

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Кафедра цивільного права

ІТ-ПРАВО ТА КІБЕРБЕЗПЕКА В УМОВАХ ГІБРИДНОЇ ВІЙНИ

**МАТЕРІАЛИ
Всеукраїнського круглого столу**

Одеса,
12 квітня 2025 року

Одеса
Фенікс
2025

УДК 342.95 : 343.32 (477): 351.863
I-52

За загальною редакцією

доктора юридичних наук, професора **Є. Харитонova**,
кандидатки юридичних наук, доцентки **Ю. Кривенко**.

Упорядники-укладачі:

Кривенко Юлія – к.ю.н., доцентка кафедри цивільного права Національного університету «Одеська юридична академія», доцентка;

Лешкова Єлизавета – лаборантка кафедри цивільного права Національного університету «Одеська юридична академія».

ІТ-право та кібербезпека в умовах гібридної війни :
I-52 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. – 138 с. – Режим доступу:

ISBN 978-617-8430-57-3

Збірник містить матеріали доповідей з теоретичних, історичних і методологічних проблем ІТ-права та кібербезпеки, які були оприлюднені на Всеукраїнському круглому столі «ІТ-право та кібербезпека в умовах гібридної війни» 12 квітня 2025 у Національному університеті «Одеська юридична академія».

Збірник спрямований на ознайомлення громадськості з дослідженнями науковців у сфері ІТ-права та кібербезпеки і може бути корисний як у навчальному процесі, так і в практичній діяльності.

УДК 342.95 : 343.32 (477): 351.863

*Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть
учасники конференції, їхні наукові керівники, рецензенти,
які рекомендували ці матеріали до друку.*

ISBN 978-617-8430-57-3

© Колектив авторів, 2025

© НУ «Одеська юридична академія»,
2025

- розробки спеціального законодавства щодо цифрової спадщини та цифрових прав особи;
- введення спеціального режиму правового регулювання соціальних мереж, який забезпечить реальний захист цифрової ідентичності, включаючи право розпорядження контентом, створеним користувачем;
- врахування ризиків кіберзагроз і масового привласнення цифрової особистості у період гібридної війни – як додаткового чинника, що потребує негайного юридичного реагування.

Вивчення цифрової ідентичності на стику права, філософії та соціальних комунікацій дає змогу сформулювати нові підходи до розуміння особистості в епоху інформаційного суспільства.

ЛІТЕРАТУРА:

1. Харитонova О. І., Харитонов Є. О. Цифрова людина, цифрова особа та цифрова особистість: до проблеми співвідношення. *Часопис цивілістики*. 2023. Вип. 49. С. 5–13. URL: http://nbuv.gov.ua/UJRN/Chas_2023_49_3
2. Відшкодування шкоди завданої розповсюдженням недостовірної інформації в соціальних мережах. *Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція»*. 2019. № 42. Т. 1. С. 162–165.
3. Усанова Л. А., Супрун Г. Г. Цифрова ідентичність як відображення інформаційного суспільства. *Актуальні проблеми філософії та соціології*. 2021. № 13. С. 67–70. URL: http://apfs.nuoua.od.ua/archive/30_2021/13.pdf

Токарева Віра Олександрівна,

*кандидатка юридичних наук, доцентка, доцентка кафедри цивільного права
Національного університету «Одеська юридична академія»*

ДО ПИТАННЯ ВИКОРИСТАННЯ АВТОНОМНИХ СИСТЕМ У ЗБРОЙНОМУ КОНФЛІКТІ

Протягом останнього десятиліття дискусії навколо використання автономних систем у військовій сфері значною мірою були зосереджені на автономних системах зброї. Використання автономних систем зброї дійсно викликають гостре занепокоєння, оскільки використання автономних систем полягає в тому, що вони вико-

ристовується для збору розвідданих та для підтримки військових для вибору і ураження цілей. Останній аспект викликає занепокоєння.

Наразі випадки ІІІ під час ведення ввоєнних дій не завершуються наданням автономії збройовим системам, таким як включення системи в командування і управління даними, логістику та навчання. Занепокоєння викликає саме те, що автономні системи у озброєнні можуть запропонувати військові цілі та давати рекомендації своїм (людським) операторам, які можуть самостійно атакувати цілі, з урахуванням оброблених даних.

Відповідно до оборонних стратегій Організації Північноатлантичного договору зазначається, що критичними проблемами майбутніх десятиліт може саме дані які генеруються системами, а не робототехнік як така або притаманна їй автономія. Адже стверджується, що такі системи здатні розробляти дієві автономні системи для поліпшення таргетування, з огляду на оброблені данні[1]. Разом з тим, ефективність систем штучного інтелекту визначається якістю навчальних даних, оскільки вони забезпечують їх основні специфікації. Крім того, автономним системам властива непередбачуваність як призводить до проблем, ставлячи виклик міжнародному гуманітарному праві в цілому. В свою чергу виклики автономних систем полягають у відсутності розуміння та чинності для людини функціонування «чорного ящик». Тому, постає актуальними підтримання якості та походження даних, а також збереження за людиною прийняття остаточного рішення щодо вибору та залучення цілі.

Таргетування широко визначається як застосування сили сторін конфлікту проти окремих осіб або об'єктів поза їх контролем. Відповідно до міжнародного гуманітарного права цільовий відбір та залучення повинні дотримуватися основних принципів розрізнення, пропорційності, людяності та вимоги вжити всіх можливих запобіжних заходів.

Слід зазначити, що міжнародне гуманітарне право зобов'язує військових командирів та інших осіб, відповідальних за напади, за-

сновувати свої рішення на інформації з усіх джерел, доступних їм у відповідний момент часу. Зокрема, Міжнародний Комітет Червоного Хреста (далі МКЧХ) в контексті ведення міської війни рекомендує, проводити перевірку даних про наявність цивільних осіб та цивільних об'єктів, яка міститься у відкритих джерелах, таких як Інтернет. Відповідно до висновків МКЧХ системи підтримки прийняття рішень на основі ІІІ можуть допомагати збору та обробці даних, для сприяння оперативного прийняття рішень в умовах конфлікту та мінімізації ризиків для цивільного населення [2].

Прихильники використання систем штучного інтелекту у воєнних конфліктах стверджують, що ця технологія покликана «підвищити» військову точність. Разом з цим, дане твердження є не однозначним, оскільки походження та надійності даних які обробляються системою може бути сумнівним. Відтак одна із провідних проблем пов'язана із низькою якістю навчальних даних, що може призводити до упереджень, неправильних оцінок, ризиків втручання у приватність та втрати контролю управління над системою, які в поєднанні з непередбачуваністю технології створюють проблеми для ідентифікації цілей. Відсутність репрезентативності в навчальних даних здатно призвести до того, що автономні системи можуть некоректно ідентифікувати представників різних етнічних груп, в якості мішені або сприймати цивільних чоловіків, в якості як учасників бойових дій, через заковані гендерні упередження [3].

Не лише держави змагаються у лідерству озброєння але й лідери Big Tech також активно створюють та просувають свої технології збройним силам держав. Незважаючи на виникаючі ризики, автономні системи озброєння активно використовуються під час конфліктів, що не виключає ризиків ураження та цивільного населення.

Слід зазначити, що використання ІІІ протягом всього процесу таргетування спирається на прогнози, засновані на розпізнаванні образів і класифікації, через узагальнення даних, що використовуються під час навчання системи. Таким чином, здатність автономних систем рекомендувати цілі залежить від здатності «виявляти»

подібність між наявними та непрямими даними про населення та даними на яких систем навчалась. Це може викликати проблеми, через недосконалість автономних систем та можливі проблеми коректної ідентифікації через те, що навчальні данні та реальні поля відрізняються [3]. Оскільки, попри всі зусилля розробників, не можливо заздалегідь спроектувати усі варіанти можливих сценаріїв

Враховуючи викладене слід констатувати наступні основні проблеми використання автономних систем під час збройних конфліктів: ризики некоректної ідентифікації цивільного населення в якості цілі; неякісні початкові дані без належної репрезентативності вразливих груп та меншин, що призводить до упередженості даних та упередженості автономних систем.

ЛІТЕРАТУРА:

1. Summary of the NATO Artificial Intelligence Strategy. 2021. URL: https://www.nato.int/cps/en/natohq/official_texts_187617.htm
2. Stewart R. Hinds G. Algorithms of war: The use of artificial intelligence in decision making in armed conflict. October 24, 2023. URL: <https://blogs.icrc.org/law-and-policy/2023/10/24/algorithms-of-war-use-of-artificial-intelligence-decision-making-armed-conflict/>
3. Alvarez J.S. The risks and inefficacies of AI systems in military targetingsupport. 2024. URL: <https://blogs.icrc.org/law-and-policy/2024/09/04/the-risks-and-inefficacies-of-ai-systems-in-military-targeting-support/>

Вовчок Руслан Володимирович,

аспірант 2 року навчання Миколаївського навчально-наукового інституту права Національного університету «Одеська юридична академія».

Науковий керівник: к.ю.н., доц., доц. кафедри цивільного права Фасій Б. В.

ІНФОРМАТИЗАЦІЯ ТА ЦИФРОВІЗАЦІЯ СУСПІЛЬСТВА В ЕПОХУ СТІМКОГО РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

У XXI столітті світ вступив у фазу глобальної цифрової трансформації. Інформатизація та цифровізація стали невід'ємною частиною розвитку суспільства. На цьому тлі особливе місце займає стрімкий розвиток штучного інтелекту (ШІ), який змінює не лише технологічні підходи, а й соціальні, економічні та культурні процеси.

Резніченко Семен Васильович НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ПЕРЕВЕЗЕНЬ ПАСАЖИРІВ АВТОБУСАМИ	67
Святошнюк Арина Леонідівна ЗМІСТ ЦИВІЛЬНО-ПРАВОВИХ ВІДНОСИН У МЕРЕЖІ ІНТЕРНЕТ	73
Спасова Катерина Іванівна ЦИВІЛЬНО-ПРАВОВІ АСПЕКТИ ЦИФРОВОЇ ІДЕНТИЧНОСТІ В СОЦІАЛЬНИХ МЕРЕЖАХ	75
Токарева Віра Олександрівна ДО ПИТАННЯ ВИКОРИСТАННЯ АВТОНОМНИХ СИСТЕМ У ЗБРОЙНОМУ КОНФЛІКТІ	78
Вовчок Руслан Володимирович ІНФОРМАТИЗАЦІЯ ТА ЦИФРОВІЗАЦІЯ СУСПІЛЬСТВА В ЕПОХУ СТІМКОГО РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ	81
Кірсанов Олексій Володимирович ВЕРИФІКАЦІЯ БАНКІВСЬКИХ КАРТ КЛІЄНТА	85
Коштура Богдан Вячеславович ШТУЧНИЙ ІНТЕЛЕКТ ЯК УЧАСНИК ЕЛЕКТРОННИХ ПРАВОЧИНІВ	87
Романовський Денис Сергійович ІТ ПРАВА ТА КІБЕРБЕЗПЕКА ЛЮДЕЙ ПОХИЛОГО ВІКУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ	91
Рябченко Вікторія Олександрівна ПРОБЛЕМИ ЗАХИСТУ НЕПОВНОЛІТНІХ ВІД ВЕРБУВАННЯ ФСБ У СОЦМЕРЕЖІ «ТЕЛЕГРАМ»	95
Балик Даша Вікторівна ОСОБЛИВОСТІ ЗДІЙСНЕННЯ ПРАВА ВЛАСНОСТІ НА ЦИФРОВІ РЕЧІ	99
Білошкурський Микола Миколайович ЦИВІЛЬНО-ПРАВОВИЙ СТАТУС ІГРОВОЇ ОНЛАЙН-РЕЧІ НА ПРИКЛАДІ СЕРВІСУ STEAM	104
Забудько Анастасія Сергіївна ОСОБЛИВОСТІ СПАДКУВАННЯ ЦИФРОВИХ АКТИВІВ	111
Костенко Олександр Сергійович АВТОРСЬКІ ПРАВА НА ОБ'ЄКТИ, СТВОРЕНІ ШТУЧНИМ ІНТЕЛЕКТОМ: ПРАВОВІ АСПЕКТИ РЕГУЛЮВАННЯ	115
Мурашева Катерина Василівна ПЕРСОНАЛЬНІ ДАНІ ТА ЇХ ЗАХИСТ: ЦИВІЛЬНО-ПРАВОВІ АСПЕКТИ В УМОВАХ КІБЕРЗАГРОЗ	119
Рогожа Валерія Василівна РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ: ЗАХИСТ ЧИ ЗАГРОЗА?	124
Фасій Анастасія Володимирівна ДО ПИТАННЯ ПРО ПРАВОВЕ РЕГУЛЮВАННЯ РЕКЛАМИ В СОЦІАЛЬНИХ МЕРЕЖАХ	128
ВИСНОВКИ	132