Майбутнє національної безпеки, ймовірно, передбачатиме тісну співпрацю між людьми-операторами та системами ШІ. Це може включати вдосконалені ШІ системи підтримки прийняття рішень для командирів, ШІ-пілотів винищувачів або помічників ШІ для аналітиків розвідки. Розробка ефективних протоколів та інтерфейсів для об'єднання людини та штучного інтелекту буде ключовою сферою уваги.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Adam Kilsby (2024). Artificial intelligence: threats and opportunities in national security. *Zaizi.* URL: https://www.zaizi.com/blog/artificial-intelligence-threats-and-opportunities-in-national-security/

2. Застосування штучного інтелекту у сфері національної безпеки та обороноздатності держави (2024). *Сідкон.* URL: https://sidcon.com.ua/tpost/7vuygong71-zastosuvannya-shtuchnogo-ntelektu-u-sfer

Діордіца Ігор Володимирович,
д.ю.н., професор, професор кафедри приватного та публічного права,
Київський національний університет технологій та дизайну (м. Київ)

НОРМАТИВНО-ПРАВОВИЙ АНАЛІЗ ПРОБЛЕМАТИКИ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ УКРАЇНИ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ З УРАХУВАННЯМ ДОСВІДУ ОЛІМПІЙСЬКИХ ІГОР В ПАРИЖІ 2024 РОКУ

На початку 2024 року, із метою гарантування безпеки під час проведення Олімпійських ігор в Парижі, французький уряд уклав контракти з чотирма компаніями – Videtics, Orange Business, ChapsVision та Wintics, які активно використовують можливості штучного інтелекту (ШІ).

Наріжним каменем впровадження технологій ШІ задля забезпечення безпеки Олімпійських ігор стала позиція низки правозахисних організацій щодо використання системи розпізнавання облич.

Так, 23 листопада 2022 року у французькій газеті Le Parisien було опубліковано статтю, в якій інформувалося про те, що уряд Франції відмовився від проєкту впровадження системи розпізнавання облич для підтримки заходів безпеки на Олімпійських іграх 2024 року в Парижі [1]. Однак, дебати про можливе впровадження систем розпізнавання облич під час Олімпійських ігор набули широкої дискусії, яка розділила політичних лідерів, науковців, новаторів сегменту ШІ щодо того, чи необхідно використовувати біометричні системи, керовані штучним інтелектом, для моніторингу громадських місць.

Незважаючи на те, що французький уряд для забезпечення безпеки спортивних заходів під час Олімпійських ігор 2024 року в Парижі зрештою відмовився від свого проекту з розпізнавання облич, він вирішив дозволити впровадження інших відеопристроїв, керованих штучним інтелектом.

Тобто, замість розгортання технологій розпізнавання облич французький уряд обрав іншу технологію, яка є менш інвазійною, а саме використання смарт-камер. Основна відмінність між смарт-камерами і розпізнаванням облич полягає в тому, що в той час як метою розпізнавання облич є ідентифікація або автентифікація особи, смарт-камери можуть мати кілька цілей, починаючи від аналізу і закінчуючи категоризацією об'єктів або осіб.

Смарт-камери не обробляють біометричні дані і не призначені для ідентифікації осіб. Однак, навіть якщо смарт-камери не обробляють біометричні дані, це не означає, що вони не становлять ризиків для прав і свобод людини, оскільки вони можуть обробляти інші типи персональних даних. Це також означає, що їх слід вважати більш інтрузивними, ніж «традиційні» системи відеоспостереження, оскільки, як пояснює CNIL, смарт-камери за своєю природою дуже відрізняються від традиційних систем

відеоспостереження, оскільки «людей більше не просто знімають, а аналізують в автоматизованому режимі, в реальному часі, щоб зібрати певну інформацію про них» [2].

Ризики, які становлять системи розумних камер, залежать від мети і способу їх використання. Наприклад, система, яка впливає або приймає рішення, що індивідуально впливає на людину, не становить такого ж ризику, як система, спрямована на невизначену групу людей або розгорнута в статистичних цілях.

У Франції немає спеціального закону, який би регулював використання розумних камер, однак це не означає, що ці системи не підлягають регулюванню або що вони де-факто дозволені чи заборонені.

Загалом, якщо системи розумних камер обробляють персональні дані, їх використання повинно відповідати принципам і правилам захисту даних: французькому Закону про обробку даних і свободи (loi informatique et libertés), а також Загальному регламенту про захист даних або Директиві про правоохоронні органи, якщо обробка здійснюється правоохоронними органами. Крім того, CNIL зазначає, що оцінка впливу на захист даних повинна проводитися «через інноваційний характер технології». Крім того, в деяких конкретних випадках законодавство про захист даних передбачає необхідність прийняття внутрішніх положень, наприклад, коли технологія використовується правоохоронними органами для запобігання злочинам. У таких випадках розгортання «розумного» відео вимагає наявності законодавчого або іншого нормативного документа, який би дозволяв або контролював їх законне застосування [3].

Узагальнюючи окреслену проблематику та проектуючи її на національну правову систему, не можемо оминути увагою той факт, що Конституція України забороняє втручання в особисте і сімейне життя людини крім випадків, безпосередньо зазначених у самому Основному Законі (наприклад, якщо таке втручання передбачено законом та здійснюється в інтересах національної безпеки).

У розрізі предмета нашого дослідження констатуємо, що Стратегія забезпечення державної безпеки від 16.02.2022 р. (далі – Стратегія) визначає реальні й потенційні загрози державній безпеці України, напрями та завдання державної політики у сфері державної безпеки, є основою для планування і реалізації політики у сфері державної безпеки [4].

Однак, безпосередньо у самій Стратегії не наводиться поняття «державна безпека». Звертаємо увагу, що поняття «державна безпека» закріплено в п. 1 ст. 1 Закону України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII і визначається як захищеність державного суверенітету, територіальної цілісності і *демократичного конституційного ладу* та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного характеру [5].

У п. 3 Стратегії конкретизуються об'єкти забезпечення державної безпеки – державний суверенітет, конституційний лад, територіальна цілісність України, оборонний, економічний і науково-технічний потенціал, кібербезпека, інформаційна безпека, об'єкти критичної інфраструктури, державна таємниця та службова інформація.

Також нормативно інтерпретовано поняття «загрози державній безпеці» – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити захищеність державного суверенітету, територіальної цілісності та демократичного конституційного ладу й інших життєво важливих національних інтересів.

Зважаючи на те, що до об'єктів забезпечення державної безпеки РНБО віднесла *конституційний лад*, а з-поміж загроз державній безпеці визначено ті можливі явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити, зокрема, захищеність *демократичного конституційного ладу*, висновуємо прагнення авторів даної Стратегії нормативно гарантувати, зокрема й забезпечення приватності громадян та уникнення можливих порушень прав людини.

Зазначене вище корелюється зі змістом структурних складових поняття «інформаційна безпека» (визначеного у п. 3 Стратегії) – стан захищеності національних інтересів людини, суспільства і держави в інформаційній сфері, за якого унеможливлено завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується, негативний інформаційний вплив; витік державної таємниці та службової інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації, у тому числі шляхом проведення іноземними спецслужбами, окремими організаціями, групами, особами спеціальних інформаційних операцій та деструктивних інформаційних впливів, а також забезпечується своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національним інтересам та національній безпеці України.

Отже, визначаючи реальні загрози державній безпеці України на сучасному етапі у контексті можливого впровадження технології розпізнавання облич важливо мати детальні правила, що регулюють обсяг і застосування заходів, а також надійні гарантії проти ризику зловживань і свавілля.

Невідворотна необхідність у правових гарантіях щодо реалізації та захисту приватності громадян, особливо коли йдеться про використання технології розпізнавання облич в реальному часі, висновується зі змісту Стратегії забезпечення державної безпеки, а саме:

1. До об’єктів забезпечення державної безпеки віднесено *конституційний лад*.

2. З-поміж загроз державній безпеці визначено ті можливі явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити, зокрема, захищеність *демократичного конституційного ладу,* при якому людина, її життя і здоров'я, честь і гідність, *недоторканність і безпека* визнаються найвищою соціальною цінністю.

3. У структурі елементів *інформаційної безпеки* чітко виокремлено стан захищеності національних інтересів людини, суспільства і держави в інформаційній сфері, за якого унеможливлено завдання шкоди, зокрема, через: неповноту, невчасність та невірогідність інформації, що використовується, негативний інформаційний вплив; *негативні наслідки застосування інформаційних технологій*; *несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації* і т. ін.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Wesfreid M. Paris 2024 : pas de reconnaissance faciale aux JO. *Le Parisien*. November 23rd, 2022. URL: https://www.leparisien.fr/politique/paris-2024-pas-de-reconnaissance-faciale-aux-jo-23-11-2022-4E3FP2XBWZC4LBY3B4UMPA3QPE.php?ts=1669200293918.

2. Caméras dit «augmentées» dans les espaces publics: la position de la CNIL. *CNIL.* July 19th, 2022. URL: https://www.cnil.fr/fr/cameras-dites-augmentees-dans-les-espaces-publics-la-position-de-la-cnil.

3. Emery P. Toulouse : le pouvoir des caméras de vidéosurveillance. *La Dépêche*. January 3, 2019. URL: https://www.ladepeche.fr/article/2019/01/03/2934369-toulouse-le-pouvoir-des-cameras.html.

4. Указ Президента України від 16 лютого 2022 року № 56/2022 «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки». *Президент України*. URL: https://www.president.gov.ua/documents/562022-41377.

5. Закон України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII. *Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.