідно зі спеціальним звітом Сінгапурської академії права (2024), використання генеративного ШІ дозволяє скоротити часові витрати на підготовку першої редакції позову, меморандуму або проекту судового рішення на 60–70%, що змінює економіку юридичної праці [74, с. 22]. Водночас це породжує нову категорію професійних обов'язків: стандарт «людського аудиту» (human verification) стає не просто етичною порадою, а імперативною вимогою процесуального законодавства та етичних правил поведінки з ШІ та сучасними технологіями загалом. У світовій практиці вже фіксуються випадки дисциплінарної відповідальності адвокатів за «алгоритмічні галюцинації» (використання вигаданих ШІ прецедентів), що підкреслює: відповідальність за кінцевий результат у цифрову епоху залишається виключно персональною та людською [60, с. 8].

Трансформація юридичної професії також зумовлює кардинальні зміни в системі юридичної освіти. Провідні світові університети інтегрують курси з юридичного промт-інжинірингу, етики алгоритмів та кібербезпеки правових даних у магістерські програми [33, с. 14; 77, с. 160]. Це свідчить про глобальне визнання того, що технологічна неграмотність у майбутньому буде ототожнюватися з професійною непридатністю фахівця. Штучний інтелект у цьому контексті виступає не як заміник правника, а як фактор формування інтелектуального симбіозу, де машина забезпечує безпрецедентну швидкість та точність аналізу, а людина фокусується на етичних дилемах, принципах справедливості та складних переговорах, де емпатія та контекстуальне розуміння залишаються недосяжними для алгоритмів.

Таким чином, роль ШІ в трансформації юриспруденції полягає у переході до «інженерної моделі права», де ефективність правосуддя безпосередньо залежить від синергії між обчислювальною потужністю систем та професійною відповідальністю людини. Світові тенденції підтверджують, що виграють ті правові системи, які зможуть найшвидше адаптувати свої кадри до роботи в умовах доповненої алгоритмами реальності.

ВИСНОВОК ДО РОЗДІЛУ 1

Проведене у першому розділі комплексне дослідження теоретико-правових засад та технологічних аспектів застосування штучного інтелекту в правничій діяльності дозволяє сформулювати низку концептуальних висновків, що становлять підґрунтя для подальшого аналізу. Передусім, встановлено, що ШІ у правовій площині не є статичним програмним продуктом, а являє собою складну, динамічну систему, здатну до автономного формування результатів (прогнозів, рекомендацій, рішень) на основі алгоритмічного опрацювання великих масивів даних. Визначено, що ключовою ознакою, яка відрізняє ШІ від традиційних засобів автоматизації, є його когнітивна здатність до імітації інтелектуальних функцій людини, сприйняття, аналізу та предиктивної генерації юридично значущої інформації, що в контексті

юриспруденції слід розглядати як «цифровий когнітивний актив», який потребує специфічного правового статусу.

Систематизація систем ІІІ за рівнем автономності, архітектурою та ризико-орієнтованим підходом доводить, що для правозастосовної діяльності найбільш релевантними у практичному застосуванні є системи «доповненого інтелекту» (Augmented Intelligence), оскільки вони не заміняють спеціалістів, а доповнюють їх експертизу оптимізацією діяльності. Доведено, що класифікація за ступенем ризику від низького до неприйняттого є фундаментальною для майбутньої нормотворчості, оскільки дозволяє розмежувати сфери, де ІІІ може діяти відносно автономно (наприклад, адміністративна підтримка), від сфер, де присутність людини («human-in-the-loop») є імперативною вимогою через необхідність забезпечення етичного виміру правосуддя [64, с. 8]. Аналіз практичних форм використання ІІІ в судочинстві продемонстрував перехід від горизонтальної цифровізації (Електронний суд, автоматизований розподіл справ) до вертикальної інтелектуалізації процесів, таких як предиктивне правосуддя, семантичний аналіз доказів та інтелектуальна онлайн-медіація.

Дослідження світових тенденцій LegalTech підтвердило існування глобального процесу руйнування традиційних моделей юридичної практики, відомого як «Великий розрив» (The Great Disruption) [62, с. 3045]. Економіка права трансформується від продажу часового ресурсу юриста до надання високотехнологічного інтелектуального продукту, що зумовлює зміну професійного профілю правника. Поява таких ролей як «Legal Engineer» та вимога до формування «T-shaped» компетенцій свідчить про зародження нової парадигми «Права 4.0», де правова експертиза поєднується з інженерним підходом до управління даними [77, с. 140; 77, с. 145; 38, с. 24]. Водночас, ключовим теоретичним висновком розділу є те, що відповідальність за етичний та правовий результат застосування ІІІ залишається виключно персональною відповідальністю людини, що актуалізує необхідність розробки ефективних міжнародних та національних механізмів контролю.

Отримані результати теоретико-технологічного аналізу створюють необхідний науковий базис для переходу до другого розділу роботи, де буде детально

проаналізовано систему міжнародного та національного правового регулювання ШІ. Зокрема, виявлені тенденції та ризики диктують потребу в глибокому вивченні Актів Європейського Союзу та етичних хартій міжнародних організацій як інструментів «приборкання» технології без пригнічення її інноваційного потенціалу.

РОЗДІЛ 2.

ПРАВОВЕ РЕГУЛЮВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ: МІЖНАРОДНИЙ ТА НАЦІОНАЛЬНИЙ КОНТЕКСТ

2.1. Міжнародні стандарти та етичні принципи регулювання ШІ: досвід ООН, ОЕСР та Ради Європи, тощо.

Другий розділ магістерської роботи присвячений комплексному дослідженню архітектури нормативно-правового ландшафту, що формується навколо технологій штучного інтелекту на глобальному, регіональному та національному рівнях. Актуальність даного аналізу зумовлена глобальним переходом від стадії декларативного етичного регулювання до стадії імперативної законотворчості, оскільки стрімке впровадження алгоритмічних систем у публічну сферу актуалізує питання гарантування фундаментальних прав людини та збереження верховенства права в умовах цифрової трансформації. Метою цього розділу є визначення ключових регуляторних моделей та аналіз ієрархічної системи джерел права, що визначають межі допустимого використання ШІ в судочинстві та правозастосовній діяльності.

Порядок основних елементів аналізу в межах розділу побудований за принципом від загальносвітових стандартів до національної специфіки. У першому підрозділі дослідження фокусується на роль міжнародних організацій, таких як ООН, ОЕСР та Рада Європи, у розробці концептуальних засад «м'якого права», що стали ціннісним орієнтиром для всієї світової спільноти. Наступний аналітичний етап у другому підрозділі присвячено детальному розбору Регламенту ЄС про штучний інтелект (EU AI Act), який постає як перший у світі комплексний законодавчий акт, що запроваджує ризико-орієнтований підхід та встановлює жорсткі стандарти безпеки для інтелектуальних систем. Завершальна частина розділу зосереджена на критичному аналізі стану нормативно-правового регулювання ШІ в Україні, оцінці його відповідності європейському вектору розвитку та виявленні прогалин, що потребують законодавчого врегулювання в контексті євроінтеграційних процесів.

Такий системний підхід дозволить не лише описати існуючі норми, а й виявити тенденції формування глобального цифрового врегулювання.

Формування міжнародних стандартів у сфері регулювання ШІ постає як пріоритетне завдання сучасної глобальної правової політики, оскільки транскордонна та екстериторіальна природа цифрових алгоритмів унеможлиблює їх ефективний контроль виключно в межах національних юрисдикцій. На сучасному етапі міжнародне співтовариство зробило розгалужену систему етико-правових орієнтирів, які спрямовані на гармонізацію технологічного прогресу з фундаментальними цінностями демократичного суспільства та верховенства права. Роль ключових міжнародних інституцій, таких як ООН, ОЕСР та Рада Європи, у цьому процесі є визначальною, оскільки саме вони виступили майданчиками для розробки «м'якого права» (soft law) - сукупності принципів, які, не маючи прямої імперативної сили, формують глобальний стандарт «належної поведінки» для розробників та користувачів інтелектуальних систем [64, с. 3].

Метою цього підрозділу є системний аналіз еволюції міжнародного регулювання: від загальних декларативних принципів до вузькоспеціалізованих етичних хартій, що безпосередньо регламентують використання ШІ у правозастосовній діяльності. У межах підрозділу досліджено, як універсальні вимоги щодо прозорості, недискримінації та підзвітності інтегруються в міжнародні договори та технічні стандарти, створюючи передумови для формування єдиного світового безпекового простору у сфері штучного інтелекту. Розуміння цих засад є критично важливим, оскільки вони становлять ідеологічний та нормативний базис, на якому в подальшому вибудовується жорстке законодавство Європейського Союзу та національні стратегії держав, включно з Україною.

Процес формування міжнародного нормативного каркаса для систем ШІ розпочався з усвідомлення того, що технологічний прогрес у цій сфері несе в собі не лише колосальні можливості для розвитку людства, а й екзистенційні загрози для архітектури прав людини. У цьому контексті ключову роль відіграла Організація економічного співробітництва та розвитку (ОЕСР), яка у травні 2019 року ухвалила Рекомендації Ради щодо штучного інтелекту (OECD AI Principles), що стали першим

міжурядовим стандартом у цій царині [64, с. 3]. Ці принципи заклали фундамент так званого «надійного ШІ» (trustworthy AI), де основний акцент зміщено з суто економічної ефективності на етичну прийнятність та безпеку. Згідно з оновленими положеннями 2024 року, ОЕСР вимагає від держав-членів та країн, що приєдналися до Рекомендацій, стимулювати розробку систем ШІ, які б сприяли інклюзивному зростанню та сталому розвитку, забезпечуючи при цьому суворе дотримання людиноцентричних цінностей та справедливості [64, с. 5]. Важливо підкреслити, що ОЕСР розглядає прозорість та пояснюваність алгоритмів не як опцію, а як імперативну умову, що дозволяє користувачам та суб'єктам, на яких впливає ШІ, розуміти логіку прийнятих рішень та, за потреби, оскаржувати їх.

Паралельно з людиноцентричним підходом ОЕСР, Організація Об'єднаних Націй (ООН) вибудувала глобальну гуманітарну рамку регулювання, що ґрунтується на універсальності прав людини. У доповідях Спеціальних доповідачів ООН та відповідних Резолюціях Генеральної Асамблеї послідовно наводиться теза про те, що цифровізація не може бути підставою для звуження обсягу прав, закріплених у Загальній декларації прав людини [5, ст. 12]. Особлива увага ООН зосереджена на запобіганні використанню ШІ для масового стеження, соціального скорингу та інших практик, що порушують право на приватність та людську гідність. У 2024 році Генеральна Асамблея ООН ухвалила знакову резолюцію щодо безпечного та надійного ШІ, де закликала держави та приватний сектор розробити механізми аудиту алгоритмів, які б гарантували відсутність вбудованої дискримінації за ознаками раси, статі чи соціального походження [80, с. 2]. Такий підхід ООН створює глобальний етичний фільтр, який вимагає від розробників систем ШІ враховувати довгострокові соціальні наслідки їхнього впровадження.

Детальний розгляд міжнародних ініціатив також висвітлює роль ЮНЕСКО, яка у 2021 році представила Рекомендацію про етику штучного інтелекту, ухвалену всіма 193 країнами-членами [79, с. 14]. Цей документ є унікальним за своєю глибиною, оскільки він пропонує конкретні інструменти для оцінки етичного впливу (Ethical Impact Assessment) протягом усього життєвого циклу системи ШІ - від розробки концепції до виведення з експлуатації. ЮНЕСКО акцентує увагу на тому, що ШІ

повинен сприяти збереженню культурного різноманіття та не ставати інструментом культурної уніфікації. У контексті правничої діяльності це означає, що алгоритми, які використовуються в судах або поліції, мають бути адаптовані до місцевого правового та культурного контексту, а не просто сліпо копіювати моделі, розроблені в інших юрисдикціях [79, с. 14].

В рамках аналізу глобальних ініціатив слід зауважити, що синергія між принципами ОЕСР та стандартами ООН створила те, що в науці називають «світовим етичним консенсусом». Цей консенсус базується на трьох китах: підзвітність розробників, безпека користувачів та недоторканність прав людини. Незважаючи на те, що ці норми мають характер «м'якого права», вони виконують критичну функцію, а саме заповнюють правовий вакуум до моменту ухвалення національних законів та слугують джерелом інтерпретації для суддів при вирішенні спорів, пов'язаних з новими технологіями. Таким чином, внесок ООН та ОЕСР полягає у формуванні інтелектуальної та ціннісної матриці, на якій в подальшому вибудовується вся архітектура регіонального регулювання, зокрема досвід Ради Європи та Європейського Союзу [64, с. 5; 80, с. 2].

Рада Європи (РЄ) займає унікальне місце в архітектурі глобального регулювання штучного інтелекту, оскільки саме ця організація першою перейшла від загальних гуманітарних закликів до розробки прикладних стандартів для правової сфери. Фундаментальним інструментом у цьому контексті стала Європейська етична хартія про використання штучного інтелекту в судових системах та їхньому середовищі, ухвалена Європейською комісією з питань ефективності правосуддя (CEREPJ) у грудні 2018 року [41, с. 4; 37, с. 5]. Даний документ не лише декларує цінності, а й пропонує методологічну рамку для суддів, прокурорів та розробників LegalTech рішень, базуючись на п'яти стрижневих принципах, які мають на меті запобігти ерозії верховенства права під тиском технологізації.

Першим і найбільш вагомим є принцип дотримання основоположних прав, який імперативно вимагає, щоб розробка та впровадження інструментів ШІ здійснювалися у повній відповідності до Європейської конвенції з прав людини

(ЄКПЛ) та Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних [4, ст. 8; 8, ст. 5].

Другим за ієрархією, але не менш значущим, є принцип недискримінації, який набуває особливої гостроти у контексті використання ШІ для предиктивної аналітики чи оцінки ризиків у кримінальних провадженнях. Хартія ЄРЕЛ наголошує на необхідності запобігання будь-якій упередженості, яка може бути зашита в алгоритм через історичні дані, що відображають соціальні чи расові стереотипи. У зв'язку з цим, Рада Європи впроваджує принцип якості та безпеки, який передбачає, що всі системи ШІ, які використовуються в судах, повинні проходити суворий аудит на предмет достовірності джерел даних та стійкості до маніпуляцій. Така «сертифікація етичності» має гарантувати, що судові рішення, підготовлене за допомогою алгоритму, буде базуватися на верифікованій та об'єктивній базі, а не на статистичних помилках [41, с. 10].

Окрему увагу в межах стандартів Ради Європи приділено принципам прозорості, неупередженості та справедливості, які безпосередньо корелюють зі статтею 6 ЄКПЛ, що закріплює право на справедливий суд [4, ст. 6]. Згідно з Хартією, методи обробки даних мають бути доступними та зрозумілими для учасників процесу, що означає подолання проблеми «чорної скриньки» через забезпечення пояснюваності алгоритмічних висновків [66, с. 55]. Завершальним та найбільш концептуальним є принцип «під контролем користувача» (under user control). Цей принцип встановлює сувору заборону на автоматизоване правосуддя без участі людини: суддя повинен мати право в будь-який момент відхилити рекомендацію ШІ та самостійно оцінити обставини справи. Це положення підтверджує, що в європейській правовій традиції ШІ розглядається лише як асистент (augmented intelligence), а не як суверенний суб'єкт прийняття рішень [41, с. 10].

Розвиваючи ці напрацювання, Рада Європи у 2024 році відкрила для підписання Рамкову конвенцію про штучний інтелект, права людини, демократію та верховенство права [39, ст. 1; 72, с. 45]. Цей договір є першою юридично обов'язковою міжнародною угодою, яка трансформує етичні принципи Хартії ЄРЕЛ у чіткі зобов'язання держав. Конвенція зобов'язує сторони впроваджувати ефективні

засоби правового захисту для осіб, чий права були порушені системами ШІ, та створювати незалежні наглядові органи для моніторингу алгоритмічних ризиків. Таким чином, внесок Ради Європи полягає у створенні цілісної нормативної архітектури, яка захищає «людський елемент» у правосудді, забезпечуючи, щоб цифрова трансформація судів відбувалася без втрати морально-етичного фундаменту права [41, с. 10].

У сучасній системі глобального управління щодо штучного інтелекту спостерігається унікальний процес конвергенції правових норм та технічних регламентів. Якщо етичні хартії та декларації ООН чи Ради Європи задають ціннісний вектор, то міжнародні технічні стандарти, розроблені Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC), забезпечують практичну можливість реалізації цих цінностей. Ключовим документом у цій сфері став стандарт ISO/IEC 22989:2022, який вперше на міжнародному рівні встановив єдину термінологію та концептуальну базу для систем ШІ, що є критично важливим для уникнення правових колізій при транскордонному використанні LegalTech рішень [53, с. 1]. Юридичне значення таких стандартів полягає в тому, що вони де-факто стають джерелом, на основі якого здійснюється оцінка відповідності (conformity assessment) систем ШІ вимогам безпеки та надійності.

Особливе місце в архітектурі регулювання посідає стандарт ISO/IEC 42001:2023, який впроваджує систему менеджменту штучного інтелекту (AIMS) [55, с. 2]. Цей стандарт вимагає від організацій, що розробляють або впроваджують ШІ (включаючи органи судової влади та правоохоронні органи), створювати внутрішні механізми контролю ризиків, забезпечувати прозорість алгоритмічних процесів та здійснювати регулярний моніторинг впливу ШІ на кінцевих користувачів. У контексті судочинства дотримання стандартів ISO/IEC стає вагомим доказом «належної обачності» (due diligence) суб'єкта правозастосування. Якщо алгоритм, використаний для аналізу доказів, відповідає міжнародним стандартам стійкості до маніпуляцій та пояснюваності (explainability), це значно підвищує легітимність отриманих результатів у процесуальному сенсі.

Крім того, технічна стандартизація виконує функцію підкріплення етичних принципів недискримінації та справедливості. Стандарти групи ISO/IEC 24027 надають методики виявлення та вимірювання системних упереджень у навчальних даних та результатах роботи алгоритмів [54, с. 5]. Це дозволяє трансформувати абстрактну вимогу «недискримінації» у конкретні математичні метрики, які можуть бути перевірені незалежними аудитором або фахівцями під час проведення призначеної судом ІТ-експертизи. Таким чином, міжнародні технічні стандарти виступають як сполучна ланка між «м'яким правом» етичних декларацій та «жорстким правом» законодавчих актів, забезпечуючи уніфікацію вимог до якості систем ШІ у глобальному масштабі та створюючи доказову базу для захисту прав людини в цифрову епоху.

Завершуючи аналіз міжнародного складника регулювання штучного інтелекту, слід констатувати, що за останнє десятиліття світова спільнота пройшла стрімку еволюцію від фрагментарних технологічних дискусій до формування цілісної глобальної архітектури «м'якого права». Провідна роль ООН, ОЕСР та Ради Європи у цьому процесі полягала у створенні ціннісного консенсусу, який базується на пріоритеті людиноцентричності, прозорості та підзвітності алгоритмічних систем. В рамках аналізу чітко встановлено, що Рекомендації ОЕСР та Резолюції ООН виконали функцію ідеологічного фундаменту, визначивши, що будь-який технологічний прогрес у сфері ШІ є легітимним лише за умови неухильного дотримання основоположних прав і свобод людини [64, с. 7; 80, с. 4; 46, с. 3].

Особливе значення для судочинства та правозастосовної діяльності має спеціалізований доробок Ради Європи, зокрема Етична хартія СЕРЕJ. Даний документ став першим у світі інструментом, що адаптував абстрактні етичні категорії до жорстких вимог процесуального права, встановивши принцип людського контролю як ключовий запобіжник проти дегуманізації правосуддя та перетворення судді на пасивного виконавця алгоритмічних рекомендацій [41, с. 12]. Разом із тим, синергія етичних норм із міжнародними технічними стандартами ISO/IEC дозволила перетворити декларативні вимоги на вимірювані параметри надійності та безпеки, що

створює об'єктивну базу для юридичного аудиту та експертизи інтелектуальних систем [53, с. 10; 55, с. 8].

Таким чином, міжнародні стандарти сформували флюїдний кодекс поведінки для цифрової епохи, який став необхідним етапом перед переходом до імперативного законодавчого регулювання [72, с. 20; 73, с. 360]. Вивчення цих принципів дозволяє стверджувати, що глобальний тренд спрямований на створення безпечного та передбачуваного середовища для використання ШІ, де технологія виступає інструментом зміцнення верховенства права, а не його руйнації. Цей міжнародний досвід став безпосереднім поштовхом для розробки Регламенту ЄС про штучний інтелект (EU AI Act), який трансформує згадані етичні орієнтири у систему юридичних обов'язків та санкцій, що буде детально розглянуто у наступному підрозділі

2.2. Правове регулювання ШІ в Європейському Союзі: аналіз EU AI Act та вплив сучасного законодавства ЄС на глобальні правові процеси

Ухвалення Регламенту Європейського Парламенту і Ради Європи про встановлення гармонізованих правил щодо штучного інтелекту (EU AI Act) у 2024 році стало історичною віхою в еволюції цифрового права, оскільки це перший у світі комплексний законодавчий акт, що запроваджує пряме імперативне регулювання систем штучного інтелекту [27, ст. 1]. На відміну від попередніх етапів, які базувалися на принципах «м'якого права», Регламент ЄС трансформує етичні орієнтири у систему чітких юридичних зобов'язань, недотримання яких тягне за собою суворі адміністративні та фінансові санкції. Актуальність аналізу цього документа зумовлена тим, що він запроваджує ризико-орієнтований підхід (risk-based approach), який стає методологічним еталоном для більшості демократичних країн, включаючи Україну як кандидата на вступ до ЄС.

Метою цього підрозділу є критичний аналіз архітектури EU AI Act, дослідження критеріїв класифікації систем ШІ за рівнем ризику та оцінка специфічних вимог до систем «високого ризику», що використовуються в

правоохоронній та судовій діяльності. У межах дослідження розкрито механізми забезпечення алгоритмічної прозорості, нагляду з боку людини та захисту фундаментальних прав, що закладені в основу європейської моделі цифрового суверенітету. Розуміння положень Регламенту є критично важливим для прогнозування майбутніх змін у національному законодавстві, оскільки EU AI Act формує глобальний регуляторний стандарт, який змушує технологічні корпорації в усьому світі адаптувати свої продукти під високі європейські вимоги безпеки.

Фундаментальною новацією Регламенту ЄС про штучний інтелект є запровадження ризико-орієнтованого підходу, який відходить від спроб регулювати технологію як таку, натомість зосереджуючись на контексті її застосування та потенційних наслідках для безпеки і прав людини [27, ст. 5]. Ця модель вибудовує чітку пірамідальну ієрархію, яка поділяє всі системи ШІ на чотири категорії залежно від ступеня загрози, яку вони становлять. Першу групу становлять системи з неприйнятним ризиком (*unacceptable risk*), використання яких на території ЄС підпадає під повну законодавчу заборону. До цієї категорії віднесено технології «соціального скорингу» (державного оцінювання поведінки громадян), системи маніпулятивного впливу на підсвідомість, а також біометричну ідентифікацію в реальному часі в публічних місцях для цілей правоохоронної діяльності (за певними винятками), оскільки вони визнані такими, що суперечать цінностям людської гідності та демократії [27, ст. 5].

Другим, найбільш детально регламентованим рівнем, є системи високого ризику (*high-risk AI systems*). До цієї групи включено ШІ-рішення, що використовуються в критично важливих сферах: освіта, підбір персоналу, критична інфраструктура, охорона здоров'я та, що є ключовим для нашого дослідження, правоохоронна діяльність і правосуддя [27, ст. 5]. Регламент встановлює суворі вимоги до таких систем ще до їх виходу на ринок: вони повинні мати високу якість наборів даних для навчання, забезпечувати належний рівень кібербезпеки та гарантувати «пояснюваність» алгоритмічних результатів [27, ст. 6]. Більше того, розробники зобов'язані впроваджувати механізми постійного нагляду з боку людини

(human oversight), що є безпосереднім втіленням принципів Ради Європи в імперативну норму права [27, ст. 5].

Третя категорія охоплює системи з обмеженим ризиком (limited risk), до яких висуваються переважно вимоги щодо прозорості. Користувачі таких систем (наприклад, чат-ботів або сервісів генерації контенту) мають бути чітко поінформовані про те, що вони взаємодіють зі штучним інтелектом [27, ст. 52].

Четвертий рівень - це системи з мінімальним ризиком (minimal risk), такі як відеоігри з елементами ШІ або спам-фільтри, регулювання яких залишається на розсуд розробників через механізми саморегулювання. Слід зазначити, що EU AI Act також виокремлює системи ШІ загального призначення (GPAI), включаючи потужні мовні моделі, встановлюючи для них додаткові зобов'язання щодо управління ризиками та звітності, якщо вони використовуються як база для створення додатків високого ризику [27, ст. 53; 27, ст. 69].

Аналіз класифікаційної моделі Регламенту дозволяє стверджувати, що європейський законодавець прагне знайти баланс між стимулюванням інновацій та захистом безпеки громадян. Встановлюючи жорсткі бар'єри для систем високого ризику, ЄС де-факто створює умови для формування ринку довіри, де споживач може бути впевнений у безпечності технологічного продукту. Такий підхід має глобальне значення, оскільки створює прецедент для міжнародної стандартизації: будь-яка компанія (включаючи українські стартапи), що прагне працювати на ринку ЄС, повинна адаптувати свою архітектуру під ці чотири рівні ризику, що робить EU AI Act глобальним регулятором технологічного сектору.

Регламент ЄС про штучний інтелект виходить за межі простої класифікації ризиків, запроваджуючи комплексну систему операційних вимог, що мають на меті подолання ефекту «чорної скриньки» [66, с. 55]. Центральне місце в цій системі посідає принцип прозорості (transparency), який не обмежується лише змістовним наповненням, а реалізується через низку взаємопов'язаних елементів. Для систем високого ризику цей принцип, перш за все, трансформується у вимогу пояснюваності (explainability), що передбачає можливість інтерпретації логіки алгоритму користувачем-людиною для розуміння причин отримання конкретного результату

[27, ст. 13]. Однак, архітектура прозорості за Регламентом є значно ширшою і включає також відстежуваність (traceability) — обов'язок забезпечити автоматичне ведення журналів подій (логіювання) протягом усього життєвого циклу системи для можливості ретроспективного аналізу її роботи [27, ст. 12]. Важливим компонентом є належне інформування (provision of information), згідно з яким постачальники зобов'язані супроводжувати свої продукти детальною технічною документацією та зрозумілими інструкціями. Ці документи мають розкривати не лише логіку алгоритму, а і його обмеження, ймовірні похибки та рівень точності. У сукупності з вимогами до людського нагляду (human oversight), ці елементи дозволяють перетворити ШІ з непередбачуваного інструмента на підконтрольну технологію, роботу якої можна піддати повноцінному юридичному аудиту.

Іншим наріжним каменем європейської моделі регулювання є принцип нагляду з боку людини (human oversight). EU AI Act імперативно встановлює, що системи високого ризику мають бути спроектовані та розроблені таким чином, щоб фізичні особи могли ефективно контролювати їхнє функціонування. Цей механізм передбачає не просто формальну присутність людини, а її реальну можливість втручатися в роботу алгоритму, зупинити його або ігнорувати його висновки без негативних наслідків для процесу прийняття рішення [27, ст. 14]. У контексті правосуддя це означає, що будь-яка аналітична довідка, сформована ШІ для судді, повинна супроводжуватися позначкою про її автоматизоване походження, а суддя зобов'язаний провести самостійну верифікацію наданих даних.

Для забезпечення реальної підзвітності (accountability), Регламент впроваджує багаторівневу систему контролю. По-перше, це обов'язкова реєстрація систем високого ризику в загальноєвропейській базі даних (EU Database for High-Risk AI Systems), що забезпечує публічний нагляд та можливість моніторингу ринків [27, ст. 71]. По-друге, це створення Європейського офісу з питань штучного інтелекту (EU AI Office), який виконує роль центрального координатора та наглядового органу на рівні Союзу, а також мережі національних наглядових органів у кожній країні-члені [27, ст. 99; 73, с. 362]. Важливою складовою підзвітності є також проведення «Оцінки впливу на фундаментальні права» (Fundamental Rights Impact Assessment), яку

зобов'язані здійснювати державні органи перед впровадженням систем високого ризику в свою діяльність [27, с. 27; 52, с. 6; 34, ст. 8].

Критичний аналіз цих механізмів дозволяє стверджувати, що EU AI Act створює безпрецедентний рівень відповідальності для технологічного сектору. Порухення вимог щодо прозорості або ігнорування стандартів людського нагляду може призвести до накладення штрафів у розмірі до 35 мільйонів євро або 7% від світового річного обороту компанії [27, ст. 99]. Таким чином, європейський законодавець не просто пропонує етичні орієнтири, а вибудовує жорстку систему примусу, яка гарантує, що штучний інтелект буде залишатися безпечним, передбачуваним та підконтрольним суспільству інструментом, а не автономним джерелом правових ризиків.

Регламент ЄС про штучний інтелект не обмежений суто географічними кордонами держав-членів Союзу, оскільки він закладає фундамент для так званого «Брюссельського ефекту» (Brussels Effect) - явища, за якого європейські стандарти стають де-факто глобальними нормами через значну вагу європейського ринку [31, с. 130]. Екстериторіальна дія EU AI Act виявляється у тому, що будь-який розробник ШІ, незалежно від місця реєстрації (США, Китай чи Україна), зобов'язаний дотримуватися вимог Регламенту, якщо його продукт виводиться на ринок ЄС або якщо результати роботи алгоритму використовуються на території Союзу. Це створює потужний стимул для технологічних корпорацій уніфікувати свої внутрішні стандарти безпеки та етики згідно з найсуворішим європейським зразком, щоб уникнути фрагментації виробничих процесів.

Для того, щоб підкреслити вплив сучасного регулювання на цифрову трансформацію суспільства, слід також проаналізувати поняття «цифрового суверенітету», а саме здатність держав або інших стейкхолдерів самостійно контролювати власні цифрові ресурси, дані, інфраструктуру, тощо. Основними ознаками досягнення цифрового суверенітету визначають забезпечення операційної автономії, управління даними відповідно до локального та міжнародного законодавства, зменшення залежності від окремих вендорів програмного

забезпечення, побудова стійкої інфраструктури, впровадження заходів для захисту чутливої інформації на всіх вищеперерахованих рівнях [14, с. 37; 25, с. 26].

В даному контексті значення EU AI Act для міжнародного публічного права полягає у формуванні нового стандарту цифрового суверенітету, який базується на захисті прав людини, а не на інтересах держави чи корпорацій, і зсовує перспективу держав на забезпечення не тільки цифрової, а й правової інфраструктури при впровадженні нових технологій. Регламент виступає моделлю для оновлення міжнародних торговельних угод та двосторонніх договорів, де питання сертифікації ШІ та транскордонної передачі алгоритмічних моделей стають ключовими елементами правового регулювання [27, с. 1]. У сфері міжнародного приватного права EU AI Act створює нову рамку деліктної відповідальності: встановлення чітких зобов'язань для постачальників систем високого ризику спрощує процес доказування вини у транскордонних спорах, пов'язаних із завданням шкоди алгоритмами, оскільки недотримання стандартів Регламенту є апріорним свідченням неналежної обачності [27, с. 1].

Більше того, EU AI Act виконує роль нормативного маяка для країн, що перебувають у процесі гармонізації свого законодавства з правом ЄС, зокрема для України. Регламент пропонує готовий методологічний інструментарій, який надає необхідну базу від визначень термінів до процедур оцінки відповідності, що дозволяє іншим країнам уникати регуляторного хаосу та швидко інтегруватися у глобальний цифровий ринок. Таким чином, глобальний вплив європейського акта полягає не лише у примусі, а й у створенні передбачуваного правового середовища, де інновації розвиваються у межах чітких етичних координат, що визнаються міжнародною спільнотою як стандарт безпеки та надійності. Це перетворює Європейський Союз на головного архітектора світового правопорядку в епоху штучного інтелекту.

Аналізуючи нормативне регулювання штучного інтелекту в ЄС, неможливо оминати його тісний взаємозв'язок із Загальним регламентом про захист даних (GDPR) [45, ст. 1]. Хоча EU AI Act фокусується на безпеці систем та управлінні ризиками, GDPR залишається фундаментальним актом, що регулює обробку персональних даних, які використовуються для навчання та експлуатації алгоритмів.

Зокрема, стаття 22 GDPR встановлює право особи не підлягати рішення, що ґрунтується виключно на автоматизованій обробці, включаючи профілювання, якщо таке рішення породжує правові наслідки для особи або подібним чином істотно впливає на неї [45, ст. 22; 81, с. 14]. Це створює необхідний юридичний бар'єр проти безконтрольного використання ШІ у сферах, де автоматизовані вердикти можуть обмежити права людини без належного людського нагляду.

Синергія між цими двома актами проявляється і в питаннях прозорості. Якщо EU AI Act вимагає технічної пояснюваності алгоритмів високого ризику, то GDPR забезпечує право суб'єкта даних на отримання змістовної інформації про логіку автоматизованої обробки (статті 13-14). Таким чином, розробники систем ШІ, що функціонують на ринку ЄС, зобов'язані дотримуватися принципу "приватності за замовчуванням" (privacy by design), що передбачає мінімізацію даних та забезпечення їхньої конфіденційності ще на етапі архітектурного проектування моделі [42, с. 6]. Такий комплексний підхід гарантує, що інноваційний розвиток інтелектуальних систем не відбуватиметься за рахунок порушення приватного життя та автономії особи.

Підсумовуючи аналіз Регламенту ЄС про штучний інтелект (EU AI Act), слід констатувати, що цей документ знаменує собою остаточний перехід глобальної правової думки від стадії етичних декларацій до стадії жорсткого нормативного регулювання. Впровадження ризико-орієнтованого підходу дозволило європейському законодавцю створити гнучку, але водночас сувору ієрархію вимог, де ступінь втручання права прямо пропорційний ступеню загрози для безпеки та фундаментальних прав людини. Встановлено, що класифікація систем ШІ на чотири рівні ризику створює чіткий алгоритм дій для розробників, де системи високого ризику, зокрема деякі, що застосовуються в правосудді (ті що призначені для безпосередньої допомоги органам правосуддя в дослідженні фактів, інтерпретації права та застосуванні норм до конкретних обставин справи), підпадають під безпрецедентний нагляд, включаючи обов'язкову прозорість, високу якість даних та невід'ємний людський контроль [27, ст. 6].

Особливе значення EU AI Act полягає в його екстериторіальному впливі, що реалізується через механізм «Брюссельського ефекту». Встановлюючи найвищі у світі стандарти безпеки та підзвітності, Європейський Союз де-факто диктує правила гри для глобального технологічного сектору, змушуючи розробників в усьому світі адаптувати свої продукти під європейські вимоги [31, с. 145]. Для юридичної спільноти цей Регламент створює нову рамку професійної відповідальності та процесуальних стандартів, де використання алгоритмів у суді чи правоохоронній діяльності стає легітимним лише за умови повної відповідності принципам пояснюваності та людського нагляду.

Таким чином, EU AI Act постає не лише як внутрішній регламент Союзу, а як перший у світі протокол «цифрового конституціоналізму», що захищає людську гідність у відносинах з автономними системами. Розуміння архітектури цього акта є критично важливим для України, оскільки подальша адаптація національного законодавства має відбуватися не шляхом сліпого копіювання, а через глибоку інтеграцію принципів безпеки та прав людини, закладених у європейську модель регулювання.

2.3. Сучасний стан та перспективи правового регулювання ШІ в Україні в контексті європейської інтеграції

Для України питання правового регулювання штучного інтелекту набуло особливої гостроти у зв'язку з набуттям статусу кандидата на вступ до Європейського Союзу та необхідністю гармонізації національного законодавства з європейським цифровим порядком денним. На відміну від розвинених юрисдикцій, що вже мають сталу нормативну базу, вітчизняний підхід характеризується динамічним переходом від повної відсутності спеціального регулювання до впровадження моделі «м'якого права» та підготовки до імплементації норм EU AI Act. Актуальність дослідження цього процесу зумовлена потребою створення безпечного правового середовища для використання ШІ в умовах воєнного стану, а також забезпечення конкурентоспроможності українських LegalTech стартапів на глобальному ринку.

Метою цього підрозділу є аналіз поточної нормативної бази України, зокрема «Білої книги» щодо регулювання ШІ, та оцінка стратегічних кроків Міністерства цифрової трансформації України у напрямку адаптації європейських стандартів [2, с. 12]. У межах підрозділу буде досліджено специфіку українського підходу, який базується на поетапному запровадженні регуляторних вимог, та виявлено ключові правові бар'єри, що заважають ефективній інтеграції інтелектуальних систем у національну судову та правоохоронну системи. Окрему увагу буде приділено перспективам створення національної системи нагляду за ШІ-технологіями, що має стати дзеркальним відображенням європейської моделі підзвітності та прозорості в умовах цифровізації публічного сектору.

Формування вітчизняного правового поля у сфері штучного інтелекту розпочалося із прийняття Концепції розвитку штучного інтелекту в Україні (2020 р.), яка визначила пріоритетні напрями впровадження технології в економіку, державне управління та правосуддя [10, розд. 1; 11, с. 48]. Цей документ заклав фундамент для розуміння ШІ як стратегічного чинника підвищення конкурентоспроможності держави, акцентуючи при цьому на необхідності дотримання конституційних прав і свобод людини. Важливим етапом реалізації цієї стратегії стала публікація Міністерством цифрової трансформації України Білої книги з регулювання ШІ, яка проголосила перехід до моделі «м'якого регулювання» (soft law) [2, с. 5]. Такий підхід передбачає надання бізнесу та державним органам часу на адаптацію до майбутніх жорстких норм через добровільні інструменти.

Центральним елементом такої адаптивної моделі став Добровільний кодекс поведінки з етичного та відповідального використання ШІ (2024 р.) [3, с. 4]. Документ фокусується на принципах людиноцентричності, прозорості та недискримінації, пропонуючи розробникам самостійно проводити оцінку впливу своїх систем на права громадян. У контексті правничої діяльності цей Кодекс слугує орієнтиром для розробників LegalTech-рішень, спонукаючи їх до створення «прозорих» алгоритмів ще до моменту офіційного прийняття аналога європейського AI Act в Україні. Таким чином, сучасний стан українського регулювання характеризується поєднанням довгострокового стратегічного планування із гнучкими інструментами

саморегулювання, що дозволяє створювати безпечне інноваційне середовище без надмірного адміністративного тиску на початкових етапах [3, с. 4].

Українська стратегія регулювання штучного інтелекту, презентована Міністерством цифрової трансформації України у 2023–2024 роках, базується на унікальному підході «знизу-вгору» (bottom-up approach), що має на меті підготувати бізнес та державний сектор до майбутніх жорстких обмежень без передчасного пригнічення інноваційного потенціалу. Ключовим стратегічним документом у цьому контексті стала «Біла книга з регулювання ШІ в Україні», яка визначає поетапний план дій на шляху до повної гармонізації з EU AI Act [2, с. 12]. На першому етапі, що триває наразі, держава фокусується на методологічній підтримці та саморегулюванні: розробці добровільних кодексів поведінки для розробників, запровадженні маркування систем ШІ та створенні «регуляторних пісочниць» (regulatory sandboxes) для тестування інтелектуальних рішень у контрольованому середовищі. Такий підхід дозволяє національним компаніям поступово адаптувати свої архітектури до європейських стандартів прозорості та безпеки, уникаючи шокової регуляторної дії [2, с. 12].

Дорожня карта регулювання передбачає поступову трансформацію «м'яких» етичних рекомендацій у нормативні акти, що дзеркально відображають структуру європейського Регламенту. Зокрема, Україна планує впровадити аналогічну чотирирівневу класифікацію ризиків, де особлива увага приділятиметься системам високого ризику, що використовуються в державному управлінні та судовій системі. Важливим аспектом «Білої книги» є акцент на створенні національного органу нагляду, який би координував свою діяльність із Європейським офісом ШІ, забезпечуючи безперешкодний доступ українських ІТ-продуктів на ринок ЄС. Це стратегічне планування свідчить про те, що Україна розглядає регулювання ШІ не лише як юридичне зобов'язання кандидата на вступ до ЄС, а й як інструмент цифрової дипломатії, що дозволяє інтегруватися в єдиний європейський цифровий ринок (Digital Single Market) на паритетних засадах [2, с. 15].

Критичний аналіз дорожньої карти також виявляє специфічні виклики, пов'язані з умовами воєнного стану, де використання ШІ в оборонній сфері та сфері

безпеки потребує особливих правових режимів, які часто виходять за межі цивільного EU AI Act. Проте, загальний вектор залишається незмінним: Україна обирає шлях випереджальної адаптації, коли нормативна база готується заздалегідь, щоб у момент вступу до ЄС національна екосистема ШІ вже була повністю сумісною з європейськими вимогами щодо прозорості, підзвітності та нагляду з боку людини. Таким чином, «Біла книга» є не просто декларацією, а детальним інженерним планом побудови безпечного цифрового простору, де інновації розвиваються у межах чітких етико-правових координат [2, с. 10].

Процес імплементації положень Регламенту ЄС про штучний інтелект у правову систему України виходить далеко за межі простої трансляції тексту документа, вимагаючи глибокої адаптації національних правових інститутів до специфіки алгоритмічного управління. Однією з ключових проблем є розбіжність у концептуальних підходах до суб'єктності та відповідальності. В українському цивільному та адміністративному праві категорія «відповідальності без вини» або деліктної відповідальності за дії автономних систем залишається недостатньо розробленою, що створює ризик правового вакууму у разі завдання шкоди системами ШІ. Адаптація EU AI Act потребує не лише впровадження технічних стандартів, а й внесення змін до Цивільного кодексу України та релевантних дотичних законодавчих актів з метою чіткого розмежування відповідальності між розробником, постачальником та кінцевим користувачем інтелектуальної системи [23, ст. 1166].

Важливим аспектом адаптації є гармонізація процесуального законодавства. Вимоги EU AI Act щодо «пояснюваності» та «прозорості» систем високого ризику безпосередньо корелюють із засадами змагальності та відкритості судового процесу в Україні [27, с. 6]. Проте існуючі норми ЦПК та КПК України не містять спеціальних правил щодо оцінки доказів, сформованих або оброблених ШІ, що може призвести до оскарження таких доказів через їхню «непрозорість» [24, ст. 76; 13, ст. 84]. Перспективи вирішення цієї проблеми полягають у запровадженні інституту обов'язкового технічного аудиту та сертифікації алгоритмів, що використовуються в правоохоронних органах, за аналогією з європейськими стандартами оцінки відповідності. Це дозволить створити презумпцію надійності для сертифікованих

систем, одночасно залишаючи за сторонами право на експертне дослідження логіки алгоритму.

Крім того, серйозним викликом є інституційна спроможність. Створення національного органу нагляду за ШІ, як того вимагає європейська модель, потребує не лише значних фінансових ресурсів, а й підготовки нового класу державних службовців - «цифрових регуляторів», здатних здійснювати аудит складних нейронних мереж. Україна має потенціал стати регіональним лідером у тестуванні ШІ-рішень через механізм «регуляторних пісочниць», однак це вимагає чіткого законодавчого закріплення правового режиму таких експериментів, щоб інновації не виходили за межі етичних запобіжників. Таким чином, адаптація EU AI Act є не просто технічним завданням, а стратегічним викликом для української юриспруденції, успіх якого залежатиме від здатності законодавця поєднати стимулювання ІТ-сектору із безкомпромісним захистом фундаментальних прав людини [27, с. 15].

Поряд із загальнодержавними стратегіями, особливої уваги заслуговує практична імплементація технологій у вертикаль судової влади. Важливим кроком на шляху до технологічної модернізації судової влади стала Концепція побудови та функціонування Єдиної судової інформаційно-комунікаційної системи (ЄСІКС) в новій редакції 2024 року [9, розд. 2]. Цей документ визначає архітектурну основу для впровадження сервісів підсистеми «Електронний суд», де ШІ розглядається як інструмент для автоматизації рутинних процесів: від класифікації вхідної кореспонденції до інтелектуального пошуку судової практики. Проте, технологізація правосуддя чітко обмежена етичними рамками, закладеними в Кодексі суддівської етики. Зокрема, стаття 16 Кодексу наголошує, що незалежність судді є прерогативою, яку не може похитнути використання будь-яких технологічних засобів; суддя повинен здійснювати правосуддя неупереджено, а інтелектуальні системи можуть лише підтримувати процес прийняття рішення, не заміщуючи собою волевиявлення та дискрецію людини [7, ст. 16].

Паралельно з судовою системою, цифрові трансформації охоплюють і державну службу. Національним агентством з питань державної служби були

розроблені Поради з відповідального використання штучного інтелекту публічними службовцями [15, с. 3]. У них акцентується увага на принципах «алгоритмічної обережності», прозорості та обов'язкової перевірки результатів, згенерованих ШІ, перед їх використанням у державно-управлінських рішеннях. Такий підхід корелює із загальним курсом держави на забезпечення того, щоб цифрові помічники не ставали джерелом помилок чи дискримінації. Таким чином, впровадження ШІ в українському державному секторі відбувається через призму професійної відповідальності, де технологія розглядається як сервісна функція, що підпорядковується етичним стандартам державної служби та незалежності правосуддя

Формування безпечної екосистеми штучного інтелекту в Україні значною мірою залежить від ефективності координації між державними органами, експертним середовищем та приватним сектором. Ключовим інституційним флагманом цього процесу виступає Міністерство цифрової трансформації України, яке виконує роль головного методолога та розробника регуляторної політики. Важливим елементом архітектури управління є Експертний комітет з питань розвитку сфери штучного інтелекту при Мінцифри, до складу якого входять провідні науковці, юристи та представники ІТ-індустрії. Саме цей консультативно-дорадчий орган забезпечує професійну експертизу законопроектів та готує рекомендації щодо етичного використання ШІ, що дозволяє державі приймати збалансовані рішення, які враховують як потреби безпеки, так і динаміку технологічного ринку [2, с. 10].

Особливе місце в українській моделі регулювання посідає концепція саморегулювання бізнесу через впровадження етичних кодексів. З огляду на те, що повна імплементація EU AI Act потребує часу, українським компаніям пропонується добровільне приєднання до «Загальних принципів етики ШІ», розроблених на основі стандартів ОЕСР та ЮНЕСКО [3, с. 7]. Такі кодекси слугують інструментом «м'якого» контролю, де розробники зобов'язуються забезпечувати прозорість своїх алгоритмів та проводити внутрішню оцінку ризиків для прав людини ще до моменту законодавчого примусу. Це сприяє формуванню культури «відповідальних

інновацій», де етика стає конкурентною перевагою на міжнародному ринку, а не просто регуляторним тягарем.

Крім того, розвиток національної екосистеми передбачає створення спеціалізованих центрів компетенцій та сертифікаційних лабораторій, які в майбутньому здійснюватимуть технічну перевірку систем високого ризику на відповідність державним та міжнародним стандартам (ISO/IEC) [10, розд. 1; 53, с. 10; 55, с. 8]. У контексті правової системи це означає посилення ролі Національної академії правових наук та провідних юридичних ВНЗ у підготовці кадрів, здатних здійснювати кваліфікований правовий аудит ШІ-систем. Таким чином, роль національних інституцій в Україні трансформується від суто контролюючих функцій до функцій фасилітації та підтримки, де держава створює «правила гри», а професійна спільнота забезпечує їх наповнення етичним змістом та технічною якістю.

Окремим вектором розвитку вітчизняного регулювання є формування професійних стандартів для юридичної спільноти. Міністерством цифрової трансформації були розроблені Рекомендації з відповідального використання штучного інтелекту для правників, які акцентують увагу на тому, що ШІ не звільняє юриста від обов'язку дотримання адвокатської таємниці та персональної відповідальності за якість правової допомоги [19, с. 5]. У цих рекомендаціях підкреслюється, що використання генеративних моделей для підготовки процесуальних документів вимагає ретельної верифікації на предмет «галюцинацій» алгоритму та фальсифікації нормативної бази. Це корелює з ширшим правовим контекстом захисту інформації: згідно зі статтею 8 Закону України «Про захист персональних даних», кожна особа має право на захист від автоматизованого рішення, яке має для неї юридичні наслідки [17, ст. 8]. Це положення корелює з положеннями статті 22 європейського GDPR і виступає ключовим запобіжником проти безконтрольного використання ШІ у сферах, де зачіпаються права і свободи громадян [45, ст. 22].

Не менш важливим аспектом адаптації українського права до викликів ШІ є сфера інтелектуальної власності. Закон України «Про авторське право і суміжні права» (стаття 33) запровадив інноваційну норму про право особливого роду (*sui*

generis) на неохоронювані об'єкти, згенеровані комп'ютерною програмою [16, ст. 33]. Згідно з цією нормою, результати роботи ШІ не визнаються об'єктами авторського права у класичному розумінні (оскільки відсутній творчий внесок людини), проте вони отримують специфічний правовий режим охорони, що дозволяє суб'єктам господарювання юридично закріплювати свої інтереси щодо використання таких продуктів. Таким чином, українське законодавство вже зараз пропонує точкові, але дієві механізми вирішення конфліктів, що виникають на перетині технологій та права, створюючи надійне підґрунтя для подальшої повної імплементації Регламенту ЄС про штучний інтелект.

Підсумовуючи аналіз сучасного стану та перспектив правового регулювання штучного інтелекту в Україні, слід зазначити, що держава обрала стратегічно виважену модель «м'якої адаптації», яка базується на поетапному переході від добровільних етичних стандартів до обов'язкового гармонізованого законодавства. Розроблена Міністерством цифрової трансформації «Біла книга» та відповідна дорожня карта створюють унікальний для постсоціалістичних правових систем механізм «випереджального регулювання», що дозволяє національному ІТ-сектору інтегруватися в європейський цифровий простір ще до моменту офіційного набуття повноправного членства в ЄС [2, с. 20]. Наразі ключовим викликом для України залишається не стільки копіювання норм EU AI Act, скільки розробка власних процесуальних та деліктних запобіжників, які б дозволили ефективно використовувати ШІ в судах та правоохоронних органах без ризику порушення конституційних прав громадян та чинного законодавства.

Перспективи розвитку українського законодавства нерозривно пов'язані з розбудовою інституційної спроможності, а саме створенням національного наглядового органу та мережі сертифікаційних лабораторій, що забезпечуватимуть технічний аудит алгоритмів. Важливим висновком є те, що успіх цифрової трансформації правової системи в Україні залежатиме від синергії між державним регулюванням та професійним саморегулюванням бізнесу, де етичні кодекси та «регуляторні пісочниці» слугують полігоном для відпрацювання безпечних моделей взаємодії людини та машини. Таким чином, Україна демонструє здатність не лише

покладатись на європейські стандарти, а й адаптувати їх до специфічних умов воєнного стану та активного розвитку мілітарі-технологій, закладаючи фундамент для формування сучасної, безпечної та інноваційної правової екосистеми [21, с. 12].

ВИСНОВОК ДО РОЗДІЛУ 2

Проведений у другому розділі комплексний аналіз нормативно-правового ландшафту дозволяє сформулювати цілісне бачення сучасної архітектури регулювання штучного інтелекту, що базується на трьох ієрархічних рівнях: глобальному, регіональному та національному. З основних результатів аналізу важливо відмітити, що світова спільнота успішно подолала етап регуляторної невизначеності, сформувавши в межах ООН, ОЕСР та Ради Європи стійкий етико-правовий консенсус у форматі «м'якого права» [39, с. 2; 64, с. 5; 80, с. 3]. Даний консенсус ґрунтується на парадигмі «людиноцентричного ШІ», де технологічна ефективність завжди підпорядкована вимогам захисту фундаментальних прав людини, прозорості алгоритмів та невід'ємності людського контролю в юридично значущих процесах.

Визначальним етапом переходу від базових етичних принципів у жорсткі імперативні норми стало ухвалення Регламенту ЄС про штучний інтелект (EU AI Act) [27, ст. 1]. Доведено, що запроваджений у ЄС ризико-орієнтований підхід є найбільш прогресивною моделлю цифрового конституціоналізму, яка дозволяє диференціювати правовий вплив залежно від ступеня загрози системи для суспільства. Особливе значення для сфери правосуддя має віднесення судових та правоохоронних ШІ-систем до категорії «високого ризику», що вимагає від них відповідності суворим стандартам якості даних, кібербезпеки та обов'язкової «пояснюваності» (explainability) результатів для кінцевого споживача. Завдяки «Брюссельському ефекту» ці норми де-факто стають глобальними, визначаючи вектор розвитку технологічного права в усьому світі [31, с. 145].

Аналіз локального контексту свідчить про те, що Україна обрала шлях активної гармонізації свого правового поля з європейськими стандартами. Розробка «Білої книги» та поетапна дорожня карта впровадження регулювання демонструють

здатність національної правової системи до випереджальної адаптації (proactive adaptation) [2, с. 22]. Встановлено, що ключовим викликом для України є не лише технічна імплементація норм EU AI Act, а й оновлення матеріального та процесуального права для вирішення питань деліктної відповідальності та доказової сили алгоритмічних висновків. Створення національної системи нагляду та розвиток культури професійної етики через саморегулювання бізнесу є необхідними умовами для побудови безпечної екосистеми ШІ.

Таким чином, результати другого розділу підтверджують, що правове регулювання ШІ еволюціонує в напрямку створення інтелектуального правопорядку, де технологія обмежена чіткими правовими та етичними кордонами. Це створює надійний нормативний фундамент для переходу до Розділу 3, де буде детально проаналізовано практичні аспекти впровадження ШІ безпосередньо в діяльність судових органів України та світу, з оцінкою конкретних кейсів, ризиків та перспектив цифрового правосуддя.

РОЗДІЛ 3.

РИЗИКИ, ВИКЛИКИ ТА СТРАТЕГІЧНІ НАПРЯМИ ВДОСКОНАЛЕННЯ МЕХАНІЗМІВ РЕГУЛЮВАННЯ ІІІ ТА ПРАКТИК ВИКОРИСТАННЯ ІІІ В ПРАВНИЧІЙ ДІЯЛЬНОСТІ

3.1. Основні правові ризики застосування ІІІ в правозастосовній діяльності

Третій розділ магістерської роботи присвячений критичному аналізу практичної площини впровадження штучного інтелекту, де технологічні можливості стикаються з реальними правовими та етичними бар'єрами. Якщо попередні розділи заклали теоретичний та нормативний фундамент, то цей розділ спрямований на деконструкцію ризиків, які виникають під час безпосереднього застосування алгоритмів у правозастосовній діяльності. Перехід до «Права 4.0» потребує не лише автоматизації, а й створення стійких механізмів захисту від алгоритмічних помилок, які можуть мати незворотні наслідки для прав людини та стабільності правопорядку [38, с. 24].

Послідовність аналізу в розділі побудована за принципом «від виявлення загроз до формування стратегії захисту». У підрозділі 3.1 класифікуються основні правові ризики - від порушення конфіденційності до загрози суддівській незалежності. Підрозділ 3.2 фокусується на емпіричному аналізі конкретних випадків неправомірного використання ІІІ, що вже стали прецедентами у світовій практиці, дозволяючи виявити типові причини та наслідки «алгоритмічної недбалості». На завершення, у підрозділі 3.3 аналізуються успішні практики використання ІІІ та надається розробка ефективних системних запобіжників та механізмів контролю за діяльністю постачальників і користувачів систем ІІІ. Це дозволить запропонувати цілісну концепцію безпечної інтеграції ІІІ в правову систему України з урахуванням європейських стандартів підзвітності.

Інтеграція систем штучного інтелекту в правозастосовну практику, попри очевидні переваги в швидкості та аналітичній потужності, створює комплекс

специфічних правових ризиків, що можуть деформувати класичні принципи судочинства та державного управління. Основна небезпека полягає в тому, що ШІ не просто автоматизує процеси, а стає активним учасником формування правових позицій, часто діючи в межах «чорної скриньки», логіка якої залишається недоступною для перевірки учасниками процесу [66, с. 55]. Актуальність аналізу цих ризиків зумовлена необхідністю завчасного створення правових запобіжників, які б не дозволили технологічному прогресу нівелювати засади верховенства права та справедливого суду.

Метою цього підрозділу є ідентифікація та систематизація ключових правових ризиків, що виникають при використанні ШІ в судах, правоохоронних органах та адвокатській діяльності. В роботі проаналізовано ризики порушення фундаментальних прав людини (зокрема, права на приватність та захист даних), загрози незалежності суддівського розсуду через надмірну довіру до алгоритмічних підказок, а також проблему «алгоритмічної дискримінації», яка впливає з упередженості навчальних вибірок. Розуміння природи цих ризиків є критично важливим для розробки національних стандартів безпечного використання ШІ в Україні, що відповідатимуть вимогам європейського Регламенту (EU AI Act) [27, ст. 1].

Використання штучного інтелекту в правозастосовній діяльності створює системні загрози для фундаментальних прав, насамперед через специфіку обробки великих масивів даних (Big Data) [83, с. 625]. Головним ризиком у цій сфері є порушення права на приватність та захист персональних даних. Оскільки навчання алгоритмів потребує доступу до реальних судових справ та матеріалів розслідувань, виникає небезпека деанонізації учасників процесу навіть за умови використання методів знеособлення. У контексті адвокатської діяльності використання хмарних ШІ-сервісів (наприклад, для аналізу документів) створює пряму загрозу адвокатській таємниці, оскільки дані передаються на сервери третіх сторін (провайдерів ШІ), що може призвести до їхнього несанкціонованого витоку або використання для перенавчання моделей [45, с. 1].

Не менш критичним є ризик порушення права на належну правову процедуру (due process) та права на справедливий суд [4, ст. 6]. Згідно з європейськими стандартами, кожна особа має право на мотивоване рішення, прийняте людиною. Однак, як обґрунтовує Ф. Паскуале, використання непрозорих алгоритмів через ефект «чорної скриньки» унеможлиблює для сторін спору розуміння того, на підставі яких саме критеріїв ШІ сформував ту чи іншу рекомендацію чи висновок [66, с. 55; 47, с. 52]. Це обмежує право на захист, оскільки адвокат не може ефективно оскаржити логіку алгоритму, якщо вона є закритим корпоративним секретом розробника. Такий стан справ створює процесуальну нерівність та ставить під сумнів легітимність будь-якого судового акта чи процесуального рішення, сформованого за підтримки ШІ.

Крім того, існує специфічний ризик порушення таємниці нарадчої кімнати. Якщо суддя використовує цифрового асистента для автоматичної генерації проекту рішення, виникає питання: чи не є це формою стороннього втручання в процес формування внутрішнього переконання?. В українських реаліях, де незалежність суду є конституційною цінністю, відсутність чітких меж між «технічною допомогою» та «інтелектуальним впливом» системи ШІ може стати підставою для масового оскарження рішень через порушення процедури їх прийняття. Таким чином, правові ризики в цій сфері вимагають не лише технічних рішень (шифрування, локальні сервери), а й оновлення процесуальних кодексів для гарантування права на «людський аудит» кожного алгоритмічного кроку та захисту балансу інтересів всіх сторін судового процесу.

Згідно з дослідженнями Р. Парасурамана, одним із найбільш підступних ризиків інтеграції ШІ в суди є «когнітивна упередженість автоматизації» (automation bias) - психологічна схильність судді чи правоохоронця беззастережно довіряти висновкам алгоритму, сприймаючи їх як об'єктивну істину [65, с. 385]. У правозастосовній діяльності це призводить до ерозії суддівського розсуду. Замість глибокого аналізу унікальних обставин справи, суддя може стати простим «верифікатором» рішення, яке вже підготувала машина. Такий підхід загрожує перетворенням правосуддя на механічний процес, де втрачається здатність

враховувати етичні нюанси та принципи справедливості, що не піддаються математичному моделюванню.

Як наголошує С. Вахтер, критичне значення має ризик «алгоритмічної дискримінації» [68, с. 3; 81, с. 14]. Оскільки системи ШІ навчаються на масивах історичних судових рішень, вони мимоволі вбирають у себе всі системні помилки та упередження минулого. Якщо в минулому певні соціальні групи піддавалися більш жорсткому переслідуванню, ШІ екстраполює цю тенденцію в майбутнє, створюючи замкнене коло несправедливості під маскою нейтральної статистики. Це прямо суперечить принципу неупередженості суду, оскільки алгоритм може приховано дискримінувати особу за ознаками, які формально не враховуються, але корелюють з іншими параметрами (наприклад, поштовий індекс або рівень доходу) [68, с. 3; 81, с. 14].

Крім того, виникає загроза інституційній незалежності суду. Якщо алгоритми розробляються приватними компаніями або виконавчою владою (наприклад, через Мінцифри), виникає ризик регуляторного захоплення контролю. Суддя, стаючи залежним від програмного забезпечення, логіка якого контролюється іншою гілкою влади або корпоративним сектором, втрачає свою автономію. У перспективі це може призвести до ситуації, коли правосуддя де-факто здійснюватиметься не за законом, а за внутрішніми специфікаціями коду, який не пройшов демократичного обговорення та прийняття. Таким чином, захист суддівського розсуду від диктату алгоритму стає ключовим завданням для збереження суті правової держави в епоху цифровізації.

Більше того, як зазначає М. Шерер, впровадження ШІ у правозастосовну практику створює гостру проблему розподілу юридичної відповідальності (liability gap) [61, с. 177; 73, с. 360]. Традиційні правові інститути ґрунтуються на доведенні вини людини, проте у випадку з автономними системами нюанс, адже розробник може стверджувати, що система сама навчилася і видала непередбачуваний результат, а користувач (юрист чи суддя) натомість може скинути відповідальність, заявивши, що він лише покладався на сертифіковану технологію. Ризик полягає у виникненні ситуацій безвідповідальної шкоди, коли через помилку алгоритму у розрахунках строків або аналізі даних сторона зазнає несправедливого ставлення, але

не може притягнути до відповідальності жодного іншого суб'єкта правового процесу [61, с. 177; 73, с. 360].

Окремим блоком стоять ризики інтелектуальної власності. При навчанні юридичних ШІ-моделей часто використовуються авторські методики аналізу, бази даних приватних власників або навіть конфіденційні тексти процесуальних документів. Виникає ризик неправомірного використання об'єктів авторського права для тренування комерційних моделей без згоди правовласників, особливо якщо мова йде про ШІ моделі, що використовують будь-які дані з відкритого доступу [70, с. 12].

Нарешті, існує ризик «технологічної залежності» (vendor lock-in) [51, с. 210]. Держава або великі юридичні фірми, інтегруючи пропрієтарні алгоритми (власність приватних корпорацій) у свої внутрішні системи, ризикують втратити суверенітет над власними даними та процесами. Якщо розробник змінить алгоритм або припинить підтримку, правозастосовна діяльність може бути паралізована. Наслідком цих ризиків є необхідність переходу від моделі «відповідальності за вину» до моделі «суворої відповідальності» постачальників ШІ високого ризику, що передбачено в EU AI Act і має бути адаптовано в українське законодавство для захисту кінцевих користувачів [27, с. 12; 28, ст. 4].

Окрім технічних та процесуальних загроз, масове впровадження ШІ несе в собі латентний ризик інтелектуального збіднення правової системи. Право - це жива матерія, що розвивається через творче тлумачення норм та адаптацію до нових суспільних відносин. Використання ШІ, який орієнтований на ретроспективний аналіз минулої практики аналіз, може призвести до доктринального застою. Алгоритм завжди пропонуватиме найбільш статистично ймовірний варіант вирішення спору, що значно зменшує можливість виникнення нових прецедентів та еволюційних змін у праві і призводить до поступової стагнації розвитку права, як динамічної системи. Ризик полягає у формуванні замкненого кола правозастосування, де майбутні рішення стають копіями минулих, а право втрачає здатність адекватно реагувати на динамічні зміни в суспільстві [25, с. 276].

Іншим аспектом є ризик професійної деградації юристів та суддів. Надмірна автоматизація процесів збору доказів, підготовки позовів та проектів судових актів

призводить до атрофії навичок критичного мислення та глибокого правового аналізу. Для молодих правників виникає загроза втрати здатності самостійно вибудовувати складні логічні конструкції, оскільки ІІІ пропонує готові шаблони, а юристи з проактивних діячів перетворюються скоріше на пасивних клерків, зосереджених на обробці роботи ІІІ систем. У правозастосовній діяльності це може призвести до появи юристів-операторів, які здатні керувати програмою, але не можуть досягнути дух закону або розпізнати тонку маніпуляцію в аргументах протилежної сторони, що крім всіх інших негативних наслідків ще й підриває інституційну цінність юридичної освіти для здобуття даної професії [25, с. 30].

Крім того, існує ризик втрати емпатичного складника правосуддя. Правозастосування, особливо у сімейних, кримінальних чи трудових спорах, вимагає врахування морально-етичного контексту, який неможливо оцифрувати. ІІІ позбавлений емоційного інтелекту та почуття справедливості, що може призвести до винесення формально законних, але соціально несправедливих рішень. Це створює загрозу легітимності судової влади в очах суспільства, оскільки громадяни очікують від суду захисту своєї гідності, а не просто сухої обробки даних. Таким чином, як зауважує М. Гільдебрандт, стратегічним ризиком є перетворення права з мистецтва доброго і справедливого (*ars boni et aequi*) на суто технічний сервіс з обробки запитів. [51, с. 45]

Впровадження ІІІ в правозастосовну діяльність створює нові вектори кіберзагроз, які можуть підірвати цілісність правосуддя. Основним ризиком у цьому контексті є здійснення прямих атак (*adversarial attacks*), серед яких особливе місце посідає «отруєння даних» (*data poisoning*) - навмисне внесення неправдивої або маніпулятивної інформації в навчальні вибірки ІІІ [36, с. 10; 36, с. 12]. Такі атаки спрямовані на компрометацію цілісності моделі, що призводить до створення системою завідомо некоректних, упереджених або контрпродуктивних результатів, які зовні можуть виглядати переконливо, але фактично спотворюють правову логіку. Якщо зловмисники можуть вплинути на дані, на яких навчається судова аналітика, система почне видавати викривлені рекомендації, що може призвести до системних помилок у вироках або рішеннях відповідальних осіб. Це створює загрозу не лише

конкретним справам, а й національній безпеці, оскільки правосуддя стає вразливим до зовнішніх технологічних диверсій [36, с. 10].

З цих самих міркувань окремої уваги заслуговує проблема цифрового суверенітету. Використання іноземних пропрієтарних алгоритмів (наприклад, розробок великих технологічних корпорацій США чи Китаю) у державних судах створює залежність правової системи від геополітичних інтересів та технічних регламентів інших держав. У разі припинення підтримки або введення санкцій, критичні елементи електронного судочинства можуть бути паралізовані. Крім того, зберігання чутливої юридичної інформації (матеріалів кримінальних проваджень, таємниці слідства) на серверах іноземних провайдерів створює ризик несанкціонованого доступу іноземних спецслужб до стратегічних даних України, особливо в умовах постійно наявної загрози технологічних диверсій та шпіонажу з боку росії [25, с. 22].

Нарешті, як попереджають дослідники Р. Чесней та Д. Сітрон, існує ризик направлених атак на системи розпізнавання образів чи голосу, що використовуються в судах. Зловмисники можуть використовувати ШІ для створення ідеальних підробок (Deepfakes), які неможливо розпізнати стандартними засобами експертизи, що ставить під загрозу інститут доказування [35, с. 1755; 36, с. 10]. Без створення власної захищеної інфраструктури та сертифікованих національних алгоритмів, правозастосовна діяльність ризикує стати об'єктом маніпуляцій, що нівелює будь-які переваги від автоматизації. Таким чином, кібер загрози вимагають від держави переходу до концепції «безпечного ШІ за замовчуванням» (Secure AI by Design), де технологічний суверенітет є невід'ємною частиною правової незалежності [48, с. 5].

Комплексний аналіз правових ризиків впровадження штучного інтелекту в правозастосовну діяльність дозволяє констатувати, що технологічна трансформація юстиції несе в собі не лише інноваційний потенціал, а й фундаментальні загрози класичній архітектурі права. Встановлено, що ключовою проблемою є цифрова деформація конституційних гарантій: від ризику порушення приватності та адвокатської таємниці через неконтрольовану обробку даних до загрози праву на справедливий суд через непрозорість алгоритмічних «чорних скриньок». Особливу

небезпеку становить корозія суддівського розсуду, коли психологічна довіра до машинної об'єктивності призводить до автоматизації дискримінаційних практик, закладених у недосконалі навчальні вибірки.

Ризики використання ШІ виходять за межі технічних помилок, охоплюючи рівень правової доктрини та професійної етики. Загроза доктринального застою та професійної деградації правничої спільноти через надмірну експлуатацію ретроспективних алгоритмів ставить під удар здатність права еволюціонувати. Крім того, в умовах глобальних кіберзагроз та воєнного стану, питання цифрового суверенітету та захисту від маніпуляцій даними та шпіонажу стають невід'ємною частиною національної безпеки у сфері правосуддя [25, с. 30].

Таким чином, правові ризики застосування ШІ є багаторівневими та потребують не точкових правок, а системного оновлення процесуального законодавства та деонтологічних норм. Розуміння цих загроз дозволяє перейти від теоретичного висвітлення основних загроз ШІ до емпіричного аналізу в підрозділі 3.2, де на прикладі конкретних випадків досліджено, як саме ці ризики реалізуються на практиці та до яких правових наслідків призводить нехтування стандартами безпеки.

3.2. Аналіз причин та наслідків актуальних випадків неправомірного застосування систем ШІ

Практична реалізація систем штучного інтелекту в правозастосовній діяльності вже накопичила критичну масу негативних прецедентів, що дозволяють перейти від гіпотетичних побоювань до об'єктивного аналізу помилок. Неправомірне застосування ШІ в судах та адвокатурі США, ЄС та Китаю продемонструвало, що технологічна недосконалість у поєднанні з низькою цифровою грамотністю правників створює загрозу винесення завідомо неправосудних рішень та фальсифікації доказів. Актуальність цього аналізу полягає у виявленні причинно-наслідкових зв'язків між алгоритмічними збоями та порушенням процесуальних норм, що є необхідною умовою для формування майбутньої стратегії безпеки.

Метою підрозділу є окреслення факторів, що призводять до зловживань або помилок при використанні ШІ, та оцінка їхнього впливу на правопорядок. Фокус підрозділу зосереджено на аналізі резонансних кейсів, де ШІ виступав інструментом дискримінації або джерелом недостовірної інформації, а також дослідженні юридичної відповідальності осіб, які допустили алгоритмічну недбалість, та оцінці репутаційних та правових наслідків для судової системи загалом. Такий емпіричний підхід при дослідженні правильних методів імплементації ШІ дозволяє Україні уникати повторення чужих помилок при розбудові власних систем сучасного цифрового правосуддя.

Найбільш резонансним випадком неправомірного та необережного використання ШІ, що призвів до реальних процесуальних наслідків, стала справа *Mata v. Avianca (2023)* у Федеральному окружному суді Південного округу Нью-Йорка [60, с. 2]. Адвокат Стівен Шварц, намагаючись підготувати заперечення проти клопотання про закриття справи, скористався ChatGPT для пошуку судової практики. Система згенерувала переконливу відповідь, посилаючись на шість судових прецедентів (наприклад, *Varghese v. China Southern Airlines Co Ltd*), які містили детальні цитати та правильну структуру [60, с. 4]. Однак під час перевірки судом та опонентами з'ясувалося, що жодної з цих справ не існує в природі, натомість вони були повністю вигадані алгоритмом, що є класичним прикладом «юридичної галюцинації».

Причини інциденту:

1. Технологічна неписьменність: Адвокат сприймав чат-бот як пошукову систему (на кшталт Google або Westlaw), не розуміючи, що LLM-моделі працюють за принципом статистичного прогнозування наступного слова, а не перевірки фактів [33, с. 4; 60, с. 5].
2. Надмірна довіра: Відсутність елементарної верифікації посилань через офіційні реєстри, навіть після того, як суддя висловив сумнів у автентичності справ [65, с. 388].

3. Етичний розрив: Делегування інтелектуальної функції написання правового документа машині без належного нагляду та дотримання принципу human-in-the-loop [41, с. 12; 44, с. 4].

Наслідки для правової системи:

- Процесуальні санкції: Суддя Кевін Кастел наклав на адвокатів та їхню фірму штраф у розмірі 5000 доларів, проте репутаційні збитки виявилися значно вищими [60, с. 8].
- Прецедент відповідальності: Суд чітко постановив, що використання ШІ не є правопорушенням саме по собі, але подання суду неіснуючих посилань через ШІ є «дією в недобросовісній манері» (bad faith), що прирівнюється до фальсифікації [60, с.6].
- Системні зміни: Після цього кейсу сотні федеральних суддів США видали «Накази щодо використання штучного інтелекту» (Standing Orders on AI), які зобов'язують юристів підписувати сертифікат про те, що жодна частина документа не була створена ШІ без перевірки людиною [44, с. 3].

Цей випадок довів, що ШІ у руках непідготовленого правника стає інструментом дезінформації, який підриває авторитет правосуддя. Наслідком стало формування нової юридичної доктрини «технологічної компетентності», згідно з якою юрист зобов'язаний розуміти ризики інструментів, які він використовує.

Не менш резонансним прикладом неправомірного впливу ШІ на долю людини у кримінальному процесі є використання системи COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) у США [59, с. 2]. Цей алгоритм призначений для оцінки ризику рецидиву та надання рекомендацій суддям щодо обрання запобіжного заходу або міри покарання[59, с. 1]. У справі *State v. Loomis (2016)* підсудний оскаржив використання звіту COMPAS, стверджуючи, що врахування алгоритмічних балів порушує його право на належну правову процедуру, оскільки методика розрахунку є комерційною таємницею компанії Northpointe [59, с. 4].

Причини виникнення дискримінації:

1. «Брудні» історичні дані (Data Bias): Алгоритм навчався на статистиці арештів минулих років. Оскільки правоохоронна система США історично частіше патрулювала райони з переважно афроамериканським населенням, статистика зафіксувала більше арештів саме в цій групі. ШІ сприйняв це не як соціальний фактор, а як математичну закономірність [68, с. 5].
2. Проблема «чорної скриньки»: Суддя та сторони процесу отримували лише фінальний бал ризику (від 1 до 10), не маючи можливості перевірити, які саме фактори (місце проживання, освіта, дохід) вплинули на результат. Це унеможливлювало ефективне спростування висновку [66, с. 55].

Наслідки для правозастосування:

- Системна несправедливість: Дослідження ProPublica виявило, що COMPAS у два рази частіше помилково позначав афроамериканців як «високоризикових» порівняно з білими правопорушниками [68, с. 6]. Наслідком цього стали нерівні умови для отримання дострокового звільнення.
- Обмеження використання: Верховний суд штату Вісконсин, хоч і дозволив використання COMPAS, встановив жорстке обмеження: бали ШІ не можуть бути вирішальним фактором при винесенні вироку і повинні супроводжуватися попередженням про можливу упередженість алгоритму [59, с. 12].
- Етичний стандарт: Цей кейс заклав основу для вимоги «алгоритмічної прозорості» в EU AI Act, забороняючи використання систем оцінки ризиків у судах, якщо їхня логіка не може бути пояснена [27, ст. 13].

Кейс COMPAS продемонстрував, що неправомірне застосування ШІ може призвести до цифрового кріпацтва, де майбутнє людини визначається не її вчинками, а статистичним профілем її соціальної групи. Це змусило правові системи світу переглянути концепцію довіри до об'єктивності цифр та повернути пріоритет людському контролю.

З розвитком генеративного ШІ судова система зіткнулася з новим викликом «дідфейків», які дозволяють створювати гіперреалістичні аудіо та відео записи, що імітують поведінку або мовлення реальних осіб [35, с. 1760]. Неправомірне використання таких технологій спрямоване на пряму маніпуляцію внутрішнім

переконанням людей через подання сфальсифікованих цифрових доказів. Найбільш вразливими до таких атак виявилися сімейні спори (визначення місця проживання дитини) та корпоративні конфлікти.

Аналіз кейсів та способів маніпуляції:

1. Справа про опіку (Велика Британія, 2020): Один із батьків надав суду аудіозапис, на якому інший нібито погрожував дитині фізичною розправою. Лише глибока фоноскопична експертиза виявила, що запис був створений за допомогою ШІ-клонування голосу. Наслідком стала не лише відмова у позові, а й кримінальне переслідування за фальсифікацію доказів [35, с. 1765].
2. Шахрайство в корпоративному секторі: Як описують дослідники кіберзагроз Р. Чесні та М. Комітер, існують кейси, де за допомогою відеоконференцій, де за допомогою відеоконференцій (Deepfake-відео) зловмисники імітували керівництво компаній для санкціонування незаконних транзакцій, що згодом ставали предметом тривалих господарських судів щодо нікчемності правочинів [35, с. 1768; 36, с. 15].

Причини успішності маніпуляцій:

- Ефект реальності: Людське око та вухо більше не здатні самостійно розпізнати високоякісний фейк, що змушує суддів покладатися виключно на експертів.
- Відсутність цифрової ідентифікації: У багатьох юрисдикціях (зокрема в Україні) процедура перевірки автентичності метаданих цифрового доказу на стадії подання позову залишається недосконалою [71, с. 1980].

Наслідки для правосуддя:

- Криза довіри до цифрових доказів: Суди змушені підвищувати стандарт доказування (standard of proof), вимагаючи додаткового підтвердження для будь-якого відео чи аудіо, що не має чіткого ланцюжка володіння (chain of custody) [71, с. 1985].
- Процесуальні затримки: Необхідність призначення складних ШІ-експертиз значно подовжує строки розгляду справ та здорожчує процес для сторін.

- Право на спростування: Як обґрунтовує А. Рот у дослідженні машинного доказування, виникає потреба в «презумпції сумніву» щодо цифрових файлів, які не мають цифрового підпису або часових міток [35, с. 1770; 71, с. 1990].

Таким чином, неправомірне використання технологій Deepfakes руйнує класичну модель «побачити значить повірити». Це вимагає від законодавця термінового впровадження кримінальної відповідальності за створення неправомірних або завідомо хибних доказів та розробки державних стандартів анти-ШІ експертизи для захисту істини в судовому процесі [35, с. 1760].

Неправомірне застосування штучного інтелекту не обмежується судовою чи адвокатською діяльністю, воно охоплює ширшу сферу правозастосування, зокрема предиктивне патрулювання та автоматизацію соціальних виплат. Найбільш масштабним наслідком «алгоритмічної недбалості» в європейській практиці став кейс системи SyRI (System Risk Indication) у Нідерландах [63, с. 1]. Ця система ШІ була розроблена для аналізу великих масивів даних громадян з метою виявлення потенційних шахраїв у сфері соціального страхування. Проте у 2020 році Окружний суд Гааги визнав використання SyRI неправомірним, оскільки алгоритм демонстрував виражену соціальну упередженість. Система непропорційно часто фокусувалася на мешканцях бідних кварталів та іммігрантах, фактично створюючи для них презумпцію винуватості лише на основі їхнього соціально-економічного статусу [63, с. 10].

Причиною цього системного збою стало використання маніпулятивних критеріїв профілювання. Алгоритми предиктивної поліції та соціального моніторингу часто ідентифікують зони ризику не за реальною криміногенною ситуацією, а за частотою попередніх звернень або перевірок, що створює ефект самопідсилюваного упередження [67, с. 45]. У результаті державні органи чинили надмірний тиск на вразливі верстви населення, позбавляючи їх виплат або піддаючи додатковим обшукам без належних правових підстав. Крім того, громадяни опинилися в ситуації повної відсутності права на пояснення, а автоматизовані відмови у наданні соціальної допомоги не містили жодних змістовних обґрунтувань, що унеможливлювало їхнє ефективне оскарження в адміністративному чи судовому порядку [63, с. 10].

Наслідки використання таких систем виявилися катастрофічними для довіри до державних інститутів. Суди вказали, що тотальний збір та автоматизована обробка даних без чітко визначеної індивідуальної підозри грубо порушують статтю 8 ЄКПЛ щодо права на повагу до приватного життя [4, ст. 8; 63, с. 10]. У Нідерландах цей скандал призвів до глибокої політичної кризи та відставки уряду, продемонструвавши, що юридична та політична ціна за некоректне використання ШІ державою може бути надзвичайно високою. Цей досвід безпосередньо вплинув на формування Регламенту ЄС про штучний інтелект, у якому системи предиктивного профілювання в правоохоронній сфері були віднесені до категорії неприйняттого ризику та офіційно заборонені [27, ст. 5]. Для України цей кейс є критично важливим застереженням про те, що автоматизація правозастосування без жорсткого незалежного нагляду здатна перетворити цифрову державу на інструмент системної дискримінації, де права людини нівелюються заради ілюзорної технічної ефективності.

Окремим вектором потенційно дискусійного застосування систем штучного інтелекту є їх використання для повної або часткової автоматизації винесення судових рішень у справах, що вважаються типовими або малозначними. Це питання є вкрай актуальним, враховуючи, що така імплементація ШІ в судочинстві поступово ставатиме більш актуальною в Україні, а отже слід звертати увагу на вже наявний досвід щоб уникати негативних наслідків, з якими стикались інші країни [10, розд. 1]. Найбільш показовим у цьому контексті є досвід країн, що впровадили системи «цифрових суддів» для розгляду спорів щодо стягнення дрібних боргів або штрафів за порушення правил дорожнього руху [40, с. 670]. Причиною виникнення масових правопорушень у цій сфері став перекис у бік процесуальної швидкості на шкоду змістовній перевірці обставин справи. За результатами аналізу наявних випадків встановлено, що алгоритми часто не здатні розпізнати специфічні юридичні заперечення сторін, як-от вплив строків позовної давності або наявність обставин непереборної сили, якщо вони не подані у суворо визначеному машиною форматі. Це призводить до ситуації, коли система автоматично генерує наказ про стягнення

коштів, ігноруючи матеріальне право, що фактично позбавляє відповідача права на ефективний судовий захист ще на стадії ініціювання спору.

Наслідком такої алгоритмічної сліпоти стає лавиноподібне зростання кількості апеляційних скарг, що парадоксальним чином не зменшує, а збільшує навантаження на судову систему. У практиці деяких азійських юрисдикцій зафіксовані випадки, коли через технічну помилку в коді алгоритму тисячі рішень про стягнення були винесені з неправильним розрахунком пені або відсотків, що потребувало масового перегляду справ за нововиявленими обставинами [40, с. 670]. Окрім суто юридичних наслідків, такі випадки провокують глибоку кризу довіри до цифрового правосуддя та й системи правосуддя як такої. Громадяни країн з такими проблемами починають сприймати суд не як орган захисту прав, а як бездушний формальний інструмент, з яким неможливо вступити в правову дискусію для захисту власних прав. Це підкреслює фундаментальну проблему делегування прийняття рішень системам ШІ, оскільки вони позбавлені здатності до правової рефлексії, а будь-яка похибка в логіці масштабується на тисячі справ, створюючи системну загрозу правопорядку.

Для української правової системи цей досвід є критично важливим застереженням проти повної автоматизації навіть, на перший погляд, простих судових процедур. Аналіз причин невдач іноземних практиків доводить, що за кожним алгоритмічним проектом рішення має стояти жива верифікація суддею, який несе персональну відповідальність за кінцевий акт. Наслідки некритичного копіювання іноземних моделей «цифрових суддів» без адаптації під стандарти справедливого суду можуть призвести до колапсу наказного провадження та масових звернень громадян до Європейського суду з прав людини через порушення статті 6 ЄКПЛ [4, ст. 6]. Таким чином, деякі наслідки застосування ШІ в цій сфері доводять, що ефективність правосуддя не може вимірюватися лише кількістю закритих справ за одиницю часу, якщо при цьому втрачається якість та законність кожного окремого рішення.

Проведений аналіз міжнародної та локальних практик дозволяє констатувати, що в деяких випадках необережне застосування систем штучного інтелекту в правовій сфері перетворилося з теоретичного ризику на реальну процесуальну

загрозу. Вивчення резонансних справ, таких як *Mata v. Avianca* та *State v. Loomis*, а також збоїв у системах на кшталт *SyRI*, свідчить, що головною причиною юридичних катастроф є не стільки технічна недосконалість алгоритмів, скільки криза відповідальності користувача [59, с. 1; 60, с. 2]. Встановлено, що некритична довіра до ШІ-галюцинацій та ігнорування алгоритмічної упередженості призводять до фальсифікації доказової бази, системної дискримінації вразливих груп та руйнування стандарту належної правової процедури [63, с. 15].

Наслідки таких зловживань мають кумулятивний характер, від персональних санкцій проти адвокатів та скасування судових рішень до глобальної корозії довіри до інституту правосуддя як такого. Використання дипфейків та автоматизованих систем винесення наказів без людського контролю створює прецеденти конвеєрного правосуддя, де швидкість розгляду справ досягається ціною нівелювання якості винесених за результатами розгляду рішень. Без впровадження обов'язкового декларування використання ШІ та створення механізмів анти-ШІ експертизи, цифровізація ЄСІКС в Україні ризикує масштабувати системні помилки, перетворюючи їх на невід'ємну частину національної судової практики [9, с. 1].

Таким чином, аналіз негативного досвіду доводить, що правова система потребує не просто косметичних правок, а радикального перегляду процесуальної відповідальності за алгоритмічні дії. Це створює необхідний фактологічний фундамент для переходу до підрозділу 3.3, де на основі виявлених помилок ми сформулюємо стратегічні напрями вдосконалення механізмів контролю та розробимо систему ефективних запобіжників для постачальників і користувачів систем ШІ.

3.3. Встановлення успішних практик і переваг використання ШІ в правозастосовній діяльності та розробка ефективних запобіжників і механізмів контролю за діяльністю постачальників та користувачів систем ШІ

Завершальний етап дослідження спрямований на формування конструктивної стратегії інтеграції штучного інтелекту в правову систему України, яка б базувалася на балансі між технологічними перевагами та безпековими гарантіями. Попри

виявлені ризики та негативні прецеденти, міжнародний досвід демонструє низку успішних практик, де ШІ виступає не заміном людини, а потужним інтелектуальним підсилювачем, що підвищує доступність та ефективність правосуддя. Актуальність цього підрозділу полягає у необхідності переходу від пасивного спостереження за розвитком технологій до активного формування регуляторного середовища, здатного забезпечити ефективний та безпечний формат імплементації ШІ в правову реальність та уникнення катастрофічних наслідків, що без необхідних застережень є практично неминучими.

Метою підрозділу є систематизація позитивного досвіду використання ШІ та розробка практичних рекомендацій щодо створення надійної системи контролю. В основу дослідження взято успішні моделі автоматизації рутинних процесів (e-discovery, аналіз судової практики), які не порушують прав людини, та на основі цих позитивних практик й з урахуванням всіх ризиків запропоновано багаторівневу систему запобіжників від технічної сертифікації алгоритмів постачальників до етичних кодексів професійної діяльності юристів. Окрему увагу приділено розробці механізмів «алгоритмічного аудиту» та впровадженню принципу пояснюваності, що дозволить Україні побудувати модель розумного правосуддя, де технологія служить верховенству права, а не підміняє його.

Попри критичний аналіз ризиків, світова та національна практика демонструють низку напрямів, де використання ШІ є не лише безпечним, а й стратегічно необхідним для забезпечення права на розгляд справи в розумні строки. Першою успішною практикою є впровадження систем e-discovery та інтелектуального аналізу великих масивів документів. У складних господарських чи антикорупційних спорах, де кількість доказів вимірюється терабайтами, алгоритми машинного навчання (Predictive Coding) здатні за лічені години виявити релевантні зв'язки та аномалії, на що команді юристів знадобилися б місяці [29, с. 250]. Перевагою такої практики є радикальне зниження вартості правосуддя та мінімізація людського фактору при технічній обробці даних.

Другим вектором успіху є предиктивна судова аналітика - метод використання ШІ для прогнозування результатів судових розглядів, поведінки учасників процесу

або оцінки ризиків на основі історичних даних, що використовується для забезпечення єдності судової практики. Системи типу *LIGA360* в Україні або *Lextenso* у Франції дозволяють суддям та адвокатам миттєво знаходити релевантні правові позиції, що виключає винесення суперечливих рішень у подібних справах [6, с. 1; 58, с. 1]. Це зміцнює принцип правової визначеності та дозволяє сторонам реалістично оцінювати шанси на успіх, що стимулює розвиток інституту медіації та позасудового врегулювання спорів. Важливою перевагою тут є роль ШІ як навігатора у морі прецедентів, що не підміняє волю юриста чи судді, а лише надає йому максимально повну інформаційну базу для прийняття самостійного рішення.

Третьою групою успішних практик є автоматизація рутинної комунікації та підготовки типових документів через юридичні асистенти. Кейси використання ШІ для автоматичного розрахунку судового збору, перевірки реквізитів чи формування проектів заяв про видачу судового наказу у справах про аліменти чи комунальні борги доводять свою ефективність у зниженні бар'єрів доступу до юстиції для незахищених верств населення. У цьому контексті ШІ виконує соціальну функцію, знімаючи з судів навантаження за безспірними вимогами та дозволяючи зосередити людський ресурс на вирішенні складних правових дилем. Таким чином, успішна практика використання ШІ базується на делегуванні машині технічного інтелекту, залишаючи за людиною виключне право на ціннісне судження [25, с. 67].

Ефективний контроль за використанням ШІ у правозастосовній діяльності має починатися з етапу розробки та виведення технологічного продукту на ринок. Ключовим запобіжником тут виступає обов'язкова сертифікація та оцінка ризиків постачальників систем ШІ, що відповідає стандартам EU AI Act [27, ст. 43]. Для правових систем «високого ризику» (судова аналітика, оцінка рецидивів, автоматизація доказів) необхідно впровадити процедуру «алгоритмічного аудиту», яка передбачає перевірку репрезентативності навчальних вибірок на відсутність дискримінаційних маркерів. Згідно з дослідженням Б. Гудмана, постачальник зобов'язаний гарантувати принцип «прозорості коду» (explainability), що дозволяє юристу або судді отримати логічне пояснення того, як саме алгоритм прийшов до

конкретного висновку і тим самим мінімізувати ефект «чорної скриньки» [66, с. 55; 47, с. 52; 27, ст. 13].

Важливим механізмом контролю є впровадження стандарту «human-in-the-loop» [41, с. 12]. Це означає, що жодна система ШІ в правозастосуванні не може діяти повністю автономно, натомість архітектура програми повинна передбачати обов'язкову стадію людського схвалення перед генерацією фінального результату. Розробники мають забезпечити технічну можливість втручання людини в роботу алгоритму на будь-якому етапі (human-on-the-loop) та можливість негайного відключення системи у разі виявлення аномальної поведінки (kill switch) [27, ст. 14; 64, с. 8]. Такий підхід перекладає тягар доведення безпеки технології на її постачальника, знімаючи з користувача в юридичній професії необхідність бути псевдо програмістом для розуміння інструменту.

Крім того, стратегічним запобіжником є встановлення суворої відповідальності розробників за технічні дефекти алгоритмів, що призвели до порушення процесуальних норм або майнових збитків. Це стимулює постачальників впроваджувати системи внутрішнього моніторингу та страхування професійної відповідальності. В українському контексті доцільним є створення Державного реєстру сертифікованих юридичних ШІ-систем, використання яких дозволено в органах правосуддя. Це дозволить відсіяти сирі або небезпечні продукти ще на підступах до перших процесуальних кроків, забезпечуючи цифрову гігієну всієї правової екосистеми [52, с. 20].

Належне використання ШІ в правозастосовній діяльності вимагає від користувача (юриста, судді) дотримання принципу технологічної компетентності. Першим фундаментальним запобіжником є впровадження обов'язкового декларування використання ШІ у процесуальних документах. Це означає, що будь-яка сторона, яка використовувала генеративні моделі для підготовки позову чи аналізу доказів, повинна письмово підтвердити факт перевірки результатів людиною. Такий підхід унеможливорює анонімне втручання алгоритмів у правосуддя та дозволяє суду оцінювати достовірність матеріалів з урахуванням специфіки їх підготовки [52, с. 16].

Другим рівнем захисту є оновлення кодексів професійної етики. Юрист не має права посилатися на помилку алгоритму як на обставину, що звільняє від відповідальності. Встановлюється стандарт «алгоритмічної пильності», згідно з яким адвокат несе персональну відповідальність за кожну цитату та прецедент, навіть якщо вони були запропоновані системою ШІ. Важливим елементом є також заборона делегування ШІ функцій, що становлять ядро юридичної професії, зокрема остаточне правове кваліфікування діяння, оцінка моральної шкоди та прийняття вердикту. ШІ повинен залишатися виключно інструментом підготовки, а не суб'єктом прийняття рішення [7, с. 16].

Третім запобіжником є безперервне цифрове навчання (LegalTech education) [33, с. 5]. Держава та професійні об'єднання (НААУ, РСУ) мають впровадити обов'язкові курси з критичної оцінки ШІ-результатів. Користувач повинен розуміти природу галюцинацій та вміти ідентифікувати Deepfake маніпуляції. Лише поєднання високої етичної планки з технічною грамотністю дозволить перетворити ШІ на безпечний інструмент правосуддя. Таким чином, система запобіжників замикає коло відповідальності, де розробник гарантує якість коду, а юрист - законність та етичність його застосування у конкретній справі [52, с. 28].

Сучасний стан технологічного розвитку свідчить про те, що інтеграція штучного інтелекту в правову систему є незворотним процесом, зумовленим експоненціальним зростанням обсягів інформації та потребою в надшвидкій аналітиці, що також каталізується сучасними технологічними трендами та модою. Спроби повної заборони ШІ в юриспруденції не лише приречені на поразку, а й можуть призвести до технологічного відставання національної правової системи. Проте неминучість автоматизації не означає капітуляцію перед алгоритмами. Суспільство має право і зобов'язане здійснювати свідомий селективний вибір сфер застосування ШІ, виходячи з пріоритету захисту людської гідності над технічною доцільністю.

Концепція свідомого вибору передбачає встановлення чітких червоних ліній, де використання ШІ є неприпустимим за будь-яких умов. Якщо автоматизація логістики судового процесу чи перевірки формальних реквізитів позову є безумовним

благом, то делегування ШІ функцій моральної оцінки, визначення винуватості чи позбавлення волі є ризиком, який суспільство не має права приймати. Правосуддя за своєю суттю є соціальним конструктом, що базується на людському розумінні контексту, співчутті та справедливості, тобто категоріях, які не піддаються цифровізації. Таким чином, вибір суспільства полягає в архітектурному обмеженні ШІ роллю корисного асистента, але в жодному разі не автономного суб'єкта прийняття рішень.

Реалізація цієї стратегії в Україні вимагає широкого суспільного діалогу та залучення до розробки регуляторних актів не лише програмістів, а й правозахисників, філософів та соціологів. Ми маємо обирати моделі ШІ, які є відкритими й прозорими за архітектурою та підзвітними демократичним інститутам, уникаючи монопольної залежності судової влади від приватних корпорацій. Зрештою, майбутнє правозастосовної діяльності залежить від нашої здатності впроваджувати інновації, не втрачаючи людиноцентричності права - переконання, що право існує для людини і має здійснюватися людиною, навіть якщо її очі та руки підсилені найдосконалішими технологіями.

Резюмуючи аналіз стратегій інтеграції штучного інтелекту, слід зазначити, що технологічний прогрес у правозастосовній сфері досягає своєї мети лише за умови жорсткого дотримання балансу між інноваціями та етичними фільтрами. Успішні практики впровадження e-discovery, предиктивної аналітики та автоматизації рутинних процесів доводять, що ШІ здатний радикально підвищити доступність правосуддя, якщо він залишається в ролі асистента. Ключовим висновком є необхідність переходу від стихійного використання алгоритмів до багаторівневої системи контролю, що охоплює сертифікацію постачальників за стандартами EU AI Act, алгоритмічний аудит на відсутність дискримінації та обов'язкове процесуальне декларування застосування ШІ [27, ст. 43]. Визнано, що неминучість цифровізації не знімає з суспільства відповідальності за свідомий вибір червоних ліній, де втручання алгоритму є неприпустимим, що забезпечує збереження антропоцентричного характеру права та верховенства людського розуму над кодом.

ВИСНОВОК ДО РОЗДІЛУ 3

У третьому розділі проведено комплексне дослідження правових ризиків, аналіз практичних помилок та визначення стратегічних напрямів удосконалення механізмів регулювання і використання штучного інтелекту в юридичній діяльності. Систематизація правових загроз дозволила встановити, що інтеграція ШІ в правозастосування створює багаторівневі виклики для класичної архітектури права, починаючи від порушення фундаментальних гарантій на приватність та захист персональних даних і завершуючи деформацією принципу справедливого суду через непрозорість «чорних скриньок» алгоритмів. Особливу небезпеку становить специфічний ризик «автоматизації упередженості» (automation bias), що за певних умов призводить до ерозії суддівського розсуду та поступової професійної деградації правничої спільноти через некритичне делегування інтелектуальних функцій машині [65, с. 385].

Визначення причин неправомірного застосування технологій на основі аналізу резонансних міжнародних прецедентів, таких як справи *Mata v. Avianca* та *State v. Loomis*, засвідчила, що основною причиною юридичних катастроф є «алгоритмічна недбалість» самих користувачів [59, с. 1; 60, с. 2]. Використання ШІ-галюцинацій та дискримінаційних моделей оцінки ризиків у кримінальному судочинстві доводить, що без належної верифікації цифровізація не лише не підвищує ефективність, а й масштабує системні помилки, призводячи до фальсифікації доказової бази та утисків вразливих груп населення. Наслідком таких зловживань стає глибока криза довіри до правосуддя, що вимагає негайного формування надійної архітектури запобіжників [52, с. 22].

Обґрунтовано, що ефективна модель регулювання має базуватися на чіткому розподілі відповідальності між постачальниками та користувачами систем ШІ, як професійними так і побутовими. Для розробників критично важливими є обов'язкова сертифікація систем високого ризику за стандартами EU AI Act та забезпечення принципу «пояснюваності» (explainability) алгоритмічних висновків [27, ст. 1; 47, с. 52]. Водночас для професійних правників обов'язковим має стати впровадження стандарту процесуального декларування використання ШІ та неухильне дотримання

етичного принципу «human-in-the-loop», який гарантує, що остаточне право на вердикт та моральну оцінку обставин справи завжди залишається за людиною [41, с. 12].

Підсумовуючи результати дослідження, слід наголосити на неминучості інтеграції ШІ, яка, проте, повинна відбуватися через свідомий вибір суспільством червоних ліній автоматизації. Стратегія майбутнього розвитку правової системи України має бути людиноцентричною, де цифрові алгоритми виступають виключно як потужні асистенти, що підсилюють процесуальну швидкість, але не підміняють собою сутнісні та ціннісні аспекти правосуддя. Тільки за умови збереження верховенства людського розуму над програмним кодом можлива розбудова справді гуманного та ефективного цифрового правопорядку.

ВИСНОВКИ

У магістерській роботі проведено комплексне теоретико-правове дослідження використання штучного інтелекту в судочинстві та правозастосовній діяльності. За результатами роботи сформульовано наступні висновки відповідно до поставлених завдань:

- *З'ясовано поняття, сутність та класифікацію систем ШІ в контексті правничої діяльності:* у результаті дослідження теоретичних засад встановлено, що штучний інтелект у правничій діяльності слід розуміти як комплексну технологічну систему, здатну використовувати вхідні дані для аналізу, інтерпретації та прогнозування правових документів та концепцій. З'ясовано, що сутність юридичної площини використання ШІ полягає не у механічній автоматизації, а у здатності оперувати великими масивами неструктурованих правових даних, що дозволяє виявляти приховані закономірності у законодавстві та судовій практиці. Проведена класифікація систем ШІ дозволила розмежувати технології за ступенем їхньої автономності та функціональним призначенням - від простих пошукових алгоритмів до складних нейронних мереж, здатних до генерації юридичних висновків. Доведено, що для цілей правозастосування найбільш адекватним є використання систем ШІ, які виступають інтелектуальним інструментом у руках юриста, не претендуючи на статус суб'єкта права, але вимагаючи спеціального правового режиму експлуатації, що базується на принципах підзвітності та людиноцентризму.
- *Визначено основні напрями та форми використання ШІ в судочинстві та правозастосуванні:* дослідження практичних аспектів впровадження інтелектуальних систем дозволило визначити ключові форми їх присутності у сучасному правозастосуванні, де ШІ виступає як каталізатор процесуальної ефективності. Встановлено, що найбільш динамічно ШІ інтегрується в судову систему через механізми автоматизованого розподілу справ, інтелектуального пошуку прецедентів та підготовки проектів судових рішень у малозначних

спорах. З'ясовано, що у правоохоронній діяльності пріоритетними напрямками є предиктивна аналітика для виявлення зон криміногенного ризику та системи біометричної ідентифікації, які значно пришвидшують розслідування злочинів. Доведено, що використання ІІІ у формі «цифрового помічника» дозволяє суддям та правоохоронцям звільнити часовий ресурс від рутинних операцій на користь глибокого аналізу правових дилем. Проте виявлено, що будь-яка форма застосування ІІІ в цій сфері повинна обмежуватися допоміжними функціями, оскільки остаточне правове кваліфікування та прийняття вердикту мають залишатися виключною прерогативою людини, що гарантує збереження етичного та соціального контексту правосуддя.

- *Проаналізовано світові тенденції розвитку LegalTech та роль ІІІ в трансформації юриспруденції*: аналіз глобальних трендів розвитку юридичних технологій дозволив констатувати, що LegalTech перестав бути допоміжним інструментом і став стратегічним чинником трансформації всієї екосистеми права. Встановлено, що ключовою тенденцією є перехід від простого аналізу документів до створення інтелектуальних платформ, здатних до прогнозування результатів судових спорів та автоматизованого аудиту складних корпоративних правочинів. З'ясовано, що впровадження ІІІ докорінно змінює структуру юридичного ринку, де конкурентна перевага зміщується від обсягу накопичених знань до швидкості та точності їх алгоритмічної обробки. Доведено, що роль штучного інтелекту полягає у демократизації доступу до правосуддя через розгортання систем онлайн-вирішення спорів та юридичних чат-ботів, які знижують фінансові та процедурні бар'єри для громадян. Однак виявлено, що така трансформація вимагає від юридичної професії вироблення нових стандартів «цифрової етики», оскільки технологічний прогрес не повинен нівелювати класичні принципи адвокатської таємниці та персональної відповідальності правника за надану консультацію.
- *Досліджено міжнародні стандарти та етичні принципи регулювання ІІІ (ООН, ОЕСР, Рада Європи)*: аналіз діяльності провідних міжнародних організацій, зокрема ООН, ОЕСР та Ради Європи, дозволив встановити, що

глобальне регулювання штучного інтелекту базується на переході від суто технологічного до ціннісно-орієнтованого підходу. З'ясовано, що ключовим інструментом м'якого права стали Рекомендації ОЕСР, які заклали фундамент для розуміння ШІ як системи, що повинна бути надійною, безпечною та підзвітною людині протягом усього життєвого циклу. Доведено, що концепція «людиноцентрованого ШІ» є стрижнем міжнародних етичних стандартів, що вимагає від розробників та користувачів забезпечення прозорості алгоритмів та запобігання будь-яким формам автоматизованої дискримінації. Дослідження підтвердило, що міжнародні стандарти відіграють роль універсального етичного фільтра, який не обмежує інновації, а спрямовує їх на захист демократії та верховенства права. Виявлено, що гармонізація національних законодавств із цими глобальними принципами є обов'язковою умовою для створення безпечного транскордонного цифрового простору, де технології служать інклюзивному розвитку суспільства, а не стають інструментом тотального контролю чи соціальної несправедливості.

- *Здійснено аналіз Регламенту ЄС про штучний інтелект (EU AI Act) та його впливу на глобальні процеси:* дослідження нормативного ландшафту Європейського Союзу дозволило констатувати формування першої у світі цілісної системи жорсткого регулювання інтелектуальних технологій, закріпленої у Регламенті ЄС про штучний інтелект (EU AI Act). Встановлено, що наріжним каменем європейського підходу є ризик-орієнтована класифікація, яка диференціює вимоги до систем ШІ залежно від їхньої потенційної загрози основоположним правам людини – від повної заборони систем соціального скорингу до суворого нагляду за алгоритмами високого ризику в правоохоронній та судовій сферах. З'ясовано, що запровадження стандартів алгоритмічної прозорості та обов'язкового звітування про навчання моделей загального призначення створює нову парадигму цифровізації, де технологічна потужність врівноважується юридичною відповідальністю розробників. Доведено, що «ефект Брюсселя» перетворює EU AI Act на глобальний стандарт, який змушує технологічні корпорації та національні

уряди за межами ЄС адаптувати свої інструменти до вимог етичності та безпеки. Дослідження підтвердило, що європейська модель пропонує збалансований механізм, який стимулює розвиток інноваційного ринку, водночас гарантуючи, що цифрова трансформація правосуддя не призведе до втрати людського контролю над процесуальними наслідками застосування алгоритмів.

- *Оцінено стан та перспективи формування нормативно-правового регулювання ШІ в Україні:* дослідження вітчизняного правового поля дозволило встановити, що Україна перебуває на етапі активної розбудови власної екосистеми штучного інтелекту, орієнтуючись на повну інтеграцію до Єдиного цифрового ринку ЄС. З'ясовано, що попри відсутність єдиного профільного закону, національна стратегія базується на принципах адаптивного регулювання, що поєднує інструменти «м'якого права», такі як Біла книга та етичні кодекси, із підготовкою до впровадження норм EU AI Act у внутрішнє законодавство. Встановлено, що ключовим викликом для української правової системи є необхідність створення надійних інституційних механізмів сертифікації алгоритмів, які використовуються в органах правосуддя та державного управління, особливо в умовах воєнного стану та цифровізації судочинства через ЄСІКС. Доведено, що для успішної трансформації правозастосовної діяльності необхідне запровадження «регуляторних пісочниць», які дозволять тестувати ШІ-рішення у контрольованому середовищі, мінімізуючи ризики для прав громадян. Дослідження підтвердило, що український шлях полягає у синергії між динамічним розвитком ІТ-сектору та поступовим запровадженням жорстких правових гарантій, що забезпечить цифрову стійкість держави та довіру суспільства до інноваційних методів вирішення правових спорів.
- *Ідентифіковано основні правові ризики застосування ШІ в правозастосовній діяльності:* у результаті комплексного аналізу викликів цифрової трансформації встановлено, що інтеграція штучного інтелекту в правозастосовну практику супроводжується виникненням специфічних ризиків, які загрожують фундаментальним засадам верховенства права.

З'ясовано, що найбільш критичним є «ефект чорної скриньки» (black box effect), який зумовлює непрозорість алгоритмічних висновків та унеможливляє повноцінне обґрунтування судових чи адміністративних рішень, що прямо суперечить вимогам належної правової процедури [66, с. 55]. Доведено, що використання ШІ створює латентні загрози для права на приватність та захисту персональних даних через ризики деанонізації та несанкціонованого профілювання громадян. Виявлено ризик «алгоритмічної упередженості» (algorithmic bias), що виникає внаслідок використання дискримінаційних навчальних вибірок або алгоритмів, і може призвести до відтворення соціальних стереотипів у правових вердиктах. Дослідження підтвердило, що без запровадження жорстких стандартів алгоритмічної підзвітності та пояснюваності, технологічний прогрес може спровокувати кризу довіри до інститутів правосуддя, перетворюючи об'єктивний розгляд справи на механічне обчислення, позбавлене етичного контексту та індивідуального підходу до кожного учасника процесу.

- *Проаналізовано причини та наслідки актуальних випадків неправомірного застосування систем ШІ: емпіричний аналіз резонансних міжнародних прецедентів, таких як справа Mata v. Avianca та використання алгоритму COMPAS, дозволив встановити, що основною причиною юридичних помилок є не лише технічна недосконалість систем, а й «алгоритмічна недбалість» самих користувачів. З'ясовано, що некритична довіра до результатів роботи генеративних моделей призводить до використання людиною результатів періодичних «галюцинацій», які проявляються у фальсифікації прецедентів та нормативних джерел, що підриває авторитет правосуддя. Доведено, що наслідком використання непрозорих систем оцінки ризиків у кримінальному судочинстві є масштабування системної дискримінації, наприклад, за расовими чи соціальними ознаками, що перетворює статистичну кореляцію на юридичний висновок. Дослідження підтвердило, що будь-яке небезпечне застосування ШІ без належної людської верифікації призводить до миттєвого тиражування юридичних дефектів, які важко ідентифікувати та виправити в*

межах стандартних апеляційних процедур. Виявлено, що ці випадки слугують суворим застереженням для правничої спільноти, підкреслюючи, що відмова від персональної відповідальності юриста на користь алгоритму неминуче веде до процесуального фіаско та порушення прав учасників судового розгляду.

- *Встановлені успішні практики та розроблені ефективні запобіжники і механізми контролю за діяльністю постачальників та користувачів ШІ:* завершальний етап дослідження дозволяє обґрунтувати цілісну систему стратегічних запобіжників, необхідних для безпечної інтеграції штучного інтелекту в правову систему. Встановлено, що успішні практики використання ШІ в юриспруденції ґрунтуються на впровадженні багаторівневого контролю, який включає обов'язкову технічну сертифікацію алгоритмів постачальниками та етичну верифікацію результатів кінцевими користувачами. З'ясовано, що ключовим механізмом захисту прав людини є дотримання принципу «Human-in-the-loop», який виключає можливість прийняття юридично значущих рішень виключно в автоматизованому режимі. Доведено, що для подолання технологічних викликів необхідно запровадити обов'язкове процесуальне декларування використання ШІ та розвивати «алгоритмічну пильність» серед професійних правників через систему безперервної LegalTech освіти. Узагальнюючи результати роботи, рекомендується державі та правничій спільноті зосередитися на створенні національного реєстру сертифікованих ШІ-систем для правничої діяльності, що гарантуватиме їхню прозорість та відповідність стандартам захисту даних. Головна ідея дослідження полягає у визнанні того, що поступова інтеграція ШІ у юридичну професію та безліч інших сфер людською діяльності є неминучим процесом, успіх якого залежить від здатності суспільства зберегти антропоцентричний характер права. Тільки за умови жорсткого дотримання етичних «червоних ліній» та збереження за людиною виключного права на справедливий вердикт, цифрові інновації зможуть стати надійним фундаментом для розбудови правосуддя майбутнього як ефективного, доступного та неупередженого.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Берназюк Я. О. Штучний інтелект: майбутні перспективи та ризики для правосуддя / Верховний Суд. 2024. URL: https://court.gov.ua/storage/portal/supreme/prezentacii_2025/124_AI_Future_Prospects_Risks_for_Judiciary_bernaziuk.pdf
2. Біла книга з регулювання ШІ в Україні / Міністерство цифрової трансформації України. 2024. URL: <https://backend.hromada.gov.ua/storage/uploads/files/research/bila-kniga-z-regulyuvannya-si-v-ukrayini-bacennya-minicifri/%D0%A0%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%A8%D0%86.pdf?time=1744806741842>
3. Добровільний кодекс поведінки з етичного та відповідального використання штучного інтелекту / Міністерство цифрової трансформації України. 2024. URL: <https://storage.thedigital.gov.ua/files/3/73/1bbeacc736a29e2f8a749ef9c90d4734.pdf>
4. Європейська конвенція про захист прав людини і основоположних свобод від 04.11.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text
5. Загальна декларація прав людини : прийнята і проголошена резолюцією 217 А (III) ГА ООН від 10.12.1948. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text
6. Інформаційно-аналітична система LIGA360 / LIGA ZAKON. 2024. URL: <https://ligazakon.net/>
7. Кодекс суддівської етики : затв. XI черговим з'їздом суддів України 22 лютого 2013 року (зі змінами від 04.09.2024). URL: <https://zakon.rada.gov.ua/rada/show/n0001415-13#Text>
8. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108) від 28.01.1981. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text
9. Концепція побудови та функціонування Єдиної судової інформаційно-комунікаційної системи у новій редакції : наказ Державної судової адміністрації України від 30.04.2024 № 178. URL: https://court.gov.ua/storage/portal/dsa/normatyvno-pravova%20baza/N_178_2025_dodatok.pdf
10. Концепція розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text>

11. Король В. В. Правове регулювання ІІІ: європейський досвід та українські реалії. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 75. Ч. 1. С. 45–52.
12. Котух Є. В. Штучний інтелект у судочинстві: теоретико-правовий аспект. *Юридичний часопис*. 2024. № 2. С. 112–119.
13. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>
14. Нестеренко О. Доступ до правосуддя в цифрову епоху. *Право України*. 2023. № 4. С. 88–101.
15. Поради з відповідального використання штучного інтелекту публічними службовцями / Міністерство цифрової трансформації України ; НАДС. 2024. URL: <https://ai.thedigital.gov.ua/documents>
16. Про авторське право і суміжні права : Закон України від 01.12.2022 № 2811-IX. URL: <https://zakon.rada.gov.ua/laws/show/2811-20#Text>
17. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
18. Про судоустрій і статус суддів : Закон України від 02.06.2016 № 1402-VIII. URL: <https://zakon.rada.gov.ua/laws/show/1402-19#Text>
19. Рекомендації з відповідального використання штучного інтелекту для правників / Міністерство цифрової трансформації України. 2024. URL: <https://storage.thedigital.gov.ua/files/2/72/fcf6c498e0a9f57e7a8521ff9833372d.pdf>
20. Співак В. М. Правова природа штучного інтелекту : монографія. Київ : Ліра-К, 2023. 240 с.
21. Стратегія цифровізації правосуддя в Україні до 2027 року / Вища рада правосуддя. URL: https://hcj.gov.ua/sites/default/files/field/file/plan_diyalnosti_vyshchoyi_rady_pravosuddya_na_2025-2027_roky.pdf
22. Харитонova О. І. Багатоаспектність розуміння «штучного інтелекту» / О. І. Харитонova // ІТ-право та кібербезпека в умовах гібридної війни : матеріали Всеукр. круглого столу (м. Одеса, 12 квіт. 2025 р.) / за заг. ред.: Є. О. Харитонova, Ю. Кривенко ; кафедра цив. права НУ «Одес. юрид. академія». – Одеса : Фенікс, 2025. – С. 35-40. - Режим доступу: <https://hdl.handle.net/11300/29683>
23. Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>
24. Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV. URL: <https://zakon.rada.gov.ua/laws/show/1618-15#Text>
25. Штучний інтелект, сучасні технології та право в Україні : монографія [Електронне видання] / за заг. ред.: О. А. Костенка ; Держ. наук. установа

- «Інститут інформації, безпеки і права НАПрН України». – Київ; Одеса : Фенікс, 2026. – 356 с. URL: https://ippi.org.ua/sites/default/files/2100_monografiya_finish.pdf
26. AI Index Report 2024 / Stanford Institute for Human-Centered AI. 2024. URL: <https://aiindex.stanford.edu/report/>
 27. Artificial Intelligence Act : Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>
 28. Artificial Intelligence Liability Directive : Proposal for a Directive of the European Parliament and of the Council. 2022. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496>
 29. Ashley K. D. Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age. Cambridge : Cambridge University Press, 2017. 446 p. URL: https://assets.cambridge.org/97811071/71503/frontmatter/9781107171503_frontmatter.pdf
 30. Boden M. A. Artificial Intelligence: A Very Short Introduction. Oxford : Oxford University Press, 2018. 184 p.
 31. Bradford A. The Brussels Effect: How the European Union Rules the World. Oxford : Oxford University Press, 2020. 440 p.
 32. Bridges v South Wales Police : Case EWCA Civ 1058. *Judiciary UK*. URL: <https://www.judiciary.uk/judgments/r-bridges-v-cc-south-wales/>
 33. CCBE Guide on the use of Generative AI for lawyers / Council of Bars and Law Societies of Europe. 2024. URL: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20251002_CCBE-guide-on-the-use-of-the-use-of-generative-AI-for-lawyers.pdf
 34. Charter of Fundamental Rights of the European Union. *Official Journal of the European Communities*. 2012. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>
 35. Chesney R., Citron D. K. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*. 2019. Vol. 107. P. 1753–1820.
 36. Comiter M. Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It / Belfer Center for Science and International Affairs. 2019. URL: <https://www.belfercenter.org/publication/AttackingAI>
 37. Consultative Council of European Judges (CCJE). Opinion No. 26 (2023) on assistive technology in the judiciary. URL: <https://rm.coe.int/ccje-opinion-no-26-2023-final/1680adade7>

38. Corrales Compagnucci M., Fenwick M., Forgó N. Law and Technology in a World of Law 4.0. *Journal of Strategic Contracting and Negotiation*. 2019.
39. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. 2024. URL: <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>
40. Dharma S. N. et al. Implementation of Artificial Intelligence (AI) in legal systems. *Procedia Computer Science*. 2023. Vol. 224. P. 667–672. URL: https://www.researchgate.net/publication/389160073_The_Implementation_of_Artificial_Intelligence_by_Judges_in_Law_Enforcement_Reviewed_From_Legal_Convergence_Theory
41. European Commission for the Efficiency of Justice (CEPEJ). European ethical Charter on the use of Artificial Intelligence in judicial systems. 2018. URL: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>
42. European Data Protection Board (EDPB). Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en
43. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). 2017. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0051>
44. Formal Opinion 512: Generative Artificial Intelligence in Legal Practice / American Bar Association. 2024. URL: https://www.americanbar.org/groups/professional_responsibility/publications/ethics_opinions/
45. General Data Protection Regulation (GDPR) : Regulation (EU) 2016/679. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
46. Global Partnership on Artificial Intelligence (GPAI). Ministerial Declaration. 2023. URL: [https://one.oecd.org/document/GPAI\(2023\)2/en/pdf](https://one.oecd.org/document/GPAI(2023)2/en/pdf)
47. Goodman B., Flaxman S. European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation". *AI Magazine*. 2017. Vol. 38, No. 3. P. 50–57. URL: <https://scispace.com/pdf/european-union-regulations-on-algorithmic-decision-making-66w9rc75zo.pdf>
48. Guidelines for secure AI system development / UK National Cyber Security Centre (NCSC) & US CISA. 2023. URL: <https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development>
49. Guidelines on the use of generative AI in mediation / International Bar Association. 2025. URL: <https://www.ibanet.org/Guidelines-on-the-use-of-generative-artificial-intelligence-in-mediation>

50. Hawking S. Brief Answers to the Big Questions. London : John Murray, 2018. 256 p.
51. Hildebrandt M. Law for Computer Scientists and Other Folk. Oxford : Oxford University Press, 2020. 320 p. URL: https://www.cohubicol.com/assets/uploads/law_for_computer_scientists.pdf
52. Human rights compliant use of artificial intelligence systems toolkit for civil society / Digital Security Lab Ukraine (DSLUA). URL: <https://dslua.org/publications/human-rights-compliant-use-of-artificial-intelligence-systems-toolkit-for-civil-society/>
53. ISO/IEC 22989:2022. Information technology — Artificial intelligence — Concepts and terminology. URL: <https://www.iso.org/standard/74296.html>
54. ISO/IEC 24027:2021. Information technology — Artificial intelligence — Bias in AI systems and AI aided decision making. URL: <https://www.iso.org/standard/77607.html>
55. ISO/IEC 42001:2023. Information technology — Artificial intelligence — Management system. URL: <https://www.iso.org/standard/81853.html>
56. Katsh E., Rabinovich-Einy O. Digital Justice: Technology and the Internet of Disputes. Oxford : Oxford University Press, 2017. 240 p.
57. Katz D. M. Quantitative Legal Prediction-or-How I Learned to Stop Worrying and Start Preparing for the Data-Driven Future of the Legal Services Industry. *Emory Law Journal*. 2012. Vol. 62. P. 909.
58. Lextenso. Base de données juridique / Lextenso services. 2024. URL: <https://www.lextenso.fr/>
59. Loomis v. Wisconsin : Case 881 N.W.2d 749 (Wis. 2016). *Justia Law*. URL: <https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html>
60. Mata v. Avianca, Inc. : Case 22-cv-1461 (S.D.N.Y. 2023). *Justia Law*. URL: <https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2022cv01461/575368/54/>
61. Matthias A. The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology*. 2004. Vol. 6. P. 175–183.
62. McGinnis J., Pearce R. The Great Disruption: How AI will transform the Legal Profession. *Fordham Law Review*. 2014. Vol. 82. P. 3041–3066. URL: <https://ir.lawnet.fordham.edu/flr/vol82/iss6/16/>
63. NJCM c.s. v. De Staat der Nederlanden (SyRI case) : ECLI:NL:RBDHA:2020:1878, District Court of The Hague. 2020. URL: <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878>
64. OECD. Recommendation of the Council on Artificial Intelligence. 2024. URL: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

65. Parasuraman R., Manzey D. H. Complacency and Bias in Human Use of Automation: An Attentional Integration. *Human Factors*. 2010. Vol. 52, No. 3. P. 381–410.
66. Pasquale F. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press, 2015. 320 p.
67. Perry W. L., McInnis B., Price C. C., Smith S. C., Hollywood J. S. *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. RAND Corporation, 2013. 192 p.
68. ProPublica. Machine Bias: Risk Assessments in Criminal Sentencing. 2016. URL: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>
69. Putra A. et al. Automated processing of legal information. *ResearchGate*. 2025. URL: <https://www.researchgate.net/publication/395101818>
70. Reform of copyright infringement in light of generative AI / Singapore Academy of Law. 2026. URL: <https://sal.org.sg/wp-content/uploads/2026/02/Reform-of-copyright-infringement-in-light-of-generative-AI.pdf>
71. Roth A. Machine Testimony. *Yale Law Journal*. 2017. Vol. 126, No. 7. P. 1972–2053.
72. Salloum S. A. *Implications of AI Technology on International Law*. Cham : Springer, 2024. 215 p. URL: <https://link.springer.com/book/10.1007/978-3-031-48332-5>
73. Scherer M. Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*. 2016. Vol. 29, No. 2. URL: <https://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf>
74. Singapore Academy of Law Journal Special Issue. Article 2143. URL: <https://journalonline.academypublishing.org.sg/Journals/Singapore-Academy-of-Law-Journal-Special-Issue/Current-Issue/ctl/eFirstSALPDFJournalView/mid/503/ArticleId/2143/Citation/JournalsOnlinePDF>
75. Smuha N. A. (ed.) *AI, Law and Policy*. In: *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*. Cambridge : Cambridge University Press, 2025. P. 131–258.
76. Susskind R. *Online Courts and the Future of Justice*. Oxford : Oxford University Press, 2021. 384 p.
77. Susskind R. *Tomorrow's Lawyers: An Introduction to Your Future*. 3rd ed. Oxford : Oxford University Press, 2023. 272 p.
78. Technology and innovation in legal services / Legal Services Board (UK). 2021. URL: <https://legalservicesboard.org.uk/our-work/technology-and-innovation>

79. UNESCO. Recommendation on the Ethics of Artificial Intelligence. 2021. URL: <https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence>
80. United Nations. Resolution A/RES/78/265 "Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development". 2024. URL: <https://undocs.org/A/RES/78/265>
81. Wachter S., Mittelstadt B. A Right to Reasonable Inferences. *Columbia Business Law Review*. 2019. No. 1. P. 1–114. URL: <https://journals.library.columbia.edu/index.php/cblr/article/view/3424>
82. Yeung K. Algorithmic regulation: A critical interrogation. *Regulation & Governance*. 2018. Vol. 12, No. 4. P. 505–523. URL: https://www.researchgate.net/publication/318820255_Algorithmic_regulation_A_critical_interrogation
83. Završnik A. et al. Algorithmic justice: Algorithms and big data in criminal justice settings. *European Journal of Criminology*. 2021. Vol. 18, No. 5. P. 623–642. URL: <https://journals.sagepub.com/doi/full/10.1177/1477370819876762>

Дата закінчення роботи — 23.04.2026

Підпис:

A handwritten signature in blue ink, consisting of stylized, cursive letters.