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.

У 45 **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

З М І С Т

БЕЗПЕКА, ОБОРОНА, КІБЕРЗАХИСТ ТА ВОЄННИЙ КОНТЕКСТ ПРИ РЕГУЛЮВАННІ ШІ

ЦИФРОВИЙ СУВЕРЕНІТЕТ І НАЦІОНАЛЬНА СТРАТЕГІЯ РОЗВИТКУ У СФЕРІ ШТУЧНОГО ІНТЕЛЕКТУ

ПРАВА ЛЮДИНИ, ПРИВАТНІСТЬ ТА ПИТАННЯ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

СОЦІАЛЬНИЙ ВИМІР ШТУЧНОГО ІНТЕЛЕКТУ:

ОСВІТА, ПРАЦЯ, ІНКЛЮЗІЯ

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/ijircce.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