Лабораторія Цифрової Безпеки

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

ПРЯМУЄМО РАЗОМ

Дії та Мрії: штучний інтелект у публічному секторі

Аналітичне дослідження

Лабораторія цифрової безпеки
2024

Дії та Мрії: штучний інтелект у публічному секторі - ГО “Лабораторія цифрової безпеки”, 2024.

Авторка дослідження: Тетяна Авдєєва

Розвиток технологій не оминув державну сферу, сприяючи автоматизації процесів, розробці інноваційних рішень та підвищенню якості надання публічних послуг. Як наслідок, з'являється все більше ініціатив щодо впровадження технологій штучного інтелекту (ШІ) у публічному секторі. Деякі з них спрямовані на фасилітацію процесів всередині державних органів, інші - на покращення послуг і процесів, створення зручного і доступного цифрового середовища. Ці новели впроваджуються на тлі активних регуляторних процесів в межах Європейського Союзу, Ради Європи та багатьох іноземних країн. Аналітичне дослідження окреслює ключові ініціативи регулювання ШІ на міжнародній арені, національному рівні в Україні та в інших державах, а також надає огляд проєктів ШІ, які вже застосовуються на практиці або плануються до використання найближчим часом, аналізуючи їх безпечність для прав людини і демократичних принципів. Наостанок, Лабораторія цифрової безпеки надає рекомендації для покращення регуляторного середовища та забезпечення етичного використання ШІ у публічному секторі.

Контакти:
https://dslua.org
dslua@dslua.org
Facebook: https://www.facebook.com/dslua
Twitter: @DSLab_Ukraine

Аналітичне дослідження підготовлено за підтримки Європейського союзу та Міжнародного Фонду «Відродження» в рамках спільної ініціативи «Європейське Відродження України». Аналітичне дослідження представляє позицію авторів і не обов'язково відображає позицію Європейського Союзу чи Міжнародного фонду «Відродження».

Міжнародний фонд «Відродження» – одна з найбільших благодійних фундацій в Україні, що з 1990-го року допомагає розвивати в Україні відкрите суспільство на основі демократичних цінностей. За час своєї діяльності Фонд підтримав близько 20 тисяч проектів на суму понад 350 мільйонів доларів США.

Сайт: www.irf.ua
Facebook: www.fb.com/irf.ukraine

Європейський Союз складається з 27 держав-членів та їхніх народів. Це унікальне політичне та економічне партнерство, засноване на цінностях поваги до людської гідності, свободи, рівності, верховенства права і прав людини. Понад п'ятдесят років знадобилось для створення зони миру, демократії, стабільності і процвітання на нашому континенті. Водночас нам вдалось зберегти культурне розмаїття, толерантність і свободу особистості. ЄС налаштований поділитись своїми цінностями та досягненнями з країнами-сусідами ЄС, їхніми народами, та з народами з-поза їхніх меж.

Зміст

Дії та Мрії: штучний інтелект у публічному секторі

Ймовірно, штучний інтелект призведе до кінця світу,
але водночас з'являться чудові компанії.

(c) Сем Алтман

Навесні 2023 року ChatGPT випадково створив фейкову біографію Олеся Гончара, приписавши тому роль військовополоненого у США, примусові роботи в Німеччині і навіть сплутавши його місце народження з Довженком. З'ясувалося це завдяки тому, що на річницю народження поета українське медіа вирішило нагадати читачам факти з життя Гончара - і добряче схибило! Така помилка вже не перша - раніше подібне ставалося з біографією Шевченка. І, напевно, ChatGPT перекрутив вже чимало біографій, адже його офіційно заборонили в низці країн. На додачу, Італія наголосила, що підозрює порушення правил захисту персональних даних з боку чатботу. Здавалося б, вигадані біографії не настільки вже й небезпечні, а якщо комусь не подобається можливість обробки чутливої інформації - завжди можна уникати таких додатків. Втім, подібні помилки слугують тривожним дзвіночком того, що ШІ схильний помилятися частіше, ніж ми уявляли. І якщо в додатках, створених з розважальною метою, помилка не важить надто багато, хиби під час надання публічних послуг, розслідування злочинів чи здійсненні медичних маніпуляцій можуть призвести до набагато тяжчих наслідків.

В Україні тема використання і регулювання ШІ стає популярнішою ледве не щохвилини. Ще у квітні 2023 Міністерство цифрової трансформації (Мінцифри) наголосило, що у нас працює близько 4200 розробників систем ШІ. Вочевидь, ця цифра лише зросла за останній рік. Наразі Ukrainian Tech Ecosystem Overview - державний проєкт моніторингу IT-компаній, розробників і технічних екосистем українського ринку - налічує 1659 компаній, що створюють продукти, та 550 сервісних компаній. Значна частина працює з автоматизованими системами або безпосередньо розробляє їх. Наприклад, нещодавно з'явилася система DeepGreen Ukraine — сервіс моніторингу лісових насаджень, що використовує відкриті супутникові знімки та дані Держлісагентства для виявлення незаконних вирубок. А наприкінці грудня 2023 навіть з'явилася інформація про використання ШІ в українському кінематографі, чого раніше ніколи не ставалося. Ба більше, за останній рік новинні шпальти повняться заголовками про повсюдне впровадження ШІ у державному секторі - починаючи зі створення освітніх курсів для розробників, і завершуючи автоматизацією процесів у більшості міністерств (і навіть дипломатичних місій та посольств).

Анонси нових державних ініціатив з'являються із заздрісною періодичністю - і діджиталізація, що йде повним ходом, не може не радувати. Водночас, відсутність жорстких стандартів як для державних проєктів, так і для приватних розробок є дещо лякаючою. Йдеться не тільки про український контекст - броунівський рух міжнародних організацій у спробах збалансувати інтереси індустрії з правами людини і суспільним благом змушує задуматися, чи варто взагалі очікувати адекватного регулювання найближчим часом?

I. Міжнародне регулювання: узгодити неузгоджуване?

На тлі дебатів щодо регуляторної рамки, провідні техкомпанії (як-от OpenAI, Google, Microsoft та Anthropic) об'єдналися для створення спільного дослідницького хабу. Техгіганти підкреслили, що досліджують можливості створення етичних та безпечних продуктів ШІ. Спершу ініціатива викликала занепокоєння - правозахисники вважали цей крок спробою довести спроможність розробляти стандарти на рівні саморегулювання і сигналом про "відсутність потреби у державних стандартах". Своєрідною відповіддю стали публічні заяви виконавчих директорів провідних компаній на британському AI Safety Summit 2023. Вони наголосили на необхідності розробити універсальні для всіх розробників міжнародні стандарти. Це, в свою чергу, спричинило хвилю невдоволення серед дрібних стартапів, для яких деякі пропоновані вимоги можуть стати надмірним фінансовим тягарем. Здавалося б, які підходи не пропонуй - хтось точно залишиться невдоволеним. Втім, чи насправді принципові рамки аж настільки відсутні? Насправді, ні.

Відповідно до статистики Організації економічного співробітництва та розвитку (OECD), у світі наразі існує близько 1600 регуляторних ініціатив щодо стандартів розробки і використання ШІ. Найбільше їх у США (81 ініціатива), Сполученому Королівстві (61), Австралія (43), Німеччина (37), Туреччина та Португалія (по 36). Статистика не враховує ініціативи, які наразі обговорюються на рівні ЄС в національне регулювання відповідних країн-членів. Втім, навіть без міжнародних актів, кількість пропозицій регулювання, стратегій, політик і фінансових програм наразі є вражаючою. І вимоги до систем ШІ, які пропонують затвердити на національному рівні в "материнських країнах" техгігантів, є принципово і ціннісно схожими (вимоги щодо прозорості, захисту даних, позначення контенту, генерованого ШІ тощо). Тож, що наразі відбувається у світі з регуляторними ініціативами?

Проєкт Акту про штучний інтелект та Біла книга (ЄС). Два основні документи, які є основоположними стовпами регулювання ШІ в ЄС, і які

зібрали довкола себе ледве не всіх критиків, які так чи інакше пов'язані з цифровими правами та регулюванням цифрового середовища. Першою звісно ж була **Біла книга** - стратегічний документ, що окреслює пріоритети розвитку ШІ та ключові принципи розробки та застосування систем. За своєю суттю Біла книга стала спробою поєднати три сфери: бізнес, добробут громадян і публічний інтерес (державні пріоритети). Незважаючи на те, що документ не був проєктом юридично обов'язкового акту, ЄС всіляко заохочував публічну участь в його напрацюванні - надання коментарів, участь в робочих групах представників різних зацікавлених сторін тощо. Як наслідок, Біла книга викликала скоріше схвальні відгуки, вважався позитивним і збалансованим кроком у регулюванні ШІ і гарною дорожною картою для подальших ініціатив. Про що ж була Біла книга?

- інвестування у розробку ШІ з аналізом ринкових потреб, готовності переходу до автоматизованих систем у певних галузях та в цілому визначення ШІ як пріоритетного напрямку для розвитку економіки;
- розвиток технічної індустрії, збільшення спроможностей (в тому числі освітніх) та навичок у сфері створення систем ШІ та їх інтеграції у суспільне життя - зокрема, для сприяння таким цілям пропонувалося створювати цифрові хаби у кожній державі-членкині ЄС (щонайменше один хаб у кожній країні);
- партнерство з приватним сектором (у форматі публічно-приватних партнерств) та загальне впровадження технологій ШІ у публічному секторі, розробка інфраструктури, яка сприяє розвитку ШІ - як-от доступ до даних, міжнародна співпраця, зрозумілі національні регулювання;
- створення зрозумілої регуляторної системи (зокрема, пересвідчитись, що дотримуються основоположних принципів, таких як нагляд, безпечність, захист даних, прозорість, недискримінація, суспільний і довкільний добробут, відповідальність);
- загальний меппінг ризиків (для прав людини, безпекових ризиків, браку механізму відповідальності тощо) та рамкування ШІ в межах існуючих в ЄС актів на період, доки спеціального регулювання не буде розроблено і прийнято;
- “спойлери” щодо майбутнього регулювання - розставлення віх і постановка проблем, які мають вирішитися Актом про штучний інтелект, надання переліку принципів щодо безпечної розробки і використання ШІ, окреслення питання захисту та передачі даних при розробці систем з огляду на існування Загального регламенту про захист даних (GDPR), і що важливо - закладення ідеї маркування контенту, генерованого ШІ, для забезпечення прозорості і якості високоризикових систем.

Проєкт Акту про штучний інтелект не настільки успішний з точки зору швидкого прийняття, але явно популярніший документ. І перша причина - звісно ж його обов'язковий характер. Щойно Акт буде проголосовано - багатьом компаніям доведеться значною мірою переглянути власні політики, а деяким - ймовірно навіть залишити ринок ЄС. Звісно ж така ситуація суттєво впливає на економіку держав-членів, що є частковою причиною для гальмування процесу прийняття Акту. Іншою причиною були і фундаментальні розбіжності між ключовими стейкхолдерами - чого лише варта дискусія щодо регулювання генеративного ШІ та так званих моделей-основ (від англ. "*foundation models*"). Зокрема, ключовим питанням тривалий час залишалася дилема: що варто регулювати - технологію чи її застосування? Іншим викликом була розробка прийнятної для всіх системи оцінки ризиків для прав людини.

Втім, наприкінці 2023 року з'явилися новини про політичну угоду, якої вдалося досягнути в рамках перемовин між Європейським парламентом та Європейською радою. Набрання чинності змінами, втім, все ще потребує формального затвердження. Застосовним Акт про штучний інтелект стане через 2 роки після такого голосування (а деякі обмеження - вже через 6 місяців). Оновленого текст після політичної угоди має досить багато косметичних правок, в той час як загальні принципові підходи було окреслено у прес-релізах Європейської комісії та Європейської ради. Наприклад, системи ШІ загальної мети (від англ. "general purpose") - тобто технічні рішення, що можуть використовуватися в десятках різних систем і є базовими для будь-якого продукту - все ж таки планується регулювати в рамках Акту про штучний інтелект.

Питання прийняття Акту найближчим часом як ніколи актуальне, адже незабаром на ЄС очікує зміна керівництва і перевибори до Європарламенту. Спрогнозувати майбутню позицію новосформованого органу і новопризначеної Єврокомісії відверто складно, тому надія залишається на прийняття Акту до "переломного моменту" перерозподілу політичних сил всередині ЄС. Що пропонує Акт про штучний інтелект і якого політичного компромісу вдалося досягнути?

- Перш за все, нашуміла модель класифікації систем ШІ залежно від рівня ризику. Акт пропонує поділити системи на чотири групи: заборонені, високоризикові, системи з обмеженим рівнем ризику та низькоризикові системи. Найбільше вимог майбутній Акт містить саме до високоризикових систем (інформування користувачів, людський нагляд, реєстрація діяльності, висока якість наборів даних, детальна документація для органів влади, що здійснюють державний моніторинг, розробка адекватних систем оцінки, високий рівень

надійності, безпеки та точності). Водночас, не менш важливим є список заборонених систем, до яких належать, наприклад, технології соціального ранкування (за китайською моделлю), технології, що використовуються для переслідувань чи маніпуляцій людьми. У цьому випадку важко оцінити, до якої категорії належить та чи інша система, адже багато технологій цілком можуть мати подвійне використання (те ж саме розпізнавання облич є чудовим прикладом). Перелік заборонених систем став ще більш розширеним після політичної угоди (він доповнився забороною на розпізнавання емоцій і скрепінг (від англ. "scraping") даних);

- Введення обов'язкової сертифікації для певних систем ШІ (високоризикових). Зокрема, систем біометричної ідентифікації, систем, створених для підтримання роботи критичної інфраструктури, систем, які застосовуються державою для надання публічних послуг (що особливо актуально в контексті цієї аналітики), освітніх або професійних оцінювальних систем тощо;
- Вимоги щодо необхідності інформування користувачів про взаємодію з системою ШІ, а не реальною людиною, а також можливість відмовитися від такої взаємодії у випадках застосування таких систем, як біометрична ідентифікація (крім випадків використання органами правопорядку для розслідування злочинів);
- Встановлення правил прозорості для систем, призначених для взаємодії з людьми, систем розпізнавання емоцій, а також систем, які використовуються для створення або оброблення зображень, аудіо- або відеоконтенту;
- Створення єдиного європейського ринку ШІ, який передбачає застосування класичних правил ЄС щодо вільного руху товарів і технологій і, водночас, застосовність єдиних і уніфікованих правил для роботи з технологіями ШІ на території ЄС;
- Формування наглядового органу на рівні ЄС - Європейської ради зі штучного інтелекту (EAIB) та паралельне створення національних регуляторів (чи уповноваження вже існуючих займатися наглядом за ринком ШІ). На додачу, є вимога повідомлення наглядових органів про інциденти у високоризикових системах (як-от несправності, випадки дискримінації, витоки даних тощо), а загальний список таких систем планується вести у формі Бази даних ЄС. Втім, в рамках політичної угоди досягнуто згоди щодо створення нового Офісу зі штучного інтелекту, що буде розробляти більш деталізовані стандарти у цій сфері, що зробить регулювання більш централізованим і дещо посуне його з національних рівнів на рівень ЄС в принципових питаннях. Враховуючи, що текст після політичної угоди досі відсутній,

актуальним залишається обсяг повноважень, які все ж залишаться в національних регуляторів

- Впровадження системи штрафів. До політичної угоди система штрафів передбачала ранжування штрафів до 30 мільйонів євро або 6% світового річного обороту компанії (у разі заборонених практик як-от біометричне стеження в режимі реального часу чи порушень у сфері захисту даних), до 20 мільйонів євро або 4% світового річного обороту компанії (за інші порушення), до 10 мільйонів євро або 2% світового річного обороту (за повідомлення неправильної, неповної чи неправдивої інформації регуляторам). Після політичної угоди шкала штрафів варіюється в межах 35-7,5 мільйонів євро та 7-1,5% світового річного обороту компанії. Такі зміни є досить тривожним дзвіночком для індустрії, адже вони свідчать про збільшення штрафів в тому числі і за процедурні порушення (як-от повідомлення регуляторів).
- Створення регуляторної пісочниці (ініціатива, про яку ми поговоримо в деталях трошки згодом).

Проєкт Директиви про відповідальність у сфері ШІ (ЄС). На відміну від Акту про штучний інтелект, Директива не є документом прямої дії - тобто держави мають вживати додаткових заходів для її імплементації та розробляти відповідні механізми на національному рівні. Передумовою розробки цього документу став Звіт щодо безпеки і відповідальності у сфері ШІ, робототехніки та інтернету речей, в якому було окреслено досить багато викликів, пов'язаних з автоматизованим прийняттям рішень. Документ є комплементарним до загальних правил щодо цивільної відповідальності та, власне, Акту про штучний інтелект. Останній, на відміну від досить поширеної серед неекспертної аудиторії думки, жодним чином не вказує на те, хто має нести відповідальність за помилки систем ШІ в індивідуальних випадках - починаючи від самокерованих машин і завершуючи умовним ChatGPT. Саме тому на рівні ЄС з'явилася пропозиція напрацювати окремі правила гри:

- Доступ до інформації щодо потенційного порушення, що може слугувати важливою передумовою для подальшого притягнення до відповідальності - зокрема, можливості вимагати відшкодування шкоди;
- Ідентифікація відповідальної за порушення особи, що передбачає визначення етапу, на якому сталася помилка у функціонуванні системи ШІ - наприклад, проти кого саме варто розпочинати цивільне провадження щодо відшкодування: розробника, тестувальника, користувача тощо;

- Право вимагати розкриття необхідних доказів на підставі ухвали суду у випадках, коли неможливо інакше оцінити, чи була помилка у відповідній системі ШІ;
- Реформування системи тягаря доведення. Зокрема, позивач, права якого порушено системою ШІ, може обґрунтовувати свої вимоги тим, що компанія не дотрималася правил щодо належної обачності при розробці і застосуванні систем, що призвело до настання шкоди. При цьому пропонується ввести презумпцію наявності такого причинно-наслідкового зв'язку між необачністю і шкодою.

Міжнародні керівні принципи для організацій, що розробляють складні системи ШІ та Кодекс поведінки для організацій, що розробляють складні системи ШІ (ЄС). Принципи та Кодекс поведінки напрацьовані в межах так званого процесу Хірошіма. Обидва документи є досить коротким викладом основних принципів та підходів для регулювання сфери ШІ. Водночас, їх ціллю є не стільки розробка стандартів, скільки об'єднання індустрії і створення майданчику для діалогу. Як слідує зі змісту документів, їх планують зробити "живими інструментами" - тобто регулярно оновлювати і доповнювати релевантною інформацією (наприклад, з розвитком генеративного ШІ точно варто буде розробити окремі положення і візію щодо його розробки, тестування і застосування). Короткий зміст документів:

- **Керівні принципи**: здійснення оцінки ризиків протягом усього "життєвого циклу" систем, відслідковувати можливі способи зловмисного використання систем та розробляти системи зменшення ризиків, дотримуватися принципу прозорості (в тому числі і щодо вразливостей систем), поширювати інформацію щодо інцидентів, пов'язаних з системами (наприклад, витоки даних), розробити кризові і безпекові політки, безпекові механізми (в тому числі фізичної безпеки, як-от питання зберігання інформації на серверах у країнах, де не відсутній високий індекс порушень прав людини), розробити систему позначення контенту, генерованого ШІ, пріоритезувати ефективні засоби зменшення ризиком (по суті, обрати проактивний, а не реактивний підхід), а також пріоритезувати розробку систем, які несуть публічне благо (освітні, медичні, кліматичні зміни) з дотриманням міжнародних технічних стандартів та вимог щодо захисту даних і права інтелектуальної власності;
- **Кодекс поведінки**: адресує керівні принципи з деталізацією того, як вони мають бути імплементовані на практиці. Зокрема, у документі зазначається, наприклад, які можуть бути ризики у систем (на кшталт їх використання у сфері виготовлення хімічної, біологічної чи ядерної зброї - з кожним роком цей ризик видається все більш реалістичним),

зміст публічних звітів для дотримання прозорості (щодо можливостей систем, детального аналізу потенційної шкоди персональним даним чи дискримінації тощо). Тобто документ є радше “планом дій” для розробників систем ШІ, що розповідає, як саме варто імплементувати стандарти і вимоги, передбачені Керівними принципами.

Проєкт Рамкової конвенції про штучний інтелект, права людини, демократію та верховенство права (Рада Європи). В рамках спеціального Комітету Ради Європи зі штучного інтелекту останні п'ять років на працьовується документ, спрямований на кодифікацію основних принципів і стандартів у сфері регулювання ШІ. На відміну від Акта про штучний інтелект, Конвенція є більш загальною і скоріше виступає спробою об'єднати універсальними зобов'язаннями як можна більше держав (крім країн Ради Європи активну участь у розробці беруть США, Канада, Австралія та багато інших). Зокрема, основні її положення (у редакції від грудня 2023) передбачають:

- Введення поняття ШІ, яке робить фокус на можливість автоматизованих систем допомагати людині приймати рішення чи робити це за неї, базуючись на статистичних та математичних методах;
- Повага до прав людини, демократичних процесів та верховенства права як фокус Конвенції та будь-якого регуляторного документу, розробленого на її основі на національному рівні;
- Принципи розробки і застосування ШІ: прозорість і нагляд, відповідальність, рівність і недискримінація, повага до приватності і захист даних, надійність і безпека, безпечні інновації, а також забезпечення інклюзії у стандартах (щодо осіб з інвалідністю та дітей) і тлумачення Конвенції у ширшому контексті - тобто у світлі інших інструментів захисту прав людини;
- Розробка механізму здійснення впливу на права людини, демократію та верховенство права та застосовність такого механізму протягом усього життєвого циклу систем;
- Забезпечення засобами правового захисту (хоч Конвенції і бракує деталей щодо того, які засоби мають бути надані і що станеться у випадку їх відсутності), процедурними гарантіями, здійснення оцінки ризиків і тлумачення методології для такої оцінки (аби ті, хто її застосовує для перевірки створених систем ШІ, розуміли принципи та підходи зменшення ризиків).

Водночас, на початку 2024 року довкола Проєкту Конвенції точаться запеклі дебати - зокрема, в частині сфери дії її майбутніх положень. Так, наразі серед

експертів, залучених до розробки Конвенції поширюється інформація про незастосовність пропонованих правил до приватного сектору і до розробок в оборонній сфері (а точніше, питань національної безпеки). Як наслідок, дія документу потенційно звужується лише до технологій, застосовуваних державою у цивільній сфері, що передбачає надзвичайно багато ризиків для користувачів. У відповідь на це представники громадянського суспільства підготували відкритий лист до країн-учасниць процесу обговорення із закликом не звужувати сфери дії Конвенції.

Керівництва до Конвенції 108+ щодо ШІ (Рада Європи). Цей досить короткий документ доповнює (а точніше модернізує інтерпретацію) Конвенцію 108+ та дозволяє застосовувати її у сучасних реаліях. Порівняно з іншими регуляторними актами та проєктами, ці Керівництва є досить загальними (як і вся Конвенція 108+), втім важливими з огляду рамкування систем ШІ у питаннях захисту персональних даних. Про що цей документ?

- Загальні рекомендації. Наприклад, проведення оцінки ризиків та застосування загальних принципів, передбачених Конвенцією 108+ до сфери ШІ;
- Рекомендації для розробників, виробників та провайдерів сервісів. Так, цим акторам пропонується розробити систему, що ґрунтується на ціннісному підході. Це передбачає орієнтованість на захист прав людини та дотримання належної обачності при розробці і застосуванні систем ШІ, вимогу здійснювати оцінку ризиків. Крім того, представникам індустрії рекомендують створювати експертні та дорадчі органи, які дозволятимуть отримувати зворотній зв'язок щодо відповідності продуктів стандартам у сфері прав людини. Крім того, основний акцент робиться на розробці гарантій та механізмів відповідальності за порушення;
- Рекомендації для законодавців та регуляторів. Зокрема, їм радять звернути увагу на розробку системи відповідальності, сертифікаційні механізми та кодекси поведінки, де актуально, поширити на сферу ШІ вимоги у сфері публічних закупівель, залишати систему прийняття рішень залежною від людини, а не автоматизованих систем, підвищувати рівень експертизи національних регуляторів та вкладати ресурси у розвиток цифрової грамотності.

Європейська етична хартія про використання ШІ в судочинстві та його середовищі (Рада Європи). Хартія є документом м'якого права, який за своєю суттю кодифікує п'ять основних принципів застосування ШІ у сфері правосуддя, а також наголошує на типових прикладах використання систем та (не)безпеці, породженій таким застосуванням. Про які принципи йдеться?

- Принцип поваги основних прав: забезпечення сумісності розробки та впровадження інструментів і сервісів ШІ з фундаментальними правами у сфері правосуддя;
- Принцип недискримінації: спеціальне запобігання розвитку чи посиленню будь-якої дискримінації між окремими особами чи групами осіб;
- Принцип якості та безпеки: щодо обробки судових рішень і даних, використовуючи сертифіковані джерела та нематеріальні дані з моделями, розробленими на міждисциплінарній основі, у безпечному технологічному середовищі;
- Принцип прозорості, неупередженості та справедливості: зробити методи обробки даних доступними та зрозумілими, дозволити зовнішній аудит;
- Принцип контролю систем користувачем: гарантує, що користувачі є поінформованими учасниками та контролюють свій вибір;
- Також пропонується чотири категорії: використання ШІ у сфері правосуддя, що заохочується з боку авторів Хартії, використання, що потребує застережень і таке, що потребує додаткових наукових досліджень, а також використання, що має ґрунтуватись на найбільш жорстких обмеженнях.

Керівні принципи щодо відповідального використання ШІ в журналістиці (Рада Європи). Після тривалих перемовин, в яких брала участь і Національна рада з питань телебачення і радіомовлення, Керівний комітет з медіа та інформаційного суспільства Ради Європи погодив фінальний текст рекомендаційного документу щодо застосування ШІ в роботі медіа. В цілому, Керівні принципи окреслюють рамку і надають медіа алгоритм для прийняття рішення: чи справді редакції потрібно використовувати системи ШІ в роботі? Серед ключових питань, на які варто надати відповідь перед використанням таких систем слід виокремити:

- рішення застосовувати ШІ має відповідати місії медіа, бути редакційним рішенням, яке супроводжується регулярною оцінкою ризиків та передбачає баланс інтересів усіх, на кого таке рішення впливає;
- розрізнення систем, розроблених медіа самостійно, та систем, які медіа використовує як частину загальнодоступних технологій (зокрема, чат-боти на кшталт ChatGPT, Bard та інших). Так, медіа мають забезпечувати якість даних в системах ШІ, отримувати дані законним шляхом та дотримуватися інших вимог, передбачених законодавством щодо персональних даних, здійснювати редакційний нагляд за якістю функціонування таких систем (який має бути практичною, а не формалізованою процедурою);

- важливим є наголос на тому, що традиційні журналістські стандарти - як-от, повноти, правдивості і об'єктивності, поваги до приватного життя і неупередженості, та інші етичні вимоги є застосовними і до систем ШІ, які вирішило використовувати медіа;
- використання систем ШІ, особливо з метою генерування контенту, має обов'язково супроводжуватися маркуванням такої штучно створеної інформації у формат і спосіб, зрозумілий для аудиторії.

Документ також встановлює обов'язки для платформ та Інтернет-посередників, які надають простір для поширення медійних матеріалів. Крім того, окремі зобов'язання (зокрема, щодо розробки законодавчих норм і рекомендацій) покладаються і на держави.

Декларація щодо маніпулятивних здатностей алгоритмічних процесів та Рекомендація щодо впливу алгоритмічних систем на права людини (Рада Європи). Декларація - це короткий документ, прийнятий у 2019 році, який виокремлює ряд проблем, пов'язаних із застосуванням алгоритмічних систем. Основним її фокусом є підвищення обізнаності щодо ризиків, зокрема і у сфері публічного адміністрування. Наприклад, серед проблем згадуються вплив алгоритмічних систем на комунікацію між органами влади та громадянами, проблема захисту даних в контексті розробки таких систем, вплив на автономію і самовизначення особи, а також здатність технологій впливати на свободу прийняття рішень у економічній, соціальній та інших сферах. Деталізованих пропозицій Декларація не містить, послуговуючись загальною рекомендацією вживати пропорційних заходів і моніторити ризики, що повсякчас виникають.

Рекомендація спрямована, перш за все, на держави і їх регуляторні органи, які мають вживати ефективних законодавчих та практичних заходів для захисту прав людини від негативного впливу алгоритмічних систем. По суті, документ є продовженням Декларації та своєрідною пропозицією алгоритму вирішення окреслених у ній проблем та викликів. Рекомендація є досить загальною і, будучи прийнятою у 2020 році, не покриває частини актуальних викликів, які сягнули порядку денного відносно нещодавно. Втім, документ викладає основні принципи застосовні до сфери ШІ та обов'язки добросовісної реакції на виклики у цій галузі:

- Залучення до обговорення регуляторних ініціатив усіх зацікавлених сторін (зокрема, держава має запрошувати індустрію, громадянське суспільство, представників академічної спільноти тощо);
- Сприяння нарощуванню експертного потенціалу у публічних та приватних установах, які використовують алгоритмічні системи;

- враховувати вплив алгоритмічних систем на медіа, навколишнє середовище та інші вразливі сфери;
- Виклад основних принципів, серед яких згадуються демократична участь, обізнаність, інституційні рамки, безпечне управління даними та тестування систем, а також прозорість, підзвітність і гарантування засобів правового захисту. Крім того, серед заходів безпеки виокремлено обов'язок постійного нагляду за такими системами.

Рекомендації Ради зі штучного інтелекту (OECD). Рекомендації є одним з перших документів, які комплексно адресують тему розробки систем ШІ у відповідності із етичними вимогами та стандартами у сфері прав людини, хоча і орієнтовані радше на реформатування екосистеми у суспільстві. В цілому документ є досить коротким та структурованим, і ґрунтується на дослідженні OECD щодо впливу ШІ на суспільство. Рекомендації поділені на дві частини - загальні принципи (які орієнтовані більшою мірою на розробників систем ШІ) та рекомендації для тих, хто приймає законодавчі рішення та впливає на формування політик:

- П'ять згаданих принципів включають: сталий розвиток і добробут, справедливість та людиноцентричність (зокрема, верховенства права і повага до прав людини), прозорість і обґрунтованість рішень (зрозумілість для користувача), надійність і безпека, а також відповідальність;
- П'ять рекомендацій щодо політик і регулювання: інвестування у дослідження і розробки ШІ, створення цифрової екосистеми, створення сприятливого правового середовища для розвитку ШІ, підготовка до трансформації ринку праці і створення людського капіталу, здатного взаємодіяти з ШІ, міжнародна співпраця у напрямку створення надійного ШІ.

Нещодавно OECD оновила визначення ШІ для його гармонізації з положеннями майбутнього Акту про штучний інтелект. Основною зміною була адаптація поняття до генеративного ШІ (раніше дефініція вимагала певний рівень людської залученості або внеску у процес прийняття рішень системою). Наразі OECD комунікує з відповідальними органами ЄС щодо внесення змін і правок у Акт про штучний інтелект для забезпечення життєздатності нового регулювання і відповідності стандартам у сфері захисту прав людини.

Рекомендації щодо етики штучного інтелекту (ЮНЕСКО). Орієнтовані переважно на державний сектор принципи і цінності, які країнам слід імплементувати в національну практику при розробці підходів до

регулювання. Також містить рекомендації для приватного сектору та для громадянського суспільства (останні, зокрема, згадуються як невід'ємний елемент процесу розробки політик та їх практичного застосування до технологій ШІ, особливо тих, що виконують функції у суспільному інтересі). Варто підкреслити, що документ є досить людиноцентричним і сфокусованим на захисті прав людини і демократичних цінностей. Зокрема, ключовими акцентами є:

- Дотримання принципів пропорційності, відсутності шкоди (від англ. "*do no harm principle*"), справедливості і відсутності дискримінації, сталого розвитку, безпеки і захищеності, захисту даних та наявності людського нагляду за ШІ, прозорості та обґрунтованості рішень, відповідальності, а також цифрової грамотності і залучення максимальної кількості зацікавлених сторін;
- Забезпечення проведення етичної оцінки впливу систем ШІ та врахування результатів при прийнятті управлінських рішень, розробка безпечної цифрової екосистеми, створення законодавчих рамок і політик у питаннях захисту даних (враховуючи системи ШІ та їх вплив на приватність), розробка методології для оцінки ефективності політик щодо ШІ;
- Забезпечення міжнародної співпраці з питань регулювання ШІ і напрацювання етичних стандартів розробки і застосування таких систем;
- Моніторинг, оцінка та зменшення негативного впливу у тематичних питаннях (гендер, довкілля, культура, освіта і дослідження, комунікація та інформаційне середовище, економіка і праця, здоров'я та добробут).

Позиція щодо регулювання штучного інтелекту у сфері охорони здоров'я (ВООЗ). Досить багато організацій, що мають вужчий профіль та спеціалізацію, також почали робити внесок у напрацювання стандартів у сфері ШІ. Переважно розроблені ними документи носять аналітичний характер з невеликими порціями рекомендацій для ключових зацікавлених сторін (розробників, законотворців і тих, хто застосовує ШІ). Так, ВООЗ напрацювала рекомендації щодо регулювання ШІ у сфері охорони здоров'я, які вона оприлюднила у жовтні 2023 року. Документ підтримує загальний тренд щодо напрацювання як етичних, так і законодавчих рамок, фокусуючись у деталях на шести ключових питаннях:

- Зміцнення довіри: так, важливо забезпечувати прозорість і документування всього життєвого циклу продукту та відстежувати процеси розробки;

- Управління ризиками, зокрема, використання технологій за призначенням, людське втручання, безперервне навчання (у значенні оновлення відповідно до суспільних реалій та потреб), моделі навчання та загрози кібербезпеці, повинні розглядатися комплексно і з ціллю максимально спростити моделі;
- Зовнішня перевірка даних і чітке уявлення про передбачуване використання ШІ допомагає забезпечити безпеку та полегшити регулювання;
- Забезпечення якості даних: шляхом ретельної оцінки попередніх версій систем (висновки з позитивних та негативних досвідів, оцінка причин хиби тощо), є життєво важливим, щоб системи не посилювали упередженості та помилки;
- Виклики, пов'язані з важливими складними нормативними актами, такими як GDPR у Європі та Закон про перенесення і підзвітність медичного страхування (HIPAA) у США, слід оцінювати з розумінням юрисдикції і вимог щодо згоди в питаннях конфіденційності та захисту даних.
- Сприяння співпраці між регуляторними органами, пацієнтами, медичними працівниками, представниками промисловості та урядовими партнерами може допомогти забезпечити відповідність систем ШІ відповідним стандартам протягом усього життєвого циклу.

Декларація Блетчлі (AI Safety Summit). Документ був розроблений та підписаний державами-учасницями AI Safety Summit і орієнтується переважно на забезпечення сталого розвитку, економічного зростання та інновацій. 29 держав (серед яких і Україна) погодилися, що наразі світ стикається з багатьма викликами, ризиками і можливостями, особливо з боку генеративного ШІ. Водночас, дехто критикував зміст документу за уникнення згадок про відкриті системи ШІ, відсутність фокусу на розробці жорсткого регулювання і надто загальному підході. Про що взагалі говорить Декларація?

- Міжнародний підхід: Декларація містить чітке визнання того, що суть систем ШІ означає, що їх ризики *"найкраще вирішуються через міжнародну співпрацю"* – визнаючи транскордонний характер технології та мало переваг для країн, які застосовують повністю незалежний підхід;
- Основні напрямки: хоча Декларація є досить загальною, вона виділяє конкретні проблеми щодо передових програм, що впливають на кібербезпеку, біотехнології та дезінформацію, відображаючи ширші занепокоєння щодо того, як ШІ може використовуватися "поганими

акторами", щоб завдати шкоди громадянам або підірвати демократичні процеси;

- Простір для розбіжностей: у рамках міжнародного співробітництва сьогодні не варто дивуватися відкритому визнанню того, що "*підходи можуть відрізнятися залежно від національних обставин і застосовної правової бази*" - безсумнівно це відображає нервозність багатьох країн, адже вони надто покладаються на регуляторні тренди ЄС через майбутній Акт про штучний інтелект;
- Залежність від розробників ШІ: фокусом Декларації є заклик до співпраці, прозорості та підзвітності з боку приватних компаній;
- Загальні стандарти: висловлено намір розробити загальноприйняті принципи прозорості, стандартів і тестування, а також використання можливостей державного сектору для управління та моніторингу систем ШІ.

Паризька хартія ШІ (RSF & Others). Міжнародна неурядова організація Репортери без кордонів у партнерстві з представниками громадянського суспільства, журналістами, медіа та експертами у сфері ШІ підготувала перелік принципів використання технологій ШІ у медіа та журналістиці. Хартія містить десять ключових рекомендацій, серед яких Репортери без кордонів вважають ключовими чотири:

- Медіа мають керуватися етичними принципами при виборі технологій, в тому числі застосуванні чи розробці систем ШІ;
- Людські рішення мають залишатися центральними в редакційних рішеннях;
- Медіа повинні сприяти тому, щоб суспільство чітко розрізняло оригінальний і штучно згенерований контент;
- Медіа мають брати участь у процесах глобального регулювання ШІ та захищати життєздатність журналістики під час переговорів із технологічними компаніями.

Також важливими є питання відповідальності, яка покладається на медіа незалежно від того, хто створив певний матеріал - системи чи реальна людина. Іншим досить фундаментальним принципом є забезпечення плюралізму думок при використанні систем пріоритезації контенту (зокрема, йдеться про пошукові системи, вбудовані у вебсайти медіа).

II. Іноземне регулювання: врегулювати не можна розвивати

Дещо іншою є ситуація з національними ініціативами. По-перше, більшість із них намагаються оцінити ризики і можливості для ринку своїх розробників, а тому переважно послуговуються м'якими правилами та сприянням етичним стандартам. По-друге, національні ринки дуже сильно відрізняються, тож потреби і запити на регулювання не є уніфікованими між собою в межах національних підходів. То якою є позиція флагманів у регулюванні ШІ - держав, які є материнськими для більшості передових представників індустрії?

Біла книга і Керівництва з безпечної розробки систем ШІ (Сполучене Королівство). Офіс комісара з інформації (ОКІ) у 2020 році напрацював рекомендації стосовно використання ШІ, опублікувавши проєкт керівництва щодо системи аудиту ШІ, який окреслює ризики, пов'язані з впливом ШІ на права і свободи й пропонує стратегії їх уникнення або пом'якшення. Пізніше ОКІ видав Керівництво, що пояснює рішення, ухвалені за допомогою ШІ, а також Керівництва щодо ШІ та захисту даних. На додачу, уряд опублікував і Стандарти алгоритмічної прозорості - тут назва документу говорить сама за себе. Втім, ці ініціативи є загальними і орієнтованими скоріше на те, щоб адаптувати чинні стандарти до сфери ШІ. Першими фундаментальними документами ж стали Біла книга та Керівництва щодо безпечної розробки ШІ - документи м'якого права, які визначили основні віхи щодо майбутнього регулювання і розвитку індустрії.

Гнучкий і адаптивний підхід, який вирішили обрати у Британії свідчить про усвідомлення державою ризиків, які походять від ШІ, та одночасне визнанням браку інформації для розробки комплексного регулювання. З огляду на те, які палкі дискусії наразі точаться довкола генеративного ШІ в рамках процесу розробки Акту про штучний інтелект, цілком можливо, що "вичікувальний" підхід дозволить розробити регуляторну рамку, яка стане найсприятливішою для безпечного розвитку технологій. Водночас, дослідницькі організації, як-от Ada Lovelace Institute, підкреслюють, що брак регулювання скоріше шкодить в середньостроковій перспективі, адже це робить регуляторний простір досить непередбачуваним для індустрії, створюючи ризики для прав людини. Втім, що ж таке **Біла книга**?

- П'ять принципів роботи ШІ: безпека та захищеність, прозорість і зрозумілість, справедливість, підзвітність та належне управління, можливість відшкодування, уникнення використання ШІ (заперечення проти автоматизації процесів);

- Уповноваження вже існуючих органів і розширення сфери дії чинних актів так, щоб вони охоплювали сферу ШІ; підтримка вже існуючих ініціатив, переважно у формі фінансових програм від уряду, але без жорсткого регламентування сфер і видів пропонованих проєктів - тобто відкриті тендери без формування чіткого державного запиту;
- Пріоритет розвитку індустрії й імплементації принципів добровільно у практику розробки і застосування ШІ, контекстуальне застосування згаданих стандартів та адаптація до обставин ринку;
- Пріоритетні напрямки діяльності: моніторинг і оцінка ефективності правової бази та впровадження принципів, орієнтуючись на підтримку інновацій; оцінка та моніторинг ризиків, пов'язаних із ШІ, в економіці; проведення меппінгу горизонту та аналіз прогалин і викликів; підтримка тестових ініціатив, щоб допомогти розробника вивести нові технології на ринок; забезпечення якісної освіти; сприяння сумісності з міжнародними нормативними рамками;
- Пріоритет участі в міжнародних програмах розвитку ШІ, форумах для обговорення викликів і пріоритетів у сфері інновацій, участь в напрацюванні міжнародних стандартів та узгодження британської моделі регулювання з міжнародною для відкриття ринку для іноземних розробників.

Керівництва з безпечної розробки ШІ є трохи більш технічним документом. Він встановлює стандарти для безпечного дизайну, розробки, застосування, та підтримки роботи системи. Документ орієнтований саме на розробників ШІ. За своєю суттю документ є скоріше поясненням того, як загальні стандарти (прозорості, зрозумілості, технічної захищеності фізичної інфраструктури тощо). Документ є дуже прикладним керівництвом щодо того, як побудувати "ланцюг постачання" на всіх етапах життєвого циклу системи ШІ (зокрема, в контексті доступу і обробки даних, їх походження і якості тощо). Важливим елементом також є менеджмент ризиків та інцидентів протягом стадії впровадження та підтримки роботи системи.

Проєкт Білля про права ШІ та Указ Байдена щодо штучного інтелекту (США). Перш за все, оцінюючи правовий ландшафт США в контексті регулювання інновацій, слід зауважити, що він суттєво різниться від штату до штату, тож спеціалізовані регуляції переважно не мають федеральної дії. Electronic Privacy Information Center, зокрема, підсумував, що станом на початок серпня 2023 року на рівні штатів існувало близько 50 регуляторних ініціатив (серед яких 30 документів були зареєстровані як законопроєкти у 2023 році). Частина з них є секторальними: регулюють ШІ і працевлаштування, захист персональних даних, використання ШІ у публічній сфері тощо. Водночас, є досить багато пропозицій, що стосуються регулювання генеративного

ШІ, запобігання загальній шкоді від ШІ та інших концептуальних питань. Втім, усі місцеві регуляції так чи інакше муситимуть відповідати федеральному законодавству. І тут є дві основні ініціативи, які пропонують врегулювати ШІ:

- **Проєкт Білля про права ШІ**. Документ пропонує закласти фундамент для регулювання ШІ у США, виокремивши п'ять основних принципів, яких слід дотримуватися представникам індустрії: безпечність і надійність систем, захист від дискримінації алгоритмами, захист приватності, повідомлення і пояснення (щодо взаємодії з ШІ та його характеру), альтернативне отримання послуг від людини та право на відмову. При цьому Проєкт наголошує на необхідності в подальшому прийняти цілу низку законів, спрямованих на імплементацію таких принципів на практиці у різних сферах.
- **Указ Байдена щодо ШІ**. Величезний документ містить ідеї регулювання багатьох сфер, маючи секторальний підхід до розробки нормативних рамок. Так, він охоплює нові стандарти надійності і безпеки (вимога до розробників критичних систем поширювати результати безпекових перевірок уряду США, захист від кібершахрайства за допомогою ШІ тощо), захист приватності (пріоритезація і державна підтримка технік створення ШІ, які є безпечними для приватності, розробка рекомендацій для оцінки державними органами ефективності політик і практик захисту даних), протидія дискримінації (зважати на дискримінацію алгоритмами і усувати її, забезпечити справедливість у системі правосуддя), захист прав споживачів, пацієнтів, студентів (забезпечити відповідальне використання ШІ та розвивати освітню сферу), захист трудових прав (здійснити моніторинг впливу ШІ на ринок праці), забезпечення конкуренції на ринку інновацій (відкритість і чесність процесів, сприяння дослідженням в різних частинах держави на місцевому рівні), відповідальне та ефективне використання ШІ урядом (наймати експертів у сфері ШІ, навчати персонал, робити меппінг потреб різних державних структур). В цілому документ є дуже детальним керівництвом щодо того, які новели варто очікувати у американському регулюванні.

Важливою ініціативою також є проєкт Акту про розкриття інформації про ШІ, який пропонує маркувати увесь контент, створений за допомогою генеративного ШІ і, по суті, закликає до виконання вимоги прозорості щодо технічного компонування системи для розуміння принципів її функціонування користувачами. Цікаво, що це вже далеко не перша пропозиція такого характеру - раніше схожі ідеї вже презентували у Сенаті.

Заходи щодо управління сервісами генеративного ШІ, **Положення про адміністрування інформаційних Інтернет-сервісів глибинного синтезу**, **Положення про управління алгоритмічними рекомендаціями в інформаційних Інтернет-сервісах** та **Висновок щодо посилення етики та управління в науці та техніці** **(Китай)**. В цілому Китай досить сильно просунувся не тільки в розробках систем ШІ, а і в регулюванні цієї сфери. Найновішим актом, який з'явився лише в середині серпня 2023 року, є закон, присвячений генеративному ШІ - і це перший у світі регуляторний акт так званого "жорсткого права" у цій сфері. Втім, крім нього у Китаї є ще чимало напрацювань у сфері регулювання технологій ШІ. Давайте з'ясуємо, як наразі виглядає законодавство у цій сфері і наскільки воно відрізняється від європейського підходу.

- **Заходи щодо генеративного ШІ**. Документ застосовується до використання всіх технологій генеративного ШІ для надання послуг населенню в КНР (сфера дії закону стосується саме послуг на території держави). Закон розроблений у відповідь на різке зростання популярності чат-ботів на основі ШІ, таких як ChatGPT, і має акцент на генерації тексту та навчальних даних. Він вимагає, щоб постачальники гарантували, що навчальні дані та створений контент є «*правдивими та точними*». Тобто по суті акт регулює інформаційну сферу з невеликими "домішками" регулювання у галузі захисту даних. Важливо, що Китай став першою державою серед тих, в яких активно ведуться розробки генеративного ШІ, яка врегулювала явище чат-ботів. Відповідальними за результати діяльності таких технологій закон пропонує зробити розробників систем ШІ, а надавати такі послуги анонімно - заборонено (наприклад, незаконним буде створити і поширювати додаток з елементами генеративного ШІ не розкриваючи особи розробника).
- **Положення про Інтернет-сервіси глибинного синтезу**. По суті, це акт, який стосується регулювання так званих діпфейків (від англ. "deepfake"), а точніше - технологій, які створюють будь-які види синтетичних медіа (в тому числі і для розважальних цілей). Ключовою новелою є заборона використання такої технології для генерування неправдивих новин, а також вимоги позначення будь-якого штучно згенерованого контенту (тобто аналог вимоги маркування, яка зараз повсюдно з'являється у проєктах регулівних актів). Крім того, акт містить ще й вимоги щодо нагляду за роботою систем, а також встановлює відповідальність розробників у випадку порушень.
- **Положення про алгоритмічні рекомендації**. Основною мотивацією розробки цього регулювання стали побоювання щодо значного впливу алгоритмів на фільтрування контенту та пріоритезацію новин.

Серед обов'язків для провайдерів Інтернет-сервісів варто згадати обов'язок не використовувати алгоритми для порушення прав інших, а також створити орган, відповідальний за безпеку алгоритмів. Крім того, закон по суті впроваджує вимогу регулярних оцінок впливу роботи алгоритмів на права людини, а також захист від використання алгоритмів для поширення неправдивих новин чи маніпуляцій. Додатково закон містить положення про посилений захист прав дітей, захист трудових прав та інші галузеві норми.

- **Висновок щодо етики і управління**. Документ зосереджується на внутрішній етиці і механізмах управління, які мають використовувати науковці і розробники технологій, а ШІ зазначається як одна з трьох сфер, що викликають особливе занепокоєння, поряд із розробками, що прямо впливають на життя, та медициною. На відміну від інших актів, це регулювання є більш технічним. Втім, воно також є важливим свідченням того, що в Китаї етичні питання намагаються врегулювати на законодавчому рівні (що є певним оксюмороном). Це є тривожним дзвіночком (як і багато інших питань, пов'язаних із захистом прав людини у Китаї, але все ж), адже етика і етичні стандарти - це те, що переважно має бути залишеним на відкуп саморегулівних органів та індустрії, а не державного регулювання.

На додачу до описаних документів існує великий масив інших нормативних актів - переважно дуже тематичних і вузькопрофільних. Ключовою відмінністю від європейського підходу є саме сегментарне регулювання та вирішення конкретних проблем, а не розробка загальних правил гри для усіх розробників систем ШІ.

Втім, навіть тематичних актів у Китаї стає все більше, а кількість врегульованих сфер постійно зростає. Так, поруч з актами, присвяченим алгоритмічним рекомендаціям в Інтернет сервісах і діпфейкам, є багато рекомендацій, як-от щодо роботи Інтернет-посередників. У дослідженні Carnegie Endowment for International Peace також згадують ряд рекомендаційних документів, які слугують своєрідною стратегією для розробок ШІ, пріоритезації сфер та регуляторних актів. З цікавих варто виокремити регулювання щодо захисту особистої інформації, яке враховує факт існування алгоритмічних систем і конкретні ризики для персональнальних даних. На додачу до регулювання, китайський уряд також створює фінансові можливості для стартапів та активно підтримує розробників технологій, які вважаються суспільно корисними.

Саморегулювання від індустрії. В цілому існує досить багато ініціатив щодо розробки саморегулівних актів (переважно колективних), або індивідуальних

публічних заяв з боку компаній-розробниць ШІ щодо стандартів, застосовних до їх продуктів. Звісно ж, такі заяви часто розбиваються об гранітні стіни реальності через брак процедури для притягнення до відповідальності за їх порушення, а також часто відсутність змоги перевірити дотримання технічних обіцянок на практиці. Втім, є і позитивні приклади - переважно від великих корпорацій, які мають фінансовий ресурс та достатньо велику команду, щоб інвестувати в додаткові методи захисту, оцінку впливу систем на права людини тощо. Хорошим прикладом індивідуальних ініціатив є нещодавній анонс від Microsoft щодо впровадження системи маркування контенту, який є штучно згенерованим. Так, компанія демонструє добросовісність у впровадження систем ШІ та вжиття можливих запобіжних заходів для уникнення зловживань. Аналогічно Google оприлюднив сім принципів щодо ШІ, яких він дотримується при розробці і застосуванні технологій.

Водночас, серед колаборацій найпотужнішою є Partnership on AI - некомерційна ініціатива, спрямована на відповідальне використання ШІ. В рамках цієї коаліції проводять дослідження впливу систем ШІ на етичні принципи і права людини та напрацьовують рекомендації щодо безпечного використання технологій. Зокрема, це стосується розробки документів, які кодифікують цінності, постульовані індустрією в рамках процесів створення технологій ШІ. Аналогічно, Google, Microsoft, OpenAI і Anthropic оголосили про заснування наглядового органу, який визначатиме наявність порушень стандартів у сфері ШІ.

До речі, Акт про штучний інтелект на рівні ЄС також залишає багато питань саме на відкуп саморегулювання - оцінка ризиків і загроз та самостійна розробка методологій, визначення статусу ризиковості системи, дотримання етичних принципів тощо. В цьому ключі, цікаво буде побачити його фінальний текст і оцінити “індекс довіри” до індустрії на тлі останніх політичних домовленостей між Європейським парламентом та Європейською комісією.

Інші ініціативи. Повсякчас з'являються й інші ідеї щодо регулювання і розробки стандартів (як і спроби їх впроваджувати). Більшість таких кроків є скоріше свідченням про невпевненість ключових акторів в успіху пропонованої Конвенції на рівні Ради Європи чи неспроможності дійти згоди щодо Акта про штучний інтелект (або непевність у застосовності його стандартів за межами ЄС). Наприклад, не так давно 18 країн підписали міжнародну угоду про безпечний ШІ, яка ще раз наголошує на необхідності створювати безпечні та орієнтовані на захист прав людини системи ШІ. Конкретних вимог і зобов'язань у ній не міститься, втім навіть такий крок цілком можна прийняти за чергову декларацію намірів нарешті врегулювати ШІ та розробити щонайменше етичні вимоги у цій сфері. Іншою цікавою

ініціативою є спроби розробити систему маркування контенту, генерованого ШІ. Поки що у цій сфері є напрацювання від дослідницьких центрів Європейського парламенту.

Також минулоріч ООН створив Дорадчий орган з ШІ, який складається з експертів у сфері ШІ, прав людини та розробки стандартів для нових технологій. Його робота ґрунтується на принципах інклюзії, поваги до суспільного інтересу та міжнародного права, залучення усіх зацікавлених сторін і особливої уваги до управління даними (невід'ємної частини управління ШІ). Дорадчий орган нещодавно видав перший звіт "Управління ШІ для людяності". Документ, зокрема, як і більшість інших фундаментальних рекомендацій у цій сфері, містить два ключові компоненти: перелік принципів у сфері управління ШІ та інституційні функції (розробників, користувачів та інших акторів, дотичних до цієї сфери).

Як помітно з короткого огляду ключових напрацювань у сфері регулювання і стандартизації ШІ, більшість рекомендаційних документів на міжнародному рівні є схожими за принциповими підходами і орієнтуються на забезпечення прозорості і етичності систем ШІ. Водночас, національні стратегії, управлінські рішення та декларації є більш заточеними під створення сприятливого середовища для інновацій (зокрема, і через потужне лоббі індустрії). Як наслідок, більшість документів є або рамковими, або викладають принципи загального характеру, або ще не перетворилися на юридично обов'язкове регулювання (і питання, коли вони на нього перетворяться - як ніколи актуальне).

III. Українські стандарти: між етикою і законом

Яке регулювання наразі існує на українських теренах? З грудня 2020 року набрала чинності **Концепція розвитку штучного інтелекту в Україні** (з невеликими доповненнями щодо пріоритезації напрямку законодавчого регулювання у 2021 році). За своєю суттю це скоріше стратегічний документ, що пріоритезує напрямки розвитку ШІ та вказує на актуальні сфери для української індустрії. Жодних стандартів для безпечного створення і застосування ШІ він не містить, про що неодноразово заявляли українські громадські організації. Така тенденція викликала занепокоєння ще у 2020 році, коли активний розвиток технологій стимулювався без будь-яких "червоних ліній". Не змінив ситуації і План заходів. Прийнятий на виконання Концепції, він містить завдання для кількох профільних державних органів - МОЗу, Міносвіти, Мінкульту, інших міністерств, серед яких, звичайно ж, Мінцифри. Переважно перелік завдань стосується можливих напрямів

і сфер для впровадження технологій ШІ, але аж ніяк не розробки регуляторної рамки, запровадження стандартів чи безпекових гарантій, в тому числі і у сфері захисту прав людини.

Ситуація змінилася у 2023 році, коли Мінцифри презентувало **Дорожню карту з регулювання ШІ в Україні**. Цей документ був розроблений із залученням Експертного комітету з розвитку штучного інтелекту в Україні, який є майданчиком для співпраці самого Міністерства, індустрії, академії та представників громадянського суспільства. В цілому документ передбачає "bottom up approach" - початок розробки стандартів на рівні індустрії з поступовим напрацюванням законодавчого регулювання. Це дозволить національним розробникам краще адаптуватися до появи регулювання, а державі - зрозуміти, яким чином імплементовувати зобов'язання за Актом про штучний інтелект (що може породити досить багато викликів для України, адже ми не маємо доступу до більшості інституцій ЄС). На відміну від згаданої Концепції, Дорожня карта запропонувала конкретні механізми для розвитку галузі. І вони включають в тому числі і так званий "краш-тест" щодо захисту прав людини. Які ідеї пропонується впровадити найближчим часом?

- **Біла книга**. До кінця 2024 року планується підготовка, обговорення та оприлюднення Білої книги (за зразком британської моделі), яка допоможе вписати технології ШІ у вже існуючі рамки чинного українського законодавства щонайменше до моменту розробки комплексного регулювання. Зокрема, в документі планується окреслити принципові підходи та зробити майбутнє регулювання прогнозованим для індустрії. Біла книга також значною мірою ґрунтуватиметься на підходах Акта про штучний інтелект, який згодом буде імплементовано в національне законодавство як частину зобов'язань з євроінтеграції. По суті, Біла книга слугуватиме більш деталізованим керівництвом і своєрідним меппінгом регуляторних перспектив. Перший драфт презентували під час заходу «The AI State: Government Tech with Startups», зазначивши, що наразі документ планується як розширена версія Дорожньої карти з деталізованими заходами, що реалізуватиме держава.
- **Загальні та секторальні рекомендації**. У 2023 році планувалося почати напрацювання загальних рекомендацій щодо розробки та використання ШІ, які окреслять систему цінностей та ключові принципи для створення таких систем, незалежно від сфери їх застосування чи призначення. Трохи згодом, у 2024 році, планують розробити ще й секторальні рекомендації - вони будуть більш детальними і заточеними під конкретні суспільні потреби, виклики певних галузей (як-от медичної чи правоохоронної) і перспективи стандартів, які

безпосередньо адресуватимуть такі виклики. Також в рекомендаціях побіжно зачіпатиметься питання створення інструментів і механізмів саморегулювання. На практиці першими з'явилися секторальні Рекомендації щодо відповідального використання ШІ у медіа, які окреслюють основні підходи, етичні принципи та цінності, яких має дотримуватися індустрія (серед них розмежування генерованого і автентичного контенту, маркування генерованих матеріалів, прозорість щодо використання ШІ тощо).

- **Регуляторна пісочниця (від англ. "*regulatory sandbox*")**. Ще в березні 2023 року Мінцифри анонсувало запуск "регуляторної пісочниці", яка уможливить тестування продуктів індустрії у захищеному закритому середовищі на закритих наборах даних, перевірку ефективності нових систем та дотримання стандартів у сфері прав людини тощо. Це буде здійснюватися перед тим, як продукти виходять на ринок. Підготовчі роботи за проєктом плануються на 2024 рік, запуск - на 2025. Наразі ведуться роботи над технічною складовою "регуляторної пісочниці". Для цього Мінцфири проводить опитування щодо формату і можливостей такого проєкту, потреб індустрії та попиту на такий інструмент. Зокрема, через його обмежені спроможності попередньо планується долучати до тестування саме ті проєкти у сфері ШІ, які мають значну суспільну цінність.
- **Процедура маркування ШІ (від англ. "*AI labelling*")**. Маркування включає висвітлення процесів та методів, задіяних у анотації даних, у створенні програмної архітектури, у використанні сторонніх компонентів і типах вихідних даних. Це, зокрема, забезпечує дотримання принципу прозорості, що надає користувачам більше прогнозованості в якості результатів, а стандартизація робить можливим планомірне використання підходів до покращення систем ШІ. Використання критеріїв відкритих даних (open data) для результатів маркування є обов'язковим і дає можливість встановлення балансу між потребою прозорості та конфіденційності (збереженням комерційної таємниці).
- **Маркування контенту, створеного ШІ (від англ. "*AI content labelling*")**. Маркування контенту допомагає встановити автентичність створеного контенту, допомагаючи ідентифікувати та пом'якшити потенційне зловживання матеріалами, створеними системами з генеративним ШІ. Розробка системи маркування контенту, продукованого ШІ, є важливою для забезпечення прозорості роботи цих систем і їх використання (і тут корисними ініціативами можуть бути Content Autheticity Initiative, C2PA тощо).

- **Оцінка впливу на права людини**. Дорожня карта пропонує впровадити механізми оцінки впливу систем ШІ на права людини, демократію та верховенство права. Серед таких інструментів основним є проєкт HUDERIA - методологія, яка допомагає ідентифікувати ризики у системах, оцінити їх вплив і розробити механізм пом'якшення негативних наслідків. В процесі передбачається залучення різноманітних зацікавлених сторін для комплексного встановлення прогалин і потенційних небезпек. Наразі вже погоджена участь українських представників у пілотному проєкті HUDERIA. Крім цього, є ряд інших схожих ініціатив, включно з AIIA, Canvas, NIST AI Risk та багатьма іншими, які можуть використовуватися для здійснення такої оцінки.
- **Розробка кодексів поведінки**. Такі документи переважно є наслідком об'єднання представників індустрії у саморегулівний орган (або ж секторальні органи), який слугуватиме майданчиком для комунікації, обговорення ціннісних орієнтирів та принципових засад функціонування сфери ШІ в Україні. Такі добровільні зобов'язання, долучення до їх розробки та їх визнання дозволять ідентифікувати добросовісних гравців на ринку. Більше того, це стане платформою для колаборації з компаніями, які готові дотримуватися етичних стандартів (зокрема, і державно-приватних партнерств).
- **Розробка комплексного законодавчого регулювання (до 2027 року)**. З огляду на те, що Акт про штучний інтелект на рівні ЄС досі не прийняли (а перспективи залишаються досить туманними), наразі про розробку національного регулювання ШІ в Україні годі й говорити. Зокрема тому, що регуляторні акти потім доведеться оновлювати або й повністю змінювати, якщо вони матимуть розбіжності зі стандартами ЄС. Ба, навіть після прийняття Акту про штучний інтелект залишатиметься багато питань, які стримуватимуть Україну від його транспозиції (буквально, дослівного перенесення) в національне регулювання. Так, як і будь-який документ подібного характеру, Акт про штучний інтелект має досить багато відсилок до інституцій ЄС, доступу до яких Україна поки що не має. Крім того, як і в ситуації з Актом про цифрові послуги, у сфері ШІ можуть виникнути проблеми імплементації Регламенту навіть на рівні ЄС, не кажучи вже про країн-кандидаток. Тож, поспішати з розробкою національного регулювання не варто щонайменше, щоб не довелося вносити численні правки у вже прийняті закони. Тому Дорожня карта передбачає розробку і прийняття комплексного регулювання за 4 роки, коли система буде відтестованою на європейському ринку.

- **Інші інструменти**, які виникатимуть на національному або міжнародному рівні (в тому числі і “знизу-вгору” тобто від індустрії до держави).

Стратегія розвитку інновацій. У грудні 2023 року Мінцифри представило документ, яким планується окреслити запити та пріоритети у сфері інновацій до 2030 року. Якщо українські інновації видаються надміру футуристичними - на практиці це зовсім не так, адже Стратегія містить детальний аналіз іноземних практик. Серед них японське Society 5.0 (масштабна діджиталізація публічних послуг), екосистема ШІ-стартапів Тайваню, довгострокова стратегія інновацій у Сполученому Королівстві (до 2050 року) і багато інших практик. В інформаційному центрі “Дії” також згадують низку інших сервісів, які Мінцифри вважає зразковими у сфері ШІ-розробок: Patenttranslate (сервіс перекладу патентів 32 мовами), Serenata.ai (сервіс громадського контролю публічних витрат) та Kaggle (платформа для змагань зі створення моделей ШІ).

В українській Стратегії ШІ отримав особливу увагу в багатьох галузях, включно з оборонною, освітньою, сферою охорони здоров'я та управлінською. Серед цілей також було зазначено необхідність розробити регулювання у сфері ШІ, напрацювати етичні та нормативні правила, а також заохочувати індустрію працювати у пріоритетних галузях. Трьома основними проєктами у сфері ШІ ж назвали регуляторну пісочницю, Government BI та GovTech AI Center of Excellence (відкриття якого анонсували на початку січня 2024 року). Для реалізації Стратегії пропонується реструктурувати менеджмент, організувавши його таким чином:

- Мінцифри відповідатиме за загальну координацію;
- Рада з розвитку інновацій — за обговорення, підготовку й погодження Стратегії;
- Заступники з цифрової трансформації (CDTO) у міністерствах — за формування інноваційної політики в різних галузях;
- CDTO в областях — за впровадження політики в регіонах;
- Державна агенція з розвитку інновацій — за реалізацію Стратегії й пошук інвестицій.

Напрацьована модель (як на рівні Дорожньої карти, так і на рівні Стратегії) є деталізованою, багатошаровою та достатньо амбітною (особливо, у короткостроковій перспективі). І тут важливо пам'ятати, що пропоновані заходи орієнтовані на приватний сектор і налагодження державно-приватного партнерства, і лише як наслідок - розробку етичних стандартів

чи добровільне тестування систем (“краш-тест” на дотримання прав людини). Втім, багато технологій ШІ вже активно використовуються. І далеко не всі вони є низько ризиковими (наприклад, розважальними). Навпаки - більшість технологій, розроблених для державного сектору мають значний вплив на права людини. Тож, давайте з'ясуємо, які наразі є ініціативи використання ШІ державою та чи не нависає часом дамоклів меч над правами людини внаслідок гонитви за діджиталізацією.

IV. Публічне управління: нові дії у “Дії”?

У липні 2023 дослідження Центру Разумкова показало, що лише близько 15% українців активно використовують технології ШІ. Втім, цифровізація відбувається швидко і на багатьох рівнях. Одним з її рушіїв є цифрова реформа сфери публічного адміністрування. Державні органи регулярно оголошують про впровадження автоматизованих систем в процеси прийняття рішень, аналіз даних чи надання публічних послуг. ШІ у своїй роботі почали використовувати навіть українські дипломати, про що нещодавно заявив Міністр закордонних справ Дмитро Кулеба під час EquAllity Hackathon. Сфери застосування ШІ в дипломатії, втім, досить безпечні: аналіз великих масивів даних, розробка комунікаційних стратегій, аналітики та пошукових запитів.

Втім, у сфері публічного управління є комплексніші ініціативи, де ШІ має більше “автономії” та здатен впливати на організацію і отримання публічних послуг, масову обробку даних в цілях ведення статистики і прийняття та перевірку інших систем. Крім того, у шквалі анонсів від Мінцифри можна зустріти ідеї моніторингу соціальних мереж та інших публічних платформ, що змушує стурбовано замислитися. Про які ініціативи йдеться і чи безпечні вони з точки зору дотримання прав людини?

Державний застосунок “Дія”. Хоча сама по собі “Дія” першопочатково не мала елементів ШІ - вона не приймала жодних самостійних рішень і не робила значного внеску у прийняття таких рішень держслужбовцями - наразі існує ідея посилити спроможності додатку за допомогою додаткового **інструменту ШІ “Надія”**. За словами Міністра цифрової трансформації Федорова, ШІ в дії матиме форму віртуального помічника і зможе консультувати користувачів платформи, пояснюючи технічні аспекти або, наприклад, радячи людині, де знайти найближчий ЦНАП. Такий проєкт планується реалізувати разом з OpenAI та Microsoft, з якими наразі ведуться перемовини про інтеграцію ШІ в “Дію”.

Тобто планується розробити чат-бот, який буде давати безпомилково правильні відповіді на будь-які запитання, що стосуються державних сервісів

- причому легкою і зрозумілою мовою. Поки що, за словами розробників, цього досягнути не вдалося, тож система перебуває на тестуванні у спеціальної команди і не доступна широкому загалу. Водночас, йдеться саме про недостатню ефективність технології станом на зараз. Так, Федоров окремо підкреслив, що з безпекової точки зору "Надія" буде дуже надійною, бо архітектура системи не передбачатиме використання персональних даних. Команда, яка працює над розробкою "Надії", зазначає, що в планах є розробити асистента, яка прогнозуватиме потреби особи в певних видах послуг (зокрема, державних) і проактивно пропонуватиме їх. Це нагадує своєрідний "рекламний таргетинг" держпослуг і тут ключове питання виникатиме щодо порядку реалізації цієї ідеї: чи можливо робити профайлінг і меппінг потреб без аналізу персональних даних користувача (його місця знаходження,)

Іншою ініціативою в рамках застосунку "Дія" є **проєкт "Дія Office"**, покликаний цифровізувати роботу міністерств, зробити її прозорою і забезпечити публічний контроль за виконанням цілей та планів органів влади. За словами Федорова, пересічні громадяни не матимуть доступу до усього функціоналу системи, доступного держслужбовцю. Втім, вони зможуть слідкувати за розподілом компетенцій і відповідальною за виконання конкретних завдань особою, строками їх виконання, виділенням коштів тощо. Водночас, держслужбовці зможуть провести опитування чи пропонувати ідеї в межах свого міністерства/відомства, призначати зустрічі чи комунікувати між собою.

Ще однією метою цієї інновації є внесення елементу гейміфікації в роботу чиновників. Так, держслужбовці матимуть змогу оцінити досягнення колег, вручити заохочувальну нагороду в "Дія Office", відслідковувати прогрес у виконанні цілей інших департаментів. Наразі проєкт перебуває на стадії бета-тестування, також не готове і правове регулювання для такого типу застосунків. І саме цей аспект може стати справді проблемним, враховуючи, як багато зусиль потребують законодавчі зміни у сфері державної служби.

Державна служба статистики. У Плані дій на виконання Концепції з розвитку ШІ значна роль відводиться колаборації між Мінцифри і Держстату з метою покращення обробки інформації та оцінки ефективності державного управління. Так, Мінцифри запустила пілотний проєкт щодо оцифрування та посилення спроможностей органів державної влади - Government BI (GBI). Наразі відбувається бета-тестування проєкту, після успішного завершення якого його планують масштабувати і на інші органи влади. До розробки проєкту долучений Держстат, дані від якого використовуються для створення системи ШІ.

В цілому, ініціатива передбачає впровадження аналітичних інструментів, в тому числі ШІ, для покращення і пришвидшення управлінських рішень.

Розробники наголошують, що система GBI не буде замінювати людські рішення, а лише допомагатиме виконувати організаційні задачі. Останні етапи проєкту передбачають розбудову інститутів BigData, що забезпечуватимуть розвиток системи відкритих даних за участі Державної служби статистики (оцифрування якої триває з 2021 року). Це надзвичайно важлива ініціатива, адже аналітики вже тривалий час наполягають на відкритті статистичних даних для прогнозування економіки (що підтримує і Мінфін).

У другій половині 2023 року планується запустити новий портал Держстату з реорганізацією адміністративної структури, створенням внутрішньої IT-системи і перенесенням даних за останні тридцять років у цифровий вигляд. Це також сприятиме швидшій обробці даних та залученню Держстату до державних процесів у форматі більш інтенсивної співпраці.

“Голос громадян”. Поміж інших проєктів з діджиталізації та цифровізації виринула цікава ініціатива під назвою “Голос громадян”, у якій Мінцифри поставило перед собою амбітну ціль - сканувати усе, що відбувається у соцмережах, в режимі реального часу. Метою є збирати інформацію про дискусії на форумах, у Facebook, Instagram, Telegram, щоб з'ясувати суспільні проблеми і потреби: де погано надають послуги, які існують скарги тощо. Згодом інформацію планується передавати в контакт-центри і комунікувати профільним державним органам.

Розповідаючи про проєкт, представники Мінцифри наголосили, що Україна наразі “*напевно, найкраща територія в світі, де можна застосовувати різні технології*”, а “Голос громадян” має можливість подолати прогалину між бюрократичними процесами і реальністю. Відповідно до анонсів проєкту в медіа, ініціатива буде інтегрована з віртуальним асистентом “Надія”, через якого громадяни зможуть записати голосові повідомлення зі скаргами і пропозиціями, а держслужбовці - отримувати зворотній зв'язок у режимі реального часу.

Втім, важливо усвідомлювати різницю між свідомим повідомленням державних органів про проблеми за допомогою віртуального асистента (голосові чи текстові скарги) та невибірковим моніторингом соціальних мереж (які юридично є недержавним простором). В контексті цього проєкту моніторинг, по-перше, може передбачати обробку персональних даних (адже часто скарги онлайн можуть бути дуже персоніфіковані), по-друге, впровадження таких технологій потребує окремого правового регулювання, адже вплив такої ініціативи на права людини є дуже суттєвим. І хоча доки не буде відомо більше інформації про архітектуру проєкту, зарано говорити про технічні ризики, концептуально така система йде врозріз з обов'язком держави не втручатися у сферу свободи вираження.

V. Інформаційна сфера: на вершині новинного Евересту

Використання ШІ в інформаційній сфері постійно на порядку денному: починаючи від вже згаданого ChatGPT, який не відрізняє адекватну інформацію від російської пропаганди, і завершуючи створенням діпфейків (чого лише варті відео Зеленського, Залужного та скандал з мімікруванням під Кличка). І саме засилля дезінформації спонукає шукати механізми для протидії маніпулятивному, пропагандистському і при цьому штучно згенерованому контенту. Наразі державні органи досить обережно ставляться до питання дезінформації, а профільні міністерства намагаються вживати заходів, щоб забезпечити медійну і цифрову грамотність (наприклад, Мінкульт має проєкт "Фільтр").

Під час конференції «Штучний інтелект і дезінформація: викриття цифрової пропаганди» заступник Міністра культури та інформаційної політики Тарас Шевченко наголосив, що національна Стратегія інформаційної безпеки передбачає низку цілей та інструментів, серед яких і використання технологій з метою протидії дезінформації. Водночас, жодних конкретних систем, додатків чи партнерств з техкомпаніями Мінкульт наразі не встановлює (принаймні у частині застосування технологій ШІ чи їх розробки для цілей протидії російській пропаганді).

Центр стратегічних комунікацій та інформаційної безпеки використовує ШІ для моніторингу медіапростору та аналізу онлайн-публікацій на предмет поширення дезінформації. Серед автоматизованих засобів згадують платформи SemanticForce і Attack Index. Перший аналізує інформаційний простір, включно з соцмережами, та виявляє інформаційні тренди. Другий - застосовує машинне навчання, кластерний аналіз та комп'ютерну лінгвістику, щоб виявляти шкідливі наративи, прогнозувати майбутні інформаційні атаки, виявляти автоматизовані системи поширення дезінформації або координовані кампанії, та категоризувати небезпечний контент. Втім, власних розробок чи проєктів Центр стратегічних комунікацій також не має - принаймні поки що.

Водночас, наприкінці жовтня 2023 року, Мінкульт оголосив про співпрацю з Google у сфері протидії дезінформації та збереження культурної спадщини. Одним з напрямків співпраці планується мати розвиток технологій ШІ. Тож, брак національних розробок ШІ у інформаційній сфері не видається вироком, а колаборація з техгігантами, навпаки, може надати ефективніші та безпечніші заходи для захисту прав людини. Жодних оновлень на цю тему з жовтня 2023, втім, не спостерігалося. Тож, залишається сподіватися, що на операційному рівні це питання не зависло в бюрократичних тенетах.

Також Мінцифри повідомило, що українські розробники створити платформу Mantis Analytics, за допомогою якої можна моніторити та аналізувати маніпуляції в інформаційному просторі. Це включає аналіз медіа, соцмереж та інформаційних платформ, і компонування даних на інтерактивній карті (що є публічно доступною). Така ініціатива існує в межах проєкту Brave1 - defense-tech-кластера, який орієнтований на надання технологічних рішень для наближення перемоги. Що важливо - на відміну від "Голосу громадян", Brave1 анонсована як платформа, що стосується сфери оборони. Тож існує вірогідність, що моніторинг соцмереж припиниться після української перемоги.

Втім, на централізованому (державному) рівні все ще досить мало технологій застосовуються для протидії дезінформації та інших інформаційним загрозам. Для порівняння, Міноборони США підписало контракт зі стартапом DeepMedia на використання технологій ШІ для виявлення діпфейків. Що важливо - США планує використовувати такі можливості в тому числі і для виявлення російської пропаганди. Інструменти, які планує розробити DeepMedia, навчалися на зразках 50 мов для виявлення того, чи контент є справжнім, чи він штучно згенерований. Ці практики свідчать про серйозне занепокоєння темою дезінформації, а також про можливість залучати сторонні компанії для розробки програмного забезпечення, яке може бути корисним та ефективним для протидії інформаційній агресії.

VI. Освітня сфера: час для втілення "Мрії"

Онлайн-освіта вперше постукалася у двері з початком COVID-19, коли навчання мігрувало у Zoom, Teams та GoogleMeets. Результати були не надто втішними, адже дослідження вказали на погірше якості освіти (або щонайменше - успішності учнів у школах). Ще тяжчою ситуація стала під час повномасштабного вторгнення (особливо, зима 2022-2023 років), коли відсутність доступу до інтернету, постійна необхідність пересуватися між класним кабінетом і укриттям та руйнування освітньої інфраструктури призвели до значного просідання у рівні освіти. Більше того, виникла необхідність поєднувати освіту для тих, хто виїхав за кордон із освітою для тих учнів, які залишилися на території України.

У відповідь на виклики останніх чотирьох років Міністр цифрової трансформації Федоров анонсував запуск **цифрового помічника "Мрія"**. Презентація проєкту відбулася 1 вересня 2023 року. Під час неї Президент Зеленський наголосив, що застосунок покликаний допомагати дітям розкривати їх потенціал та, на основі рекомендацій, надавати алгоритм того,

яким предметам варто приділяти більше часу, які освітні програми обирати, які матеріали можуть бути цікавими. Основним завданням “Мрії” є аналіз місця навчання, кваліфікацій вчителів та контенту, який дитина споживає, щоб визначити траєкторію її подальшої освіти. З практичних заходів “Мрія” дозволятиме пропонувати інновації, шукати гранти, секції для додаткових занять тощо - тобто надавати необхідну інформацію на запит (на зразок проєкту “Надія”).

Впровадження проєкту першопочатково очікувалося наприкінці осені або на початку зими, втім у листопаді Федоров презентував інтерфейс застосунку і оголосив, що запуск повної версії планується на 2024 рік. В ній можна буде отримувати доступ до щоденників, даних про вчителів, навчальні програми, пропозиції щодо змін тощо.

Цікаво, що про “Мрію” вже ширилися фейки. У мережі масово репостили відео Остапа Стахіва про те, що застосунок “Мрія” заганяє дітей у цифровий концтабір, адже ШІ визначає їхні пріоритети життя, поведінку та майбутню професію. Також Стахів зазначав, що “Мрія” мала б встановлювати порядок спілкування батьків з дітьми. Відповідно до фактчекінгу від VoxCheck, жодне публічне джерело не вказувало, що застосунок будь-яким чином зачіпатиме відносини батьків та дітей. Натомість він надасть можливість батькам комунікувати з вчителями онлайн, усередині “Мрії”. В цілому, особливо в обставинах дистанційного навчання, застосунок може стати дуже зручним способом комунікації та покращення якості освіти.

“Обери професію своєї мрії”. Міносвіти спільно з Інститутом модернізації змісту освіти й Асоціацією інноваційної і цифрової освіти реалізують всеукраїнський проєкт «Обери професію своєї мрії». Зокрема, цей проєкт передбачає можливість пройти профорієнтаційне тестування на основі ШІ, яке дозволить школярам визначити власну схильність до однієї або кількох професій. Відповідно до даних від кінця липня 2023 року на сайті МОН, тестування пройшли вже 100 000 здобувачів освіти. Цей проєкт є одним з багатьох інструментів, які застосовують для допомоги у виборі професії.

Окрім ініціатив в межах шкільної освіти планується сприяти розвитку ШІ в університетах. Так, серед ідей розвитку ШІ все частіше фігурує варіант створення дослідницьких лабораторій спільно з Комітетом з розвитку штучного інтелекту в Україні при Мінцифри та Міносвіти. Одна з таких лабораторій вже є в УКУ - наразі вона є першою і працює скоріше у тестовому форматі. Згодом планується розробити типовий пакет договорів між компаніями та університетами для полегшення формалізації співпраці. На додачу до цього, Мінцифри розробило каталог освітніх програм для майбутніх студентів з інформацією про підготовку фахівців у галузі ШІ (наприклад, про машинне навчання, аналіз даних, обробку мови тощо).

Зрештою, Мінцифри розробляє **освітні серіали** про ШІ, які окреслюють особливості і виклики, пов'язані зі створенням автоматизованих систем та їх застосуванням. Частина лекцій орієнтована на молодші аудиторії, але є й онлайн-курси, спрямовані на представників індустрії - наприклад, щодо дотримання прав людини при створенні новітніх технологій. Серед навчальних програм слід згадати і анонс чергової колаборації Мінцифри з Google Україна, які домовилися про створення курсу з використання ШІ для розвитку бізнесу та персонального бренду. Це є надзвичайно актуальним питанням, адже у грудні 2023 року дослідження МАН України спільно з Projector Creative & Tech Institute вказало, що 70% учнів вже використовують ШІ. Тож, розвиток навичок безпечного і етичного використання технологій як ніколи на часі.

З важливого - на жаль, далеко не всі ініціативи згадують про безпечний та орієнтований на права людини ШІ. Лекції часто охоплюють теми того, якими корисними можуть бути технології та як їх найефективніше застосовувати. Водночас, дуже рідко йдеться про захист даних або про масштабніший вплив на права людини. Так, колаборація з Google враховує радше переваги технологій для бізнесу, ніж проведення тестувань систем, розробки кризових протоколів чи оцінки небезпек. І це є однією з небезпек при розробці навчальних програм, адже питання етики та захисту прав людини є ключовими при створенні і застосуванні систем, а тому виключення таких тематик з фокусу може сильно нашкодити у майбутньому. Водночас, станом на грудень 2023 року, щонайменше 5% школярів використовують ШІ для підготовки домашніх завдань і написання робіт, що далеко не завжди відбувається доброчесно. Відсутність правил, принаймні на рівні університетів (не кажучи про рекомендації від Міністерства освіти і науки), явно не сприяє етичному застосуванню технологій, особливо, якщо вони перебувають у вільному доступі.

VII. Охорона здоров'я: хто тримає руку на пульсі?

Стратегія розвитку телемедицини в Україні, схвалена у липні 2023 року, не має жодної згадки про системи ШІ або перспективи їх розвитку у медичній сфері. Звісно ж, жодного регулювання не пропонує і профільне законодавство. Як наслідок, виникало чимало ситуацій, коли співпраця держави з приватними сервісами чи розробка власних ініціатив гальмували через брак стандартів і основних принципів застосування ШІ в сфері охорони здоров'я (принаймні і українському правовому полі). Наприклад, держава досить тісно співпрацювала з Helsi.me, який мав досить багато скандальних випадків з незаконною обробкою персональних даних та їх використанням

у розріз з метою збору таких даних. Годі й казати, що більшість даних були чутливими, адже йдеться про медичну сферу.

На державному рівні, елементи обробки даних автоматизованою системою застосовувалися у проєкті "Централь 103", який передбачав створення і підтримання екосистеми, яка контролює якість надання екстреної медичної допомоги і пришвидшує прибуття швидкої. По суті, система координувала диспетчерські та інші служби, дозволяючи скоротити час на обмін інформацією. Втім, на жаль, наразі вебсайт не має доступних звітів за минулі періоди, а дані щодо статусу розбудови мережі обнулили. Ймовірніше за все, це свідчить про паузу у проєкті.

Наразі існує два великих проєкти, в межах яких відкрито анонсували розробку і впровадження систем ШІ: ініціатива "BrainScan" і "System Carebits". Обидва проєкти запустили у 2023 році за підтримки міжнародних партнерів та за координації МОЗ. З правової точки зору регулювання діяльності таких систем немає, а тому фінальна відповідальність за технічні похибки все ще лежить на лікарі. Втім, поза правовим полем, давайте з'ясуємо, які практичні характеристики мають згадані системи і які ризики це може породжувати.

BrainScan. У пілотному форматі проєкт запустився в Одесі на початку вересня 2023 року. Згодом програма також застосовувалася у прифронтовому Краматорську на Донеччині. МОЗ зазначив, що використання ШІ для аналізу КТ-знімків головного мозку у прифронтових регіонах показало хороші результати і високу ефективність. Ця система пришвидшує процес діагностики захворювань або ушкоджень головного мозку, особливо у випадках, коли час є критичним фактором. Відповідно до описів програми, вона надає висновки щодо мозкової активності лікарю вже за 5 хвилин після початку аналізу комп'ютерної томографії головного мозку. Це здійснюється в автоматичному режимі. Важливо, що фінальне рішення щодо протоколу лікування все ж приймається лікарем, а отже жодного самостійного втручання у здоров'я людини ШІ не здійснює.

System Carebits. Цей проєкт є телемедичною онлайн-платформою, яка за допомогою переносних портативних апаратів дозволяє проводити діагностику розвитку плода у вагітних у віддаленому режимі. Апарат здійснює аналіз показників і надсилає результати на пристрій (телефон або комп'ютер) лікаря. Також програма дозволяє лікарю здійснювати консультування та комунікувати як з вагітними, так і з колегами. Така ініціатива є особливо актуальною з огляду на повномасштабне вторгнення і часту нездатність лікарів бути фізично присутніми при пологах або протягом періоду вагітності. Зокрема, вже були успішні випадки консультування онлайн під

час пологів на Миколаївщині, коли породіллю не змогли доставити у лікарню через обстріли і фізичну небезпеку. Наразі у проєкті беруть участь близько 180 закладів охорони здоров'я з усіх областей України, а лікарі проходять навчання щодо правильного використання системи. Перші прилади були передані Україні в рамках гуманітарної допомоги разом з необмеженою кількістю ліцензій на використання системи. Аналогічно до "BrainScan", цей проєкт передбачає прийняття фінальних рішень лікарем і не створює можливостей для ШІ самостійно втручатися у здоров'я людини.

Як висновок, застосування ШІ у сфері охорони здоров'я на державному рівні наразі перебуває скоріше у зародковому стані, адже за державної підтримки та координації реалізується не так багато проєктів. Водночас, не варто недооцінювати індустрію - зокрема, українські стартапи мають дуже багато проєктів, орієнтованих на фасилітацію процесів отримання медичної допомоги, внутрішнього адміністрування лікарень, міжвідомчої координації тощо (Liki.24, Tabletki.ua, Doc.ua тощо). Втім, як для державного, так і для приватного сектору бракує належних правових стандартів для розробки і застосування таких технологій.

VIII. Соціальна сфера: як підтримати систему підтримки?

З початком повномасштабного вторгнення кількість соціальної підтримки і потреба у ній зросли в рази. Звісно ж, значна частина потреб перекриваються за допомогою ресурсів від благодійних організацій, міжнародних донорів, іноземних фондів і установ, та навіть бізнесу. Проте навантаження на державу від залученості третіх сторін не стало меншим. І питання не тільки у фінансових ресурсах та їх обмеженості з огляду на активну агресію Росії. Викликом також є адміністрування процесів надання та розподілу соціальної підтримки, пріоритезації найбільш вразливих груп населення, проведення оцінки соціального стану особи тощо. Як наслідок, виникла жорстка потреба в діджиталізації та автоматизації таких процесів.

Проєкт «Модернізація системи соціальної підтримки населення України». Ця комплексна система має на меті автоматизовано виявляти передумови порушень законодавства при отриманні державної соціальної допомоги. Програма реалізується Мінцсоцполітики за підтримки Світового банку і спершу була запущена у форматі пілотного проєкту в декількох областях. Що передбачає система? Алгоритм з елементами ШІ аналізує дані щодо порушень при отриманні коштів соціальної підтримки та формуватиме "профілі ризику" - набір характерних ознак отримувачів, які найчастіше

вдаються до шахрайства і зловживань при отриманні допомоги від держави. На початкових етапах методика тестувалася у 10-ти управліннях соціального захисту, а результати роботи ШІ сприяють його "самонавчанню" - тобто коригуванню алгоритмів залежно від доступної вибірки, статистичних даних та позначення результатів його роботи як правильних чи хибних.

Для запуску системи необхідно було зібрати надзвичайно великий масив даних від соціальних інспекторів, фахівців Мінсоцполітики, результати соціальних виплат у статистиці від Мінфіну тощо. На підставі цієї інформації вдалося розробити профайл "типових порушників". Наразі про систему говорять небагато, а отримані після завершення тестового періоду результати Мінсоцполітики так і не оприлюднило. Це, в свою чергу, викликає запитання про ефективність системи та її вплив на права осіб, чиї запити на соціальну допомогу були відхилені через їх відповідність "ризиковому профайлу".

Хоча під час обговорень у Мінфіні ініціатори впровадження системи посилалися на іноземний досвід застосування систем соціального ранкування у банківській сфері (зокрема, у Румунії і Молдові), варто усвідомлювати, що такі технології є десь на грані між високо ризиковими та забороненими системами відповідно до проєкту Акту про штучний інтелект. Особливо, якщо вони застосовуються державою. Адже банк може використовувати профайл особи винятково у цілях укладення з нею угоди щодо відкриття рахунку, кредитування чи купівлі цінних паперів (та інших активностях банківської сфери). Тобто перелік потенційних ризиків є вичерпним і зрозумілим. Водночас, надавати профайли вразливих і маргіналізованих груп державі - а саме такі групи найчастіше розраховують на соціальну допомогу - є дещо небезпечним. Згодом, зі зміною уряду чи загостренням соціальних проблем це цілком може перетворитися на списки осіб для переслідувань чи утисків, як це наразі відбувається у Китаї. Тому, більшість правозахисників активно виступають проти впровадження подібних систем навіть у приватному секторі, не кажучи вже про державні проєкти такого спрямування. Аналогічно, рано чи пізно постане питання відповідності європейським стандартам - зокрема, у сфері захисту даних та заборони дискримінації осіб на підставі соціального статусу.

Проєкт "Національний кадровий резерв". Пресслужба Державної служби зайнятості повідомила, що ініціатива представлена соціальним ліфтом, який за допомогою ШІ може допомогти українцям знайти роботу або відкрити власний бізнес. Зокрема, система зможе визначати коло професій, що підходять людині залежно від її здібностей, кваліфікацій та рівня володіння комунікаційними і менеджерськими навичками. На основі аналізу даних формуватиметься інтерактивне резюме, яке можна долучити до Єдиного порталу вакансій, використовувати при прийомі на роботу або ж як опис

власних сильних сторін та професійних якостей. Якщо ж особа має схильність до підприємництва - система пропонуватиме їй пройти онлайн-курси для покращення таких навичок. При цьому, ШІ не приймає рішення за людину та не надає дорадчих функцій, а публічний опис моделі свідчить при досить низький ризик можливих упереджень, адже результати генеруватимуться на основі інформації, наданої самою особою.

Зрештою, **Єдину інформаційну систему соціальної сфери** планують доповнити новим інструментом - кейс-менеджментом. Наразі триває бета-тестування проєкту в чотирьох пілотних областях. Ця ініціатива передбачає скоординований підхід до надання соціальної допомоги та підтримки людей і сімей, які опинилися у складних життєвих обставинах. В рамках підсистеми кейс-менеджменту створять електронні кабінети отримувачів соціальних послуг, надавачів таких послуг та, власне, кейс-менеджерів. Кожна особа, яка претендує на отримання допомоги або вже її отримує матиме власний профайл, за яким можна буде оцінити становище такої особи чи родини, а також запобігти настанню складних обставин. Застосування ШІ та алгоритмів уже дозволило пришвидшити опрацювання заявок з кількох тижнів до 2-3 днів. Це дає сподівання, що після завершення бета-тестування система буде ще ефективнішою і у швидкості, і у точності результатів.

Отже, оптимізація процесів надання соціальної допомоги є необхідною у сучасному контексті, втім до методів і пропозицій слід ставитися надзвичайно обережно. Зокрема, не варто вдаватися до технологій, які згодом можуть використовуватися для політичного тиску, утисків чи переслідувань вразливих груп. Особливо, якщо такі технології не мають особливого нагляду і регулювання у національному законодавстві станом на сьогодні.

IX. Податково-митна сфера: про долю гучних анонсів

Американські розробники з компанії Salesforce вирішили, що ШІ може зарадити у побудові ефективної податкової системи. Так, вони створили автоматизовану систему AI Economist, яка ґрунтуючись на підході “навчання з підкріпленням” (від англ. “*reinforcement learning*”) навчає систему раціонально встановлювати податкову ставку та рівномірно розподіляти податки. Передбачається, що успішні рішення система запам'ятовує і в подальшому використовує для прийняття стратегічних рішень. У підсумку з'ясувалося, що ШІ вдалося вирахувати оптимальну податкову ставку за заданих умов, незважаючи на те, що з економічної точки зору рішення було радше неординарним (високі податкові ставки для працівників з найвищим і найнижчим рівнями доходу та низька податкова ставка для працівників

із середнім рівнем доходу). Чи життєздатні такі системи і чи реально їх застосовувати в Україні?

У червня 2023 року на форумі «Ключові антикорупційні та інституційні зміни для відновлення України» анонсували декілька напрямів цифровізації **Державної податкової служби (ДПС)**. В цілому, вони охоплювали сфери "великих даних" (від англ. "*big data*"), безпеки даних, комунікації та сервісів (і деяких адміністративних питань). При цьому, в рамках форуму наголосили, що збір інформації щодо податкових зобов'язань, проведення перевірок та розслідувань не має перетворюватися на своєрідну форму державного стеження. Тобто, в цьому випадку, державні органи виступають скоріше проти профайлінгу, ніж підтримують його, як це відбувається у соціальній сфері. Проте, на жаль, жодних подальших деталей щодо ШІ у фіскальній сфері ніхто не поширював, тож цілком існує вірогідність, що наразі проєкт поставлено на паузу або щонайменше відкладено у впровадженні.

Водночас, ще з 2019 року новинні шпальти майоріли інформацією про те, що ШІ активно використовується ДПС для моніторингу сільськогосподарських земель (за допомогою супутникових даних) для перевірки, чи вони використовуються за призначенням (наприклад, чи немає на них незаконної забудови). Ймовірніше за все, під час війни такі технології обмежені у використанні, але ініціатива все ж є прикладом позитивного використання ШІ для оптимізації ресурсів та превенції порушень. Втім, найближчим часом варто очікувати збільшення кількості проєктів у сфері ШІ оскільки закордоном перші шпальти вже тривалий час майорять успіхами систем у викритті податкових махінацій. Наприклад, у Франції за допомогою ШІ виявили 20,000 незадекларованих приватних басейнів.

Така практика не є новою - закордонні фіскальні органи вже досить давно використовують ШІ у своїй роботі. У США, наприклад, Державна податкова служба повідомила, що вона буде використовувати інструменти ШІ для виявлення потенційних порушень податкового законодавства. При чому, технології планується використовувати саме для відслідковування так званих "складних" схем ухилення від сплати податків, які переважно реалізують особи з високими доходами. На додачу до цього, українське Бюро економічної безпеки (БЕБ) нещодавно оголосило про співпрацю з Державною податковою службою США. Цікаво, що ще у 2022 році, БЕБ створило робочу групу для формування технічного завдання, щоб створити систему ШІ. Її "місією" було б прогнозувати ризики і загрози у сфері економіки, шукаючи і аналізуючи релевантну інформацію. Цілком можливо, українсько-американська співпраця може також стосуватися розвитку технологій ШІ для фінансового моніторингу.

Також в рамках роботи **Державної митної служби** у квітні 2022 року було отримано доступ до платформи AI HS Code Recommendation Platform (Всесвітня митна організація надала відкритий доступ). Цей інструмент дозволяє одержати перелік рекомендованих кодів для конкретного товару. При цьому перелік формується на основі введеного опису товару і статистичних даних щодо проведення митного оформлення товарів з подібним описом за попередні періоди. По суті, це дозволяє автоматизувати класифікацію товарів і уникнути ситуацій, коли відсутність даних у базі чи компетенції працівників ускладнює процес чи призводить до неправильних результатів перевірки. Водночас, тут важливим аспектом є навчання працівників Державної митної служби, аби вони правильно використовували систему, адже в українському контексті однією з поширених проблем є доступність технологій, але брак цифрових компетентностей персоналу державних органів та служб.

В цьому, зокрема, може зарадити обмін досвідом. Наприклад, у травні 2023 року в Угорщині відбулася конференція «Інновації в державному управлінні – робота з великими об'ємами баз даних і штучний інтелект у податковій та митній справі». В рамках заходу обговорили процеси діджиталізації комерційного документообігу та впровадження ШІ для контрольних функцій щодо фінансових операцій. Так, поміж іншого, експерти обговорили труднощі використання Гармонізованої системи для класифікації окремих категорій товарів та шляхи подолання таких проблем. З огляду на те, що питання митного контролю є значною мірою транскордонними, важливо забезпечувати міжнародну співпрацю і колективне вирішення технічних викликів.

X. Правосуддя: куди сховалася електронна Феміда?

І знову почнімо з іноземного досвіду. Свого часу в США активно застосовувалася система COMPAS. За допомогою функціоналу предиктивної аналітики вона могла прогнозувати ризики вчинення злочинів (як-от, ризик рецидиву) чи визначати так звані "гарячі точки" злочинності. На практиці з'ясувалося, що система дуже сильно віддзеркалює усі суспільні упередження і нерівності. Наприклад, якщо в в певному регіоні поширеною є дискримінація за расовою чи етнічною ознакою і це історично проявлялося у судових рішеннях - "згодувати" ШІ такі судові рішення означає навчити його діяти за подібним алгоритмом. Як наслідок, основні переваги автоматизації - як-от неупередженість, точність і швидкість - переважно нівелюються. Зокрема, показник ефективності COMPAS для прогнозування рецидивізму становив близько 65%, що ненабагато краще за звичайне

вгадування. Відповідно до досліджень Дрезель та Фарід, результати, аналогічні до висновків COMPAS, показали пересічні особи, які отримали в 20 разів менше інформації про засудженого, ніж автоматизована система. Дослідження Центру Дністрянського вказує, що жоден ШІ поки що не має показників точності, що сягають хоча б 90%, а 80% вірогідність правильної відповіді є надзвичайною рідкістю. Що це означає на практиці? Кожне п'яте(!) рішення про (не)скорочення строку перебування у закладах позбавлення волі потенційно буде хибним, якщо його приймати на основі даних ШІ, а не контекстуального індивідуального аналізу конкретного випадку.

Варто визнати, що COMPAS є скоріше радикальною технологією, яка приймає рішення щодо життєво визначальних питань. Як помітно з іноземної практики, сфера правосуддя є однією з найбільш проблемних та дискусійних в контексті застосування ШІ. Втім, в Україні в цій царині наразі ледве не найбільше різноманітних проєктів та ініціатив. Чи всі вони безпечні та надійні?

Проєкт "Кассандра" - COMPAS по-українськи. Міністерство юстиції у тестовому режимі почало використовувати програмне забезпечення на основі ШІ з досить романтичною назвою "Кассандра". На практиці пропонують систему, яка на основі опитника (97 питань) визначатиме схильність особи до повторного вчинення злочинів (рецидив), що згодом інтегруватиметься у досудову доповідь. Міністр юстиції Денис Малюська підкреслив, що за кілька років внаслідок машинного навчання буде достатньо даних, щоб "Кассандра" навчилася "*аналізувати відповіді не тільки на перелік простих запитань, а й аналізувати всі інші дані, які є про злочинця*". Актуальних даних щодо ефективності системи наразі немає. Це може свідчити про те, що переходу на другий етап проєкту, коли ШІ виходить за межі опитника і аналізує масиви даних комплексно, ще не відбулося. Однією з причин такого затягнутого тестового періоду може бути зміна державних пріоритетів на більш дотичні до воєнної сфери.

"Кассандра" вже встигла отримати декілька позитивних відгуків від експертів, які вважають, що автоматизована система здатна вирішити відразу декілька проблем Міністерства юстиції та системи пробації в цілому. Так, серед переваг ШІ виокремлюють його здатність більш комплексно оцінювати масиви даних і виокремлювати причинно-наслідкові зв'язки, вести облік ув'язнених і потреби держави з точки зору забезпечення місць позбавлення волі тощо.

Водночас, як помітно з опису системи, вона нічим принципово не відрізняється від ініціативи COMPAS (крім певно того, що в українському суспільстві прояви інституційної дискримінації все ж дещо менші, ніж у США). Втім, здатність системи ефективно визначати схильність до рецидиву, а також

відсутність інших дискримінаційних проявів (наприклад, за ознакою статі, віку, місця проживання чи рівня доходу) все ще залишається на порядку денному. Українські активісти та правозахисники скоріше б'ють на сполох, коли мова заходить про "Кассандру", адже ризики від неправильних результатів системи можуть бути дуже значними. І в такому випадку, єдиним позитивним фактором залишається те, що фінальне рішення все ж приймає людина, а не ШІ. Принаймні, доки "Кассандра" працює у тестовій версії.

"Суд в смартфоні". Перші анонси впровадження "суду в смартфоні" з'явилися ще у 2021 році, коли президент Зеленський до 30 річниці незалежності України оголосив про запуск проєкту як спробу боротьби зі зловживаннями у судовій сфері. Ініціативу впровадити повноцінний електронний суд підтримували в тому числі й судді Верховного суду. Наприклад, Олена Кібенко у своїй презентації щодо цифровізації українських судів висловилася на підтримку цієї ідеї через численні можливості, які відкриває онлайн-судочинство. Загалом, ідея "суду в смартфоні" далеко не нова, але зміст таких ініціатив різниться залежно від держави: так, в Китаї блокчейн використовують для засвідчення достовірності доказів, Франція ще з 2018 року активно говорить про впровадження ШІ у систему правосуддя, а в Естонії навіть ширилися чутки про розробку "робота-судді" для розгляду малозначних справ (щоправда, останнє виявилося неправдивим).

Втім, між появою ідеї та її реалізацією - часто прірва. Так, серйозним викликом став швидкий і ефективний запуск системи електронного судочинства, якість якого критикувала Державна судова адміністрація (ДСА). Фактично, до законодавчих змін прийняття документів в електронній формі залишалося дискрецією кожного судді. Тож, на практиці жодна сторона провадження не хотіла ризикувати відмовою чи додатковими клопотами. Тому, повноцінно українська реформа щодо "Суду в смартфоні" розпочалася з прийняття змін до Закону "Про судоустрій і статус суддів", які дозволили спростити процедуру доступу до судової системи, перевести багато елементів системи правосуддя у цифровий формат, а також пришвидшити документообіг і аналіз масивів даних. Це вдалося зробити завдяки запровадженню Єдиної судової інформаційно-комунікаційної системи (ЄСІТС), завданнями якої стало:

- формування єдиного інформаційного простору для органів системи правосуддя;
- міжвідомчий обіг та обмін інформації;
- прискорений розгляд судових справ та проваджень;
- автоматизація роботи;

- перехід на електронні версії документів, оцифрування судових архівів;
- швидкий доступ користувачів ЄСІТС до інформації з урахуванням прав доступу;
- конфіденційність, цілісність, доступність інформації в ЄСІТС;
- гармонізація правозастосування судами.

Втім, створення ЄСІТС це лише перший крок до застосування ШІ у судовій системі. Після цифровізації документообігу та оцифровки баз даних, наступною ініціативою мала стати розробка системи, що може вирішувати малозначні справи без участі судді. Ця ідея з'явилася у рамках Плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні, розробленим Мінцифри і погодженим Вищою радою правосуддя (ВРП). Ще у 2022 році планувалося запустити подібний проєкт на базі одного із судів першої інстанції, і стосуватися він мав розгляду ШІ судових справ адміністративного судочинства з формальним складом. На думку ВРП, в перспективі це дозволить встановити типові помилки, запобігати корупції та гармонізувати практику у справах цієї сфери. Після тестового періоду планувалося провести "роботу над помилками" і встановити, які саме законодавчі зміни необхідні для належного впровадження проєкту на загальнонаціональному рівні.

На практиці через повномасштабну російську агресію довелося перенести імплементацію проєкту - Мінцифри, ВРП, ДСА та Верховний суд оголошували про запуск у другому-третьому кварталах 2023 року. Проте жодних нових щодо успіхів ініціативи "Суд у смартфоні", виявлених прогалин чи необхідності певних законодавчих змін поки що публічно не оголошувалося. Ймовірніше за все, через бюрократичні питання вкотре затягнувся тестовий період. Втім, експерти наголошують, що запровадження такої системи є конче необхідним з огляду на воєнний стан та підвищену небезпеку проведення оффлайн-засідань, а також обмежений доступ до судів у прифронтових регіонах.

Щодо можливості повноцінно вписати такі новели в українське законодавство досі точаться дискусії. Хоча Європейська конвенція з прав людини (стаття 6 - право на справедливий суд) та Європейська етична хартія щодо використання ШІ в судочинстві та його середовищі не забороняє використання ШІ для вирішення судових спорів, стаття 127 Конституції України вказує, що судочинство може здійснюватися лише суддею (за певних обставин - присяжними). І тут цікаво, що Концепція розвитку штучного інтелекту передбачає, не лише розробку єдиних стандартів обліку судових рішень та інших даних провадження, а і "*винесення судових рішень у справах незначної складності*". Якщо тлумачити це положення буквально - воно ймовірно не відповідає Конституції. Саме тому, у Плані заходів

уточнюється, що на початкових етапах будуть лише аналізувати попередню практику у малозначних справах, щоб випрацювати оптимальні рішення і дослідити тенденції. Тобто очікувати на повноцінну заміну суддів системами ШІ не найближчим часом не варто. Принаймні, без змін до Конституції.

Крім того, у нещодавньому інтерв'ю заступник Міністра цифрової трансформації Олександр Борняков зазначив, що українські суди також планується посилити за допомогою Clearview AI (що радше є тривожним дзвіночком з огляду на репутацію цієї компанії). З іншого боку, Борняков згадав успіх декількох українських ініціатив, серед яких є і "**Суд на долоні**". Проєкт був розроблений ініціативною групою на кошти міжнародних донорів, втім зараз активно використовується і в державному секторі (наприклад, місцеві суди рекомендують його для підготовки до судових проваджень і навіть поширюють інструкцію з використання). За своєю суттю, "Суд на долоні" є комбінацією реєстрів (реєстру судових рішень та 14 інших, тематично дотичних баз даних), у якій за допомогою пошукових слів і 39 інших фільтрів можна знаходити необхідну інформацію, яка доступна у форматі відкритих даних. Сам проєкт має дві версії: спрощену (безкоштовну) та розширену (платну, з усіма відповідними фільтрами). При цьому, доступ для журналістів є безоплатним.

Згодом в рамках проєкту зробили додатковий модуль автоматичного аналізу - WINCOURT. Він здатен оцінити подібність документів, які завантажує користувач, до тих, на основі яких вже були вирішені подібні справи, і надає прогноз стосовно успішності судового розгляду. Спершу ефективність системи була посередньою, втім система регулярно оновлюється і доповнюється новими рішеннями. Як наслідок, користувачі мають змогу тестувати стратегію захисту в суді. Для господарського судочинства існує сервіс зі схожим функціоналом - Verdictum PRO.

Іронічно, що в часи, коли ШІ активно намагаються використовувати у судочинстві та сфері правосуддя в цілому, сама технологія стає об'єктом судових позовів. Втім, крім змістовних застережень щодо високої ризиковості пропонованих технологій, є і більш "приземлені" виклики. Так, експерти наголошують на необхідності спершу належним чином діджиталізувати українські суди - наприклад, банально забезпечити усі місцеві суди доступом до стабільного інтернету - і лише потім впроваджувати високі технології. Враховуючи перебої електрики, регулярні повітряні тривоги та часту неспроможність суддів проводити оффлайн-засідання, такий запит є як ніколи актуальним. Вирішення цього питання частково можливе за рахунок прийняття законопроєкту №8358, який дозволить дистанційну роботу суддів та провадження судочинства в онлайн-форматі. Втім,

законопроєкт залишається на розгляді з січня 2023 року. А без розвиненої цифрової інфраструктури та законодавчого регулювання будь-який, навіть найбезпечніший, “Суд у смартфоні” залишиться лише проєктом.

XI. Про сферу правопорядку або куди мігрують військові технології

У соцопитуванні Kantar Україна кінця 2023 року, 73% українців вказали, що ШІ може значно полегшити життя, тоді як найбільший потенціал вбачають для сфер оптимізації виробництва (54%) та боротьби з корупцією (51%). Водночас, не набагато меншою (38%) є підтримка ідеї застосовувати ШІ в безпековій сфері - зокрема, у роботі органів правопорядку. І тут досить іронічним є те, що незважаючи на результати опитування, використання систем ШІ для підтримання громадського порядку та розслідування злочинів уже триває. І триває значно довше, ніж про це задумувалася середньостатистична особа. Що відбувається із технологіями ШІ в правоохоронній сфері?

Камери відеостеження. Ще з 2019 року правозахисники б'ють на сполох щодо використання камер відеостеження, які мають функцію розпізнавання облич. Так, в рамках програми “Безпечне місто”, яка реалізувалася органами місцевого самоврядування, більшість обласних центрів були обладнані такими камерами. Закон “Про місцеве самоврядування”, при цьому, не наділяє органи муніципальної влади жодними повноваженнями у сфері стеження чи роботи з біометричними даними для підтримання публічного порядку. Деякі місцеві ради навіть встигли прийняти підзаконні акти, як-от Регламент використання та функціонування системи відеоспостереження міста Запоріжжя. Втім, навіть це не зняло проблеми відсутності законних підстав і відповідних повноважень в органів місцевого самоврядування. Коли дискурс щодо використання ШІ поліцією лише почав очолювати порядок денний, правозахисні організації вже активно критикували таку модель, наполягаючи на необхідності щонайменше розробити систему запобіжників від зловживань.

Втім, у 2021 році, на вебсайті Міністерства внутрішніх справ (МВС) з'явився проєкт “Безпечна країна” - таке собі масштабування ініціатив “Безпечне місто.” Важливо, що презентація проєкту не містила жодного слова про законодавчі зміни чи необхідність розширення повноважень органів правопорядку. Публічні виступи заступника Міністра внутрішніх справ Ігоря Бондаренка на початку 2022 року також не прояснили законодавче підґрунтя для впровадження цієї системи. Варто нагадати, що схожі ініціативи

вже пропонувалися у 2019 році, принаймні маючи форму законопроєктів, що намагаються визначити повноваження державних органів. Водночас, розширення повноважень передбачало нелімітований доступ поліції та інших органів правопорядку до вуличних камер (та в цілому інших інформаційно-комунікаційних систем). Це, в свою чергу, наштовхнулося на значну критику Головного науково-експертного управління парламенту. Саме тому, що у 2019, що в 2021 роках ініціатива не здобула значної підтримки.

Нова ітерація цієї дискусії ризикує початися "ще вчора", адже медійні заголовки початку 2024 року активно висвітлюють ідею запровадження єдиної платформи відеоспостереження. І, крім самого факту комплексної системи стеження, цікавою є і мотивація, яка підштовхнула МВС на такий крок. Як з'ясувалося з розслідування "Схем", відео з тисяч камер, встановлених по всій Україні, за допомогою російського програмного забезпечення TRASSIR, перш ніж потрапити на телефон чи комп'ютер споживача опиняється на серверах в Москві, які належать компаніям, що мають зв'язки з ФСБ. Ці камери активно закуповувалися як приватними, так і державними підприємствами, а обмеження на використання цієї технології з'явилося лише 27 лютого 2022 року - тобто вже після початку повномасштабного вторгнення. Серед державних структур, які використовували програмне забезпечення TRASSIR були Чорнобильська АЕС, Полтавська міська рада та Адміністрація морських портів. Важливо, що на момент, коли журналісти "Схем" брали інтерв'ю в заступника міського голови Полтави, система "Безпечне місто" працювала, а впевненості щодо змін у програмному забезпеченні не було.

Крім того, у 2023 році, на український ринок потрапило програмне забезпечення AziGuard від румунської компанії AziTrend. Це програмне забезпечення складається з софту TRASSIR, але його продають як румунський продукт. Тож небезпека використання технічного обладнання з країни-агресора нікуди не зникла. Ба більше, якщо наразі деякі державні органи досі використовують програмне забезпечення російського походження, запровадження єдиної платформи відеоспостереження може бути небезпечним.

Водночас, на Закарпатті при в'їзді на територію області осіб розпізнають за допомогою камер з ШІ. Відповідно до слів голови Закарпатської обласної військової адміністрації: "*безпідставне перебування поруч з об'єктами інфраструктури система відстежує, інформує правоохоронців і далі вживаються заходи - затримання чи опитування громадян*". Такі заходи активно використовувалися у травні 2022 року. Тоді осіб перевіряли щодо наявності їх фото та номерів автівок у системі, а у випадку їх відсутності - з ними проводила додатковий контроль поліція. Тобто, на відміну від звичної

ситуації, коли є база даних осіб, що перебувають у розшуку, в цій ситуації була загальна база даних всіх жителів області. Як наслідок, величезні масиви чутливих даних зберігалися представниками поліції. Чи використовується система зараз - невідомо, але її застосування зі зниженням рівня небезпеки в Закарпатській області і, тим більше, після завершення дії воєнного стану - явно буде непропорційним.

Зрештою, ще з 2021 року у Вінниці планувалося встановити систему "Vezha", яка давала б можливість розпізнавати обличчя, визначати параметри людей для подальшої ідентифікації, а також зчитувати номерні знаки на автомобілях, що рухаються навіть зі швидкістю до 250 км/год. Після анонсування жодних оновлень на цю тему не було, але наприкінці 2023 року оголосили про впровадження нової системи відеонагляду на Вінниччині. Хоч це й здійснюється в рамках проєкту щодо єдиної платформи відеостеження, ініціатива цілком може бути розвитком проєкту "Vezha". І тут важливо розуміти, наскільки надійними є технології, які стануть частиною загальної інтегрованої системи (оскільки до лютого 2022 року цим питанням не настільки переймалися на муніципальному рівні), а також яким буде обсяг законних повноважень і практичних можливостей, що отримають органи правопорядку після запуску системи.

Clearview AI. Початок використання цієї системи розпізнавання облич все ж таки стосується початку повномасштабного вторгнення і був мотивований потребою розпізнавати загиблих росіян для подальшого встановлення відповідальних за воєнні злочини. Втім, на практиці технологія "мігрувала" і в невійськову сферу (наприклад, компанія уклала договір про доступ до сервісу для МВС). У інтерв'ю в квітні 2023 року, Міністр цифрової трансформації Федоров зазначив, що сервіси Clearview AI вже впроваджені в роботу 14 державних органів (на вебсайті Clearview AI наразі згадано 18 агенцій). Серед планів "на перспективу" американська компанія повідомила про ідею впровадити інновації в українську митницю і банківську сфери. Також планувалося відкрити офіс Clearview AI у Києві, втім поки що жодних зрушень в цьому напрямку не було зроблено. І, напевно, на краще.

Для чого наразі використовують Clearview AI в Україні? Серед цілей використання згадують возз'єднання сімей, спростування неправдивих дописів у соцмережах, підвищення безпеки у пунктах пропуску (ідентифікація осіб на блокпостах), ідентифікація загиблих солдатів та виявлення російських шпигунів. При цьому, статистика станом на листопад 2023 року, що за допомогою системи було здійснено більше 350,000 пошуків. В інтерв'ю для медіа згадують, що принаймні 230,000 з цих пошукових запитів стосувалися загиблих солдатів. Тобто близько 100,000 запитів передбачали аналіз персональних даних живих осіб. Неодноразово Мінцифри зазначало

про ефективність технології Clearview AI і пришвидшення процесів, що дозволило перерозподілити ресурс для важливіших військових завдань. В чому ж проблема з настільки ефективною технологією?

- Мета і точність. У інтерв'ю для BBC правозахисники і експерти з безпеки наголошують, що використання Clearview AI як головної і єдиної підстави для прийняття рішень щодо життя і смерті є явно неправомірним кроком. І тут важливо, щоб органи правопорядку, які використовують технологію, теж це усвідомлювали. На жаль, жодних законодавчих (чи навіть підзаконних обмежень) наразі немає. Тож, теоретично, затримання особи чи навіть застосування зброї іноді може бути вмотивоване результатом роботи системи. При цьому про 100% точність таких результатів годі й казати. Зокрема, в новинах вже з'являлася інформація щодо помилок у ідентифікації осіб за допомогою Clearview AI. За відсутності впевненості у надійності системи, її точно не варто використовувати у ризикових контекстах, коли емоційна реакція на результат роботи системи, страх чи інші чинники можуть слугувати рушієм для фатальних наслідків.
- Порушення законодавства. Clearview AI неодноразово критикувався за нелегальний збір персональних даних - формування бази даних на основі інформації, зібраної з соцмереж (як виявляється на практиці, в тому числі і приватних сторінок і зображень). Неправомірні практики у сфері захисту даних стали не лише предметом теоретичної дискусії, а і підставою для численних штрафів (щонайменше у п'яти країнах). Наприклад, Clearview AI вже був вимушений заплатити 20 мільйонів євро італійському регулятору за незаконне використання персональних даних. Аналогічні спори виникали з французьким регулятором, де компанія вже декілька разів була оштрафована. Основна причина штрафів - нелегальний скрепінг даних - тобто збір великих масивів даних користувачів без їхньої згоди, а зачасту навіть без повідомлення про обробку даних.
- Технічна безпека. Враховуючи, що компанія чітко не розкриває принципів формування бази даних, цілком вірогідно, що інформація, яка аналізується в українському контексті, стає частиною загальної бази даних. Хоч сьогодні Clearview AI активно заявляє, що не співпрацюватиме з жодним актором, який вдається до порушень прав людини (наприклад. Росією), ніхто не може зі стовідсотковою впевненістю гарантувати. що технологія не потрапить до рук окупантів. Більше того, немає гарантій, що після чергового штрафу щодо недотримання правил захисту даних компанія не почне співпрацю з державами, які мають високий індекс порушень прав людини. В цьому випадку, йдеться навіть не про Росію, а про передачу даних до Китаю, Ірану чи інших авторитарних країн.

- Репутаційні ризики для України. Ні для кого не секрет, що репутація Clearview AI явно не найкраща. Компанія, маючи багато штрафів і скарг в національних юрисдикціях, намагається використати війну в Україні як спосіб відбілити власну репутацію (від англ. “whitewashing”). Зокрема, Clearview AI регулярно наголошує на ефективності системи в умовах збройного конфлікту, фактично не відповідаючи на змістовну критику - як-от на те, що компанія займається нелегальним збором даних. Україна також регулярно акцентує на користі від системи (як-от для ідентифікації членів незаконних збройних формувань в Криму), ігноруючи критичні питання щодо легальності технології.
- Євроінтеграція. Враховуючи, що оновлений після політичної угоди проєкт Акту про штучний інтелект містить заборону скрепінгу даних, Clearview AI, ймовірніше за все, потрапить до списку заборонених ШІ систем. Відповідно, факт використання Україною сервісів цієї компанії може суттєво вплинути на євроінтеграційні зусилля і рано чи пізно доведеться зробити вибір - використовувати ефективні, але неправомірні технології, порушуючи євроінтеграційні вимоги, або шукати альтернативи, що більш відповідні правам людини.

Серед низки проблем ключовою залишається фактична законодавча неврегульованість таких систем в Україні і відсутність будь-яких гарантій, що завтра програмне забезпечення Clearview AI не мігрує кудись далі - наприклад, у вуличні камери відеостеження чи в додаток “Дія”. І з огляду на кількість ризиків таке масове використання неправомірно створених технологій явно не можна виправдати суспільною необхідністю.

Розслідування. Державні органи, що діють у безпековій та правоохоронній сферах, почали активно розробляти системи ШІ або залучатися до проєктів їх розробки, аби ефективніше моніторити дотримання законодавства, відслідковувати порушення і розслідувати злочини. Наразі найбільше систем ШІ планують застосовувати у сфері економічних злочинів (адже це передбачає легшу процедуру аналізу даних порівняно з, наприклад, злочинами проти життя і здоров'я особи). Втім, цілком ймовірно у найближчі кілька років відбудеться масштабування таких технологій з огляду на активну міжнародну співпрацю України та обмін досвідом з державами, де ШІ часто відіграє ключову роль для розслідувань. Втім, що українські органи правопорядку використовують вже зараз?

- **Служба безпеки України (СБУ)**. На iForum очільник Департаменту кібербезпеки СБУ Ілля Вітюк розповів про ініціативу впровадження ШІ. Зокрема, це стосується розбудови власних нейромереж, розпізнавання ворожої техніки (через аналіз знімків і відео з камер спостереження),

а також інформаційної сфери (як-от моніторингу відкритих ресурсів для протидії дезінформації). Деталей щодо масштабу застосування технологій наразі не оприлюднюють, втім важливо, щоб моніторингові ініціативи не виходили за межі воєнного стану, залишаючись частиною "побуту" безпекових служб після української перемоги.

- **Національна поліція України (Нацпол)**. В різних куточках земної кулі поліція масово використовує ШІ для відстеження злочинців, і Україна не є винятком. Так, ще в 2017 році Департаменті патрульної поліції створили підрозділ аеророзвідки, оснащений останніми зразками дронів. Їх, зокрема, використовували для виявлення незаконних посівів маку і конопель, вирубки лісів і насаджень, місць незаконного видобутку бурштину і вугілля тощо. Крім того, з початком повномасштабного вторгнення Нацпол використовує ШІ для ідентифікації осіб на блокпостах (йдеться як про розпізнавання облич за допомогою систем на кшталт Clearview AI, так і про використання систем для перевірки документів, пошуку за базою даних тощо).
  Зрештою, ШІ застосовують для пошуку зниклих безвісти, серед яких і діти. Зокрема, за ініціативи Уповноваженого з питань осіб, зниклих безвісти за особливих обставин, Україні намагається знайти осіб, які внаслідок воєнних дій або вчинення воєнних злочинів (примусового переселення) опинилися на території Росії. Для цього використовують додаток Reunite Ukraine, розроблений у співпраці з американською компанією Find My Parent. Застосунок передбачає можливість створити власний профіль і профіль особи, яку шукають. Потім система порівнює дані різних заповнених профайлів і, якщо встановлюються збіги, люди можуть обмінюватися повідомленнями. Як наслідок, що більше інформації буде надано - то більше шансів, що вдасться знайти загублених родичів. В додатку також можуть зареєструватися усі охочі і передати інформацію про українських дітей, що перебувають в Росії чи на окупованій території.
- **Національне антикорупційне бюро України (НАБУ), Спеціалізована антикорупційна прокуратура (САП)**. В рамках Національної програми інформатизації планується посилити спроможності антикорупційних органів щодо обробки великих масивів даних. Директор НАБУ Семен Кривонос повідомив, що Агенство планує використовувати ШІ під час розслідування кримінальних справ для аналізу масивів даних та відстежування взаємозв'язків (зокрема, на основі аналізу трафіків, довіреностей та прописок, розпізнавання обличчя та транскрибування аудіо у текстові повідомлення). Кривонос уточнив, що система здатна до самонавчання і розроблятиметься приватною компанією. Хоча конкретних деталей не було озвучено, за описом такі здатності має, в тому числі, програмне забезпечення Clearview AI. З огляду

на те, як українські державні органи дуже прагнуть співпрацювати з цим “магнатом персональних даних”, саме час згадати невеселі думки щодо порушень приватності. Єдине, що змушує сподіватися на краще - система використовуватиметься під контролем операторів. Тільки-от чи справді це зменшить ризики, а не, до прикладу, призведе до цільових атак на конкретних підприємців, активістів, представників медіа чи інші вразливі групи? Жодних гарантій наразі немає навіть “на папері”.

Окрім того, НАБУ разом із САП наразі використовують eCase Management System для обміну документами із Вищим анти корупційним судом (ВАКС) та внутрішньої організації завдань (як-от встановлення дедлайнів, створення календаря завдань, оперативний обмін даними тощо). Наприклад, на кінець 2023 року в системі доступні 70 шаблонів процесуальних документів, що знімає майже 90% паперової роботи з детективів. Працює система на підставі спільного наказу НАБУ, Офісу ГПУ, Ради суддів і ВАКС, яким в 2021 році затвердили Положення про інформаційну-телекомунікаційну систему досудового розслідування. В цьому випадку, після тестового періоду вирішили розробити нормативне регулювання, яке досить чітко регламентує порядок використання системи, умови доступу до неї та її можливості.

- **Національне агентство з питань запобігання корупції (НАЗК)**. У грудні 2023 року НАЗК оголосило про використання нових автоматизованих інструментів для перевірки декларацій. Зокрема, йдеться про порівняння даних у декларації з іншими реєстрами, перевірку певними “формулами” (як-от, щодо наявності ознак незаконного збагачення, необґрунтованих активів тощо). Лише декларації з найнижчим рейтингом ризику будуть перевірятися автоматизовано, а декларантів повідомлятимуть про проведення такої перевірки. Таким чином планується перевіряти 30% від загальної кількості декларацій. В цілому, автоматизація є логічним кроком, адже кількість декларацій, які мають проходити перевірку збільшилася після ухвалення змін до антикорупційного законодавства.

  Крім того, НАЗК використовує ШІ для моніторингу політичної реклами в Інтернеті, що, поміж іншого, включає аналіз текстової інформації за допомогою автоматизованих систем. Втім, жодних деталей щодо цієї ініціативи наразі немає.

- **БЕБ**. Як вже згадувалося раніше, БЕБ активно співпрацює із Державною податковою службою США для виявлення злочинів у податковій сфері. На додачу до цього, БЕБ наразі працює над створенням нейронної мережі на основі ШІ, яка буде призначена для пошуку та аналізу інформації, а також прогнозування ризиків у сфері

економіки. На думку БЕБ, це дозволить розслідувати економічні злочини без впливу людського фактора, що знизить ризик корупції та мінімізує тіньовий сектор. Для розробки проєкту зібрали велику робочу групу, до складу якої увійшли і представники Офісу Генерального прокурора (ГПУ), і МВС, і СБУ, і, ДПС, і навіть Збройних Сил України. Єдиним питанням тут залишається обсяг моніторингу, який можна здійснювати за допомогою такої системи та наявність запобіжників від зловживань і надмірного втручання у приватне життя осіб та підприємницьку діяльність.

Як наслідок, існує досить багато ініціатив щодо використання ШІ у правоохоронній сфері, але більшість систем, які пропонуються до використання, описані у дуже загальних рисах, що часто не дає змоги встановити, наскільки інтрузивними вони є або можуть стати для прав людини. Брак прозорості є однією з найбільших проблем в тому числі і для обговорення технологій, застосовуваних органами правопорядку, з представниками академічних інституцій, громадянського суспільства і громадськості в цілому. В інших випадках (як-от камери з функцією розпізнавання облич чи Clearview AI), проблема полягає у високій ризиковості або відвертій неправомірності систем. На жаль, наразі українське законодавство не надає достатніх гарантій і запобіжників від зловживань або потенційних порушень, а також механізму для оскарження шкоди, яку можуть спричинити такі системи. Більше того, в багатьох випадках держава має доступ до альтернативних механізмів, які не є настільки інтрузивними, втім віддає перевагу механізмам, які легше імплементувати.

XII. Оборонна сфера: індустрія єдиним фронтом

Голова Служби безпеки Великої Британії (MI5) Кен МакКаллум та його колеги зі Сполучених Штатів, Канади, Австралії та Нової Зеландії наголошують на загрозах від ШІ, особливо у сфері “перегонів” розробок у військовій сфері. Так, Сили оборони Ізраїлю активно використовують ШІ для планування авіаударів та матеріально-технічного забезпечення армії. Поки що такі технології застосовуються з людським наглядом та авторизацією кожної критичної дії. Та чи довго це триватиме з огляду на динаміку розвитку технологій в сучасних конфліктах?

Ідеї використовувати системи ШІ в українській оборонній сфері обговорювалися ще задовго до повномасштабного вторгнення. Зокрема, у серпні 2021 року Укроборонпром та Мінцифри підписали меморандум про цифровізацію оборонної сфери, в тому числі за допомогою ШІ. Серед

пріоритетів під час обговорення наголосили на сферах кібербезпеки, а також розробки зброї нового зразка (на кшталт безпілотників з ШІ). Ці новели стали як ніколи актуальними з новим витком російської агресії в Україні у лютому 2022 року.

Нещодавно DOU зробили великий путівник компаніями, що розробляють військові технології, з'ясувавши, що наразі їх існує близько 46. Серед ініціатив є багато керованих ШІ систем. Враховуючи, що з повномасштабного вторгнення межа між приватними розробниками військових технологій і державними ініціативами стала дуже розмитою, бо в результаті всі технічні новації так чи інакше потрапляють у підрозділи Генштабу Збройних Сил України (ЗСУ), Нацгвардії чи Міністерства оборони України (Міноборони), в цьому аналітичному матеріалі ми розглянемо проєкти, які підтримуються, координуються, фінансуються чи прямо реалізуються державою. Серед пріоритетів держави Міністр цифрової трансформації Федоров виокремив фіксування переміщення техніки і ворожого особового складу, збиття ракет та ефективне наведення цілей безпілотників.

Clearview AI. Як вже згадувалося в аналізі застосування ШІ органами правопорядку, основною метою застосування Clearview AI в Україні була спроба вирішувати військові завдання за його допомогою. Серед них, зокрема, ідентифікація російських загиблих солдатів (для подальшого повідомлення їхніх родичів) та російських військових, які вчиняли на території України воєнні злочини (з метою притягнення до відповідальності). Хоч, як розпізнавання облич померлих осіб, так і пошук воєнних злочинців можуть виправдати використання таких технологій, багато питань щодо репутації компанії, її надійності і подальшого використання сервісів залишаються без відповіді. Більше того, мають існувати серйозні гарантії того, що Clearview AI не будуть використовувати для прийняття рішень “життя і смерті” без додаткової перевірки і залучення людського фактору.

Водночас, навіть розпізнавання облич на блокпостах за допомогою Clearview AI вже не буде пропорційним у всіх випадках. Якщо йдеться про застосування подібних заходів при перетині кордонів між, до прикладу, Вінницькою і Хмельницькою областями, де на третьому році повномасштабної війни навряд очікують на диверсійні групи, актуальним є пошук менш інтрузивних і більш відповідних правам людини технологій.

Тож навіть коли йдеться про використання послуг компанії для цілей отримання переваги у збройному конфлікті, варто чітко розмежовувати військове використання ШІ та його плавний перехід у цивільну сферу. Другий варіант, детально проаналізований у попередньому розділі, є явно небажаним. В той час як перший - має альтернативи, які за два роки

повномасштабної російської агресії можна було протестувати і почати застосовувати. Наприклад, вже почали використовувати послуги Primer (збір і трансляція аудіоматеріалів, усунення шуму, переклад та виділення ключових тверджень, які стосуються інформації на полі бою) та Scale AI (аналіз зображень). Більше того, українські розробники YouControl і Artellence створили систему "ТиХто", яка дозволяє перевіряти номери паспортів і ПІП осіб і звіряти їх з базою "Миротворця". Комбінація таких сервісів цілком може замінити неправомірні за своєю природою послуги Clearview AI.

Системи ситуаційної обізнаності. Наразі активно використовують небойові автоматизовані технології - як-от, системи ситуаційної обізнаності. Їх уже є досить багато - зокрема, не так давно анонсували впровадження системи Vegvisir Core, багато проєктів у цій сфері має і профільна громадська організація "Аеророзвідка". Водночас, в цій галузі двома найбільшими і наймасштабнішими проєктами є Palantir та Delta (більш цільовими аналогами є "Кропива", "Дзвін" (щодо якого, до слова, були звинувачення у відмиванні коштів), "Віраж-планшет", "Броня", "ГісАрта" та інші). Тож, давайте з'ясуємо, якими є їх особливості та чи не створюють вони ризиків схожих до тих, які несе Clearview AI, а якщо так - чи є достатні запобіжники від зловживань і потенційної шкоди?

- **Palantir.** На початку повномасштабного вторгнення провідна IT-компанія, яка є одним з найбільших постачальників програмного забезпечення та хмарних рішень, оголосила про партнерство з Мінцифри. Основний продукт - Palantir Edge AI - модульна система, яка містить різні набори даних і може налаштовуватися на різні завдання. На практиці її часто порівнюють з Lego для автоматизації процесів. Наразі найчастіше застосування системи - візуалізація місцевості (перенесення даних із супутників та інших джерел на карту). Однією з останніх розробок компанії є Skykit - мобільний центр розвідки, який вже активно використовують на полі бою. Водночас, розробники систем наголошують, що вони не є провайдерами даних, надаючи лише технічні інструменти і аналітику. На практиці система збирає інформацію від комерційних постачальників (комерційних супутників) і об'єднує дані з різних джерел. Така система показала свою ефективність під час деокупації Херсонщини. Важливо, що система отримує дані легально, а обсяг отримуваної і фільтрованої інформації адаптує до запиту - варіює кількість джерел залежно від мети і часових проміжків.

  Також систему використовують для викриття воєнних злочинів. Таке застосування і розширення можливостей фактично сталося на запит Офісу ГПУ, який оголошував про потребу використовувати технологію для систематизації та аналізу доказів воєнних злочинів, вчинених росіянами.

Держава планує продовжувати співпрацю з Palantir у сфері відбудови України та цифровізації. Зокрема, Мінцифри підписало з компанією меморандум про подальшу співпрацю, а Palantir вже працює над створенням продуктів у сфері освіти, розмінування та за іншими напрямками. Наприклад, з метою розмінування територій платформа інтегрувала 82 набори даних, що поєднує 6 мільйонів будівель, 60,000 потягів і 1 мільйон сегментів доріг. За допомогою супутникових знімків встановлюється нещодавня активність на цих територіях, а також рівень ушкоджень, що дозволяє визначати пріоритетність розмінування. Компанія вже має офіс в Україні, а нещодавно анонсувала проєкт з розробки ШІ для оптимізації закупівлі продукції та поповнення запасів. Компанія також активно співпрацює з українськими розробниками.

- **Delta.** Український аналог Palantir, який дозволяє аналізувати дані щодо бойових дій у режимі реального часу, інтегрує інформацію про супротивника від різних сенсорів і джерел, і може працювати на будь-якому пристрої – навіть в мобільному телефоні. Фактично, система переносить інформацію у хмарне сховище, а в майбутньому ще і підтримуватиме критичні сервери. Важливо, що розроблена Центром інновацій і розвитку оборонних технологій Міністерства оборони України система побудована за стандартами НАТО, що було підтверджено у червні 2023 року. Крім того, у Delta інтегровані два чат-боти Мінцифри і СБУ - «єВорог» і «STOP Russian War» відповідно. Зазначають, що система готова інтегрувати навіть винищувачі F-16. Деяку інформацію в системі верифікують в ручному режимі, а також можуть обмежувати доступ до певних шарів системи, надаючи його вузькому колу осіб. Також зазначають, що ШІ у Delta постійно навчається і покращує систему.
  В цілому, Delta вважається однієї з найнадійніших систем сьогодні в Україні (у військовій сфері) і використовується (на відміну від Palantir) лише для військових цілей. Втім, два акаунти росіянам вдалося зламати за допомогою фішингу (тобто питання було на рівні цифрової грамотності користувачів, а не технічного захисту системи). Ситуацію швидко виправили, забравши у відповідних акаунтів доступ.

Тобто обидві системи (як і згадані секторальні аналоги) є хмарними і дозволяють оперувати інформацією незалежно від серверів. Крім того, вони показують досить високий рівень технічного захисту, а у випадку Delta - ще й чітке військове призначення. Ба більше, на відміну від Clearview AI, системи легально оперують даними і обробляють чутливу інформацію.

Армія дронів. Державна програма передбачає системну закупівлю, ремонт і заміну дронів. В рамках проєкту на фронт відправили вже близько 2000

дронів, оснащених ШІ. Основні функції передбачають безпечну розвідку, коригування артилерії та пошук навіть добре замаскованих супротивників. Також система ШІ дозволяє стабілізувати дрони та утримувати заздалегідь обрану ціль. Кількість національних проєктів у цій сфері постійно збільшується після Постанови Кабінету Міністрів України, яка стимулює виробництво і закупівлю безпілотників, а також 40 мільярдів гривень інвестицій в українське виробництво.

Одним із прикладів таких безпілотників з ШІ є система SAKER SCOUT, яка здатна самостійно розпізнавати і фіксувати координати ворожої техніки, передаючи інформацію у командний пункт в режимі реального часу. Розробники переконують, що система також може працювати повністю автономно, розрізняючи 64 типи цілей. Проєкт має як дрони-розвідники, так і дрони-камікадзе.

Одним з найважливіших питань, втім, залишається проблема належного нагляду за діяльністю систем ШІ. І особливо актуальним це є для військової сфери. Наразі розгортається дискурс щодо використання Росією дронів із повністю автономними системами наведення. Критика полягає у можливості помилкової ідентифікації цілей. Навіть виконавчий директор Palantir Алекс Карп зазначає, що на полі бою є "великі етичні проблеми", що часто передбачає дилему між належним захистом держави і спробою не втратити воєнну перевагу. Чи має Україна відповісти аналогічними технологіями, зберігши своєрідний "статус кво" у гонці озброєнь? Наразі експерти переймаються, що навіть використання протитанкових автономних дронів є нелегальним, адже зрештою призводить до людських жертв. Тому міжнародні організації закликають не поступатися принципом людського контролю (від англ. "human-in-the-loop") заради швидкого отримання військової переваги. Втім, питання залишається у пошуку альтернативи, яка буде достатньо ефективною, щоб переважити використання автономних дронів російською стороною. І це вже ризикує стати справжнім викликом.

Brave1. Державний кластер, що координується Мінцифри, Міноборони, Генштабом ЗСУ, Радою національної безпеки і оборони, Міністерством економіки та Міністерством стратегічних галузей промисловості, і об'єднує представників військової індустрії під "однією парасолькою". В рамках цього кластеру розробники мають можливість отримувати державні гранти і підтримку, а також отримувати доступ до центрів досліджень і розробок. Долучитися може будь-який розробник, а серед пріоритетних сфер виокремлюють і ШІ (який взагалі оголошено пріоритетом на 2024 рік). Наразі у Brave1 зареєстровано 35 розробок з ШІ, з яких 29 пройшли військову експертизу (тобто є ефективними на практиці і відповідають стандартам у сфері гуманітарного права).

Однією з найяскравіших ШІ-розробок в межах кластеру є система ситуаційної обізнаності Griselda. Вона є інтегрованою у Delta і дозволяє збирати розвідувальні дані. Відповідно до опису, від появи інформації в системі до її отримання проходить 28 секунд. Інформація проходить 4 ступені перевірки і лише після цього передається військовим. Працює система за принципом диверсифікації джерел даних. Кількість ініціатив в рамках Brave1 постійно збільшується, а сама наявність кластеру дозволяє не лише координуватися, а і контролювати вид та якість військових технологій, які на сьогодні розробляються в Україні.

Інші технології. Ще в червні 2022 року повідомили, що Київ захищає ППО оснащене ШІ, який визначає траєкторії польотів об'єктів і дозволяє за потреби спрацювати на випередження. На додачу, у військовій сфері планують використовувати просунуті медичні технології (зокрема, так звані "розумні жетони"), прогнозують і швидкий розвиток сфери біонічного протезування, щоб адресувати потреби поранених військових. Також активно розробляють застосунки для моделювання бойових дій та подальшого стратегічного навчання, окремі месенджери для військових, технології для пошуку загиблих та зниклих безвісти військових та багато інших секторальних ініціатив. Більшість з них є не комплексними рішеннями, а скоріше цільовим вирішенням проблем у оборонній сфері. Міноборони навіть організовує Хакатони для пошуку найкращих рішень та подальшої колаборації з такими розробниками. Майже всі ініціативи є приватними (що знову ж таки породжує питання - яким чином потім буде регулюватися транскордонна торгівля такими технологіями та контроль за їх експортом з України).

Зрештою, використовується багато технологій, дотичних до військової сфери - наприклад, Міністерство аграрної політики та продовольства застосовує ШІ для мапування потенційно небезпечних територій. Це значно пришвидшує процеси розмінування звільнених територій і дозволяє убезпечити людські життя при ідентифікації небезпечних зон. Розмінування здійснюватиметься в рамках Стратегії, розробленої Міністерством економіки України, яка робить значну ставку саме на системи ШІ. Як зазначалося, не останню роль в цьому грає компанія Palantir. Наразі існує багато розробок у сфері машин для розмінування, а також БПЛА, які можуть швидко і ефективно виявляти міни. Після завершення війни Міноборони планує запропонувати Україні нову стратегію розвитку армії - Future Force Concept, яка буде враховувати технічні можливості і ефективно їх використовувати для вибудування архітектури внутрішньої та глобальної безпеки.

Рекомендації

Активне і, фактично, повсюдне використання ШІ в українському публічному секторі вказує на ефективність спроб діджиталізації, а також - на популярність цієї теми. Втім, напрацювання у сфері розробки адекватної правової бази, що може підкріпити практичні новели, з'явились відносно нещодавно. Більше того, вони значною мірою віддзеркалюють міжнародні тренди, які є загальними, водночас оминаючи багато проблем, притаманних українській правовій системі та контексту. Хоча більшість ініціатив відповідають тенденціям у сфері діджиталізації, деякі з них потребують як практичного доопрацювання, так і законодавчого підґрунтя. Саме тому, Лабораторія цифрової безпеки пропонує звернути увагу на такі питання при формуванні політики у галузі ШІ:

- В майбутньому потрібно **розробити загальну регуляторну рамку**, яка буде адекватно імплементувати міжнародні стандарти у сфері ШІ на національному рівні. При цьому, Цифролаба підтримує підхід, що передбачає відтермінування імплементації Акту про штучний інтелект з огляду на необхідність визначитися, як Україна може адаптувати вимоги документу без доступу до європейських інституцій, а також загалом зрозуміти, яким чином варто застосовувати регулювання на практиці. З огляду на це, Цифролаба вітає впровадження “м'якого” регулювання через розробку загальних та секторальних рекомендацій та стимулювання інститутів саморегулювання.
- На додачу до загального регулювання ШІ, **тематичні і цільові зміни до законодавства** потрібно дизайнувати та імплементувати вже зараз, щоб забезпечити громадян належними гарантіями від зловживань. Зокрема, це є особливо актуальним для сфери правосуддя, правоохоронної сфери, військової сфери.
- Потрібно адаптувати законодавство про **публічні закупівлі** до систем ШІ. Наприклад, напрацювати підзаконні акти, які встановлюють мінімальні стандарти до розробників систем ШІ, дизайнованих для публічного сектору, вимоги до проведення тендерів та інші гарантії. Так, DOZORRO впроваджує модель машинного навчання для виявлення ризикових закупівель, але існує потреба регламентувати і систему закупівель самих систем ШІ. Особливо, враховуючи, що багато розробок передбачають державно-приватне партнерство.
- Слід розробити прийнятну **модель регулятора у сфері ШІ** та адекватно вписати його у функціонуючу правову систему. Зокрема, слід враховувати наявність тематичних регуляторів, як-от Національна рада з питань телебачення і радіомовлення і майбутній регулятор у сфері

захисту персональних даних. Напрацювання моделі регулятора також передбачає дизайн системи скарг - визначення кола суб'єктів скарг, тем і того, який орган буде їх розглядати.

- Слід **позбутися систем ШІ, які працюють на російському, білоруському, китайському або іншому програмному забезпеченні**, що походить з країн з високим індексом порушення прав людини. Держава має пересвідчитися, що після виявлення факту зв'язку систем ШІ з такими країнами їх не використовують щонайменше у публічному секторі (зокрема, це потребує як мінімум реакції на розслідування "Схем" щодо системи TRASSIR), а в ідеалі - заборонити такі системи на території України навіть для приватних акторів. Також держава має контролювати, щоб таке програмне забезпечення не потрапляло на український ринок - і зокрема в публічний сектор - як закордонний продукт, завезений через треті держави.
- Державі потрібно заздалегідь **розробити стратегію перехідного періоду** між воєнним станом і мирним часом, яка після української перемоги передбачатиме правовий та практичний механізми для вилучення технологій, призначених для застосування винятково під час дії воєнного стану. Зокрема, це дозволить попередити іноземні компанії, що надають послуги, актуальні під час війни, про плавний та чіткий алгоритм щодо припинення використання деяких сервісів або застосування до них абсолютно інших стандартів (більш обмежувальний підхід в оцінці пропорційності втручання у права людини тощо).
- Державі варто **уникати застосування технологій, які за замовчуванням порушують права людини**, як-от міжнародні стандарти у галузі захисту персональних даних, протидії дискримінації, створюють ризики переслідувань тощо. Наприклад, слід розглянути альтернативи до сервісів Clearview AI, особливо враховуючи заборону скрепінгу в Акті про штучний інтелект і пов'язані з цим проблеми для процесів євроінтеграції України.
- Державі слід розробити **систему технічних стандартів**, що передбачає мінімальні вимоги до розробників систем та оцінити перспективи створення органу, який буде відповідальним за сертифікацію систем ШІ, або покладення таких обов'язків на вже існуючий орган.
- Державі варто проводити **оцінку ризиків систем ШІ**, які застосовуються у публічному секторі, на всіх етапах життєвого циклу таких систем. При цьому, можна керуватися різними методологіями, включно з HUDERIA, в якому Україна і так долучена до тестової фази проєкту. Оцінка впливу, поміж іншого, має враховувати можливість створення охолоджуючого ефекту (від англ. "chilling effect") на права людини та стимулювати державу мінімізувати його і розробляти запобіжники від зловживань.

- Держава має **розробити уніфіковану систему маркування контенту, генерованого системами ШІ**, для забезпечення більшої прозорості щодо функціонування систем, а також уникнення безвідповідального поширення неправдивої інформації.
- При наданні публічних послуг за допомогою систем ШІ, держава має **забезпечити можливість легко і зрозуміло контактувати з операторами-людьми**. Зокрема, варто уникати ситуацій, коли автоматизована система є зацикленою або забирає надміру багато часу на розмову з ботом (прикладом таких систем у приватному секторі є описані у дослідженні Texty.org популярні банківські чат-боти і системи телефонних операторів, які мають дуже незручні алгоритми, що не дозволяють реалізувати право не бути підданим впливу автоматизованих систем).
- Державі варто забезпечити **відкритий код для систем ШІ**, які використовуються у публічному секторі (крім технологій у сфері безпеки та оборони), щоб уможливити пошук прогалин незалежними експертами та ефективний контроль громадськості за видом і особливостями застосовних систем, їх впливом на права людини.
- Після анонсування ініціативи впровадження системи ШІ у певному публічному секторі державі слід **регулярно оновлювати інформацію** щодо результатів тестових періодів, проблем, з якими стикнулися під час застосування системи, стадії імплементації проєктів тощо, щоб забезпечувати принцип прозорості та дозволяти ефективний громадський контроль за впровадженням проєктів та їх надійністю і безпечністю.
- Державі варто **продовжувати міжнародну співпрацю** як на рівні колаборацій з компаніями, так і на рівні кооперації в рамках регуляторних ініціатив на кшталт Комітету Ради Європи зі штучного інтелекту. Це дозволить відслідковувати останні тенденції та формувати міжнародний порядок денний з урахуванням українського досвіду застосування ШІ.
- Державі варто **забезпечити участь громадянського суспільства** при обговоренні ідей запровадження систем ШІ в публічному секторі, та враховувати результати таких обговорень при прийнятті політичних та законодавчих рішень, напрацюванні візійних документів та стратегій.
- Державі варто інвестувати зусилля у **посилення цифрової грамотності публічних службовців**. Зокрема, хорошими ініціативами в цій царині є освітні проєкти в рамках Дія.Освіта. Втім, заохочується також проведення більш цільових тренінгів, особливо для публічних

службовців, які регулярно мають справу зі складними високо ризиковими ШІ системами.

- При **напрацюванні освітніх програм для розробників ШІ** держава має включати у навчальні плани такі дисципліни як етика і міжнародні стандарти у сфері захисту прав людини для забезпечення побудови систем ШІ, які за замовчуванням є етичними і відповідають правам людини та демократичним принципам.

Наостанок, як би не рухалися процеси міжнародного регулювання сфери ШІ, напрацювання національних практик має відповідати базовим принципам і стандартам у сфері захисту прав людини незалежно від наявності галузевого регулювання. Контроль за такою відповідністю, в свою чергу, неможливий без залучення усіх зацікавлених сторін та створення середовища, яке фасилітує вільну дискусію. І варто пам'ятати, що ігнорування викликів і небезпек сьогодні створить більше проблем завтра. Тож, краще не відкладати пошук рішень у далеку скриню, а шукати способи збалансувати інтереси стейкхолдерів уже зараз.

Лабораторія
Цифрової
Безпеки