



Державна наукова установа «Інститут інформації, безпеки і права
Національної академії правових наук України»

Науково-дослідний інститут інтелектуальної власності
Національної академії правових наук України

УКРАЇНА В УМОВАХ СОЦІАЛЬНОЇ ТА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: ТЕОРЕТИЧНІ МОДЕЛІ ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

Київ, 5 листопада 2025 року

Київ-Одеса

2025

УДК 340.132:004.8(477)

У 45

Рекомендовано до друку

Вченою радою Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України».

Протокол № 10 від 09.12.2025 р.

Україна в умовах соціальної та цифрової трансформації: теоретичні моделі правового регулювання штучного інтелекту : матеріали наук.-практ. конф. (Київ, 5 листоп. 2025 р.) [Електронне видання] / упоряд.: М. В. Дубняк, С. О. Дорогих, І. Ф. Корж, В. М. Фурашев. Київ; Одеса : Фенікс, 2025. 240 с. Режим доступу: https://ippi.org.ua/sites/default/files/zbirnik_tez_05.11.2025_1.pdf

ISBN 978-617-8430-97-9

Збірник містить матеріали щодо стратегічних напрямів правового регулювання штучного інтелекту в Україні; розвитку національної LLM та впровадження агентних ШІ-рішень у державні сервіси; формування цифрових прав і оновлення цивільного законодавства; проблем використання ШІ в умовах воєнного стану, забезпечення кібербезпеки, захисту персональних даних та інтелектуальної власності; етичних і методологічних засад застосування ШІ у сфері освіти та науки.

Доповіді учасників конференції можуть бути корисними для фахівців, експертів і вчених, науково-педагогічних працівників та здобувачів вищої освіти.

УДК 340.132:004.8(477)

Матеріали подано у авторській редакції.

ISBN 978-617-8430-97-9

© Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», 2025

© Науково-дослідний інститут інтелектуальної власності Національної академії правових наук України, 2025

© Колектив авторів, 2025

З М І С Т

<i>ВСТУП</i>	8
<i>ВИСТУПИ НА ПЛЕНАРНОМУ ЗАСІДАННІ</i>	
<i>Іван ДОРОНІН</i>	12
Безпекові виклики та правові проблеми створення «національного штучного інтелекту» (у межах LLM)	
<i>Микола КАРЧЕВСЬКИЙ</i>	19
Трирівнева модель правового регулювання ШІ	
<i>Олег ЗАЯРНИЙ</i>	26
Правове забезпечення застосування ШІ-агентів у механізмі цифрової трансформації територіальних громад: деякі концептуально-прикладні аспекти	
<i>Олена АНДРІЄНКО</i>	32
Спочатку було слово: правові виклики великих мовних моделей	
<i>Наталія САВІНОВА</i>	38
Маніпулювання свідомістю з використанням візуальних продуктів ШІ: кримінологічні рефлексії	
<i>Ігор КОРЖ, Тетяна КОРЖ</i>	43
Майбутнє штучного інтелекту в науці: бачення зарубіжних фахівців	
<i>Марія ДУБНЯК</i>	50
Проблеми гармонізації термінології при імplementації AI Act в Україні	
<i>Ярослава САВЧЕНКО</i>	56
Повернення культурних цінностей України: перспективи використання штучного інтелекту	
<i>Софія АВДІЮК</i>	64
"Машинне рознавчання" (machine unlearning) як правовий імператив: забезпечення права на стирання даних в архітектурі великих мовних моделей (LLM)	

Світлана КЕЛИП	71
Нормативно-правова модернізація сфери прикордонної безпеки України в умовах розвитку технологій штучного інтелекту	
Михайло МИХАЙЛЕНКО	74
Проблеми та перспективи використання технологій ШІ під час розгляду заявок про державну реєстрацію торговельних марок	
Дмитро ЛАНДЕ, Юрій ЦИРУЛЬНЄВ	81
Теоретична модель правового регулювання аспектів створення та використання електронних інформаційних ресурсів та електронних архівів	
ФІЛОСОФСЬКО-ПРАВОВІ, КОНЦЕПТУАЛЬНО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ТА РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ	
Геннадій АНДРОЩУК	86
Методологія виявлення нових технологій ШІ з використанням патентних даних	
Олександр БУТНІК-СІВЕРСЬКИЙ	97
Розвиток інтелектуальної техніко-технологічної комп'ютерної платформи цифровізації	
Олеся АНДРУЩЕНКО	103
Філософсько-правові засади легітимації ШІ в системі політико-правових відносин сучасної України	
Яна ЛУКАШОВА	107
Правове регулювання штучного інтелекту у сфері національної безпеки і оборони	
Вадим ГАРАЩЕНКО	111
Правове регулювання штучного інтелекту в Європейському Союзі: теоретико-методологічні та практичні аспекти	
Владислав ВАРИНСЬКИЙ	116
Основні критерії заборон використання ШІ за AI Act	

<i>ДЕГТЯРЬОВ І.М., ПЕТРОВСЬКИЙ М.В., ЛЕОНТЬЄВ П.В.</i>	121
Методологія тестування програмного забезпечення для системи автономної навігації наземних роботизованих комплексів	
<i>ПЕТРОВСЬКИЙ М.В., ДЕГТЯРЬОВ І.М., ЛЕОНТЬЄВ П.В.</i>	124
Важливість розроблення методики випробувань для контролю технічних характеристик наземних роботизованих комплексів з використанням штучного інтелекту, як альтернатива перевірці в реальних умовах експлуатації	
БЕЗПЕКА, ОБОРОНА, КІБЕРЗАХИСТ ТА ВОЄННИЙ КОНТЕКСТ ПРИ РЕГУЛЮВАННІ ШІ	
<i>Дар'я ГЛУШКОВА</i>	130
Штучний інтелект у системі національної безпеки України. правові засади регулювання в умовах воєнного стану	
<i>Олена ГРЕЗІНА</i>	133
Захист інформаційних ресурсів держави в умовах воєнних загроз та роль штучного інтелекту	
<i>Вікторія КОЩИНЕЦЬ</i>	136
Симбіоз штучного інтелекту та розподілених технологій для захисту оборонних даних	
<i>Марина ГРИГОР'ЄВА</i>	142
Формування етичних норм і стандартів при використанні штучного інтелекту в умовах воєнного стану	
<i>ФЕДОРЧЕНКО О.С.</i>	148
Штучний інтелект проти кіберзлочинців: еволюція захисту в епоху складних кібератак	
<i>Ганна ФОРΟΣ</i>	153
Автоматизований моніторинг кіберзагроз за допомогою систем машинного навчання	

**ЦИФРОВИЙ СУВЕРЕНІТЕТ І НАЦІОНАЛЬНА СТРАТЕГІЯ
РОЗВИТКУ У СФЕРІ
ШТУЧНОГО ІНТЕЛЕКТУ**

- АВДІЮК С.С., ГАБЕЛКО В. О., ДРАЧУК Є.М.*** **157**
Правові механізми забезпечення цифрового суверенітету України в епоху штучного інтелекту
- Людмила ЗАСЛАВСЬКА*** **165**
Національна велика мовна модель як інструмент цифрового суверенітету України
- Василь ОРИЩУК, Максим ВАЛІН*** **170**
LLM та «Дія.АІ» як основа побудови Smart City-екосистем
- НИКОЛИНА К.В.*** **177**
Національна ВММ як основа цифрового суверенітету України
- Ярослав МАНУІЛОВ*** **182**
Стратегія розвитку міжнародного кіберпростору та цифрової політики США

**ПРАВА ЛЮДИНИ, ПРИВАТНІСТЬ ТА ПИТАННЯ
ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ**

- ПАШИНСЬКИЙ В.Й., ЦЬОМЕНКО А.В.*** **186**
Адміністративно-правове забезпечення захисту персональних даних в умовах розвитку штучного інтелекту
- Жанна ЛУПАК . Науковий керівник: ЗАЯРНИЙ О.А.*** **192**
Право особи на справедливе рішення в адміністративних процедурах із застосуванням штучного інтелекту суб'єктами публічного адміністрування
- Наталія ДЕДЮЄВА, Ольга ГОЛОВКО*** **198**
Баланс приватності та свободи вираження поглядів через призму законопроекту № 14057
- Юрій КАПІЦА*** **204**
Правові аспекти використання контенту для навчання штучного інтелекту: підходи в ЄС, Україні та США

Олена БАХАРЕВА	210
Штучний інтелект як «порушник» авторського права	
КОВАЛЕНКО Т.В.	215
Штучний інтелект і права інтелектуальної власності	
Олена ГОНЧАРЕНКО, Анастасія ЛЕВКІВСЬКА	220
Криза інтелектуальної власності в умовах генеративного штучного інтелекту	

**СОЦІАЛЬНИЙ ВИМІР ШТУЧНОГО ІНТЕЛЕКТУ:
ОСВІТА, ПРАЦЯ, ІНКЛЮЗІЯ**

Андрій ОЗАРЧУК	227
Персоналізація та інклюзія: можливості штучного інтелекту для сучасної педагогіки	
Олександр ОСТАПЕНКО	232
Штучний інтелект у сфері освіти та науки: правові виклики цифрової епохи	
Світлана САДОВА	235
Штучний інтелект і ринок праці: соціальні ризики та виклики перерозподілу вигод	

Олена Грезіна

доктор філософії у галузі права,
доцент кафедри кримінального аналізу та інформаційних технологій
Одеський державний університет внутрішніх справ
ORCID: <https://orcid.org/0000-0002-2491-6529>

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ ДЕРЖАВИ В УМОВАХ ВОЄННИХ ЗАГРОЗ ТА РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ

Забезпечення інформаційної безпеки держави в умовах воєнних загроз набуває стратегічного значення, оскільки воєнні конфлікти створюють комплекс підвищених ризиків втручання у критично важливі інформаційні системи, порушення цілісності та достовірності даних, а також дестабілізації ключових державних процесів і функцій. У таких умовах кібератаки виступають не лише інструментом отримання конфіденційної інформації, але й засобом реалізації стратегічних та тактичних завдань противника, включаючи паралізацію критично важливих об'єктів інфраструктури, порушення логістичних ланцюгів, дезорганізацію енергетичних та комунікаційних мереж, а також маніпулювання громадською свідомістю.

Основними загрозами інформаційній безпеці держави в умовах воєнних загроз є несанкціоноване втручання в державні інформаційні системи, модифікація або знищення критично важливих даних, маніпуляції, що впливають на процес ухвалення рішень на всіх рівнях управління, порушення функціонування транспортної, енергетичної та комунікаційної інфраструктури, а також психологічний тиск на населення та державні установи через масовані інформаційні кампанії. Виявлення, оцінка та нейтралізація таких загроз вимагають високого рівня організаційної підготовки, узгодженості дій між державними органами та застосування передових технологічних рішень для забезпечення безперервності роботи інформаційних систем.

Розвиток алгоритмічних систем дозволяє підвищити ефективність захисту державних інформаційних ресурсів за рахунок автоматизації процесів моніторингу, аналізу подій та реагування на загрози у режимі реального часу. Алгоритмічні системи здатні здійснювати аналіз великих обсягів даних, виявляти аномалії у функціонуванні мереж, прогнозувати потенційні загрози

та формувати оперативні рішення для нейтралізації інцидентів, що значно скорочує час від виявлення загрози до її усунення. Використання таких рішень забезпечує безперервний контроль інформаційних потоків, раннє попередження про спроби несанкціонованого доступу, а також реалізацію автоматизованих механізмів протидії кібератакам, що дозволяє знизити негативні наслідки атак і забезпечити стійкість критично важливих об'єктів інфраструктури.

Інтеграція алгоритмічних систем у державні структури та об'єкти критичної інфраструктури здійснюється на основі централізованих платформ обробки даних, систем виявлення загроз, аналізу поведінки потенційних нападників і прогнозування сценаріїв кібератак [1]. Така інтеграція передбачає використання алгоритмічних рішень у державних органах, відповідальних за кібербезпеку, а також у системах контролю доступу, мережевого моніторингу та аналітичного управління інформаційними потоками. Комплексний підхід до захисту державних ресурсів дозволяє підвищити надійність інформаційних систем, знизити ризики, пов'язані з людським фактором, забезпечити масштабованість та адаптивність механізмів безпеки при збільшенні обсягів даних і ускладненні кіберзагроз.

Переваги застосування алгоритмічних систем у сфері інформаційної безпеки проявляються у підвищенні ефективності виявлення та оперативного реагування на загрози, скороченні часу ухвалення рішень, формуванні аналітичної бази для стратегічного планування та забезпеченні стійкості державних інформаційних ресурсів у надзвичайних умовах [2]. Використання таких рішень дозволяє підвищити здатність держави протидіяти кібератакам та інформаційним впливам, мінімізувати негативні наслідки порушень безпеки та підтримувати безперервність функціонування критично важливих об'єктів.

Забезпечення інформаційної безпеки держави в умовах воєнних загроз потребує комплексного поєднання технологічних, організаційних та правових механізмів. Алгоритмічні системи виконують ключову роль у підвищенні стійкості державних інформаційних ресурсів, забезпеченні автоматизованого та оперативного реагування на загрози, а також у створенні аналітичної платформи для стратегічного управління кібербезпекою. Подальший розвиток методів аналізу даних, прогнозування та автоматизації процесів безпеки сприятиме зміцненню національної інформаційної безпеки, підвищенню

готовності державних органів до протидії складним кібератакам та забезпеченню ефективного управління критично важливою інфраструктурою у кризових умовах.

Список використаних джерел

1. Adewusi, Adebunmi Okechukwu, Ugochukwu Ikechukwu Okoli, Temidayo Olorunsogo, Ejuma Adaga, Donald Obinna Daraojimba, and Ogugua Chimezie Obi. 2024. «Artificial Intelligence in Cybersecurity: Protecting National Infrastructure: A USA Review». *World Journal of Advanced Research and Reviews* 21, no. 1: 2263–2275. <https://doi.org/10.30574/wjarr.2024.21.1.0313>
2. M., V., and R. Murugan. 2024. «The Role of Artificial Intelligence in Cyber Security». *International Journal of Innovative Research in Computer and Communication Engineering* 12, no. 03: 1635–1641. <https://doi.org/10.15680/ijircee.2024.1203044>

НАУКОВЕ ВИДАННЯ

**УКРАЇНА В УМОВАХ СОЦІАЛЬНОЇ ТА ЦИФРОВОЇ
ТРАНСФОРМАЦІЇ: ТЕОРЕТИЧНІ МОДЕЛІ ПРАВОВОГО
РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ**

МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

Київ, 5 листопада 2025 року

Електронне видання

Макет збірника та комп'ютерна верстка:

М. Дубняк, С. Дорогих

Упорядкування:

І. Корж, В. Фурашев

Ум-друк. арк. 12.

Зам. № 2512-03.

Видавець ПП «Фенікс»

(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).

Україна, м. Одеса, 65009, вул. Зоопаркова, 25.

e-mail: fenix-izd@ukr.net