

8. Шекспір В. Ромео і Джульєтта. Трагедія. Пер. з англ. Ю.Андрухович. Київ, Видавництво «А-БА-БА-ГА-ЛА-МА-ГА», 2016.

9. Фулей Т.І. Підміна понять як вид законотворчих помилок: необхідність наукового осмислення. *Альманах права*. Правові засади нормотворчої діяльності: національний і зарубіжний досвід: До 75-річчя Інституту держави і права імені В. М. Корещького НАН України, 1949–2024. Випуск 15. Київ: Інститут держави і права імені В. М. Корещького НАН України, 2024. С. 455-465. DOI: 10.33663/2524-017X-2024-15-455-465

10. Податковий кодекс України : Закон України від 02.12.2010 № 2755-VI. URL: <https://zakon.rada.gov.ua/laws/show/2755-17#Text>

DOI <https://doi.org/10.36059/978-966-397-501-6-32>

ПРОБЛЕМИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У КОНТЕКСТІ ЗАХИСТУ ПРАВ ЛЮДИНИ

Харитонов Євген Олегович

<https://orcid.org/0000-0001-5521-0839>

доктор юридичних наук, професор,

член-кореспондент Національної академії правових наук України,

зав. кафедри цивільного права,

Національний університет «Одеська юридична академія»

м. Одеса, Україна

Харитонova Олена Іванівна

<https://orcid.org/0000-0002-9681-9605>

докторка юридичних наук, професорка,

член-кореспондент Національної академії правових наук України,

зав. кафедрою інтелектуальної власності та патентної юстиції,

Національний університет «Одеська юридична академія»

м. Одеса, Україна

У пошуках відповіді на питання щодо ролі штучного інтелекту у захисті прав людини, зокрема, під час війни, на нашу думку, у контексті проблематики «штучний інтелект і війна» варто розрізняти, умовно поійменовані концепти – «оборонний штучний інтелект» та «наступальний штучний інтелект».

Перший з них спрямований, передусім, на «кібернетичне забезпечення» оборонних військових/ воєнних потреб країни, а також на відвернення (переважно – пасивне) кіберзагроз.

Другий – на ведення активних (наступальних) дій у кібервійні, котра може провадитись/ вестися окремо або бути складовою частини мілітарної війни.

Оборонний ІІІ є потужним інструментом у боротьбі з кіберзагрозами. Наприклад, волонтерські організації давно використовують штучний інтелект в інформаційній війні, викриваючи фейкові ЗМІ та мережі ботів, а також даючи відсіч наративам, які націлені на завдання шкоди репутації України. З 2014 по 2015 роки вони розробили такі цінні інструменти, такі як Кгорува – система ситуаційної поінформованості, та додаток GIS Arta, що отримав назву «артилерійський Uber», які прискорюють і допомагають синхронізувати наведення артилерії і сьогодні розгортаються у великих масштабах з великим ефектом [1]. У логістиці широко використовується передиктивний штучний інтелект, який може допомогти у плануванні технічного обслуговування, запобіганні дефіциту на військових складах та прогнозуванні потенційних перешкод для поповнення місій шляхом попереднього моделювання оперативної обстановки. Тим часом, безлюдні логістичні транспортні засоби з навігаційними системами штучного інтелекту можуть доставляти боєприпаси та евакуювати поранених. Штучний інтелект може підтримувати підключення до мереж зв'язку супротивника та покращувати операції радіоелектронної боротьби (РЕБ). Він також може посилювати шифрування даних та мережі обміну, у той час як системи кібербезпеки на основі штучного інтелекту можуть автоматично визначати, аналізувати та класифікувати загрози, забезпечуючи швидші та ефективніші реакції. Необхідним у сфері оборонного ІІІ є прийняття законодавства для забезпечення прозорості, стандартизації та оптимізованих протоколів ліцензування та імпорту. Цей широкий спектр додатків на основі штучного інтелекту особливо важливий для підвищення обізнаності, готовності та можливостей під час війни, зокрема шляхом моделювання сценаріїв бойової підготовки, моніторингу відеоспостереження, збору та аналізу даних з відкритих джерел, аналізу розпізнавання осіб, розвідки та оцінки збитків. Він також стимулює внутрішнє виробництво продукції подвійного призначення, такої як тепловізійні камери, датчики та безпілотники [1].

Наступальний штучний інтелект викликає зростаюче занепокоєння щодо глобальної стабільності. Наступальний штучний інтелект відноситься до систем, призначених для допомоги або виконання шкідливих дій. Дослідження автора DarkTrace виявляє тривожну тенденцію: майже 74% експертів з кібербезпеки вважають, що загрози штучного інтелекту зараз є серйозною проблемою. Ці атаки не просто швидші й непомітніші; вони здатні розробляти стратегії, що виходять за межі людських можливостей, і здатні трансформувати поле бою в сфері

кібербезпеки. Використання образливого штучного інтелекту може поширювати дезінформацію, порушувати політичні процеси та маніпулювати громадською думкою. Крім того, зростає бажання використовувати автономну зброю на основі штучного інтелекту викликає занепокоєння, оскільки це може призвести до порушень прав людини. Встановлення керівних принципів їх відповідального використання є важливим для підтримки глобальної стабільності та підтримки гуманітарних цінностей [2]. Крім встановлення керівних принципів відповідального використання, на нашу думку, вже зараз необхідним є встановлення меж використання штучного інтелекту у військових цілях.

Застосування штучного інтелекту в кіберпросторі істотно змінює хід протистояння між оборонними та наступальними технологіями. Так, на сучасному етапі розвитку інформаційних технологій, системи та/або моделі штучного інтелекту використовуються не лише для посилення систем кіберзахисту, а й для розробки нових типів (видів) інформаційно-руйнівних впливів у вигляді адаптивних кібератак, потенційно спроможних уникати виявлення існуючими захисними системами. Кібератаки, створені з використанням штучного інтелекту характеризуються прикладною новизною, складністю, швидкістю адаптації та масштабованістю, що робить існуючі методи виявлення кібератак майже не ефективними, що у свою чергу створює серйозну загрозу для інформаційних систем як державного, так і комерційного призначення. До того ж, останнім часом спостерігається значне зростання кількості випадків створення кібератак і шкідливого програмного забезпечення з використанням моделей штучного інтелекту, як наслідок загальнодоступності та фактичної відсутності обмежень на їх використання [3].

Таким чином, маємо справу з кіберконфліктами, як проявами гібридної війни у кіберпросторі. При цьому обидві сторони протистояння використовують унікальні властивості штучного інтелекту як для вдосконалення своїх атак, так і для активного виявлення кіберзагроз і пом'якшення або нівелювання їх наслідків. В таких умовах наголошувати на пріоритетності забезпечення захисту прав людини за будь-яких умов означає бути слабкою стороною у війні з ворогом, для якого не існує жодних правил і пріоритетом є знищення противника за всяку ціну. Тому не дарма наголошується на тому, що країнам необхідно оновити свої політики захисту даних та конфіденційності, які не підходять для воєнного часу. Під час війни збір, аналіз та обмін великими обсягами державних та приватних даних можуть забезпечити значні переваги у таких галузях, як розвідка, стратегічна комунікація, цивільна оборона чи мобілізація. Необхідний реалістичний погляд на правове обмеження прав людини у воєнний час, і перевизначення

принципу «людина у контурі» матиме вирішальне значення для майбутніх стандартів сертифікації, відповідності та верифікації штучного інтелекту [1].

Література:

1. Гончарук В. Як Україна використовує штучний інтелект для оборони від російської агресії – Foreign Ukraine
2. Хазіка Саджид. Загроза наступального ШІ та як від неї захиститися. URL: <https://www.unite.ai/uk/загроза-наступального-AI-i-як-від-нього-захиститися/>
3. Фесьоха В. Особливості протистояння оборонного та наступального штучного інтелектів у кіберпросторі. International Science Journal of Engineering & Agriculture. 2024. № 3 (4). С. 105-114.

DOI <https://doi.org/10.36059/978-966-397-501-6-33>

МОДЕЛІ ПРАВОВОГО РЕГУЛЮВАННЯ КРИПТОВАЛЮТ У США: ПЕРСПЕКТИВИ АДАПТАЦІЇ В УКРАЇНІ

Цимбалюк Андрій Ігорович

*аспірант кафедри публічного права Юридичного факультету
Чернівецький національний університет імені Юрія Федьковича,
м. Чернівці, Україна*

Глобальні процеси на фінансових ринках та швидкий прогрес цифрових технологій зумовили появу нового класу активів – криптовалют, які відіграють дедалі вагомішу роль у сучасній економіці. Зростання популярності криптовалют пов'язане з їхньою децентралізацією, відносною конфіденційністю, а також можливостями для запровадження інноваційних фінансових послуг. Втім, такі переваги супроводжуються суттєвими ризиками, зокрема шахрайством, відмиванням коштів, ухиленням від податкових зобов'язань та нестабільністю ринкових умов. Через це особливо актуальним є питання юридичного регулювання сфери криптовалют.

Сполучені Штати Америки виступають лідером у формуванні правових моделей регулювання криптовалютного ринку. Їхній підхід характеризується розвиненою системою регуляторних інструментів, яка підтримує баланс між заохоченням розвитку цифрових активів і забезпеченням захисту інтересів суспільства. Україна, яка зараз активно рухається шляхом цифрової трансформації економіки, потребує адаптації цього міжнародного досвіду.