

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

**ІТ-ПРАВО
ПІД ЧАС ГІБРИДНОЇ ВІЙНИ:
ВІД ПОШУКУ ПАРАДИГМИ
ДО ПРАГМАТИЧНИХ РІШЕНЬ**

Колективна монографія

*За редакцією
Є. Харитонова, О. Харитонової, І. Давидової*

Одеса
Фенікс
2025

*Рекомендовано рішенням вченої ради
Національного університету «Одеська юридична академія»
(протокол № 9 від 30 червня 2025 р.)*

Рецензенти:

Майданик Р. А. – академік НАПрН України, доктор юридичних наук, професор, професор кафедри цивільного процесу Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка;

Соколов А. В. – доктор технічних наук, професор, професор кафедри кібербезпеки Національного університету «Одеська юридична академія»;

Маковій В. П. – кандидат юридичних наук, професор, завідувач кафедри цивільно-правових дисциплін Одеського державного університету внутрішніх справ.

I-87 **ІТ-право під час гібридної війни: від пошуку парадигми до практичних рішень** : кол. монографія / за заг. ред. проф.: Є. Харитонова, О. Харитонової, І. Давидової. – Одеса : Фенікс, 2025. – 588 с.
ISBN 978-617-8430-70-2

Монографія є продовженням циклу праць колективу кафедри цивільного права Національного університету «Одеська юридична академія», присвячених результатам досліджень цивілістичних шкіл університету від часу їхнього формування до гібридної війни, що триває нині. У третьому томі аналізуються в контексті гібридної війни: проблеми визначення концепту «ІТ-право», особливості правового регулювання відносин, що виникають у зв'язку з використанням інформаційних технологій, особливості механізму цивільно-правового регулювання у сфері ІТ, чинник симулякру, значення та роль інформаційного середовища як стратегічного ресурсу, правові рамки для цифрових активів і перспективи цифрової власності, ІТ-правочини, порушення прав інтелектуальної власності в Інтернет, протидія кіберзагрозам у гібридній кібервійні, загрози вербування неповнолітніх через соцмережі та месенджери та юридичні заходи запобігання таким загрозам, правове регулювання стартапів, е-кредитування, цивільно-правова відповідальність за шкоду, завдану кібератаками, забезпечення інформаційної безпеки електронного судочинства в умовах гібридної війни в Україні та ін.

Авторський колектив концентрував увагу на обґрунтуванні необхідності комплексного вирішення практичних питань впорядкування інформаційно-технологічні відносини в умовах гібридної російсько-української війни. Автори прагнули розкрити особливості правового регулювання цих відносин і запропонувати власне бачення шляхів вирішення проблем, що виникають у цій сфері. Усвідомлюючи спірність низки висновків і пропозицій, автори розраховують на продовження плідних дискусій з проблем правового регулювання інформаційних технологій, зокрема в умовах гібридної війни.

Монографія може бути цікавою науковцям, практикуючим юристам, викладачам, аспірантам, здобувачам вищої освіти, а також широкому загалу небайдужих українців, які цікавляться проблемами правового регулювання у сфері ІТ, зокрема під час гібридної війни.

УДК 340:004:327:355

ЗМІСТ

Авторський колектив	5
Розділ 1. Прагматична (соціологічна) школа «ІТ-права» – відповідь цивілістики на виклики інформаційного суспільства (Євген Харитонов, Олена Харитонova, Ірина Давидова)	7
Розділ 2. Концепт ІТ-права (Євген Харитонов, Олена Харитонova)	30
Розділ 3. Гібридна інформаційна війна та інформаційні технології (Євген Харитонов, Олена Харитонova)	65
Розділ 4. ШІ як бінарна категорія ІТ (Євген Харитонов, Олена Харитонova)	93
Розділ 5. Симулякр, гібридна (інформаційна) війна і потенціал ІТ (Євген Харитонов, Олена Харитонova)	119
Розділ 6. Інформаційне середовище як стратегічний ресурс у гібридних конфліктах (Оксана Калітенко)	143
Розділ 7. Правові рамки для цифрових активів: перспективи цифрової власності (Катерина Некіт)	175
Розділ 8. Захист немайнових прав у медіапросторі в період гібридної війни (Алла Кирилюк, Лариса Галупова)	203
Розділ 9. ІТ-правочини в умовах гібридної війни (Ірина Давидова)	250
Розділ 10. Порушення прав інтелектуальної власності в мережі інтернет під час гібридної агресії в умовах воєнного стану (Наталія Бааджи)	279
Розділ 11. Кіберзагрози у гібридній кібервійні: дія і протидія (Євген Харитонов, Олена Харитонova)	323
Розділ 12. Етико-юридичні аспекти використання штучного інтелекту в мережі інтернет в умовах гібридної війни (Олександр Омельчук)	351
Розділ 13. Застосування систем автоматизованого прийняття рішень під час збройного конфлікту (Віра Токарева)	378

Розділ 14. Гібридна війна і кіберзброя (Євген Харитонов, Олена Харитонova)	388
Розділ 15. Вербування неповнолітніх через соцмережі та месенджери в умовах гібридної війни: загрози, механізми та заходи запобігання (Вікторія Рябченко).	420
Розділ 16. Правове регулювання діяльності стартапів в умовах гібридної війни: виклики, можливості та перспективи (Дмитро Розумейко).	435
Розділ 17. Е-кредитування у період воєнного стану (Олена Берназ-Лукавецька)	453
Розділ 18. Цивільно-правова відповідальність за шкоду, завдану кібератаками (Богдан Фасій)	483
Розділ 19. Сімейні правовідносини в сфері інформаційних технологій в умовах гібридної війни (Оксана Сафончик)	514
Розділ 20. Забезпечення інформаційної безпеки електронного судочинства в умовах гібридної війни в Україні (Крістіна Дрогозюк)	545
Розділ 21. Кіберспортивна дипломатія: перспективи для України (Максим Ткалич, Юлія Толмачевська)	557
Список основних праць представників школи	565

Авторський колектив

Харитонов Євген (ORCID ID: 0000-0001-5521-0839), доктор юридичних наук, професор, член-кореспондент НАПрН України, зав. кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з О. Харитоновою, І. Давидовою); розділ 2 (у співав. з О. Харитоновою); розділ 3 (у співав. з О. Харитоновою); розділ 4 (у співав. з О. Харитоновою); розділ 5 (у співав. з О. Харитоновою); розділ 11 (у співав. з О. Харитоновою); розділ 14 (у співав. з О. Харитоновою);

Харитонova Олена (ORCID ID: 0000-0002-9681-9605), докторка юридичних наук, професорка, членкиня-кореспондент НАПрН України, зав. кафедри права інтелектуальної власності і патентної юстиції НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, І. Давидовою); розділ 2 (у співав. з Є. Харитоновим); розділ 3 (у співав. з Є. Харитоновим); розділ 4 (у співав. з Є. Харитоновим); розділ 5 (у співав. з Є. Харитоновим); розділ 11 (у співав. з Є. Харитоновим); розділ 14 (у співав. з Є. Харитоновим);

Давидова Ірина (ORCID ID: 0000-0001-5622-671X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, О. Харитоновою); розділ 9;

Некіт Катерина (ORCID ID: 0000-0002-3540-350X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 7;

Сафончик Оксана (ORCID ID: 0000-0001-6781-8219), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 19;

Бааджи Наталія (ORCID ID: 0000-0002-9889-4879), кандидатка юридичних наук, доцента, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 10;

Берназ-Лукавецька Олена (ORCID ID: 0000-0002-2133-1672), кандидатка юридичних наук, доцента, доцентка кафедри цивільного права НУ «ОЮА»: розділ 17;

Галупова Лариса (ORCID ID: 0000-0001-6263-2773), кандидатка юридичних наук, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з А. Кирилюк);

Дрогозюк Крістіна (ORCID ID: 0000-0001-9254-9575), кандидатка юридичних наук, доцента, доцентка кафедри цивільного, нотаріального та виконавчого процесу НУ «ОЮА»: розділ 20;

Калітенко Оксана (ORCID ID: 0000-0003-1001-3561), кандидатка юридичних наук, доцентка, професорка кафедри цивільного права НУ «ОЮА»: розділ 6;

Кирилюк Алла (ORCID ID: 0000-0002-3051-6599), кандидатка юридичних наук, доцентка, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з Л. Галуповою);

Омельчук Олександр (ORCID ID: 0000-0002-0082-3619), кандидат юридичних наук, доцент, доцент кафедри цивільного права НУ «ОЮА»: розділ 12;

Ткалич Максим (ORCID ID: 0000-0003-4224-7231), кандидат юридичних наук, доцент, доцент кафедри цивільного права Запорізького національного університету: розділ 21 (у співав. з Ю. Толмачевською);

Токарева Віра (ORCID ID: 0000-0002-8409-1477), кандидатка юридичних наук, доцентка, доцентка кафедри цивільного права НУ «ОЮА»: розділ 13;

Толмачевська Юлія (ORCID ID: 0000-0002-7964-8875), докторка філософії (081 право): розділ 21 (у співав. з О. Ткаличем);

Фасій Богдан (ORCID ID: 0000-0002-8715-930X), кандидат юридичних наук, доцент, декан факультету судового та міжнародного права НУ «ОЮА»: розділ 18;

Розумейко Дмитро (ORCID ID: 0000-0001-8206-1031), аспірант кафедри цивільного права НУ «ОЮА»: розділ 16;

Рябченко Вікторія (ORCID ID: 0009-0007-1542-6492), аспірантка кафедри цивільного права НУ «ОЮА»: розділ 15.

Розділ 12

ЕТИКО-ЮРИДИЧНІ АСПЕКТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В МЕРЕЖІ ІНТЕРНЕТ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

DOI

Олександр Омельчук
кандидат юридичних наук, доцент

Формування інформаційного суспільства в Україні напряду пов'язане з розвитком та широким впровадженням цифрових технологій. Тотальна діджиталізація суспільного та особистого життя на даний момент об'єктивується як елемент чинної реальності, а отже актуалізуються для вивчення питання правового регулювання сучасної сфери інформаційних відносин та захисту прав та інтересів (як приватних, так і суспільних) в даній сфері.

На сьогодні перспективи використання ШІ викликають інтерес не лише в експериментальних та прикладних технічних галузях, соціальній та економічній сфері. Людство працює над удосконаленням технологій та вирішенням філософських питань стосовно ШІ, держави та міжнародні організації мізкують над іншими проблемними питаннями – про встановлення юридичної природи ШІ так про результати його діяльності, а також про те, чи може він бути застосованим у правових та організаційних аспектах використання нематеріальних активів.

Як слушно відмічає О. С. Котуха, неконтрольоване та беззастережне втручання у «цифровий світ», а також в життя людей за його допомогою може спричинити серйозні порушення прав і свобод людини та громадянина, порушення особистих кордонів, руйнування звичних підвалин життя населення, втрату звичаїв тощо.¹

¹ Котуха О. С., Попов Д. І. Штучний інтелект та права людини: проблеми цифровізації права на сучасному етапі розвитку електронної держави. *Вісник Львівського торговельно-економічного університету*. 2024. № 15. С. 22.

Вітчизняні дослідники проблем правового регулювання штучного інтелекту також вказують на проблему ризиків дезінформації, зумовлених поширенням ШІ (приклади останньої можуть з'являтися у текстах, згенерованих за допомогою ШІ), а, поряд з цим, і на проблему потенційного збільшення кількості випадків порушення авторського права.¹

На сьогоднішній день ШІ вже може обробляти велику кількість даних та навчатися, щоб вирішувати задачі, генерувати текст, фото, відео, аудіо, код, інформацію та її сукупність. ШІ вже зараз здатний аналізувати дані, змішувати їх і генерувати на їхній основі новий та неповторний результат.²

За прогнозами експертів найближчим часом ШІ перейде від узагальнених продуктів до рішень, орієнтованих на розв'язання конкретних завдань. Окрім того, ШІ проникатиме в різні сфери життя й бізнесу – від зміни клімату до охорони здоров'я.³ Більшість людей не усвідомлюють, що вже зараз використовують технології штучного інтелекту у щоденному житті, в освіті та медицині, комунікаціях та соціальній сфері, економіці та юридичній сфері.⁴

О. Косілова та Х. Солодовнікова, аналізуючи наявні застереження щодо використання ШІ, приходять до висновку, що людство не просто на порозі відкриття «надрозуму», а й може просто вже опинитися перед обличчям загрози, яка полягає в жорсткій конкуренції між людиною та штучним інтелектом, і останній стрімко завойовує усі сфери буття людини, що, на думку вченого, є серйозною загрозою основоположним правам людини. Саме тому обумовлюється необхідність відповідного всебічного захисту людини, в тому числі й юридично-правового.⁵

¹ Пертів О. Штучний інтелект та авторське право. Центр демократії та верховенства права. 2023. URL: <https://cedem.org.ua/analytics/shtuchnyi-intelekt-avtorske-pravo/>

² Спесивцева О. Право sui generis: як штучний інтелект адаптує під себе авторське право? *Юридична газета*. 2024. URL: <https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/pravo-sui-generis-yak-shtuchniy-intelekt-adaptue-pid-sebe-avtorske-pravo.html>

³ Баловсяк Н. Прикладний штучний інтелект і заборона соцмереж для дітей. Чого чекати від 2025-го технологічного. *Український тиждень*. 2024. URL: <https://tyzhden.ua/prykladnyy-shtuchniy-intelekt-i-zaborona-sotsmerezhe-dlia-ditej-choho-chekaty-vid-2025-ho-tekhnohichnoho/>

⁴ Живцова Л. І. Штучний інтелект: сутність та перспективи розвитку. *Український журнал будівництва та архітектури*. 2023. № 3. С. 67-71.

⁵ Косілова О. І., Солодовнікова Х. К. Права і свободи людини і громадянина V. S. Штучний інтелект: проблемні аспекти. *Інформація і право*. 2020. № 4(35). URL: <http://bulletin.kpi.ua/index.php/2616-6798/article/view/221218>

Для ефективного досягнення результатів даного дослідження важливим є формування коректного розуміння понять нейромережа та штучний інтелект, а також визначення природи «використання» останніх в мережі Інтернет.

Сучасна концепція штучного інтелекту (ШІ) – це сукупність наукових дисциплін і методів, призначених для обробки даних та вирішення складних обчислювальних завдань.¹

О. А. Баранов відзначає, що відсутність консенсусної дефініції терміну «штучний інтелект» хвилює практично всіх представників філософських, гуманітарних, технічних та інших наук. В той же час для представників правової науки ця проблема набуває особливо гострих форм, тому що даний термін не є спеціально-юридичним, має універсальний характер та має бути однаково зрозумілим для представників будь-яких політичних, наукових та бізнесових кіл, верств населення, сфер соціального життя тощо.²

В сучасному цивільному законодавстві неодноразово згадується штучний інтелект. В той же час, термін «штучний інтелект» є досить новим для українського законодавства, що створює проблеми з чітким правовим визначенням та регулюванням цього поняття.

Відповідно до Концепції розвитку штучного інтелекту в Україні, Окрім цього затвердженої Кабінетом Міністрів України розпорядженням № 1556-р від 02 грудня 2020 р. штучний інтелект – це організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань.³

¹ Фоміна Н. Чи можуть твори, створені за допомогою ШІ, розраховувати на авторське право. *Юридична газета*. 2023. № 11-12(769-770). URL: <https://jur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/chi-mozhut-tvori-stvoreni-za-dopomogoyu-shi-rozrahovuvati-na-avtorske-pravo.html>

² Баранов О. А. Визначення терміну «штучний інтелект». *Інформація і право*. 2023. № 1(44). С. 33.

³ Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України; Концепція від 02.12.2020 № 1556-р. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text>

Штучний інтелект представляє собою технологію, що дозволяє комп'ютерним системам виконувати завдання, які зазвичай потребують людського інтелекту, такі як розпізнавання мови, розуміння текстів, аналіз даних та прийняття рішень. Штучний інтелект широко застосовується у всіх галузях, включаючи літературу, мистецтво та інші творчі напрямки. Він є передовою галуззю розвитку технологій і має значний вплив на різні аспекти життя.¹

В юридичній науці штучний інтелект визначають як певну сукупність методів, способів, засобів та технологій, насамперед, комп'ютерних, що імітує (моделює) когнітивні функції, які мають критерії, характеристики та показники еквівалентні критеріям, характеристикам та показникам відповідних когнітивних функцій людини. Згадування у дефініції комп'ютерних технологій не впливає на основний сенс розуміння штучного інтелекту та не обмежує можливість його застосування в рамках інших фундаментальних підходів до побудови штучного інтелекту.²

Нейронна мережа, також штучна нейронна мережа, або ШНМ – це один із напрямків у створенні штучного інтелекту, який ставить своїм завданням відтворити аналітичну роботу людського мозку. Математична модель ШНМ бере свої витоки з біології, а в її основі лежить принцип роботи нервової системи живих організмів, де мільярди нейронів з'єднані синапсами, приймають вхідні дані у вигляді електричних імпульсів, обробляють і передають іншим нейронам.³

Нейромережа за допомогою штучних нейронів може визначати закономірності, збирати та аналізувати інформацію, розпізнавати звуки, символи та зображення, вчитися на власному досвіді.

Одним зі способів утілення прикладного ШІ в найближчому майбутньому має стати агентний штучний інтелект, під яким розуміється автономні системи ШІ, здатні самостійно планувати й виконувати завдання для досягнення поставлених цілей. Вони можуть діяти незалежно, ухвалюючи рішення без постійного втручання людини з

¹ Вальчук Д. В. Авторське право штучного інтелекту: проблеми та шляхи вирішення. *Modern scientific journal*. 2024. № 3 (1). С. 8-9.

² Баранов О. А. Визначення терміну «штучний інтелект». *Інформація і право*. 2023. № 1(44). С. 46.

³ Ладуба М. Нейромережі пишуть книги та рятують життя: що таке нейронна мережа і як вона працює. URL: <https://mc.today/uk/shho-take-nejronna-merezha/>

метою спростити й автоматизувати різноманітні процеси – від відповідей на електронні листи до оцінювання студентських робіт та опрацювання замовлень інтернет-магазинів.¹

Одним з найбільш поширених і зрозумілих на сьогоднішній день видів ШІ, що на сьогоднішній день використовуються в мережі Інтернет є генеративний штучний інтелект. Генеративний ШІ – це інноваційний напрямок штучного інтелекту, що дозволяє створювати унікальний контент: тексти, зображення та аудіо. Він відрізняється від традиційного ШІ тим, що не просто аналізує або класифікує дані, а генерує новий унікальний контент.²

«Творчість» штучного інтелекту вже сьогодні широко використовується та непогано монетизується. Однак, слід однак зазначити, що авторські права на творчість алгоритмів – поки сіра зона світу юриспруденції.³ Т. Харебава виділяє три підходи до визначення, хто може бути автором створеного за допомогою ШІ об'єкта:

- розробник штучного інтелекту: у цьому випадку авторство може належати особі або групі людей, які розробили алгоритми та програми штучного інтелекту, що використовуються для створення творів;
- користувач штучного інтелекту: іноді особа, яка використовує штучний інтелект, може бути визнана автором твору, який був згенерований ШІ, особливо якщо вона надала важливі вхідні дані, параметри або інструкції для генерації твору;
- безпосередньо штучний інтелект (концепція «електронної особи»): у деяких контекстах розглядається можливість визнання штучного інтелекту як автора твору, якщо він має достатньо високий рівень самостійності і творчості у генерації контенту.⁴

¹ Баловсяк Н. Прикладний штучний інтелект і заборона соцмереж для дітей. Чого чекати від 2025-го технологічного. *Український тиждень*. 2024. URL: <https://tyzhden.ua/prykladnyj-shtuchnyj-intelekt-i-zaborona-sotsmerezhi-dlia-ditej-choho-chekaty-vid-2025-ho-tekhnologichnoho/>

² Що таке генеративний штучний інтелект і де він застосовується? URL: <https://blog.colobridge.net/uk/2023/11/generative-artificial-intelligence-ua/>

³ Дудко В. Як палає Кремль. Нейромережі генерують картини з тексту і допомагають збирати на ЗСУ. Чи може нейроарт стати бізнесом. *Forbes Digital*. 2022. URL: <https://forbes.ua/inside/yak-palae-kreml-neyromerezhi-generuyut-kartini-z-tekstu-i-dopomagayut-zbirati-na-zsu-chi-mozhe-neyroart-stati-biznesom-23082022-7861>

⁴ Харебава Т. Авторські права на об'єкт, створений штучним інтелектом. *Юрліга*. 2024. URL: https://jurliga.ligazakon.net/analitics/225383_avtorsk-prava-na-obkt-stvoreniy-shtuchnim-ntelektom

Два роки тому набрав чинності Закон України «Про авторське право і суміжні права». Згідно положень даного закону результат роботи штучного інтелекту підпадає під правове регулювання як неоригінальний об'єкт, згенерований комп'ютерною програмою, що охороняється правом особливого роду (*sui generis*). Однак, як відмічають дослідники, питання авторських та суміжних прав, пов'язаних з штучним інтелектом, є складними і потребують уточнення у законодавстві. На сьогоднішній день в більшості країн законодавці продовжують вивчати цю проблему і шукати оптимальні рішення, які враховували б потреби розвитку технологій та гарантували захист прав власників інтелектуальної власності.¹

Питання застосування ШІ на сьогоднішній момент стикається з необхідністю визначення ряду факторів, що обґрунтовують етичність такого застосування.

Ю. Гайдай визначає наступні ризики етичного характеру щодо використання ШІ в мережі Інтернет:

- ризики для особистих даних і приватності. Мовні моделі, по-перше, можуть робити дуже багато узагальнень, поєднань інформації і висновків з отриманих даних, які можуть бути недоступними для людини, що аналізує інформацію. Наприклад, з наборів даних про поведінку людини у соцмережах та інтернеті загалом, тих же запитів до чатботів великих мовних моделей, можна робити глибокі висновки щодо її психічного стану, звичок, розкладу дня тощо. Поєднання великих масивів даних та їх аналіз ШІ створюють додаткові загрози приватності, які не очевидні для користувачів, бо окремо ці дані не створюють загроз.
- ризики сегрегації – мовні моделі, за рахунок того, як саме і на основі яких даних навчаються, можуть надавати перевагу окремим соціальним групам. Вони будуть краще працювати з цими групами, а іншим приділяти менше уваги і маргіналізувати їх, вилучати певні меншини (етнічні або інші) та відтворювати людські упередження щодо цих меншин;
- ризики неточності і неправдивості інформації – мовні моделі не дуже добре відрізняють факти від вигадок, але при цьому ство-

¹ Вальчук Д. В. Авторське право штучного інтелекту: проблеми та шляхи вирішення. *Modern scientific journal*. 2024. № 3 (1). С. 14.

рюють враження, що вони є достовірними співрозмовниками, що може створювати багато загроз;

- безпекові ризики – мовні моделі дуже зручно використовувати для масової дезінформації, причому персоналізованої дезінформації «з людським обличчям», заточеної під конкретні групи людей, наприклад, шляхом коментування у соцмережах та у медіа;
- загроза правам людини через використання штучного інтелекту державними органами – передбачається насамперед здатність опрацьовувати величезні масиви даних, роблячи узагальнення і висновки щодо окремих людей. Це можливості розпізнавання, а отже, відстежування людей як фізично, так і деанонімізація їхньої онлайн-поведінки. Це дає державним органам потужні інструменти втручання у приватність, а безконтрольне застосування ШІ може призвести до ухвалення неправомірних чи хибних рішень стосовно громадян – застосування санкцій, відмови у доступі до послуг, кредиту, працевлаштування тощо.¹

Для певної структуризації та побудови логіки дослідження слід визначити сфери, в яких консолідується використання штучного інтелекту в Інтернеті. Окреслення останніх дасть змогу визначити основні джерела потенційних загроз штучного інтелекту, в тому числі потенціал використання штучного інтелекту для цілей ведення гібридної війни.

Серед основних функцій мережі Інтернет зазвичай називають інформативну. Оперативність та розмаїття інформації, наявної в мережі залишається значною перевагою використання Інтернету для задоволення інформаційних потреб.

Серед вкрай важливих в умовах воєнного стану видів інформації слід окремо виділити новини в мережі Інтернет, наявність яких дає змогу реалізувати поточну потребу в доступі до даних щодо подій в Україні та світі. Дослідники природи ЗМІ підтримують позицію, що засоби масової інформації залишаються засобом формування громадської думки,² адже ще з часів появи газет, а згодом телебачен-

¹ Гайдай Ю. Тренди ШІ: які етичні загрози несе використання штучного інтелекту. URL: https://speka.media/trendi-si-yaki-etichni-zagrozi-nese-vikoristannya-stucnogo-intelektu-v4q3wp?utm_source=google&utm_medium=cpc&utm_campaign=20972733776&gad_source=1

² Мороз Н. О. Роль засобів масової інформації у формуванні громадянського суспільства в Україні. *Гуманітарний журнал*. 2012. № 2-3. С. 206.

ня, методи, способи і форма подачі новин визначалися відповідно до мети публікації такої новини.

Широке використання сучасних технологій в новинній сфері пов'язане з необхідністю якнайшвидшої трансляції новини на широку аудиторію в умовах конкуренції ЗМІ, запитом аудиторії новин на фільтрацію новин, потребою в забезпеченні доступу до новин за будь-яких обставин та з будь-якого пристрою. Залучення функціоналу нейромереж та штучного інтелекту в сфері створення та розповсюдження новинного контенту здійснюється за наступними напрямками:

- використання ШІ для збору, обробки, перекладу, фільтрування, групування, перевірки, ранжування новинного контенту;
- використання ШІ для аудіовізуального оформлення новинного контенту;
- використання ШІ для генерування фейкових новин.

Слід відзначити, що не лише зміст та інтерпретація інформації про подію, що формують новину, впливають на сприйняття адресатом даної новини. Потенційну реакцію споживача новинного контенту визначають також форма подачі матеріалу, контекст, оформлення тощо. Крім того певний новинний контент не може сприйматися відокремлено від супутніх новин, а отже при формуванні думки в споживача новинного контенту мають значення як розподіл та ранжування новин, так і новини, що подаються поряд (на фоні яких сприймається новина).

Як відзначають дослідники проблематики використання штучного інтелекту в журналістиці, попри значні перспективи та переваги широкого залучення штучного інтелекту при відборі новинного контенту, невирішеними залишаються питання дотримання прав інтелектуальної власності авторів новинного контенту.¹ Крім того, безконтрольне використання штучного інтелекту при генеруванні новинного контенту може призвести до значних етичних колізій, адже не будь-який контент слід поширювати з етичних міркувань, а методи збору інформації повинні виходити з принципів (та сама журналістська етика).

¹ Горон Д. Епоха штучного інтелекту: як журналістиці пристосуватися до змін. *Детектор медіа*. 2025. URL: <https://detector.media/infospace/article/237260/2025-01-20-epokha-shtuchnoho-intelektu-yak-zhurnalistytsi-prystosuvatysya-do-zmin/>

Шкідливий вплив використання ШІ та нейромереж в сфері генерації новинного контенту чинить також свідоме використання даного контенту в воєнних або політичних цілях. Саме в цьому контексті доречно звернутися до широко вживаного в останній час поняття ІПСО (інформаційно-психологічні спецоперації).

Під ІПСО розуміється комплекс заходів з поширення спеціально підготовленої інформації для впливу на емоції, почуття, поведінку людей. До елементів ІПСО зазвичай відносять дезінформацію, пропаганду, кібератаки, перебільшення певної інформації або применшення іншої.¹

Як зазначає І. Колеснікова, в умовах гібридної війни актуалізується проблема протидії пропаганді та дезінформації. Дослідниця відмічає значне поширення інформації, що спрямована на глорифікацію військового вторгнення РФ на територію України та його учасників, дискредитацію керівництва України, ЗСУ та правоохоронних органів, посилення фрустраційних настроїв або розпалювання ворожнечі серед населення за етнічними, релігійними та іншими ознаками. На думку науковиці, «особлива небезпека російської пропаганди та дезінформації обумовлена тим, що значна частина її здійснюється в мережі Інтернет у відкритих джерелах, зокрема, у тих, в яких відсутня цензура. Реалізація злочинного наміру пропагандистів несе у собі велику загрозу, оскільки Інтернет має низку переваг, які зловмисники використовують у злочинних цілях. Серед них такі як широке охоплення аудиторії, можливість анонімного розміщення інформації, вільний доступ та висока швидкість поширення у географічній площині. Тому російська пропаганда, яка розповсюджується в мережі Інтернет представляє масштабну загрозу для національної безпеки країни, несвочасне вирішення якої може призвести до руйнівних наслідків, як у межах України, так і для всього цивілізованого світу».²

¹ Бартельова А., Рудь О. Інформаційно-психологічні операції як основна загроза інформаційній безпеці держави. *Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи*: Матеріали конференції. 2023. URL: https://www.researchgate.net/publication/376773925_Informacijno-psihologichni_operacii_ak_osnovna_zagroza_informacijnij_bezpeki_derzavi

² Колеснікова І. А. Проблеми протидії пропаганді та дезінформації у відкритих джерелах інформаційно-телекомунікаційної мережі інтернет. *Актуальні проблеми протидії злочинності та корупції*: збірник тез Всеукраїнської науково-практичної конференції (Харків, 17 лютого 2023 р.). С. 88.

На сьогоднішній день генерування фейкових новин з метою викликати у адресата хибну впевненість у події, що не відбулася, є складовою інформаційної війни проти України. Так, свого часу російська держава створила цілу систему інформаційно-психологічного забезпечення як складову системи своєї національної безпеки.¹

Значний доробок використання ІІІ припадає на соціальні мережі. Так, соціальні мережі, з одного боку, є платформою для вільного обміну інформацією та думками, проте, з іншого боку, вони можуть стати засобом поширення ненависті, дискримінації та маніпуляцій.²

Лідером із поширення фейків у соціальних мережах є Facebook. У Facebook найрозгалуженіша інструментальна мережа, що працює в двох напрямках: для збору даних і зміни поведінки людей – впливу чи нав'язування.³

Наявні діджитал-інструменти дозволяють за допомогою ІІІ розрізняти органічне та скоординоване розповсюдження контенту, виявляти автоматизовані системи розповсюдження спаму, оцінювати вплив на аудиторію різних облікових записів користувачів соцмереж, відрізняти ботів від реальних користувачів тощо.⁴

В умовах гібридної війни штучний інтелект широко застосовується для ідентифікації та розпізнавання мертвих солдатів противника та знищеної техніки за допомогою аналізу соціальних мереж та аналогічних матеріалів в новинному сегменті мережі Інтернет.

Так, в умовах повномасштабної війни технології компанії Clearview AI використовуються для встановлення осіб російських солдатів, навіть на фото низької якості та навіть фото мертвих солдатів з поля бою.

Так за допомогою відповідного програмного забезпечення стало можливим точне розпізнавання як живих, так і мертвих противників з можливістю виявлення ім'я солдата, рідного міста та профілів у соціальних мережах.

¹ Дмитренко М. А. Інформаційно-психологічні операції в контексті інформаційної безпеки України. *Інформація і право*. 2025. № 1(52). С. 116.

² Хоменко Ю. І. Мова ворожнечі в соціальних мережах: форми прояву та механізми протидії. Запоріжжя: ЗНУ, 2024. 49 с.

³ Ейсмунт В. Як створюють фейки у Facebook, YouTube, Telegram та Viber. URL: https://zaxid.net/statti_tag50974/

⁴ Штучний інтелект і дезінформація: можливості та ризики в умовах війни. *Укрінформ*. URL: <https://www.ukrinform.ua/rubric-technology/3691961-stucnij-intelekt-i-dezinformacia-mozlivosti-ta-riziki-v-umovah-vijni.html>

Як зазначає Ю. Коваленко, застосування технологій ШІ на сьогоднішній день надає широкий спектр можливостей в військовій сфері, адже «ШІ може покращити та оптимізувати процес прийняття рішень на полі бою, поглибити обізнаність та розуміння поля бою, забезпечити перевагу, адаптивність планування сил та підвищити точність і швидкість прийняття рішень, зокрема й щодо виявлення, ідентифікації, оцінки загроз та реагування на них. Впровадження ШІ у військовій сфері може передбачати, серед іншого, розробку БпЛА, антидронових рушниць, систем управління боєм, тренувальних модулів, систем кібербезпеки. Завдяки ШІ стає можливою й розробка новітнього озброєння, впровадження автономних систем озброєнь (АСО), тобто бойових систем, що здатні самостійно ідентифікувати та вражати ціль, а також летальних автономних систем озброєнь (ЛАСО), тобто таких систем зброї, які можуть виявляти, визначати цілі та атакувати їх без прямої участі людини у прийнятті рішення про момент та об'єкт атаки. Однак використання ШІ у військових цілях нерідко викликає й певні етичні та моральні занепокоєння, особливо у контексті використання летального автономного озброєння».¹

Як відзначає В. Шевчук, у сучасних умовах гібридної війни правоохоронні органи також активно використовують технології штучного інтелекту за різними напрямками, серед яких дослідник виокремлює: 1) розпізнавання обличчя та ідентифікація російських військових-окупантів у соціальних мережах та камерах відеозапису; 2) забезпечення безпеки на дорогах, виявлення та фіксація порушень правил дорожнього руху; 3) використання безпілотників для протидії незаконному обігу вогнепальної зброї, наркозлочинності, збирання доказової інформації умовах війни і ведення активних бойових дій з метою фіксації воєнних злочинів; 4) попередження кримінальних правопорушень з використанням інтелектуальних систем безпеки з різними пристроями (датчиками) збору інформації; 5) прогнозування кримінальних правопорушень методом картографування злочинності, за допомогою якого формуються прогнози щодо місцевої злочинності та індивідуальної злочинної поведінки.²

¹ Коваленко Ю., Войнов М. Штучний інтелект та права людини: орієнтири та обмеження у контексті національної безпеки та оборони. 2024. URL: https://www.helsinki.org.ua/wp-content/uploads/2024/05/Preview_AI_human_right_A4-1.pdf

² Шевчук В. М. Використання технологій штучного інтелекту та процес цифровізації криміналістики в умовах війни. *Актуальні проблеми протидії злочинності та корупції*: збірник тез Всеукраїнської науково-практичної конференції (Харків, 17 лютого 2023 р.). С. 172-173.

Одночасно з безцінним результатом, що надає функціонал відповідного ШІ, процес ідентифікації викликає занепокоєння експертів в контексті етико-юридичної оцінки такого використання ШІ. Так, неодноразово наголошувалося на сумнівах щодо легальності збору даних, необхідних для ідентифікації, адже такі дані збираються з порушенням прав на конфіденційність, а подальше їх використання може бути пов'язане з ризиками контролю над населенням.

Так, в експертному середовищі панує думка, що використання цих інструментів для потреб безпеки у країні насправді може призвести до масового стеження чи інших зловживань. Продовження використання ШІ з подібним функціоналом на державному рівні може стати перепорою для подальшої інтеграції до європейської спільноти, адже ряд держав Європи визнали використання технології Clearview незаконним, наклали високі штрафи та намагалися заборонити збирати базу даних обличчя своїх громадян.¹

Широкого застосування штучний інтелект набув і в основних месенджерах – Telegram, Whatsapp, Viber, Messenger. Серед основних напрямків його використання – створення чат-ботів з різноманітним функціоналом (генерування зображень та відео, збереження графічного та аудіовізуального контенту з окремих інтернет-ресурсів, пошук та підбір інформації тощо), використання можливостей месенджера для генерації запитів до нейромереж та ШІ, використання останніх з метою введення в оману та шахрайських схем.

На сьогоднішній день можливості нейромереж генерувати голосі та відео-повідомлення, які є настільки реалістичними та неможливими для виявлення їх штучного походження, надають зловмисникам можливість використовувати дані технології для введення в оману користувача (або цілої групи користувачів) месенджера. Генеративний ШІ може навіть зробити застарілими найкращі на сьогодні заходи запобігання шахрайству, як-то голосова автентифікація чи «живі перевірки», коли зображення людини у реальному часі має збігатися із тим, що зберігається в системі.² На теперішній час значно-

¹ Tokariuk O. Ukraine's Secret Weapon – Artificial Intelligence. *Center for European Policy Analysis*. 2023. URL: <https://cepa.org/article/ukraines-secret-weapon-artificial-intelligence/>

² Кофлін Д. ШІ допомагає всім, навіть шахраям. Як штучний інтелект став новою зброєю кіберзлочинців та стимулював афери на \$8 млрд. *Forbes Digital*. URL: <https://forbes.ua/innovations/shi-dopomagaе-vsimi-navit-shakhrayam-yak-shtuchniy-intelekt-stimulyuvav-aferi-na-8-mlrd-19092023-16102>

го поширення набрали шахрайські схеми, в яких знайома особа просить грошові кошти в борг або доступ до якогось додатку, але сама така особа не в курсі, що від її імені і, нерідко, її голосом відбувається спроба заволодіти чужими коштами. В умовах же інформаційної війни дані технології використовуються для отримання оперативних військових даних, дезінформації військовослужбовців, що однозначно створює загрозу державній безпеці.

Боротьба ж випадками шкідливого використання генеративного ШІ ускладнюється з наступних причин:

- подальша еволюція технології дозволяє обходити технологічні засоби протидії застосування ШІ – генеративні ШІ вже зараз здатні обманювати детектори ШІ;
- розвиток даної технології напряму пов'язаний з перевагами, які вона надає при створенні ефективного голосового помічника або в допомозі особам, що мають вади мови;
- ефективність боротьби напряму пов'язана з інформаційною гігієною користувачів, а отже й залежить від раніше означеної проблеми наявності значного масиву інформації про людину в соціальних мережах.

Окрім класичних соціальних мереж широке використання штучного інтелекту та нейромереж можемо споглядати й у випадку **дейтинг-платформ** та додатків. Під дейтингом зазвичай розуміють діяльність спеціалізованих онлайн-платформ, які використовуються користувачами для онлайн-знайомств. Основною метою користувачів дейтинг-платформ є пошук людини на основі своїх уподобань, для чого означені сервіси використовують різні механіки пошуку за певними критеріями.

Вже зараз з метою забезпечення ефективності надання комунікативних послуг дейтинг-сервіси застосовують сучасні технології, в тому числі ШІ. Так, наприкінці 2024 року компанія Match Group, яка володіє такими популярними додатками для знайомств як Tinder та Hinge, оголосила про плани інтегрувати генеративний ШІ у свої сервіси для покращення біографій та профілів користувачів.¹ Крім того ШІ та нейромережі використовуються дейтинг-платформами для оцінки

¹ Довірити своє серце алгоритмам: як штучний інтелект змінює сучасний дейтинг і що з цим може бути не так? 2025. URL: <https://zaborona.com/doviryty-svoye-sercze-algorytmam-yak-shtuchnyj-intelekt-zminyuye-suchasnyj-dejtyng-i-shho-z-czym-mozhebuty-ne-tak/>

сумісності пари, надання порад в спілкуванні та оформленні профілю, опосередкованого спілкування замість користувача, здійснення перекладу текстових та голосових повідомлень тощо.

Одночасно з цим штучний інтелект в дейтинг-сфері використовується також і з метою надання користувачу послуг персоналізованого спілкування з віртуальним партнером. Слід відмітити розвиток технологічних можливостей таких платформ, що зумовлюється стрімким збільшенням попиту на такий цифровий продукт. Так, сервіси на зразок Candy.ai та Kupid.ai надають можливість користувачу, вибравши статтю майбутнього партнера, створити вигаданого персонажа, який за допомогою штучного інтелекту дає можливість спілкуватися з ним голосовими повідомленнями.¹

Відкидаючи морально-етичні моменти відносин з цифровою особою слід однак звернути увагу на юридичний контекст, а саме на захист прав користувача подібних дейтинг-платформ. В першу чергу слід говорити про захист інформації, отриманої в межах комунікації з віртуальним партнером, власником платформи від розповсюдження та витоку, а також збереження режиму приватності щодо персональних даних та самого факту надання послуг, адже користувач може не бажати публічності факту надання таких послуг дейтинг-сервісом.

Сучасні додатки для знайомств вже збирають величезну кількість чутливої інформації, такої як геолокація, їхні вподобання, історію листування та навіть фото і відео.² Окрім традиційного неконтрольованого поширення таких даних загрозу становить також використання таких даних для створення небіологічних осіб, наділених штучним інтелектом, які, навчаючись на зазначених даних, можуть створювати цифрові клони реальної людини, тим самим користуючись чужою особистістю та вводячи в оману осіб, з якими спілкується в подальшому.

Використання таких цифрових копій осіб вже зараз зумовило проблему поширення випадків свідомого використання можливостей ІІІ для маніпулювання емоціями і шахрайських схем. На даний момент

¹ Коноплицький С. Майбутнє дейтингу – «Тіндер» для знайомств із ІІІ-моделями. URL: <https://speka.media/maibutnje-deitingu-tinder-dlya-znaiomstv-iz-si-modelyami-pk4ldz>

² Довірити своє серце алгоритмам: як штучний інтелект змінює сучасний дейтинг і що з цим може бути не так? 2025. URL: <https://zaborona.com/doviryty-svoje-sercze-algorytmam-yak-shtuchnyj-intelekt-zminyuye-suchasnyj-dejtyng-i-shho-z-czym-mozhe-buty-ne-tak/>

практично надзвичайно важко захистити свої права щодо такого «викрадення» особистості через складність доказування та відсутність законодавчих механізмів захисту від використання чужої особистості без дозволу особи.

Використання таких цифрових інструментів як нейромережі та інших видів штучного інтелекту в Інтернеті не обмежується означеними сферами та методами, адже сама сфера інтернет-відносин формується та змінюється ледь не щодня, а отже на тлі цього кількість напрямків застосування даних технологічних рішень збільшується в геометричній прогресії. Вважаємо за необхідне дослідити окремі приклади застосування ШІ, що актуалізувалися саме в умовах гібридної війни.

В межах російсько-української війни зараз наявне інформаційне протиборство, яке можна аналізувати як в рамках підсистеми кібербезпеки, так і в рамках інформаційно-психологічної підсистеми. Це інформаційне протиборство проявляється за допомогою фейків, спекуляцій, маніпуляцій, дезінформації, антиукраїнських наративів, інформаційного насильства, масованих інформаційних атак, інформаційно-психологічних спецоперацій та війн, інформаційно-психологічного та кібертероризму.¹

На сьогодні представники збройних сил використовують ШІ для вербування солдатів; підготовки воєнних до виконання завдань; ухвалення стратегічних рішень; обробки даних та досліджень; прогнозування майбутнього; виявлення та розпізнавання об'єктів; ліквідації цілей; моніторингу загроз; транспортування людей та об'єктів; допомоги медикам; забезпечення режиму кібербезпеки.²

Українські збройні сили дедалі частіше використовують ШІ в мережі Інтернет для ідентифікації ворожих цілей. Як зазначають спеціалісти видання *The Economist*, оскільки російські солдати і військові блогери стали більш обережними у своїх публікаціях, прості пошуки будь-яких ознак розташування військ стали менш плідними. Однак, обробляючи велику кількість повідомлень та відео, ШІ-моделі мо-

¹ Воропасва Т., Авер'янова Н. Штучний інтелект в системі інформаційної безпеки України в умовах російсько-української війни. *Collection of Scientific Papers «SCIENTIA»*, (August 23, 2024; Valencia, Spain), P. 63.

² Війна та нейромережі: як штучний інтелект використовують на полі бою. URL: <https://forklog.com.ua/exclusive/vijna-ta-nejromerezhi-yak-shtuchnyj-intelekt-vykorystovuyut-na-poli-boyu>

жуть знайти потенційні підказки, об'єднати їх і потім видати ймовірне місце розташування системи озброєння або військ противника.¹

Спірним з етичної точки зору виглядає використання ШІ для виявлення схильних до зради співвітчизників. Так, використовуючи ШІ, здійснюється пошук зв'язки у розрізних масивах даних з метою виявлення та оцінку ризику зради окремих громадян.²

Одночасно з цим ШІ широко використовується ворогом в межах ПІСО, а також іншими суб'єктами для створення синтетичного контенту в межах інформаційної війни проти нашої держави.

Як вже зазначалося, генеративний ШІ набуває здатності до навчання та імітації творчого процесу людини, в результаті чого алгоритми штучного інтелекту можуть створювати контент, використовуючи величезні обсяги даних для аналізу структури, стилю та особливостей різних типів творів. Крім того, штучний інтелект може генерувати контент за допомогою методів машинного навчання і нейронних мереж.³

Як відзначає А. Юшина, на сьогоднішній день в наукових колах актуалізується дискусія навколо правомірності використання ШІ творів для навчання, які охороняються авторським правом, оскільки на основі їх аналізу ШІ створює нові схожі об'єкти, а автори творів не отримують винагороду за таке використання.⁴ Крім того, авторка вбачає проблемним питання, чи порушується авторське право під час генерування нового контенту ШІ, адже авторські твори використовуються для машинного навчання.

Д. Прилипко приходить до висновку, що на сьогоднішній день законодавча база стосовно авторських прав на твори, створені за допомогою штучного інтелекту, перебуває на початковому етапі формування. В світі склалася ситуація, що жодна країна на законодавчому рівні належним чином не врегулювала питання забезпечення

¹ Як Україна використовує штучний інтелект у війні з Росією – The Economist. 2024. URL: <https://texty.org.ua/fragments/112210/yak-ukrayina-vykorystovuye-shtuchnyj-intelekt-u-vijni-z-rosiyeyu-the-economist/>

² Як Україна використовує штучний інтелект у війні з Росією – The Economist. 2024. URL: <https://texty.org.ua/fragments/112210/yak-ukrayina-vykorystovuye-shtuchnyj-intelekt-u-vijni-z-rosiyeyu-the-economist/>

³ Вальчук Д. В. Авторське право штучного інтелекту: проблеми та шляхи вирішення. *Modern scientific journal*. 2024. № 3 (1). С. 10.

⁴ Юшина А. Штучний інтелект: кому належать авторські й майнові права. URL: <https://mind.ua/openmind/20255019-shtuchnij-intelekt-komu-nalezhat-avtorski-j-majnovi-prava>

правової охорони та належності авторських прав на твори, створені штучним інтелектом, однак деякі розвинені держави мають низку нормативно-правових актів, що частково регулюють сферу відносин, пов'язаних з творами, створеними штучним інтелектом.¹

Функціональні можливості генеративного ШІ успішно використовуються при створенні так званих «емоційних фейків» в соціальних мережах. У соціальних мережах зараз поширюється багато дописів, які містять фото з ознаками генерації штучним інтелектом. На них зображені нібито українські військові з закликами привітати їх чи то з днем народження, чи то з весіллям. Також є схожі дописи про врятованих тварин, дітей або літніх людей.²

Ледве не кожен в запропонованих механізмами соціальних мереж публікація стикається з зображеннями, на яких відображено надзвичайні результати творчості, що викликають захват, відображені непересічні ситуації людського горя, нестандартних ситуацій та несприятливих умов, а також з аудіовізуальним контентом, що відображає надзвичайно сентиментальні ситуації та закликає до проявлення емпатії (так звані пости «ніхто нас не вітає», «ви не повірите» або «ці брати»).

Завдання контенту таких публікацій викликати емоції та заохотити користувачів відреагувати, спіймати вразливу аудиторію в емоційну пастку і змусити поширити їх далі, тиснучи на почуття провини, викликаючи емпатію та співчуття.

Довгий час дані публікації сприймалися з гумором, адже, на перший погляд дані публікації, не загрожують шкідливими наслідками, а самі зображення, згенеровані ШІ, містять ряд кумедних для сприйняття артефактів, що очевидно свідчать про несправжність запропонованого фото та ситуації на ньому. Однак, дані публікації не просто не є нешкідливими, при подальшому вивченні можна визначити загрози, які несуть на собі такі емоційні фейки.

Так, докладний аналіз релевантних шляхів використання емоційних фейків свідчить про наступні мотиви, з яких публікують такі записи у Facebook, Instagram та TikTok:

¹ Прилипко Д. Штучний інтелект та авторське право. *Теорія і практика інтелектуальної власності*. 2021. № 2. 15-22. URL: <http://uran.inprojournal.org/article/view/236526/235043>

² Денисяка О. «У військового день народження, а його ніхто не привітав»: чим небезпечні ШІ-світлини у Facebook. URL: <https://hromadske.ua/suspilstvo/232022-u-viyskovoho-dennarodzennia-a-yoho-nikhto-ne-pryvitav-chym-nebezpechni-shi-svitlyny-u-facebook>

- збір аудиторії для подальшого просування рекламних продуктів, пропагандистських наративів тощо. В даному випадку завданням публікації виступає заохочення користувачів соціальної мережі до взаємодії, тобто йде мова про використання емоцій для прикриття шкідливого змісту самої публікації. Розміщення в соціальній мережі емоційних фейків певного характеру (співчутливі, ушановуючі, схвальні) дають змогу виділити певну групу людей, схильних до проявлення емоцій та не здатних відрізнити справжні фотографії подій від згенерованих за допомогою ШІ. В подальшому відповідний користувацький ресурс може бути використаний для успішного просування сумнівних продуктів або пропагандистських тез, що особливо небезпечно в умовах війни. Емоційні фейки в даному випадку слугують маркером людської сентиментальності та можливості нав'язувати певним особам необхідної думки;
- ілюстрація підтримки певної позиції або провокація аудиторії – особливо актуально через можливість заміни первинного матеріалу (цифрового контенту) без анулювання реакцій користувачів у вигляді лайків та коментарів. Крім того дані публікації є відомим майданчиком для використання ботів при провокуванні дискусії та м'якого просування шкідливих наративів;
- витіснення дійсно важливого та актуального контенту шляхом заповнення рекомендацій емоційними фейками та подібним шкідливим контентом;
- просування негативних настроїв в суспільстві в межах ІПСО, формування негативного ставлення до керівництва Збройних сил, політичної системи держави; формування
- збір даних про користувачів з метою подальшого використання; шахрайство, шляхом спонукання до переходу за сторонніми посиланнями, фішинг тощо.

Одним з найпоширеніших способів використання ШІ в умовах гібридної війни залишається створення дідфейків.

Дідфейки (англ. deepfake – глибока підробка), що ширяться інтернетом у формі фальшивих зображень та відео представляють собою технологію, що базується на штучному інтелекті, синтезує зображення чи відеозапис, поєднує і накладає справжні і згенеро-

вані зображення та відео.¹ Ці фальсифікації можуть виглядати дуже реалістично і використовуються для поширення дезінформації, маніпуляції громадською думкою, шантажу та навіть викрадення особистих даних.²

Головна небезпека, яку несуть дідфейки є простота виробництва та використання таких матеріалів, які використовують для поширення фальшивих наративів, паніки та з метою скомпрометувати особу. Особливої ефективності дідфейки набувають у випадках обмеженості часу на перевірку інформації, адже доведення синтетичності контенту та подальше спростування інформації здійснюється набагато повільніше, ніж вірусне поширення контенту, що потенційно має значний резонанс.

Ще в 2020 році прогнозувалося використання дідфейків в промислових масштабах з метою ведення інформаційних війн, пропаганди і маніпуляції. Крім того, експертами прогнозувалося становлення правового регулювання в даній сфері, а саме формування на рівні національних законодавств положень, які контролюють продукцію і поширення контенту з використанням дідфейків із метою дезінформації.³ Однак, попри такі прогнози, на сьогоднішній день вітчизняне законодавство не містить дієвих механізмів боротьби з дідфейками.

В ситуації повномасштабного вторгнення та інформаційної напруги використання дідфейків для створення синтетичного контенту, що відображає неправдиві способи дій та заяви високопосадовців України може мати серйозні наслідки, адже такі дії не лише спотворюють реальну картину подій, а й можуть спричиняти паніку серед населення, підривати довіру до уряду та військового керівництва, а також впливати на міжнародну підтримку України.⁴

Слід однак зазначити, що вже зараз наявні інструменти для протидії таким інформаційним атакам. Так, автоматизована система SemanticForce дозволяє аналізувати шкідливі інформаційні потоки й

¹ Голос на відео не належить мені: ворог запустив «дідфейк» про ситуацію в Покровську. Армія Інформ. 2024. URL: <https://armyinform.com.ua/2024/09/28/golos-na-video-ne-nalezhyt-meni-vorog-zapustyv-dipfejk-pro-sytuacziyu-v-pokrovsku/>

² Юридичні аспекти боротьби з дезінформацією на основі дідфейків. URL: <https://consultant.net.ua/consultant-article/5394>

³ Подус С. Дідфейки в інформаційній війні. Матеріали IV Міжнародної наукової конференції ХНУПС ім. І. Кожедуба, 21-22 травня 2020. С. 108-110.

⁴ Бірюкова А. Г., Колісникова Г. В. Способи захисту порушених прав при створенні та розповсюдженні дідфейків. *Проблеми законності*. 2024. Вип. 164. С. 8.

зображення, а також відстежувати реакцію на них користувачів, відрізняти хибні акаунти від реальних користувачів тощо. Поряд з цим, система Attack Index використовується для виявлення конкретних інформаційних операцій та їхніх характеристик (мережа поширення інформації, ініціатор операції, час, інтенсивність, масштабність тощо), а також для подальшої розробки сценаріїв ефективної протидії інформаційним загрозам.

Використання ШІ для боротьби з шкідливим ШІ виглядає перспективним, однак треба обов'язково враховувати, що штучний інтелект має деякі недоліки. Наприклад, цілком можливе порушення прав людини через недосконалість сучасних біометричних систем, а також через значну кількість помилок у їхній роботі.¹

На сьогоднішній день використання дідфейків в цивільно-правовому контексті може розглядатися з трьох сторін: з точки зору захисту персональних даних (якщо дідфейк використовує особисту інформацію або зображення), захисту честі та гідності (якщо дідфейки впливають на репутацію або наносять моральну шкоду), захисту прав інтелектуальної власності (якщо дідфейк порушує авторські права або права на торговельну марку тощо).

Використання дідфейків з неправомірних цілях напряму пов'язане з незаконним використанням чужих персональних даних. Слід відмітити, що початково наявні дані (в тому числі персональні) в мережі були відкритими для перегляду, однак ШІ несанкціоновано використовував ці дані для конкретних цілей, при цьому нехтуючи принципом транспарентності системи.²

Масивні бази даних, що зберігають конфіденційну інформацію, регулярно приваблюють зловмисників. У разі успішної атаки постраждати можуть як репутація організації, так і безпека користувачів, чії персональні відомості можуть опинитися у відкритому доступі.³

¹ Воропаєва Т., Авер'янова Н. Штучний інтелект в системі інформаційної безпеки України в умовах російсько-української війни. *Collection of Scientific Papers «SCIENTIA»*, (August 23, 2024; Valencia, Spain), P. 63.

² Остіян Є. З. Штучний інтелект та персональні дані: захист приватності в цифровому середовищі. *Науковий вісник Ужгородського Національного Університету*. 2024. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/11/9-2.pdf>

³ Петрів О. Захист персональних даних у добу штучного інтелекту: міжнародні підходи та виклики. 2025. URL: <https://cedem.org.ua/consultations/zahyst-personalnyh-danyh-udobu-shtuchnogo-intelektu-mizhnarodni-pidhody-ta-vyklyky/>

Використання технологій дідфейк може бути також пов'язане з порушенням авторських прав та інших прав інтелектуальної власності в наступних випадках:

- незаконне копіювання та розповсюдження творів автора – з метою виготовлення дідфейків зазвичай використовуються твори, захищені авторським правом, без дозволу правовласника;
- створення похідних творів без дозволу автора – створення власних творів на основі вже існуючого твору, захищеного авторським правом;
- маніпуляція та спотворення творів з метою створення хибного враження про автора або зміст твору;
- використання творів в комерційних цілях без дозволу автора – використання для створення реклами або інших комерційних матеріалів творів, захищених авторським правом, без згоди правовласника.¹

На практиці прикладами порушення прав інтелектуальної власності з використанням технологій дідфейку можуть слугувати:

- виготовлення фальшивих відео з відомими особами – такі відео можуть завдати шкоди репутації цих осіб та порушити їх права на використання свого образу;
- виготовлення синтетичних музичних творів, записів голосу відомих осіб, що може вводити в оману слухачів та порушувати авторські права на музичні твори;
- незаконне дублювання фільмів;
- просування підроблених продуктів за допомогою рекламних матеріалів, які демонструють функціональність, схожу на запатентовану, без фактичного використання запатентованої технології;
- нанесення шкоди репутації бренду шляхом створення фальшивих рекламних матеріалів або відео, які асоціюють торгову марку з негативною або компрометуючою інформацією.²

Аналіз чинного вітчизняного законодавства в сфері протидії дезінформації, що хоча національне законодавство розвивається у відповідь на сучасні виклики, існує потреба в подальших реформах. Як

¹ Deepfake та право на образ як захистити свою репутацію в епоху штучного інтелекту. URL: <https://polikarpov.legal/blogposts/deepfake-ta-pravo-na-obraz/>

² Deepfake та право на образ як захистити свою репутацію в епоху штучного інтелекту. URL: <https://polikarpov.legal/blogposts/deepfake-ta-pravo-na-obraz/>

зазначають А. Г. Бірюкова, Г. В. Колісникова, запровадження відповідальності за розповсюдження дезінформації, реалізація процедур спростування та встановлення компенсацій за завдану шкоду є критичними аспектами для забезпечення ефективного захисту прав в епоху цифрових технологій.¹

У юридичній науці III виступає каталізатором для переосмислення багатьох правових режимів, адже дана технологія може входити одночасно до декількох галузевих юридичних конструкцій через специфіку різноманіття даних, які вона збирає.²

Як вже зазначалося, машинне навчання алгоритмів штучного інтелекту потребує значних об'ємів даних, обчислювальної потужності та часу. З точки зору роботи з особистою інформацією потреба у великій кількості даних створює найбільші перешкоди розробникам, адже в більшості випадків така інформація не знаходиться у вільному доступі, навіть, соціальні мережі не розцінюють сторінки користувачів, як відкрите джерело.³ З появою великих об'ємів даних (Big Data) і швидким розвитком штучного інтелекту зростають ризики витоку (неправомірного поширення), неправомірного доступу та маніпулювання особистою інформацією.⁴

Обіг особистої інформації має певні відмінності в залежності від регіону чи країни, однак базові принципи залишаються незмінними. Головною метою є надати користувачам контроль над своїми даними та протидіяти їх неправомірному збору, збереженню та використанню.⁵

Відповідно до частин першої, другої статті 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускаєть-

¹ Бірюкова А. Г., Колісникова Г. В. Способи захисту порушених прав при створенні та розповсюдженні дипфейків. *Проблеми законності*. 2024. Вип. 164. С. 16.

² Остіян Є. З. Штучний інтелект та персональні дані: захист приватності в цифровому середовищі. *Науковий вісник Ужгородського Національного Університету*. 2024. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/11/9-2.pdf>

³ Тамашев В. Персональні дані у контексті обробки штучним інтелектом. URL: <https://legalitygroup.com/personalni-dani-u-konteksti-obrobki-shtuchnim-intelektom/>

⁴ Петрів О. Захист персональних даних у добу штучного інтелекту: міжнародні підходи та виклики. 2025. URL: <https://cedem.org.ua/consultations/zahyst-personalnyh-danyh-u-dobu-shtuchnogo-intelektu-mizhnarodni-pidhody-ta-vyklyky/>

⁵ Тамашев В. Персональні дані у контексті обробки штучним інтелектом. URL: <https://legalitygroup.com/personalni-dani-u-konteksti-obrobki-shtuchnim-intelektom/>

ся збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Водночас статтею 64 Конституції України передбачено положення, що в умовах воєнного або надзвичайного стану можуть встановлюватися окремі обмеження прав і свобод із зазначенням строку дії цих обмежень.

Як зазначають дослідники механізмів захисту персональних даних користувачів мережі Інтернет, правозастосовча практика у сфері використання персональних даних штучним інтелектом формується за такими напрямками: право власності на дані, їхня безпека, відповідальність за прозорість системи та регулювання обробки збору даних.¹

Попри те, що контроль за дотримання конфіденційності та безпеки персональних даних здійснюється відповідними органами, слід враховувати, що вони не здатні відстежувати та вчасно звертати увагу на всі порушення. Тому користувач має усвідомлювати, яку інформацію надає, та передбачати можливість її протиправного використання, особливо це стосується соціальних мереж.²

В юридичній літературі контексті порушення права на приватність в мережі Інтернет, зазвичай згадують порушення ще двох прав людини – право на свободу висловлення та право мирних зборів. Х. Солодовнікова приходить до думки, що особа, яка знає, що за нею можуть слідкувати, буде більш обережною у висловлюваннях та буде брати менш активну участь у громадському житті. Безпосередньо ж право на свободу висловлення може порушуватися через тимчасове або постійне припинення дії акаунтів у соціальних мережах за допомогою фільтрів, які відслідковують дописи, які штучний інтелект визначає як такі, що порушують права інших людей: несуть загрозу, булінг, дискримінацію за національністю, релігією тощо.³ Крім того,

¹ Остіян Є. З. Штучний інтелект та персональні дані: захист приватності в цифровому середовищі. *Науковий вісник Ужгородського Національного Університету*. 2024. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/11/9-2.pdf>

² Тамашев В. Персональні дані у контексті обробки штучним інтелектом. URL: <https://legalitgroup.com/personalni-dani-u-konteksti-obrobki-shtuchnim-intelektom/>

³ Косілова О. І., Солодовнікова Х. К. Права і свободи людини і громадянина V. S. Штучний інтелект: проблемні аспекти. *Інформація і право*. 2020. № 4(35). URL: <http://bulletin.kpi.ua/index.php/2616-6798/article/view/221218>

слід відмітити можливість зловживання системою скарг і «банів» для користувачів з використанням необмеженої кількості ботів для формування видимості небезпечності контенту.

Як вже зазначалося, вітчизняні збройні сили широко використовують технології ШІ для розпізнавання обличчя противники. Якщо використання таких інструментів лише пов'язують з ризиком подальшого порушення конфіденційності та встановлення контролю за громадянами, то в той же час російський спосіб використання даного функціоналу вже пов'язують з відстеженням, цензуруванням та контролем за власними громадянами та нашими співвітчизниками на окупованих територіях.¹

В Україні ж за допомогою технології Big Data та штучного інтелекту неодноразово викривали в такий спосіб великі ботоферми, а також піддавалися реальному кримінальному переслідуванню люди, які в соцмережах закликали до дій, що КК України кваліфіковано як «сепаратизм» та «тероризм». Аналіз відомих на сьогодні випадків використання Великих Даних та ШІ в мережі, до списку порушуваних прав можна також віднести свободу пересування, право володіти майном, право на демократію, а також різні форми дискримінації, які виникають в результаті застосування моделей, що спираються на Big Data та конвергенцію новітніх технологій.²

Ще одним шляхом використання ШІ в умовах гібридної війни може бути маскування рекламних матеріалів, в тому числі політичної реклами.

Попри стрімкий технологічний розвиток методів та форм просування рекламних продуктів, широке впровадження контекстної та нативної реклами в мережі Інтернет, значну конкуренцію методологій та бюджетів просування реклама в мережі Інтернет на сьогоднішній не має в вітчизняному законодавстві окремого режиму правового регулювання, а її використання підпорядковується загальним вимогам Закону України «Про рекламу» 1996 року прийняття.

¹ Штучний інтелект може бути ключем до перемоги України у війні – західні експерти. *Голос Америки*. 2024. URL: <https://www.radiosvoboda.org/a/ukrayina-shtuchnyy-intelekt-viyna/32785722.html>

² Косілова О. І., Солодовнікова Х. К. Права і свободи людини і громадянина V. S. Штучний інтелект: проблемні аспекти. *Інформація і право*. 2020. № 4(35). URL: <http://bulletin.kpi.ua/index.php/2616-6798/article/view/221218>

Попри цей факт законодавством передбачено ряд норм, що безпосередньо стосуються онлайн-реклами. Так, відповідно до положень ч.1 ст. 9 Закону України «Про рекламу» реклама має бути чітко відокремлена від іншої інформації, незалежно від форм чи способів розповсюдження, таким чином, щоб її можна було ідентифікувати як рекламу.

Ч.2 тієї ж статті закріплює правило, згідно якого реклама в інших (в тому числі онлайн) медіа повинна бути чітко відокремлена від іншої інформації з використанням слова «реклама».¹

Як відзначає Д. Ківелюк, порушення, які виникають у сфері виробництва та поширення інтернет-реклами, можуть стосуватись приналежності права на створені об'єкти реклами, що є результатами творчої діяльності, законності використання в рекламі чужих творів та інших охоронних об'єктів (товарних знаків, знаків обслуговування, фірмових найменувань), захисту прав споживачів інтернет-реклами.²

Слід також відмітити використання ШІ для просування прихованої реклами безпосередньо в цифровому середовищі. Зокрема, як відзначає О. Косілова, технології, що впроваджуються з метою якісного покращення повсякденного побуту передбачають такі заходи як збір персональної інформації про користувачів Інтернету. В подальшому неодноразово відмічалось використання результатів аналізу цієї інформації для таргетування осіб та груп осіб відповідно до їх уподобань та психологічних особливостей, внаслідок чого особа піддається нав'язливому тиску контекстної реклами, що зокрема відображається й у технології, використовуваній Google Maps, а саме фізичне перебування людини у певний момент часу використовується для того, щоб вчасно надсилати пропозиції з метою вплинути на її вибір при покупці або виборі ресторану, відвідуванні музею тощо.³

Отже, на сьогоднішній день за допомогою інструментів ШІ розширюються можливості аналізу та обробки великої кількості інформації, автономного приймати рішень, вчасного розпізнання загрози тощо.

¹ Про рекламу: Закон України від 03.07.1996 № 270/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80#Text>

² Ківелюк Д. А. Цивільно-правове регулювання рекламних відносин в мережі Інтернет: дис.... канд. юрид. наук: 12.00.03. Хмельницький, 2019. С. 4

³ Косілова О. І., Солодовнікова Х. К. Права і свободи людини і громадянина V. S. Штучний інтелект: проблемні аспекти. *Інформація і право*. 2020. № 4(35). URL: <http://bulletin.kpi.ua/index.php/2616-6798/article/view/221218>

Водночас використання ШІ несе й певні ризики у контексті гарантування прав людини. В цілому, технології ШІ можуть негативно впливати на право на життя, право на приватне життя та право на свободу вираження поглядів, а також інші основоположні права людини. Відтак важливим завданням є забезпечення належних гарантій, які б унеможливили порушення прав людини при використанні таких технологій, в тому числі у військовій справі.¹

Підсумовуючи вищезазначене, можна зробити висновок, що на сьогоднішній день використання штучного інтелекту окрім явних переваг несе значну загрозу порушення прав людини, може суперечити індивідуальним та суспільним інтересам, загрожує державній безпеці та є прямим інструментом ведення інформаційної війни.

Як відзначають Т. Воропаєва та Н. Авер'янова, штучний інтелект може стати ефективним засобом протидії російській дезінформації та ключовим чинником вдосконалення системи інформаційної безпеки України в умовах гібридної війни у тих випадках, коли інструменти штучного інтелекту будуть не тільки технічно досконалими й надійними, але й будуть відповідати морально-етичним нормам, діючому законодавству та демократичним цінностям суспільства.²

Сьогодні з вільним і відкритим доступом до інформації та різноманітністю творчого та розважального контенту в Інтернеті пересічному громадянину часто важко зрозуміти, що можна вільно використовувати, а що ні.³

Вітчизняне законодавство та правозастосовча практика виходять із позицій захисту прав та свобод людини, однак стрімкий розвиток технологій штучного інтелекту зумовлює значні труднощі в формуванні дійсно ефективного механізму захисту від шкідливого впливу при застосуванні штучного інтелекту.

Сфера цифрових відносин в мережі Інтернет залишається специфічною для визначення методів протидії негативному впливу ШІ в

¹ Коваленко Ю., Войнов М. Штучний інтелект та права людини: орієнтири та обмеження у контексті національної безпеки та оборони. 2024. URL: https://www.helsinki.org.ua/wp-content/uploads/2024/05/Preview_AI_human_right_A4-1.pdf

² Воропаєва Т., Авер'янова Н. Штучний інтелект в системі інформаційної безпеки України в умовах російсько-української війни. *Collection of Scientific Papers «SCIENTIA»*, (August 23, 2024; Valencia, Spain), P. 65.

³ Попович К. Г. Правове регулювання реклами (цивілістичний аспект). *Науковий вісник Ужгородського університету: серія: Право*. 2023. Т. 1. Вип. 78. С. 219.

даній сфері, адже такі її специфічні риси як анонімність та відносна свобода дій є одночасно перепонами для ефективної протидії негативному впливу, що свідчить про необхідність подальшого вивчення та врахування етико-юридичних аспектів проблематики теми при формуванні законодавства в даній сфері.

Так, на думку В. Шевчука, для вирішення етико-юридичних проблем використання штучного інтелекту, необхідно створити глобальне (обов'язкове) міжнародне законодавство щодо розробки та впровадження штучного інтелекту, зокрема для запобігання його нелегальному, тобто нецивілізаційному використанню. Крім того, уряди та компанії повинні знати про недосконалість даних, на яких базується технологія штучного інтелекту, і подбати про запобігання дискримінації та порушенням прав людини.¹

Серед практичних способів захисту від шкідливого впливу ШІ в мережі Інтернет в умовах гібридної війни серед найбільш актуальних залишаються пропаганда інформаційної гігієни на державному рівні, боротьба з фейками, шкідливими емоційними згенерованими ШІ шляхом запровадження відповідальності за таку діяльність та формування адміністративної та судової практики з даних питань. Крім того вважаємо слушним на законодавчому рівні встановити вимогу маркування зображень, створених ШІ, а також розробку концептуальних положень контролю за використанням ШІ розробниками додатків з метою уникнення випадків створення «бекдорів» для корисних та неправомірних цілей.

Ключові слова: штучний інтелект, нейромережі, соціальні мережі, месенджер, емоційні фейки, право інтелектуальної власності, інформаційна гігієна, ІПСО, маркування зображень, інформаційна війна, діпфейк, генеративний штучний інтелект, дейтинг-сервіси, викрадення особистості, синтетичний контент

¹ Шевчук В. М. Використання технологій штучного інтелекту та процес цифровізації криміналістики в умовах війни. *Актуальні проблеми протидії злочинності та корупції: збірник тез Всеукраїнської науково-практичної конференції* (Харків, 17 лютого 2023 р.). С. 175.