

Гайд для ОГС

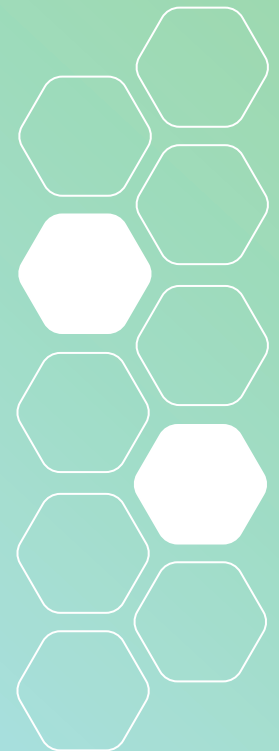
# Інструменти штучного інтелекту

2024  
КИЇВ

На основі матеріалів  
експертної дискусії  
«Штучний інтелект і організації  
громадянського суспільства»  
Щорічного Форуму «Штучний  
інтелект 2.0: регулювання  
та робота під час війни»

# ЗМІСТ

Вступ	3
Інструменти ШІ: використання, регулювання та можливі ризики	4
Генеративний ШІ	4
Використання інструментів штучного інтелекту в роботі організацій громадянського суспільства	11
Технології deepfake та shallowfake	23
Камери з технологією розпізнавання обличчя	31
Камери з розпізнаванням обличчя та CCTV-камери в Україні	36
Правове регулювання використання камер з технологією розпізнавання обличчя	40
Більше про ШІ	44
Подяка спікерам Форуму, на основі матеріалів якого підготовлено цей гайд для ОГС	47
Контакти команд організацій, які реалізують проєкт «Ініціатива секторальної підтримки громадянського суспільства України»	49



Майбутнє вже настало, адже 2023 рік зробив інструменти штучного інтелекту (ШІ) нашою незворотною реальністю. Звісно, експерти нагадують, що справжнього ШІ слід чекати орієнтовно ще тридцять років. На сучасному етапі еволюції він не може існувати без участі людини, яка «затверджуватиме» його результати.

Громадським організаціями доцільного використовувати ШІ, адже він значно спростить і пришвидшить робочі процеси. Водночас слід вчитися відповідально й раціонально користуватися його інструментами та враховувати ризики. **GPT chat**, **deepfake** (діпфейки), **shallowfake** (шеллоуфейки), цифровий фандрейзинг, формування контенту, цифрові камери відеоспостереження з функцією розпізнавання обличчя — це тільки верхівка айсберга інструментів ШІ, які можуть вплинути на роботу громадського сектору. Для організацій громадянського суспільства (ОГС) важливо вчасно розпізнати можливості й інтегрувати їх у свою операційну діяльність, визначити потенційні загрози та виробити механізми запобігання. А ще важливіше — продумати, яким має бути законодавство, яке регулюватиме ШІ, і зробити його дружнім для ОГС.

Центр демократії та верховенства права (ЦЕДЕМ) виступає за те, щоб ОГС України активно досліджували можливості й ризики, пов'язані з використанням систем ШІ. Саме тому на основі експертної дискусії «Штучний інтелект і організації громадянського суспільства», яка відбулася 24 березня 2023 року в межах Щорічного Форуму «Штучний інтелект 2.0: регулювання та робота під час війни», ЦЕДЕМ створив путівник для громадянського суспільства інструментами ШІ, інструкціями їх використання та можливими ризиками для сектору.

Ми віримо, що Форум і цей матеріал започаткують дискусію в українському громадському секторі щодо ефективного використання ШІ. Ми переконані, що вже зараз вона необхідна для ефективного розвитку як громадського сектору, так і України.

**GPT chat**

/чат-бот з ШІ/

**deepfake**

/технологія/

**shallowfake**

/технологія/

## ГЕНЕРАТИВНИЙ ШІ

На основі тез:  
**Вероніки Бойко**,  
керівниці соціального напрямку YouControl,  
експертки Асоціації відкритих даних,

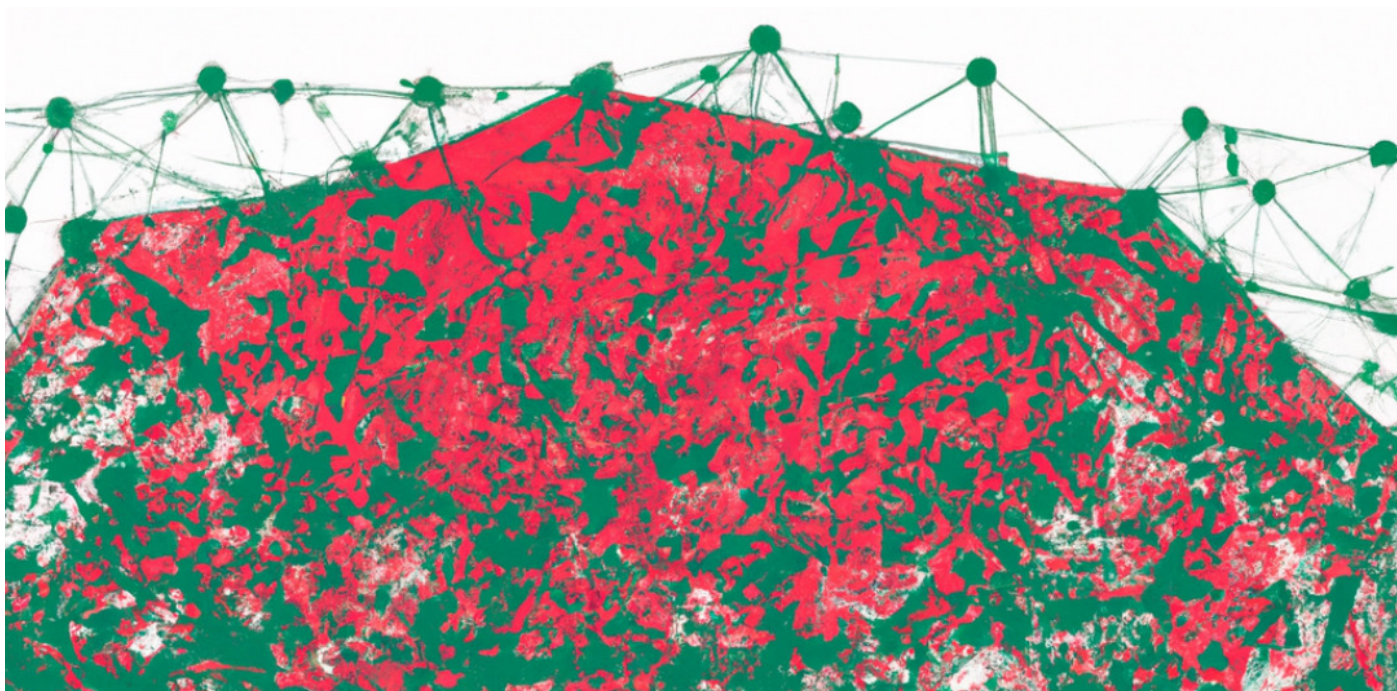
та  
**Ольги Петрів**,  
юристки ЦЕДЕМ

**Моделі генеративного ШІ (generative AI)** — це технології ШІ, яка здатні генерувати текст, фото, відео, аудіо, код, інформацію та їх поєднання. Ця технологія, як і deepfake, базується на алгоритмах deep learning. Ідеться про базовий детальний аналіз величезної бази даних за допомогою алгоритмів, який здійснюється для того, щоб генерувати нову інформацію на основі попередньої.<sup>1</sup>

<sup>1</sup> Hughes, Owen. Generative AI Defined: How it Works, Benefits and Dangers // [TechRepublic](#)



## ІНСТРУМЕНТИ ШІ: ВИКОРИСТАННЯ, РЕГУЛЮВАННЯ ТА МОЖЛИВІ РИЗИКИ



Зображення, згенероване за допомогою DALL-E

При цьому, на відміну від **machine learning** — технології, яка також допомагає машині передбачати інформацію на основі попередніх даних, **deep learning** має більш складну багатоповарову архітектуру. Завдяки їй алгоритми можна навчити розрізняти та визначати доволі складні патерни інформації (до прикладу, семантичні патерни: тобто з якими значеннями й термінами пов'язані ті чи інші слова; просторові патерни: які текстури, кути, форми та об'єкти розміщені на зображенні). Обидві технології мають на меті передбачення, класифікацію та кластеризацію інформації, проте **deep learning** дозволяє це робити на глибшому рівні<sup>2</sup>. Саме тому **generative AI** має можливість у своїй відповіді людині постійно нібито «прогнозувати» та «вгадувати» кожне наступне слово чи зображення, яке має бути згенероване.

Нині існують різні доступні публічно програми, що використовують генеративний ШІ для того, щоб згенерувати різну інформацію — текст, аудіо, відео, зображення, код тощо.

Наприклад, згенерувати текст на основі лінгвістичних моделей здатні **ChatGPT**, **Bard**, **Llama 2** тощо.

Уже створені інструкції щодо використання текстового генеративного ШІ. Наприклад, відеокурс «ChatGPT для підвищення власної ефективності» від Тимофія Милованова на порталі «Дія.Освіта» або онлайн-курс **«Основи AI» від Google**.

Machine  
learning  
/технологія/

# ІНСТРУМЕНТИ ШІ: ВИКОРИСТАННЯ, РЕГУЛЮВАННЯ ТА МОЖЛИВІ РИЗИКИ

Згенерувати різні зображення допомагають **DALL-E 2**, **Midjourney**, **Deep Dream Generator** тощо.

Також можна згенерувати музику за допомогою **JukeBox**, **AudioCraft** тощо.

Після відкриття публічного доступу до ChatGPT від OpenAI наприкінці 2022 року ці системи почали набувати значної популярності. У ChatGPT лише за два місяці після релізу з'явилось 100 мільйонів користувачів<sup>3</sup>, а за даними торішнього дослідження McKinsey, за останні п'ять років їхня кількість зросла вдвічі.<sup>4</sup> Уже зараз різні ОГС і бізнеси активно використовують генеративний ШІ для своєї роботи.

## ЯК ОГС МОЖУТЬ ВИКОРИСТОВУВАТИ ГЕНЕРАТИВНИЙ ШІ?

Цікавим досвідом використання ШІ в робочих процесах ділиться Вероніка Бойко, керівниця соціального напрямку YouControl. За її словами, у компанії YouControl уже 20 % співробітників у своїй роботі тестували системи, які використовують елементи ШІ.

Вероніка Бойко зазначає, що поки в YouControl системи ШІ найкраще проявили себе в таких завданнях:

- підготовка контенту для статей, презентацій, публікацій;
- листування з партнерами;
- формування заявок, таблиць, чеклістів;
- стратегування, планування;
- кодування елементарних функцій;
- пошук нових ідей.

Нині з усіма цими завданнями справляється генеративний ШІ на кшталт **ChatGPT**, **Bard**, **Claude.ai**, **Llama 2**. Детальніше про спеціалізовані застосунки для різних завдань ви зможете дізнатися в наступному розділі.

Обсяг безпосередніх завдань для генеративного ШІ може бути різноманітним: від первинного пошуку певної інформації до створення листів. Наприклад, одного разу в GR-відділі Обсяг безпосередніх завдань для генеративного ШІ може бути різноманітним: від первинного пошуку певної інформації до ство-

<sup>3</sup> Hu, Krystal. ChatGPT sets record for fastest-growing user base — analyst note // [Reuters](#)  
<sup>4</sup> The state of AI in 2022 — and a half decade in review // [McKinsey & Company](#)

## ІНСТРУМЕНТИ ШІ: ВИКОРИСТАННЯ, РЕГУЛЮВАННЯ ТА МОЖЛИВІ РИЗИКИ



Зображення, згенероване за допомогою DALL-E

рення листів. Наприклад, одного разу в GR-відділі YouControl поставили завдання ChatGPT змінити текст листа, який ігнорували партнери, таким чином, щоб він запам'ятався, — і на новий лист уже надійшла відповідь.

Одним з ефективних способів використання ChatGPT або інших мовних моделей є генерація ідеї чи структури певного тексту. Його також можна застосувати для пришвидшення пошуку й систематизації інформації. Як зазначає юристка ЦЕДЕМ Ольга Петрів, мовні моделі можуть бути зручними для пошуку законодавства в певній сфері. При цьому Google за запитом буде шукати лише ті нормативно-правові акти, які містять слово, вжите в пошуку. А ChatGPT здатен, наприклад, знайти документи, що регулюють діяльність ШІ, але не вживають словосполучення «штучний інтелект».

Використання мовних моделей передбачає наявність відкритої інформації у великому обсязі: тоді системи на основі ШІ можуть проаналізувати ці дані та допомогти нам щось у них знайти чи проаналізувати або навіть знайти певну аномалію в даних.

Зверніть увагу: якщо ваша громадська чи благодійна організація планує застосовувати у своїй роботі інструменти ШІ, варто подумати над тим, щоб передплатити такі сервіси та закласти в бюджет організації витрати на це.

Мовні моделі  
/технологія/



## ІНСТРУМЕНТИ ШІ: ВИКОРИСТАННЯ, РЕГУЛЮВАННЯ ТА МОЖЛИВІ РИЗИКИ

Наприклад, підписка на ChatGPT 4, більш «розумний» за безкоштовний ChatGPT 3.5, який дозволяє використовувати безліч додаткових плагінів, коштує 20 доларів на місяць. А платна підписка на Midjourney AI варіює від 10 до 120 доларів на місяць.

### СТВОРЕННЯ ІНСТРУМЕНТІВ, ЩО ВИКОРИСТОВУЮТЬ ЕЛЕМЕНТИ ШІ

Організації та компанії за наявності ресурсів можуть самостійно розробляти інструменти, що використовують елементи ШІ.

Для цього необхідні три ключові ресурси:

- 1 інформація — що більший dataset, тобто набір даних, то ефективніше машинне навчання;
- 2 програмне забезпечення та комп'ютерне обладнання — саме вони забезпечать роботу інструментів ШІ;
- 3 професіонали — для машинного навчання також необхідні досвідчені фахівці, які мають достатню експертизу.<sup>5</sup>

### ОГС МОЖУТЬ ВИКОРИСТОВУВАТИ ІНСТРУМЕНТИ ШІ В ТАКИХ ЦІЛЯХ:

ОГС можуть використовувати інструменти ШІ в таких цілях:

- створення ботів і віртуальних помічників, які допомагають представникам різних цільових аудиторій;
- передбачення фінансового планування та спрощення фінансового менеджменту;
- оптимізація інших процесів в організаціях і компаніях, таких як управління комунікаціями, проведення досліджень і розслідувань, рекрутинг.

Утім, розроблення унікальних інструментів, які використовують елементи ШІ, вимагає дуже багато інвестицій. Тож рішенням може стати використання вже готових інструментів, про які йдеться в наступному розділі цього гайду.

<sup>5</sup> This Is Why All Companies Need An AI Strategy Today // [RESEARCH BRIEFS](#)



## РИЗИКИ ВИКОРИСТАННЯ ГЕНЕРАТИВНОГО ШІ

Вероніка Бойко радить обережніше використовувати ChatGPT і подібні мовні системи для таких речей:

- 1 Підготовка досьє на компанію чи особу — часто така перевірка є нелінійною та потребує креативності.
- 2 Робота з фактами та доказами — часом ШІ може просто не надавати докази.
- 3 Посилання на джерела — вони можуть бути вигаданими.

ChatGPT надає дані на основі інформації, яка була згенерована до 2021 року. Відповідно, чат не знає про інформацію, створену після 2021 року.

Окрім того, результати даних генеративних ШІ потребують ретельної перевірки, адже мають малопрогнозований відсоток похибок і можуть вдаватися до так званих «галюцинацій», коли мовна модель починає генерувати хибну інформацію.



Зображення, згенероване за допомогою DALL-E

## ІНСТРУМЕНТИ ШІ: ВИКОРИСТАННЯ, РЕГУЛЮВАННЯ ТА МОЖЛИВІ РИЗИКИ

Також, якщо йдеться про створення тексту, потрібно перевіряти, чи не містять згенеровані частини об'єктів інтелектуальної власності. Варто розуміти, що зараз в Україні діяльність ChatGPT, Bard та інших мовних моделей регулюється Законом України про авторське право та суміжні права. У випадку з генеративним ШІ йдеться про спеціальний правовий режим, *sui generis*, який полягає в тому, що ані людина, що дала запит на генерування інформації, ані сама система ШІ не є автором цієї інформації. При цьому мовна модель спирається на інформацію з різних джерел.

Через це, якщо видати статтю, згенеровану ШІ, за свою, потенційно може йтися про плагіат. До того ж і сама стаття теоретично може порушувати чиїсь авторські права. Людина, що користується генеративним ШІ, має перевіряти, чи не містить згенерований матеріал об'єктів, захищених авторським правом. Для цього потрібно пошукати подібний контент в інтернеті, визначити правдивість інформації та вказати авторів, твори яких використав ШІ. Так, у липні 2023 року понад 9000 авторів та авторок звернулися до компаній, які розробляють генеративний ШІ, з вимогами, щоб їхні твори в цих системах використовували лише за їхньою згодою, із зазначенням авторства тих, чий матеріал було використано, та з грошовою платою за використання творів<sup>6</sup>. Так само і деякі художники та художниці вже виступають за те, щоб системи ШІ, які генерують графічні зображення, як-то Midjourney та DALL·E, не могли використовувати для навчання твори тих митців, які не давали на це своєї згоди<sup>7</sup>.



<sup>6</sup> More than 10,000 Authors Sign Authors Guild Letter Calling on AI Industry Leaders to Protect Writers // [The Authors Guild](#)

<sup>7</sup> From lawsuits to tech hacks: Here's how artists are fighting back against AI image generation // [Euronews Culture](#)

## АВТОМАТИЗАЦІЯ БІЗНЕС-ПРОЦЕСІВ

### ЧАТ-БОТИ

**ChatGPT** — чат-бот із ШІ, який знають, напевно, усі. У нього є дві версії: ChatGPT 3.5 та ChatGPT 4. ChatGPT 3.5 — це найперша версія чату, у якій безкоштовно можна вести діалог з використанням системи ШІ.

ChatGPT 3.5 як базова версія чат-бота із ШІ має такі основні функції:

- **Ведення діалогу:** людина, що використовує ChatGPT 3.5, може вести з ним діалог на будь-яку обрану нею тему.
- **Генерація контенту:** ChatGPT 3.5 може допомогти у створенні різноманітного контенту, наприклад блогів або пресрелізів для постів у соціальних мережах та інформаційних бюлетенів.
- **Підготовка пропозицій і заявок:** ChatGPT 3.5 може допомогти в складанні заявок на гранти, написанні проєктних пропозицій, рекомендаційних листів та інших офіційних документів. Ви можете зазначити, у якому стилі хотіли б, щоб він писав текст, і він це буде робити.
- **Навчальні матеріали й ресурси:** організації можуть використовувати ChatGPT 3.5 для створення навчальних матеріалів, інструкцій, путівників та інших ресурсів.
- **Підтримка в плануванні та організації:** ChatGPT 3.5 може допомогти в організації подій, плануванні стратегій, розробленні робочих планів і менеджменті проєктів.
- **Творчість: він може допомагати в написанні творчих матеріалів,** наприклад сценаріїв.

Проте не всі знають про те, що в платній версії за 20 доларів на місяць є безліч нових функцій:

- Віднедавна ChatGPT 4 може здійснювати розширений аналіз даних. Ви можете додати до ChatGPT 4 документ чи фото й попросити його проаналізувати їх. Для цього потрібно активувати режим аналізу даних. Наприклад, вам потрібно детально проаналізувати зображення клітини, на якому кожна з її частин підписана. Щоб він це зробив, завантажте зображення в чат і попросіть проаналізувати інформацію, яку він отримує із

ChatGPT 3.5 та  
ChatGPT 4  
/чат-бот з ШІ/

# ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В РОБОТІ ОРГАНІЗАЦІЙ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

зображення. Жодного плагіну для цього активувати не потрібно. Коли чат відповість, ви можете попросити його, наприклад, подати роз'яснення щодо кожного елемента клітини через плагін.

- ChatGPT 4 може згенерувати презентацію за вашим запи-

PE

IMG\_2351.PNG  
Image

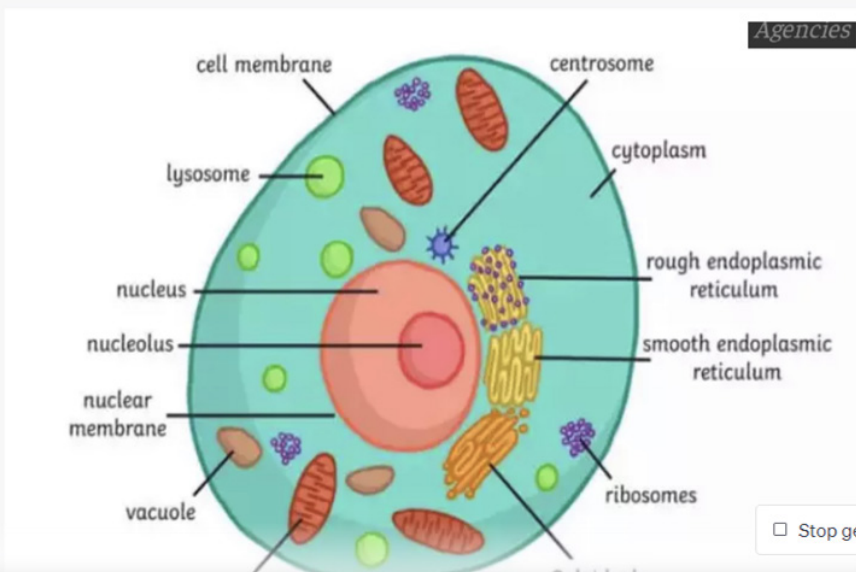
розпиши, що означає кожна частина того, що зображено на фото. Я надсилаю тобі фото зображення з інформацією про людську клітину.



Я готовий допомогти вам розібратися з зображенням, яке ви надіслали. Спершу мені потрібно його переглянути. Давайте завантажу його та подивимося, що на ньому зображено.

Finished working

Show work



+ Send a message

ChatGPT may produce inaccurate information about people, places, or facts. [ChatGPT September 25 Version](#)




На жаль, я не можу "побачити" зображення так, як це роблять люди. Я можу аналізувати зображення лише за допомогою програмного коду або отримувати текстову інформацію з нього. Я можу спробувати витягнути текст з вашого зображення за допомогою оптичного розпізнавання символів (OCR), якщо це зображення містить текст. Чи хочете ви, щоб я спробував це зробити?

PE

так




# ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В РОБОТІ ОРГАНІЗАЦІЙ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

 Добре, давайте спробуємо витягнути текст з вашого зображення за допомогою оптичного розпізнавання символів (OCR).  

Finished working Show work ▾




Здається, OCR вдалося витягнути деякі назви структур клітини з зображення. Ось їх перелік:

- cell membrane (клітинна мембрана)
- centrosome (центросома)
- cytoplasm (цитоплазма)
- nucleolus (нуклеолус)
- smooth endoplasmic reticulum (гладенька ендоплазматична сітка)
- nuclear membrane (ядерна мембрана)
- ribosomes (рибосоми)
- vacuole (вакуоль)
- Golgi body (апарат Гольджі)
- nucleus (ядро)
- mitochondrion (мітохондрія)


Я можу розповісти вам більше про кожен з цих структур клітини, якщо це буде корисно.  Regenerate



PE

розкажи

 Звісно, ось короткий опис кожної структури, яка була розпізнана на зображенні:  

- 1. Клітинна мембрана (Cell Membrane)**
  - Функції: Відокремлює внутрішнє середовище клітини від зовнішнього, контролює транспорт речовин ввоні і назовні, бере участь у передачі сигналів.
- 2. Центросома (Centrosome)**
  - Функції: Організує мітотичний вінчик під час мітозу, бере участь у регуляції клітинного циклу, організації цитоскелета.
- 3. Цитоплазма (Cytoplasm)**
  - Функції: Наповнює внутрішнє середовище клітини, містить органели і розчинені речовини, бере участь у метаболічних процесах.
- 4. Нуклеолус (Nucleolus)**
  - Функції: Місце синтезу рРНК і збірки рибосом, бере участь у регуляції клітинного циклу і стресових відповідей.

 Regenerate

 Send a message 

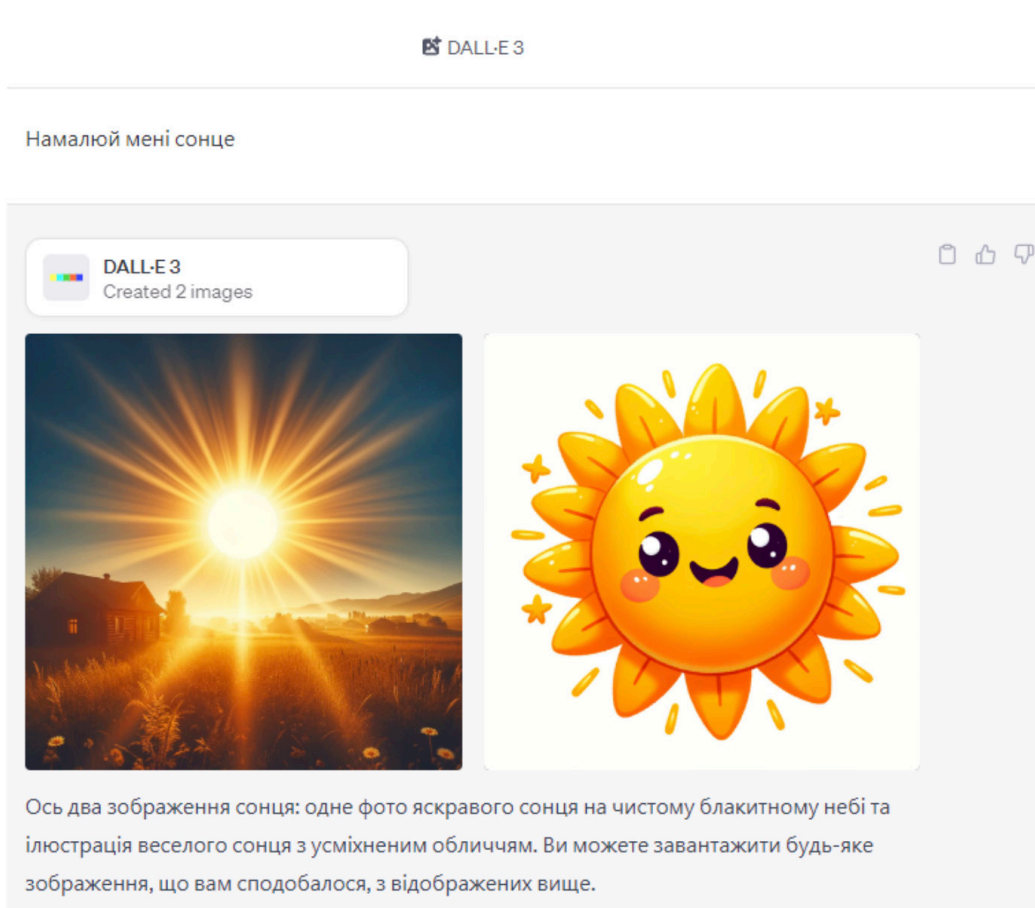
ChatGPT may produce inaccurate information about people, places, or facts. ChatGPT September 25 Version

# ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В РОБОТІ ОРГАНІЗАЦІЙ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

том у чаті. Наприклад, ви отримали детальну інформацію про кожну частину клітини. Після цього ви можете написати чату, щоб він створив презентацію, спираючись на цю інформацію. Він це зробить і дасть вам посилання на готовий документ у PowerPoint.

Для користувачів ChatGPT 4 доступна можливість використання DALL-E 3 просто в діалозі. Щоправда, попередньо треба активувати режим «DALL-E 3». DALL-E 3 автоматично активується в ChatGPT 4, коли ви просите його щось намалювати чи зобразити.

Для того, щоб максимально використовувати потенціал ChatGPT 4, варто розуміти, що таке плагіни.



**Плагіни в ChatGPT 4** — це додаткові програми або інструменти, які можна активувати, щоб розширити його можливості або додати нові функції.

За допомогою плагінів можна отримати доступ до інтернету або документів, що неможливо зробити в ChatGPT 3.5.

За один сеанс можна активувати не більше ніж три плагі-

**Плагіни в  
ChatGPT 4**  
/додаткові мо-  
дулі чат-боту/

# ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В РОБОТІ ОРГАНІЗАЦІЙ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

ни. Для цього потрібно зайти в галерею плагінів й обрати ті, які вам потрібні, потім активувати їх і почати розмову. Далі ChatGPT 4 автоматично вибирає, який з увімкнених плагінів використовувати.

**Крок 1** Зайдіть у чат. Натисніть у верхньому лівому кутку на «ChatGPT 4». Оберіть розділ «Плагіни».

ChatGPT 4 ▾



Чим я можу тобі допомогти сьогодні?

Допоможи мені вчитися словниковий запас для вступного іспиту до коледжу	Покажіть мені фрагмент коду липкого заголовка веб-сайту
Порівняйте маркетингові стратегії для сонцезахисних окулярів для покоління Z і мілені...	Розробіть контент-стратегію для інформаційного бюлетеня з безкоштовними міс...
📧 Повідомлення ChatGPT...	

ChatGPT може робити помилки. Перевірте важливу інформацію.

**Крок 2** Оберіть розділ «Плагіни».

ChatGPT 4 ▾

- 🌟 GPT-4  
З DALL-E, переглядом і аналізом  
Обмеження 40 повідомлень / 3 години
- 🔗 GPT-3.5  
Чудово підходить для щоденних завдань
- 📌 Плагіни



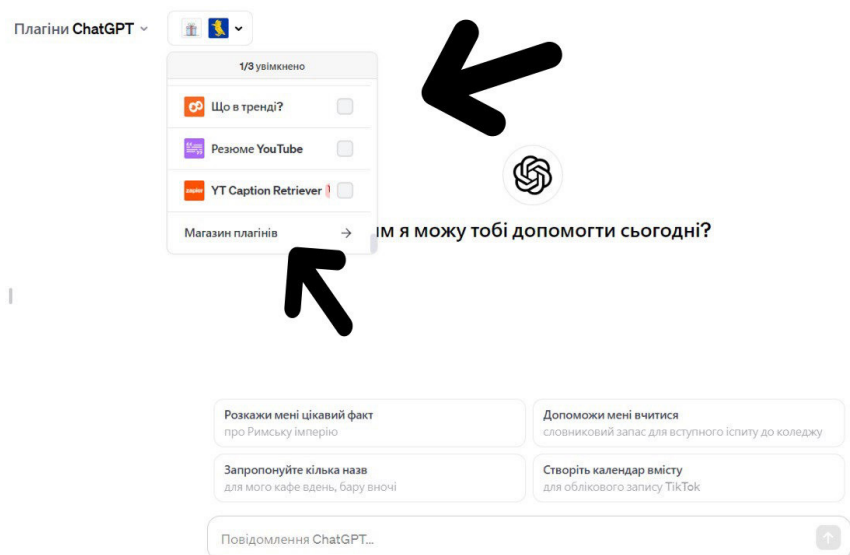
Чим я можу тобі допомогти сьогодні?

Допоможи мені вчитися словниковий запас для вступного іспиту до коледжу	Покажіть мені фрагмент коду липкого заголовка веб-сайту
Порівняйте маркетингові стратегії для сонцезахисних окулярів для покоління Z і мілені...	Розробіть контент-стратегію для інформаційного бюлетеня з безкоштовними міс...
📧 Повідомлення ChatGPT...	

# ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В РОБОТІ ОРГАНІЗАЦІЙ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

## Крок 3

Оберіть максимум три плагіни, які б ви хотіли використати. Якщо у вас немає необхідного плагіну, просто завантажте його з магазину плагінів..зображення.



**Bard** — це велика мовна модель від Google AI, навчена на величезній кількості текстових даних. Bard може генерувати текст, перекладати, аналізувати фото, писати різні види творчого контенту та відповідати на ваші запитання в інформативний спосіб. Його перевага полягає в тому, що він повністю безкоштовний і має доступ до інтернету, на відміну від ChatGPT. Також він може проаналізувати завантажену картинку, описати, що на ній зображено, а опісля вести з вами із цього приводу діалог.

**Claude AI** — це чат-бот із ШІ від компанії Anthropic. Його перевага — можливість аналізувати надзвичайно великі обсяги інформації, тому він легко впорається зі складними завданнями. Він може опрацьовувати тексти обсягом майже 75 тисяч слів, тобто, по суті, цілі книги. Claude AI не є повністю безкоштовним. Безкоштовна версія має обмеження, які можуть бути незручними для деяких користувачів. Завдяки платній підписці можна позбутися цих обмежень й отримати доступ до додаткових функцій, наприклад пріоритетного доступу в період великого трафіку, і нових функцій. Вартість платної підписки — від 20 доларів на місяць.



# ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В РОБОТІ ОРГАНІЗАЦІЙ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

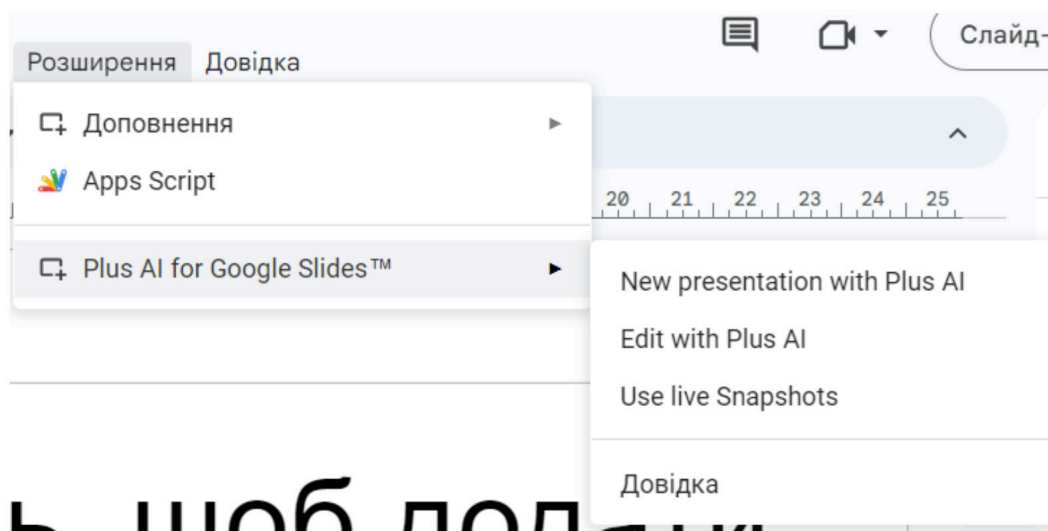
## СТВОРЕННЯ ПРЕЗЕНТАЦІЙ

### Plus AI for Google Slides

Це розширення Google Slides, у якому ШІ допомагає за декілька хвилин згенерувати та редагувати презентацію. Для того, щоб ним скористатися, у [Google Workspace Marketplace](#) вам потрібно завантажити розширення Plus AI for Google Slides. Після цього обрати значок «Розширення» та натиснути на «Plus AI for Google Slides».

Далі можна обрати одну з трьох функцій:

- створити презентацію за допомогою ШІ;
- редагувати презентацію за допомогою ШІ;
- використати Snapshots (так звані живі знімки екрана будь-якої програми або вебсайту, які автоматично оновлюються).



Щоб створити презентацію у Google Slides за допомогою ШІ, необхідно написати текст для слайдів (до 5 тисяч символів), а також опис самої презентації (до 5 тисяч символів). Під час підготовки опису ви можете обрати один із запропонованих варіантів стилю презентації, і ШІ автоматично згенерує опис, наприклад онлайн-курс, вебінар чи клієнтську пропозицію. Якщо ви хочете, то можете одразу надати структуру презентації, вставивши свій текст в окремі слайди. У цьому розширенні ви можете написати, у якому стилі варто опрацювати текст, який ви надали, наприклад «напиши текст у діловому стилі». Також ви можете обрати кількість слайдів.

# ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В РОБОТІ ОРГАНІЗАЦІЙ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Після того, як ви ввели всі потрібні дані та натиснули кнопку «згенерувати», через кілька хвилин у вас з'явиться необхідна презентація. У безкоштовній версії можна згенерувати загалом три презентації. Щоб отримати можливість генерувати більше презентацій, потрібно придбати платну підписку від 10 доларів, а для можливості додавати більше ніж 5 тисяч символів, потрібно оформити **підписку** — 20 доларів на місяць.

## ПЕРЕГЛЯД ТА АНАЛІЗ ВІДЕО

Для того, щоб швидко створити діаграми, ви можете використовувати плагін в ChatGPT **Show me diagram**. У ChatGPT 4 потрібно ввімкнути необхідний плагін і написати прохання згенерувати діаграму, використовуючи таку інформацію, вставити цю інформацію в діалог. Уже за декілька секунд ви отримаєте діаграму, яку зможете відкрити в повноекранному режимі чи відредагувати. Якщо ви хочете покращити діаграму, то можете використати ключову фразу «show ideas» й отримати «ідеї», як це зробити. Для ознайомлення з іншими типами діаграм і мовами потрібно використати ключову фразу «explore diagrams». Користувачі платної підписки ChatGPT можуть користуватися додатком безкоштовно.

## СТВОРЕННЯ ДІАГРАМ

### Summarize.tech

Якщо у вас немає часу переглядати відео в YouTube самостійно, ви можете дати завдання зробити це ШІ та швидко зрозуміти, чи варто вам дивитися довге відео. Для цього потрібно вставити посилання на відео в **Summarize.tech**, і він згенерує основну інформацію з нього. У безкоштовній версії Summarize.tech має обмеження на кількість відеороликів на день. Проте можна завантажити Summarize.tech Premium. Він не має щоденних обмежень, і ви можете підсумовувати до 200 відео на місяць. Вартість — 10 доларів на місяць.

## ТРАНСКРИБАЦІЯ ТА РОЗПІЗНАВАННЯ ТЕКСТУ

### Otter.ai

Цей інструмент для транскрипції аудіо- та відеофайлів використовує машинне навчання для підбиття підсумків нарад чи зустрічей. Після запису аудіо ви можете поспілкуватися із

# ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В РОБОТІ ОРГАНІЗАЦІЙ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

ШІ-помічником і поставити всі питання, що стосуються транскрибованої розмови. Він підтримує понад 60 мов і може транскрибувати як чистий, так і звук із шумом. Otter.ai може писати нотатки, а також підсумовувати те, що було сказано. У додатку є безкоштовний пробний період — 7 днів, після цього вартість підписки становитиме 10 доларів на місяць.

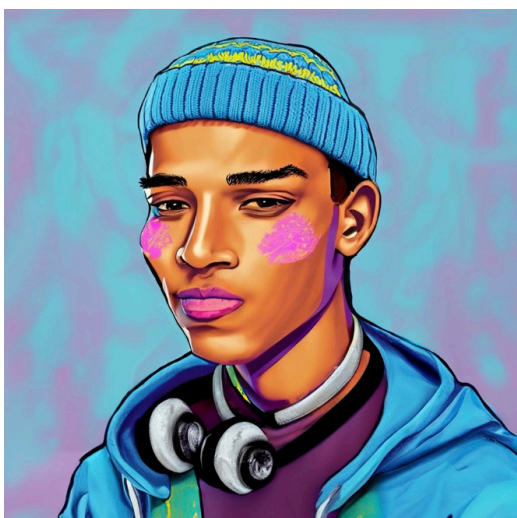
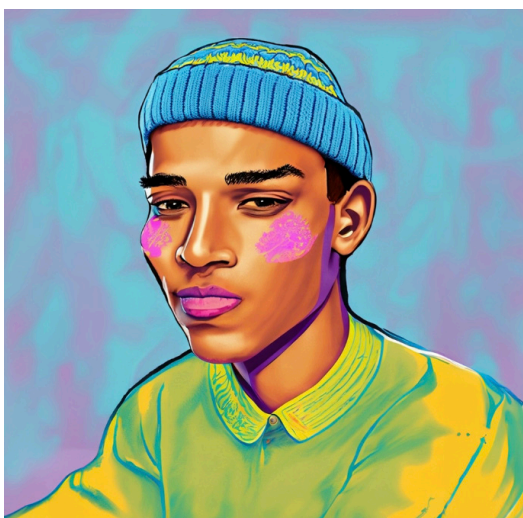
## СТВОРЕННЯ, РЕДАГУВАННЯ ТА ОБРОБКА ФОТОГРАФІЙ І ВІДЕО

### Adobe Firefly

Це інструмент, за допомогою якого ви можете замінити частину зображення на ту, яку ви захочете. Наприклад, вам не подобається, що на фото ви у футболці. Просто напишіть запит, попросивши замінити футболку на сорочку, і він досить непогано це зробить. Якщо вам потрібно зобразити текст на картинці нестандартно, ви можете попросити згенерувати будь-яку заливку, будь-якої текстури.

Якщо ви хочете змінити фон зображення, то можете скористатися інструментом генеративної заливки, написати, на який фон бажаєте змінити, і він автоматично буде згенерований на вашій картинці чи фото.

Зараз Adobe Firefly можна спробувати безкоштовно, проте кількість спроб обмежена. На цьому прикладі можна побачити, як легко замінити одну частину одягу на іншу.



Джерело: вебсайт [Adobe Firefly](#)

# ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В РОБОТІ ОРГАНІЗАЦІЙ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

В **Adobe Firefly** ви також можете прибрати об'єкт з відео та замінити його на інший. Ця функція з'явилася нещодавно.

Вартість платної підписки Adobe Creative Cloud, що охоплює всі продукти Adobe, кожний з яких має інструменти ШІ, — 35,99 долара на місяць, якщо ви купуєте річну підписку. Проте, якщо ви студент або студентка, вкажіть це під час вибору платної підписки, і її вартість стане 23,99 долара на місяць за умови придбання річної підписки.



Джерело: кадри з [відео про функціонал Adobe Firefly](#)

## **Midjourney**

Це додаток, у якому ви можете створювати зображення за допомогою текстового запиту. Для того, щоб створити зображення, потрібно завантажити Discord, оскільки генерування всіх картинок відбувається саме там. Для тих, хто про Discord чує вперше, — це платформа для обміну повідомленнями, де можна обмінюватися відео, голосовими, текстовими повідомленнями або публікаціями та спілкуватися за допомогою голосу одночасно з великими групами людей. Якщо ви бажаєте отримати безкоштовні години генерації, то можете скористатися такою можливістю в самому додатку: для цього потрібно обрати розділ **«rate images»** й оцінити зображення, розміщені там. Таким чином ви зможете отримати безкоштовні години генерації на 30 днів. Під час оцінювання потрібно обирати зображення, яке вам найбільше подобається, тому що рейтинги базуються на особистих уподобаннях.



# ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В РОБОТІ ОРГАНІЗАЦІЙ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

## **Runway**

Додаток, у якому ви можете зробити так, щоб фото «оживло», а персонаж на ньому почав рухатися. Також у ньому за текстовим запитом можна згенерувати 3D-об'єкт і змінювати його зовнішній вигляд. Доступна безкоштовна версія, у якій можна **згенерувати** три відео. Вартість платної підписки — від 15 доларів на місяць.

## **Captions**

Додаток, у якому можна зробити так, щоб ШІ сфокусував погляд людини в кадрі на камері під час відео. Навіть якщо людина дивилася не в камеру, а читала текст, ШІ зробить так, щоб цього не було видно. Для цього в додатку потрібно перейти в налаштування та ввімкнути «зоровий контакт». Також можна додати субтитри до відео або автоматично перекласти та озвучити текст будь-якою мовою. Щоправда, цю функцію додаток виконує ще не досконало. Вартість платної підписки — від 6,99 долара на тиждень.

## **СТВОРЕННЯ ЛОГОТИПІВ, ІКОНОК**

### **Design AI**

Додаток із ШІ, який самостійно створить логотип для вас. Для цього потрібно обрати галузь, стиль, ввести необхідну назву. ШІ аналізує ваші потреби в дизайні і видає результат. Є безкоштовна версія додатка. Вартість підписки — від 10 доларів на місяць.

### **Ideogram**

Безкоштовний додаток, що генерує картинки, логотипи, правильно пише текст на відміну від усіх відомого Midjourney. Можна вибрати стиль, у якому буде згенеровано результат, а також формат, наприклад 10:10, 1:1, 16:10.

# DEEPFAKE: ЩО ЦЕ І ЯК ПРАЦЮЄ?

На основі тез:  
**Ігоря Розкладая,**  
головного медійного юриста,  
заступника директорки ЦЕДЕМ

За допомогою ШІ після обробки й аналізу великої кількості аудіовізуальної інформації можна створювати відео та видавати їх за автентичні. Таке «підроблене» відео чи аудіо називається **deepfake**.

Існують три основні способи створення deepfake:

- 1 замість справжнього обличчя на відео підставляють інше;
- 2 на справжньому обличчі рухи в ділянці рота узгоджують з іншим аудіозаписом;
- 3 використовують манекен: на тіло й міміку зовсім іншої людини накладають зображення потрібної.<sup>8</sup>

В основі всіх цих способів лежить технологія deep learning algorithms. Якщо зібрати достатньо велику базу візуальних даних, за допомогою алгоритмів ШІ можна ніби як накласти одне зображення на інше. А якщо мати доступ до великої кількості аудіоданих, можна «прочитати» текст іншим голосом. Нейромережі дозволяють зробити таке накладання доволі реалістичним — це важлива риса багатьох діпфейків.

<sup>8</sup> Медійна реальність у стилі deep fake // [Детектор Медіа](#)

### ВИКОРИСТАННЯ

Для чого можуть використовувати таку технологію? За словами Ігоря Розкладая, «технології deepfake не є поганими — це просто інструмент». Прикладом позитивного використання він називає **deepfake Сальвадора Далі**, створений у музеї на його честь. Завдяки йому відвідувачі та відвідувачки мають можливість подивитися відеоролики з відомим митцем і навіть зробити з ним селфі. А портал для дослідження генеалогії «My Heritage» за допомогою інструмента **Deep Nostalgia** дозволяє на основі навіть одного фото згенерувати рухоме зображення за участі ваших померлих родичів.



Зображення, згенероване за допомогою Mojo AI

## ТЕХНОЛОГІЇ DEERFAKE ТА SHALLOWFAKE

ОГС також могли б використовувати технологію deepfake в роботі. Наприклад, «оживити» історичну постать, щоб поширити суспільну обізнаність про певну проблему (чому б Лесі Українці не заговорити про порушення прав жінок в Україні?).<sup>9</sup> ОГС, які взаємодіють з іноземними партнерами чи аудиторіями, можуть використовувати застосунки, які перекладають відео іншою мовою. Один з них — **Caption.AI**. «Корисні» deepfake-відео, які можна створювати з його допомогою, поки недосконалі, проте ця технологія точно буде розвиватися в майбутньому.

При цьому зрозуміло, що найчастіше технологію deepfake асоціюють з небезпекою: за допомогою deepfake можна вводити людей в оману. Доволі просто й ефективно підмінити слова публічних осіб: адже в загальному доступі є багато їхніх аудіовізуальних даних, а вплив таких людей великий. У березні 2022 року українці могли бачити неякісний і невдалий приклад такого введення в оману, коли представники Російської Федерації створили **відеоролик**, на якому Зеленський нібито пропонує громадянам України здатися. З багатьох причин цей ролик не досяг своєї мети з дестабілізації ситуації в країні, проте за інших умов та за більш якісно створеного зображення та аудіо deepfake справді може нести загрозу.

Загрозливими можуть бути не лише deepfake-відео, але й аудіо. Так, у 2021 році зловмисники в ОАЕ за допомогою технології deepfake підробили голос директора банку й змусили менеджера цього банку зробити трансфер розміром 35 мільйонів доларів на підставний банківський акаунт.<sup>10</sup>

Інше загрознає використання deepfake — фейкові порноролики. Їхню популярність пов'язують з 2017 роком, коли в інтернеті стали масово з'являтися deepfake-порно з відомими акторками<sup>11</sup>. Відповідно до даних Sensity AI за 2019 рік, 96 % deepfake-порно було створено без згоди на це, а 99 % із цих роликів містили зображення жінок<sup>12</sup>. Як повідомляє телеканал NBC, у соціальній мережі Discord вони зафіксували пропозиції за 65 доларів створити 5-хвилинне deepfake-порно «на замовлення»<sup>13</sup>. Такі відео порушують права людей, обличчя яких було використано, вони є глибоко травматичними, аб'юзивними та можуть вести до харасменту й погроз.<sup>14</sup>

<sup>9</sup> Зокрема, у грудні 2023 року Український інститут та українська ШІ-компанія Reface випустили відео, у якому за допомогою ШІ Вільям Шекспір та Леся Українка «розмовляють» між собою про **асоціації**

<sup>10</sup> Delić, Danka. The deepfake technology behind a \$35 million bank heist in Hong Kong // **ProPrivacy**

<sup>11</sup> Johnson, Dave and Johnson, Alexander. What are deepfakes? How fake AI-powered audio and video warps our perception of reality // **INSIDER**

<sup>12</sup> Dunn, Suzie. Women, Not Politicians, Are Targeted Most Often by Deepfake Videos // **Centre for International Governance Innovation**

<sup>13</sup> Mahdawi, Arwa. Nonconsensual deepfake porn is an emergency that is ruining lives // **The Guardian**

<sup>14</sup> Middleton, Amber. A Twitch streamer was caught watching deepfake porn of women gamers // **INSIDER**



## А ЩО TAKE SHALLOWFAKE?

**Shallowfake** — це коли медіаконтент, який насправді існує, дещо корегують.

Варто відзначити, що машинне навчання (machine learning) не так створює можливості для фейків, як розширює їх. На відміну від deepfake, щоб створити shallowfake, не потрібно використовувати технологію deep machine learning, достатньо лише елементарного монтажу. Через це shallowfake називають також «дешевим фейком», хоча окремі експерти вважають, що поки такі фейки можуть становити загрозу, не меншу за deepfake.<sup>15</sup>

До прикладу, можна створити продукт, у якому відеоряд правдивий, а от аудіоряд — ні. Таким shallowfake є **відео** зі спікеркою Палати представників США Ненсі Пелосі. На ньому на справжній відеоряд було накладено сповільнений аудіозапис її голосу. Так автори фейку хотіли створити у глядачів уявлення, що Ненсі Пелосі на відео нетвереза.

Ще більш примітивний shallowfake — просте «висмикування» **уривку відео** із ширшого контексту<sup>16</sup>. У 2022 році певної популярності набрав уривок відео, у якому Президент Зеленський нібито говорить громадянам країн-членів НАТО, що їхні діти будуть іти воювати та вмирати. Насправді йшлося про гіпотетичний напад на країни Балтії в разі поразки України, а не про російсько-українську війну. Проте цю частину не включили у фрагмент, який поширили американські конгресмени, що виступають проти допомоги Україні.

### ЯК РОЗПІЗНАТИ DEERFAKE?

Справді, уже зараз згенеровані відео можуть доволі сильно нагадувати справжні. Технологія досі не є ідеальною, хоча за останні шість років суттєво покращилася. Існує низка ознак, за якими зазвичай можна відрізнити deepfake. **Детектор Медіа** пропонує звертати увагу на такі вісім ознак:

- мерехтіння обличчя;

<sup>15</sup> Johnson, Bobbie. Deepfakes are solvable — but don't forget that "shallowfakes" are already pervasive // [MIT Technology Review](#)

<sup>16</sup> TLeetaru, Kalev. The Real Danger Today Is Shallow Fakes And Selective Editing Not Deep Fakes // [Forbes](#)

# ТЕХНОЛОГІЇ DEEPFAKE ТА SHALLOWFAKE

- невідповідність обличчя та тіла (часто замінюють лише обличчя);
- джерело публікації відеозапису (воно може бути неперевіреним);
- звук запису та його несинхронізованість з мімікою;
- неправдоподібна міміка в ділянці рота (вона є однією з найскладніших для відтворення);
- тривалість відео (зробити дуже довгий deepfake складно);
- деталі при сповільненні відео (потрібно звертати увагу на тло);
- неправдоподібне моргання чи його відсутність;
- неправдоподібна міміка в ділянці рота.

Існують й інші способи розпізнати deepfake. Наприклад, можна пошукати в інтернеті ключові слова з відео — і у випадку deepfake відеопошук може просто не дати результатів. Окрім того, якщо зробити скриншот з відео та завантажити його в інтернет-пошук, можна знайти оригінальне відео, на основі якого могли зробити deepfake, а дата завантаження цього відео, вірогідно, буде відрізнятися від дати завантаження deepfake-відео<sup>17</sup>.

Щодо аудіо, то Джордж Хатчер, засновник консультативної компанії з кібербезпеки White Knight Labs, радить звертати увагу на такі індикатори, як обірвані речення, дивно підібрані слова та незвична словозміна й тон голосу<sup>18</sup>. Ще одним індикатором можуть бути «дивні» та «підозрілі» наголоси в аудіодоріжці.

## ЯК РОЗПІЗНАТИ SHALLOWFAKE?

Залежно від типу треба звертати увагу на різні деталі, такі як:

- зміни шрифту;
- дивне або відмінне тло та освітлення, неприродні варіації кольорів і тіней;
- будь-які ознаки монтажу: аудіосклейки, невідповідність між різними об'єктами, неприродні елементи, що свідчать про використання Photoshop.<sup>19</sup>

<sup>17</sup> How to spot a deepfake // [CNA Insider](#)

<sup>18</sup> Lawton, George. How to prevent deepfakes in the era of generative AI // [Techtarget](#)

<sup>19</sup> Randall, Natalie. The rise of shallowfakes // [Chartered Insurance Institute](#)

Загальним правилом має бути критичне сприйняття будь-якої інформації: пошук джерел її походження, рефлексія над тим, чи може метою появи цієї інформації бути маніпуляція.

### ЩО РОБИТИ ЛІДЕРАМ ОГС, АКТИВІСТАМ, ВОЛОНТЕРАМ, ЯКІ СТАЛИ ЖЕРТВАМИ DEEPFAKE?

По-перше, у чинному українському законодавстві існує право на відповідь та спростування (стаття 43 Закону України «Про медіа»). Відповідно до нього «особа, яка вважає, що суб'єктом у сфері аудіовізуальних, друкованих або онлайн-медіа щодо неї було поширено відомості, які не відповідають дійсності (викладені неповно чи неточно) та принижують її честь, гідність чи ділову репутацію, має право вимагати спростування недостовірної інформації або реалізації права на відповідь».

Утім, нині дуже багато українців споживають новини із соціальних мереж. Відповідно до дослідження, яке провела соціологічна група «Рейтинг», у лютому 2023 року 41 % українців отримували суспільно-політичні новини з груп і каналів у месенджерах Telegram, Viber; 35 % — із соціальних мереж (Facebook, Twitter, Instagram). А опитування USAID-Internews, яке відбулося в листопаді 2022 року, показало, що соціальні мережі були джерелом новин для 74 % українців<sup>20</sup>. Іншими словами, популярність соцмереж зіставна з популярністю національного телебачення та інтернет-сторінок, з яких новини дізнаються 43 % та 36 % українців відповідно<sup>21</sup>. Згідно з дослідженням, проведеним на замовлення ГО «Опора», соціальні мережі є джерелом інформації для 77,9 % українців. А от телебачення та інтернет (без урахування соцмереж) — 62,5 % та 57,7 % відповідно<sup>22</sup>.

Натомість Ігор Розкладай стверджує, що в соцмережах право на відповідь реалізувати надзвичайно важко. Адже, окрім юридичних складнощів, зокрема встановлення особи, що поширила інформацію, тут ми стикаємося і з технічними. По-перше, оскільки соцмережі заганяють нас у «бульбашки» за інтересами, не факт, що ваша відповідь у вашому профілі на недостовірну інформацію охопить ту саму «бульбашку», яку охопив той, хто поширив про вас цю інформацію. Тож треба через суд зобов'язувати особу поширювати відповідь у такий самий спосіб, у який була поширена неправдива інформація. До того ж Ігор Розкладай зазначає, що через високу швидкість поширення інформації виникає негласне правило «хто перший поширив інформацію — той і має рацію». Онлайн-ресурси діють не так, як

20 Опитування USAID-Internews щодо споживання медіа // [Укрінформ](#)

21 Мельник, Роман. За рік війни українці стали споживати новини з месенджерів вчетверо частіше, — дослідження // [Детектор Медіа](#)

22 Медіаспоживання українців: другий рік повномасштабної війни. Опитування ОПОРИ // [ОПОРА](#)

## ТЕХНОЛОГІЇ DEEPFAKE ТА SHALLOWFAKE

звичайні медіа, передбачають репости (у тому числі кросплатформені). Через це навіть якщо суд зобов'яже особу зробити про вас спростування в блозі, нема гарантії, що та сама аудиторія, яка побачила перше повідомлення, побачить це спростування. Бодай тому, що доведеться зобов'язати кожну особу, що репостнула оригінальний пост, репостнути й спростування.



Зображення, згенероване за допомогою DALL-E

Через це для соцмереж одним з найдієвіших рішень є ведення кризової комунікації — уміння швидко і вчасно доносити певні меседжі. Зокрема, варто пам'ятати про правило трьох годин для першої реакції, правило доби для другої реакції, правило не виправдовуватися, а відстоювати свою позицію. На думку Ігоря Розкладая, у соцмережах такі механізми нині більш ефективні



за юридичні, адже швидкість поширення інформації настільки висока, що жоден суд не забезпечить належної відповіді: юриспруденція значно повільніша.

Запобігти збору даних про вас, які можна потім використати для створення фейків, можуть допомогти безпекові протоколи та культура використання персональних даних, наприклад непоширення своїх даних стороннім особам. Окрім того, ОГС варто мати чіткі протоколи здійснення оплат: з автентифікацією та обов'язковим залученням письмової комунікації.

### НАПОЛЕГЛИВО РЕКОМЕНДУЄМО:

- Якщо це **аудіовізуальні, друковані чи онлайн-медіа** — варто скористатися правом на спростування або правом на відповідь, передбаченим Законом України «Про медіа». А в певних випадках бути готовими дати відповідь наживо навіть без подання відповідних скарг.
- Якщо це **соцмережі** — необхідно швидко комунікувати потрібний вам меседж, щоб спростувати неправдиву інформацію.
- Необхідно **мати чіткі, надійні беззаперечні безпекові протоколи** (з внутрішньої комунікації, використання даних і т. д.).

# ЯК ПРАЦЮЮТЬ ТАКІ КАМЕРИ?

На основі тез:  
**Франчески Фануччі,**  
головної юридичної радниці  
Європейського центру некомерційного  
права (ECNL)

**Технологія розпізнавання обличчя** (тут і далі — **ТРО**) побудована на зіставленні різних зображень. Спершу вона вимірює біометричні дані обличчя, а далі порівнює ці дані з базою даних, до якої має доступ.

Це можна робити трьома способами:

- 1 Верифікація** (зіставлення один до одного) — технологія порівнює одне обличчя з іншим конкретним зображенням.  
**Мета:** встановити, що особа на двох зображеннях — та сама людина.  
**Приклади застосування:** функція FaceID для розблокування iPhone, сканування паспортів під час прикордонного контролю на виході з аеропорту.
- 2 Ідентифікація** (зіставлення один до багатьох) — технологія порівнює одне обличчя з набором інших облич (біометричних шаблонів).

## КАМЕРИ З ТЕХНОЛОГІЄЮ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ

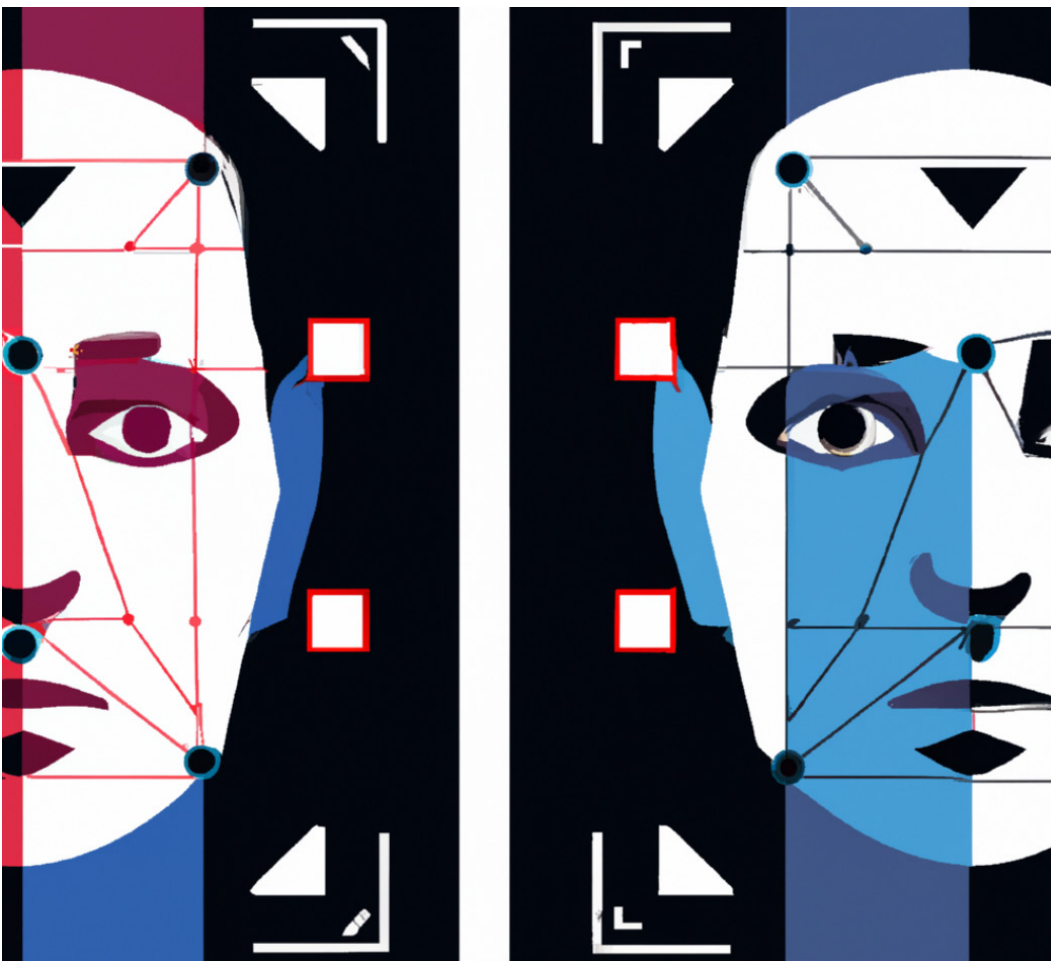
**Мета:** з'ясувати, чи обличчя відповідає одному або кільком обличчям з бази даних.

**Приклад застосування:** системи відеоспостереження (наприклад, у торговельних центрах або в інших публічних місцях). Цю технологію може використовувати поліція.

**3 Класифікація** (зіставлення за загальними характеристиками) — технологія аналізує риси обличчя однієї чи кількох осіб за певними ознаками (усмішка, сміх, насуплені брови, колір шкіри та очей, будова черепа).

**Мета:** класифікувати обличчя за ознаками, тобто визначити певні емоції, стать, вік, етнічне походження тощо.

**Приклад застосування:** камери відеоспостереження на рекламних бордах, що аналізують емоції, або камери, що передбачають емоції / потенційні порушення на масових заходах.



Зображення, згенероване за допомогою DALL-E

## КАМЕРИ З ТЕХНОЛОГІЄЮ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ

**ТРО складається з трьох етапів.** На першому на основі алгоритмів ШІ аналізується статистична інформація. **Далі — навчання** на основі певних наборів даних (це можуть бути зображення або біометричні шаблони). Після навчання технологія стає здатною **визначати послідовні закономірності** на зображеннях чи біометричних шаблонах і впізнавати подібності (це особливі характеристики ШІ — здатність навчатися ідентифікувати тренди, з певною часткою автономності та адаптуванням до обставин). ТРО на основі ШІ можуть працювати в режимі реального часу або ретроспективно. Тобто вони можуть зіставляти зображення з базою даних наживо або навіть після створення запису.

### ДЕ ВИКОРИСТОВУЮТЬ КАМЕРИ З РОЗПІЗНАВАННЯМ ОБЛИЧЧЯ?

З одного боку, використання камер з ТРО може спростувати життя людей або допомагати розкривати злочини. Наприклад, ця технологія використовується для безпечного розблокування смартфонів — в операційній системі Android вона була представлена у 2015 році, а Apple запустили її у 2017 році. Саме камери з ТРО допомогли американським військовим ідентифікувати Осаму бен Ладена у 2011 році.<sup>23</sup> У США такі системи нещодавно почали використовувати в мережах магазинів, таких як Walmart, для того, щоб ідентифікувати людей, які здійснили крадіжку<sup>24</sup>.

В Україні вже працюють камери з розпізнаванням обличчя. Їх встановлюють для охорони правопорядку: поліцейські стверджують, що такі камери нібито є ефективними для розкриття злочинів<sup>25</sup>. А в місті Новий Орлеан та в штаті Вірджинія, де у 2020 році наклали заборону на використання камер з ТРО, уже через два роки ініціювали дискусію, щоб дозволити використовувати такі камери для розслідування тяжких злочинів<sup>26</sup>.

Водночас в авторитарному Китаї використання камер з ТРО стає повсякчас більш загрозливим. В умовах масштабного поширення цих камер (станом на 2020 рік, за оцінками, у Китаї їх було від 200 до 600 мільйонів<sup>27</sup>) китайський уряд використовує ці камери для дискримінації уйгурської етнічної меншини та навіть для того, щоб публічно соромити людей, наприклад тих,

23 Klosowski, Thorin. Facial Recognition Is Everywhere. Here's What We Can Do About It // [NYT Wirecutter](#)

24 Dastin, Jeffrey. Special Report: Rite Aid deployed facial recognition systems in hundreds of U.S. stores // [Reuters](#)

25 В Україні запрацювали камери з розпізнаванням обличчя: як вони працюють і кого шукають // [Фокус](#)

26 Metz, Rachel. First, they banned facial recognition. Now they're not so sure // [CNN Business](#)

27 Cadell, Cate. 'It seemed like fun, I decided to join in': Inside the biggest human surveillance experiment on the planet // [The Sydney Morning Herald](#)



кого камери помітили на вулиці в піжамі<sup>28</sup>. А ще за допомогою таких камер уряд складає так званий індекс благонадійності громадян, який впливає на свободи громадян та їхній доступ до певних благ. У Росії використання камер з ТРО пов'язують з подальшим продажем персональних даних на чорному ринку. таких камер уряд складає так званий індекс благонадійності громадян, який впливає на свободи громадян та їхній доступ до певних благ<sup>29</sup>. У Росії використання камер з ТРО пов'язують з подальшим продажем персональних даних на чорному ринку. Також російський уряд цілком може використовувати їх для боротьби з мирними протестами й демонстраціями<sup>30</sup>.

Та проблеми з використанням цієї технології стосуються далеко не лише авторитарних режимів. Нині перед цим викликом постають і демократичні держави. Ігор Розкладай відзначає камери з ТРО як одну з найбільших загроз у сфері ШІ, яка зараз існує для ОГС та всього громадянського суспільства.

### ЯКІ ІСНУЮТЬ РИЗИКИ, ПОВ'ЯЗАНІ З ВИКОРИСТАННЯМ ТАКОЇ ТЕХНОЛОГІЇ?

На думку Франчески Фануччі, старшої юридичної радниці Європейського центру некомерційного права (ECNL), використання ТРО в системах відеоспостереження несе такі небезпеки:

- Можливість хибнопозитивної помилки у звітах та аналізах — технологія працює з імовірностями та все-таки може помилитися й почати стверджувати про подібність між різними об'єктами або людьми.
- Можлива упередженість і дискримінація — такі системи часом гірше розпізнають чорношкірих людей, можуть не розрізняти людей з інвалідністю чи незвичною зовнішністю залежно від контексту (освітлення, позиції тощо).
- Дестимуляційний вплив на зібрання / пересування — знаючи про можливість їх ідентифікації, люди будуть менше виходити на протести. Особливо (але не лише) це релевантно для авторитарних режимів, наприклад Китаю, де існує так звана система соціального рейтингу, і держава завдяки технологіям може легко вдаватися до репресивних дій.

28 Ng, Alfred. How China uses facial recognition to control human behavior // [CNET](#)

29 Авдєєва, Тетяна. Чи легально встановлювати на міських вулицях камери із системою розпізнавання облич? // [Центр демократії та верховенства права](#)

30 Там само.

## КАМЕРИ З ТЕХНОЛОГІЄЮ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ

Також часто не відомо, де можуть зберігатися зображення з камер спостереження, хто саме і з якою метою буде їх використовувати. Якщо дані в базі даних були підібрані дискримінаційно, дискримінаційними будуть і результати роботи таких камер. Часом джерела даних для навчання ТРО можуть мати сумнівне походження, а розробники не бажають розкрити інформацію про технологію.

Тож Франческа Фануччі відзначає, що використання ТРО потенційно може порушувати права людини.

У тому числі такі права:

- право на приватність;
- право на захист даних;
- свободу слова / вираження поглядів / мирних зібрань;
- право на відсутність дискримінації;
- право на гідність;
- право на ухвалення рішення людиною;
- право на доступ до інформації;
- право на оскарження / доступ до ефективного правового захисту.

ОГС, зокрема правозахисні організації, мають усвідомлювати масштаб ризиків для прав людини від використання ТРО. Щоб запобігти порушенню прав громадян України, ОГС варто звернути увагу на використання цих камер. На жаль, ця тема нині є відносно непопулярною і малозрозумілою для громадського сектору. Утім, уже зараз українські ОГС мають продовжувати адвокатувати регулювання таких систем, допомагати розробляти законодавство, яке не ігнорує цю технологію. Зокрема, саме цим нині активно займається ЦЕДЕМ. Інше завдання ОГС у цій сфері — запобігати неправомірному використанню таких технологій органами державної влади, органами місцевого самоврядування, бізнесом тощо.

Українська влада також має ухвалити надійне законодавство, яке буде застосовним до різних способів використання ТРО та залучатиме громадянське суспільство до оцінювання впливу таких камер перед їх використанням. Громадськість має мати право знати, де та чому використовуються такі камери, як вони працюють, а також мати право на перегляд рішень, що ґрунтуються на їх використанні.

## УКРАЇНСЬКИЙ ДОСВІД

На основі тез:  
**Тетяни Авдєєвої,**  
юристки Лабораторії  
цифрової безпеки

**В Україні досі фактично не існує належного національного законодавства, яке б регулювало питання використання камер з ТРО.**

Існує концепція розвитку ШІ, але в ній майже не згадано про права людини, аналогічна проблема із законодавством у сфері діяльності органів правопорядку й захисту персональних даних. Нині немає ані технічних стандартів, ані юридичних запобіжників щодо цих технологій, зазначає Тетяна Авдєєва.

На думку юристки, у поточному вигляді закон про захист персональних даних є застарілим для регулювання систем, які керуються ШІ. Зокрема, зараз документ не відповідає **Загальному регламенту про захист даних** і не бере до уваги особливостей нових технологій.

Попри це, уже у 2021 році в Україні використовувалися ССТV-камери. Їх встановлювали переважно через муніципальну владу (органи місцевого самоврядування через комунальні підприємства), проте, як відзначає Тетяна Авдєєва, закон про органи місцевого самоврядування не містить положень, які на-

## КАМЕРИ З ТРО ТА ССТV-КАМЕРИ В УКРАЇНІ

дають їм повноваження використовувати або дозволяти використання будь-яких засобів стеження. Тому будь-які підзаконні акти не ґрунтувалися на законі, а їх ухвалення було свавільними діями з боку місцевої влади.



Зображення, згенероване за допомогою DALL-E

Проблема використання камер відеоспостереження в Україні не обмежена юридичною площиною. Інше питання — технічні компетенції та відсутність достатньої кількості технічних експертів, які можуть проаналізувати нові технології. Адже якщо не будуть дотримані необхідні технологічні стандарти, система може стати об'єктом хакерських атак, у тому числі з боку Росії. Нині в Україні нема достатньої кількості технічних експертів, які можуть працювати з новими технологіями.



Часом ідеться й про використання потенційно небезпечних технологій. В Україні найпоширенішими є камери китайських виробників Hikvision та Dahua. Аналітики відзначають, що вони можуть бути вразливими до зламів<sup>31</sup>. Ба більше, такі камери можуть бути афілійовані з китайською розвідкою та буквально допомагати їй шпигувати за кордоном<sup>32</sup>. З огляду на факт кооперації між Росією та Китаєм для громадян України ця вразливість може становити пряму загрозу.

Через це Тетяна Адвєєва підкреслює:

**«Не можна виправдовувати питанням національної безпеки ситуації, у яких для національної безпеки створюються додаткові загрози».**



Зображення, згенероване за допомогою DALL-E

31 Mathews, Lee. Widely-Used Hikvision Security Cameras Vulnerable To Remote Hijacking // [Forbes](#)

32 Kupriienko, Oleksii. OPINION: Trojan Horse: How Chinese-Made Cameras Put Ukraine at Risk // [Kyiv Post](#)

## КАМЕРИ З ТРО ТА ССТV-КАМЕРИ В УКРАЇНІ

З боку влади вже з'явилися тривожні сигнали використання камер відеоспостереження. Наприклад, після протестів на підтримку активіста Сергія Стерненка представники Міністерства внутрішніх справ України заявили, що найбільш активних учасників протестів буде ідентифіковано за допомогою систем розпізнавання обличчя. Подальшого розвитку ця ситуація не мала, але сам факт таких заяв є загрозливим.

Відкритим і публічним є кейс використання українським урядом технології Clearview AI для пошуку російських військових злочинців<sup>33</sup>. Clearview AI надає користувачам інструмент для розпізнавання облич. Із цією технологією існує одразу кілька проблем. Перша — це те, що база даних Clearview AI створена шляхом сканування фотографій користувачів найбільших соціальних мереж без згоди на це самих користувачів. Завдяки такому способу збору даних компанія Clearview AI станом на квітень 2023 року могла мати 30 мільярдів зображень у своїй базі даних<sup>34</sup>.

Через проблемний шлях створення бази даних, який порушує права користувачів соціальних мереж, продукт Clearview AI заборонили у Великій Британії. А французька та італійська влада оштрафувала компанію за незаконний збір й обробку біометричних даних своїх громадян. Попри це, відомо, що вже понад 600 правоохоронних органів використовують у своїй роботі Clearview AI<sup>35</sup>.

Та навіть якщо відкинути моральний аспект використання Clearview AI, яким є юридичний статус доказів, що спираються на цю технологію? І чи можуть її результати бути достатньою підставою для відкриття провадження стосовно людини на території України? На думку Тетяни Авдєєвої, якщо суди пристануть на позицію, що така технологія є допустимим доказом, це може створити небезпечний прецедент. Адже відомо, що в США вже намагалися притягнути до відповідальності на підставі аналогічних систем, і виявилось, що системи часто видають помилковий результат. Наприклад, у 2020 році чоловіка зі штату Мічиган, попри наявність у нього алібі, хибно заарештували за крадіжку комп'ютера через те, що на цю людини вказав алгоритм з розпізнавання обличчя<sup>36</sup>.

<sup>33</sup> Сабадишина, Юлія. Як Україна використовує штучний інтелект для перемоги. У Мінцифри розповіли деталі // [DOU](#)

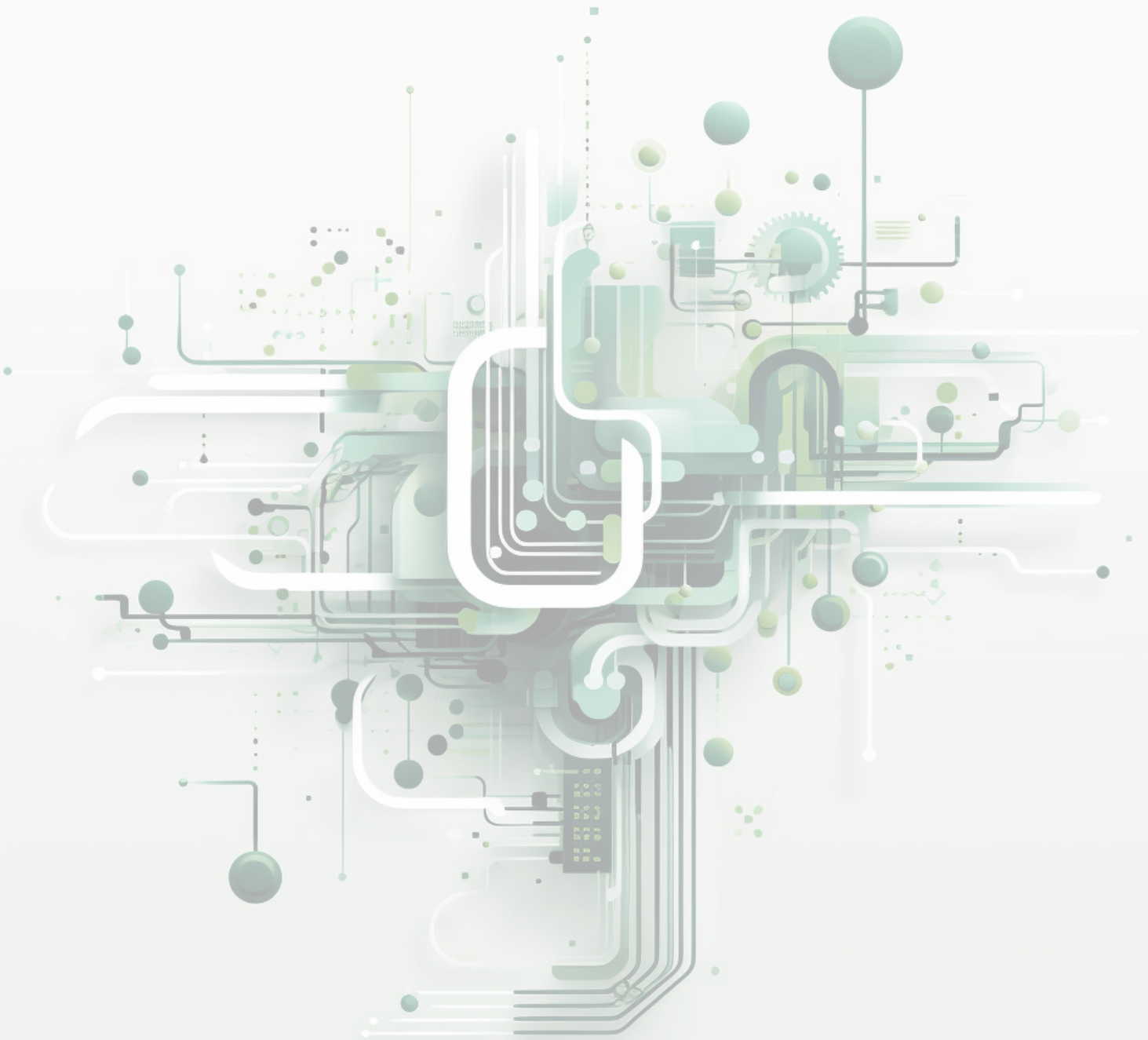
<sup>34</sup> Баловсяк, Надія. Нерівноправне партнерство. Чому співробітництво України та Clearview AI не повинно продовжуватись після війни // [Куншт](#)

<sup>35</sup> Там само.

<sup>36</sup> Hill, Kashmir. Wrongfully Accused by an Algorithm // [The New York Times](#)

## КАМЕРИ З ТРО ТА ССТV-КАМЕРИ В УКРАЇНІ

Через ці та інші проблеми, на думку Тетяни Авдєєвої, підхід до вивчення проблем, пов'язаних з використанням камер з розпізнаванням обличчя в Україні, потрібно шукати вже зараз. Ці проблеми можуть мати прямий вплив на права людини та безпеку активістів. Окрім розроблення змістового регулювання, варто звертати увагу й на процедурне регулювання.



## НОРМАТИВНО-ПРАВОВІ АКТИ ЩОДО ТРО

На основі тез:  
**Франчески Фануччі,**  
головної юридичної радниці  
Європейського центру некомерційного  
права (ECNL)

Франческа Фануччі виділяє одразу декілька нормативно-правових актів, що стосуються ТРО.

- Перший — Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (**Конвенція 108**). Україна є однією з країн-підписантів цієї Конвенції. У 2021 році Рада Європи (РЕ) додатково випустила **Керівні принципи з технології розпізнавання обличчя** на основі Конвенції 108.

Відповідно до цієї Конвенції держави мають ухвалити надійну правову базу, застосовну до різних випадків використання ТРО. Зокрема, Франческа Фануччі відзначає такі ключові пункти:

- конкретне використання та цільове призначення технології;
- мінімальні рівні надійності та точності використовуваних алгоритмів;
- тривалість зберігання отриманих зображень;



## ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ КАМЕР З ТРО

- мінімізація даних, що обробляються (неактуальні дані треба мінімізувати, наприклад замилити обличчя, які не потрібні для аналізу);
- критерії відкритості процесу;
- гарантоване право на інформацію, право на доступ, право на отримання знань про основоположні аргументи, право на заперечення, право на виправлення.

Обмеження цих принципів не мають порушувати суть прав і відповідати критеріям трискладового тесту — законність, необхідність і пропорційність. Окрім того, у рекомендаціях РЄ йдеться про можливість введення мораторію на використання ТРО до проведення повного аналізу й демократичного обговорення цієї технології.



Зображення, згенероване за допомогою DALL-E

# ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ КАМЕР З ТРО

- **Керівні принципи ОБСЄ зі свободи мирних зібрань** (2019)

Відповідно до цих принципів «використання збережених зображень з метою ідентифікації (включно з програмним забезпеченням для розпізнавання обличчя) має бути обмежене тими обставинами, за яких кримінальні правопорушення фактично мають місце або коли є обґрунтована підозра щодо неминучої злочинної поведінки».

- **Керівні принципи Європейської ради щодо використання технології розпізнавання обличчя у правоохоронній діяльності** (2022)

Відповідно до цього документа потрібно здійснювати оцінювання впливу використання цієї технології на всі права людини, зокрема тестувати на абсолютну необхідність і пропорційність та оприлюднювати результати чи основні висновки. Також завжди потрібно застосовувати згаданий принцип мінімізації даних. Заборонено обробляти персональні дані, якщо ця обробка спирається на базу даних, наповнену за допомогою масового збору персональних даних, наприклад скрепінгу («вишкрібання», збирання або витягнення даних) фотографій і зображень обличчя, доступних в інтернеті.

- **Законопроект ЄС про штучний інтелект**, який порушує питання розпізнавання облич.

Станом на час написання цього Гайду, відповідно до статті 5 цього законопроекту були заборонені системи віддаленої біометричної ідентифікації (ВБІ), які працюють у режимі реального часу в загальнодоступних місцях з метою здійснення правоохоронної діяльності, окрім цілеспрямованого пошуку жертв злочину, запобігання терористичній атаці, розшуку виконавця злочину. Проте очікувано, що статтю 5 цього законопроекту буде змінено.

### **Спільний висновок Європейської ради із захисту даних (EDPB) та Європейського інспектора із захисту даних (EDPS) щодо пропозиції до Закону ЄС про штучний інтелект** (2021)

Містить заклик до загальної заборони будь-якого використання ШІ для автоматизованого розпізнавання рис людини в загальнодоступних (громадських) місцях — включно з ТРО — у будь-якому контексті.

Такий підхід пояснюють відсутністю прозорості того, як працюють і як обробляють дані ці системи, і тим, що «використання систем ШІ може створити серйозні проблеми з точки зору пропорційності, оскільки воно може передбачати оброблення даних довільної та непропорційної кількості суб'єктів

даних для ідентифікації всього лише кількох осіб».

Позиція EDPB та EDPS полягає в тому, що незворотний серйозний вплив на (обґрунтовані) очікування населення щодо анонімності в громадських місцях призведе до прямого негативного впливу на свободу вираження поглядів, зібрань, асоціацій, а також свободу пересування.

### ВИКОРИСТАННЯ НЕБЕЗПЕЧНИХ ТЕХНОЛОГІЙ ПІД ЧАС ВОЄННОГО СТАНУ

Зрештою, в Україні триває війна та діє воєнний стан. Для таких випадків існують міжнародні стандарти дерогації (відступу) під час надзвичайного стану. Відповідно до **зауважень загального характеру № 29** Комітету ООН з прав людини до статті 4 Міжнародного пакту про громадянські та політичні права, на час надзвичайного стану передбачені процедури дерогації (відступу) від певних положень цього документа.

Проте заходи, що відступають від положень пакту, мають мати винятковий і тимчасовий характер. Вони дозволені лише в тому разі, якщо ситуація становить загрозу життю нації, а самі заходи мають бути зумовлені винятково гостротою ситуації.

Використання камер CCTV загрожує правам людини. Утім, як зауважує Франческа Фануччі, за умови їх використання під час надзвичайного стану варто все ж спробувати забезпечити збереження прав людини. Можна встановити обмежувальні положення, до прикладу зафіксувати, що ці технології використовуються для ідентифікації військових, а після завершення воєнного стану камери буде знято, а таку практику буде припинено. На думку експертки, варто враховувати інвазивність подібних технологій і витримувати баланс: з одного боку, захищати населення, а з іншого — захищати права людини.

Окрім того, процедури дерогації під час надзвичайного стану стосується стаття 15 Європейської конвенції з прав людини: «Під час війни або іншого надзвичайного стану в державі, який загрожує життю нації, будь-яка Висока Договірна Сторона може вжити заходів, які не відповідають її зобов'язанням за цією Конвенцією, виключно в тих межах, які зумовлені гостротою становища, якщо такі заходи не суперечать іншим її зобов'язанням за міжнародним правом».

Та, як відзначає Франческа Фануччі, під час використання такої процедури варто забезпечувати повну прозорість: чітко визначати, які саме права ми обмежуємо та як надовго, а далі час від часу оцінювати доцільність тих чи інших обмежень.

## АНАЛІТИКА ЦЕДЕМ:

- Ольга Петрів  
Штучний інтелект і авторське право  
ChatGPT — «споживач» російської пропаганди:  
як цьому протидіяти?  
Штучний інтелект та Artificial Intelligence:  
час для юридичних рамок.  
Штучний інтелект та дезінформація:  
(не)видима загроза сучасності
- Олена Соколова  
Регулювання штучного інтелекту: досвід США
- Тетяна Авдєєва  
Чи легально встановлювати на міських вулицях  
камери із системою розпізнавання облич



## ІНШІ МАТЕРІАЛИ:

- Arnold. What Is The Difference Between A Deepfake And Shallowfake? // [DeepFakeNow](#)
- Johnson, Dave and Johnson, Alexander. What are deepfakes? How fake AI-powered audio and video warps our perception of reality // [INSIDER](#)
- Sample, Ian. What are deepfakes — and how can you spot them? // [The Guardian](#)
- 4 Types of AI: Getting to Know Artificial Intelligence // [Coursera](#)
- Hsu, Tiffany. As Deepfakes Flourish, Countries Struggle With Response // [The New York Times](#)
- The state of AI in 2022 — and a half decade in review // [McKinsey & Company](#)
- Klosowski, Thorin. Facial Recognition Is Everywhere. Here's What We Can Do About It // [NYT Wirecutter](#)
- Медійна реальність у стилі deep fake // [Детектор Медіа](#)
- Johnson, Bobbie. Deepfakes are solvable — but don't forget that “shallowfakes” are already pervasive // [MIT Technology Review](#)
- Sanchez, Conor. Civil society can help ensure AI benefits us all. Here's how // [World Economic Forum](#)
- Sheehan, Jared and Chappell, Nathan. The State of Artificial Intelligence in the Nonprofit Sector: Ethical Considerations // [NonProfitPro](#)
- Баловсяк, Надія. Нерівноправне партнерство. Чому співробітництво України та Clearview AI не повинно продовжуватись після війни // [Куншт](#)
- Vu. The Ethics and Opportunities of Artificial Intelligence in the Nonprofit Sector // [Nonprofit AF](#)
- How to spot a deepfake // [CNA Insider](#)



# ПОДЯКА СПІКЕРАМ ФОРУМУ ЗА НАДАНІ МАТЕРІАЛИ

Центр демократії та верховенства права висловлює подяку Агентству США з міжнародного розвитку та Уряду Швеції, ICAP Єднання, Лабораторії цифрової безпеки за можливість організації та проведення Щорічного Форуму «Штучний інтелект 2.0: регулювання та робота під час війни».

Особливу подяку висловлюємо спікерам і спікеркам експертної дискусії «Штучний інтелект і організації громадянського суспільства»:

- **Олесі Холопик**, директорці ЦЕДЕМ;
- **Ігорю Розкладаю**, головному медійному юристу, заступнику директорки ЦЕДЕМ;
- **Франчесці Фануччі**, головній юридичній радниці ECNL;
- **Тетяні Авдєєвій**, юристці Лабораторії цифрової безпеки;
- **Вероніці Бойко**, керівниці соціального напрямку YouControl, експертці Асоціації відкритих даних;
- **Ользі Петрів**, юристці напрямку «Незалежні медіа» ЦЕДЕМ;

а також модераторці експертної дискусії **Марії Гелетій**, заступниці керівника проєкту «Ініціатива секторальної підтримки громадянського суспільства України» ICAP Єднання.

Форум «Штучний інтелект 2.0: регулювання та робота під час війни» стався завдяки всім спікерам і спікеркам, яким ми щиро вдячні за високий рівень експертності та дискусії:

- **Ользі Седовій**, керівниці національних програм Посольства Швеції в Україні;
- **Олесі Холопик**, директорці ЦЕДЕМ;
- **Віті Володовській**, голові Лабораторії цифрової безпеки;
- **Терезі Рібейрі**, представниці ОБСЄ з питань свободи медіа;
- **Кароліні Іванській**, радниці із цифрових прав ECNL;
- **Даніелю Лойферу**, головному раднику з політик

## ПОДЯКА СПІКЕРАМ ФОРУМУ ЗА НАДАНІ МАТЕРІАЛИ

AccessNow;

- **Гордію Румянцеву**, головному спеціалісту експертної групи із захищеності прав дітей в інтернеті Директорату європейської інтеграції Міністерства цифрової трансформації України;
- **Ліліан Едвардс**, професорці права, інновацій та суспільства університету Ньюкасл;
- **Віталію Гончаруку**, інвестору AIV Lab;
- **Тетяні Авдєєвій**, юристці Лабораторії цифрової безпеки;
- **Альоні Романюк**, засновниці проєкту «НотаЄнота», фактчекерці;
- **Ігорю Соловею**, керівнику Центру стратегічних комунікацій та інформаційної безпеки;
- **Денізі Вагнер**, радниці Офісу представника ОБСЄ з питань свободи медіа;
- **Віті Володовській**, голові Лабораторії цифрової безпеки;
- **Володимиру Бегею**, головному спеціалісту експертного комітету з питань розвитку сфери штучного інтелекту Міністерства цифрової трансформації України;
- **Андрію Лабуню**, начальнику відділу аналітики та організації захисту персональних даних Управління дотримання прав людини Національної поліції України;
- **Віталію Міняйлу**, CEO IT-компанії Neurotrack.tech і лабораторії прикладного машинного навчання EON+;
- **Миколі Печенізькому**, професору факультету математики та комп'ютерних наук Технічного університету Ейндховена, Нідерланди;
- **Юлії Хаас**, помічниці керівника проєкту Офісу представника ОБСЄ з питань свободи медіа;
- **Катерині Крук**, керівниці з публічної політики в Центральній і Східній Європі Meta;

## ПОДЯКА СПІКЕРАМ ФОРУМУ

- **Максиму Дворовому**, керівнику напрямку цифрових прав Лабораторії цифрової безпеки;
- **Шанталь Жоріс**, юристці ARTICLE 19;
- **Тарасу Шевченку**, заступнику міністра культури та інформаційної політики України з питань європейської інтеграції.

ЦЕДЕМ дякує модераторам і модераторці форуму:

- **Тетяні Авдєєвій**, юристці Лабораторії цифрової безпеки;
- **Максиму Дворовому**, керівнику напрямку цифрових прав Лабораторії цифрової безпеки;
- **Ігорю Розкладаю**, головному медійному юристу, заступнику директорки ЦЕДЕМ.

Упорядники цього довідника для ОГС:

- **Анна Ісічко**, заступниця директорки ЦЕДЕМ, і
- **Володимир Куделя**, менеджер проєктів ЦЕДЕМ.

## КОНТАКТИ КОМАНД ОРГАНІЗАЦІЙ, ЯКІ РЕАЛІЗУЮТЬ ПРОЄКТ «ІНІЦІАТИВА СЕКТОРАЛЬНОЇ ПІДТРИМКИ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА УКРАЇНИ»

### **Ініціативний центр сприяння активності та розвитку громадського почину «Єднання» (ICAP «Єднання»)**

Телефон: +38 044 201 01 60 (61)

E-mail: [office@ednannia.ua](mailto:office@ednannia.ua)

Вебсторінка: <http://ednannia.ua/>

### **Український незалежний центр політичних досліджень (УНЦПД)**

Телефон: +38 044 227 54 20, +38 063 234 74 40

E-mail: [ucipr@ucipr.org.ua](mailto:ucipr@ucipr.org.ua)

Вебсторінка: <http://www.ucipr.org.ua/>

### **Центр демократії та верховенства права (ЦЕДЕМ)**

Телефон: +380 67 828 20 74

E-mail: [info@cedem.org.ua](mailto:info@cedem.org.ua)

Вебсторінка: <https://cedem.org.ua/>

## ВІДЕОЗАПИСИ ТА ТРАНСЛЯЦІЇ

Запис експертної дискусії «Штучний інтелект і організації громадянського суспільства» українською:



Запис експертної дискусії «Штучний інтелект і організації громадянського суспільства» англійською:



Відеотрансляція першого дня Щорічного Форуму «Штучний інтелект 2.0: регулювання та робота під час війни»:





# ІНСТРУМЕНТИ ШТУЧНОГО ІНТЕЛЕКТУ. ГАЙД ДЛЯ ОГС

НА ОСНОВІ МАТЕРІАЛІВ ЕКСПЕРТНОЇ ДИСКУСІЇ  
«ШТУЧНИЙ ІНТЕЛЕКТ І ОРГАНІЗАЦІЇ ГРОМАДЯНСЬКО-  
ГО СУСПІЛЬСТВА» ЩОРІЧНОГО  
ФОРУМУ ШТУЧНИЙ ІНТЕЛЕКТ 2.0:  
РЕГУЛЮВАННЯ ТА РОБОТА ПІД ЧАС ВІЙНИ»

**КИЇВ  
2024**