DOI: 10.31359/2079-6242-2024-48-167
УДК 343.9:004.8

В. В. Журавель, аспірант Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України

ПРИНЦИПИ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

У XXI столітті в умовах стрімкої цифровізації суспільних відносин, трансформації господарського сектора суспільства у напряму так званого дистантного типу економіки, в якій значна частина робочих процесів та бізнес-операцій здійснюється на відстані за допомогою цифрових технологій і мереж, у тому числі з використанням можливостей штучного інтелекту, а так само поширення явища гібридизації воєнного протистояння проблема використання кіберпростору для вчинення різного роду протиправних діянь стає серйозним викликом для правопорядку соціальних спільнот і навіть загрозою національній безпеці будь-якого суспільства. Недаремно у Стратегії кібербезпеки України зазначається, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України[1].

Отже, сьогодні жоден соціум не убезпечений від деструктивного впливу, здавалося б, цілком корисливих процесів трансформації суспільного життя, які покликані насамперед «якісно змінити різні сфери життя і підвищити результативність будь-якої роботи»[2]. До того ж Українська держава з початку так званої повзучої агресії рф, як ніхто інший, зіштовхнулася із проблемою задіяння кіберінструментів для впровадження небезпечних наративів серед українських громадян. Така ситуації в рази загострилася від моменту повномасштабної агресії рф проти України в лютому 2022 року, що поставило на порядку денному проведення поглибленого кримінологічного аналізу проблеми використання кібрпростору як одного з потужних каналів поширення ворожої пропаганди.

На теперішній час масштаби, образно кажучи, кібердеструкції настільки є великими, що на нейтралізацію потоків шкідливої інформації, які здатні набувати нерідко характеру різноманітних небезпечних діянь кримінально-правового характеру, вже не вистачає суто людського фактору. У цьому зв'язку ще раз процитуємо положення із Стратегії кібербезпеки України: «Питома вага кіберзагроз зростає, і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься»[3].

Таким чином, виникає потреба інтегрувати наявні технології штучного інтелекту у правоохоронний сектор, і при цьому не лише для запобігання правопорушенням, що вчиняються у кіберпросторі, а й для запобігання будь-яким правопорушенням, що вчиняються так само поза кіберпростором. Відтак, для покращення ефективності роботи правоохоронних органів та забезпечення публічної безпеки може бути використаний штучний інтелект[4]. Недаремно у спеціальній літературі зазначається, що сучасні технології відіграють значну роль у реалізації стратегії зменшення можливостей вчинення злочинів[5]. Як бачимо, ці ракурси «прикладення сили» безпосередньо пов'язані з убезпеченням суспільства від злочинних проявів.

Аналіз останніх досліджень і публікацій. Новим можливостям, що відкриваються у практиці запобігання злочинності, сьогодні присвячено чимало наукових праць. Слід визнати, що цифро-

[1] Стратегія кібербезпеки України: затв. Указом Президента України від 26 серпня 2021 р. №4447/2021. *Офіційний вісник України.* 2021. №70. Ст. 4417.

[2] Турута О. В., Турута О. П. 'Штучний інтелект крізь призму фундаментальних прав людини' (2022) 71 Науковий вісник Ужгородського Національного Університету 50

[3] Стратегія кібербезпеки України: затв. Указом Президента України від 26 серпня 2021 р. №4447/2021. *Офіційний вісник України.* 2021. №70. Ст. 4417.

[4] Зачек О. І., Дмитрик Ю. І., Сеник В. В. 'Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності' (2023) 3 Науковий вісник Львівського державного університету внутрішніх справ 149

[5] Голіна В. В. (ред) *Зменшення можливостей вчинення злочинів: стратегічний підхід: монографія* (Право, 2020) 166

візація практики, про яку йдеться, є однією з активно обговорюваних тем правознавчого дискурсу. Участь у розробці зазначеного напряму боротьби з правопорушеннями беруть такі вчені, як Р. І. Благута, В. М. Брижко, О. М. Брисковська, О. І. Бугера, М. А. Грига, М. Г. Колодяжний, М. О. Кравцова, Д. О. Куковинець, К. В. Латиш, Л. В. Лефтеров, О. М. Литвинов, А. В. Мовчан, О. Е. Радутний та ін. У свою чергу, теоретичні розробки знаходять своє втілення у практичній площині. Проте явище штучного інтелекту як таке є неоднозначним. Інколи межа між правомірністю його використання та порушенням базових прав людини є достатньо тонка. Як зазначається у спеціальній літературі, системи штучного інтелекту можуть не просто виявляти, а навіть посилювати соціальні упередження в суспільстві, наприклад, несправедливо розподіляти ресурси чи можливості між представниками різних соціальних груп (відома помилка в автоматизованих рекрутингових службах, які при відборі кандидатів на ту чи іншу посаду перевагу віддавали чоловікам), відтворювати існуючі соціальні стереотипи, які можуть не відповідати дійсності в конкретній ситуації (так, система, що використовується в судочинстві, оцінює представників певної етнічної групи як більш схильних до рецидивізму), призводити до того, що рівень сервісу виявляється гіршим для однієї з груп порівняно з іншою, або принижувати статус групи, видаючи, наприклад, образливий результат (системи гірше розпізнають обличчя людей азіатського типу та обличчя темношкірих людей)[1]. Наведені приклади свідчать про те, що незайвим є звернутися до певних принципів, які покладатимуться у підґрунтя використання будь-яких інструментів штучного інтелекту та виконуватимуть роль методологічних орієнтирів. Сфера запобігання злочинності якраз й є тією сферою, в якій застосування штучного інтелекту може викликати неабиякі ризики для фундаментальних прав людини, а тому застосування діджитал-інструментів у демократичному суспільстві потребує додаткового контролю та системи гарантій для уникнення й недопущення будь-яких порушень з боку суб'єктів запобіжної діяльності.

Метою статті є визначення засадничих положень (принципів) використання технологій штучного інтелекту під час реалізації заходів запобігання злочинності.

[1] Турута О. В., Турута О. П., 53

Викладення основного матеріалу. Переваги штучного інтелекту сьогодні є очевидним. Як приклад, згадаємо нещодавно затверджені постановою Кабінету Міністрів України зміни до Положення про Єдиний державний вебпортал електронних послуг, згідно з якими користувачі зможуть серед іншого отримувати інформаційну підтримку щодо порядку користування порталом «Дія» з використанням технологій штучного інтелекту[2]. До того ж вченими у чисельних публікаціях розкриваються можливості застосування відповідних технологій для дотримання правопорядку у відповідних сферах. Так, Г. К. Авдєєва та В. О. Коновалова відмітили, що ефективність системи штучного інтелекту стає очевидною під час виявлення порушень та забезпечення дотримання правил дорожнього руху, допомагаючи ідентифікувати транспортні засоби та осіб у несприятливих умовах (низька роздільна здатність фото- або відеокамери, темрява, снігопад, дощ тощо); у свою чергу, прогнози росту злочинності, що створені спеціальними системами штучного інтелекту, дозволяють підвищити ефективність заходів її попередження[3].

Констатуючи той факт, що застосування штучного інтелекту як спеціального напряму інформаційних технологій у правоохоронній діяльності є доволі важливим та актуальним аспектом для України, водночас слід зробити акцент на такому моменті: застосування штучного інтелекту у достатньо специфічній людській діяльності нерідко пов'язується з обмеженням прав людини. Тому подібний процес має ґрунтуватися на низці принципів, які допоможуть забезпечити ефективність, етичність і безпеку використання цих технологій. Недаремно майже десять років тому О. Ю. Бусол застерігала, що «головна проблема полягає не в створенні ефективних систем штучного інтелекту – таких розробок у світі вже достатньо, а у відсутності нових підходів до створення системи контролю, насамперед, етичного характеру, над

[2] Положення про Єдиний державний вебпортал електронних послуг: затв. постановою Кабінету Міністрів України від 4 грудня 2019 р. № 1137 (в редакції постанови Кабінету Міністрів України від 16 серпня 2022 р. № 937. URL: https://zakon.rada.gov.ua/laws/show/1137–2019-%D0%BF#n15. (дата звернення: 13.10.2024)

[3] Авдєєва Г. В., Коновалова В. О. 'Штучний інтелект у боротьбі зі злочинністю: напрями використання та проблеми законодавчого врегулювання' *Цифрова трансформація кримінального провадження в умовах воєнного стану:* матеріали круглого столу, присвяч. Всеукр. тижню права (м. Харків, 23 груд. 2022 р.) 36–37

штучним інтелектом»[1]. Ці та багато інших застережень свідчать про те, що у запобіжній діяльності з використанням штучного інтелекту має бути опрацьований чіткий підхід, що, повторимося, матиме вигляд сукупності принципів, яких слід неухильно дотримуватися у зазначеній діяльності.

Таким чином, загалом організація й управління процесом запобігання злочинності, а також запобіжні заходи повинні відповідати певним принципам, вимогам[2]. Під принципом (від лат. *principium* – основа, початок) у філософській та наукознавчій царині найчастіше розуміють основне, вихідне положення якої-небудь теорії, вчення і т. д.; керівну ідею, основне правило діяльності[3]. На наш погляд, *принципи запобігання злочинності з використанням технологій штучного інтелекту* доцільно визначити як основні засади, вихідні положення, керівні ідеї чи вимоги, що висуваються до організації і реалізації системи відповідних заходів запобігання злочинності із застосуванням можливостей штучного інтелекту в широкому смислі слова, спрямованих на зниження ризику вчинення кримінально караних правопорушень і формування безпекового середовища із дотриманням прав і законних інтересів людини, суспільства та держави.

Якщо звернутися до Європейської етичної хартії про використання штучного інтелекту в судових системах (European Ethical Charter on the use of artificial intelligence in judicial systems and their environment), Регламенту Європейського Союзу про штучний інтелект (Artificial Intelligence Act), прийнятого Європейським парламентом 13 березня 2024 р. і схваленого Радою ЄС 21 травня 2024 р., та пов'язаної нормативної бази ЄС у сфері цифрових технологій, зокрема, до Загального регламенту захисту даних (GDPR), то можна побачити, що європейське законодавство активно формує принципи використання штучного інтелекту з акцентом на етичне, безпечне та прозоре впровадження технологій. Наприклад, у згаданій Хартії зазначається про такі принципи, як: 1) дотримання основних прав людини при використанні штучного інтелекту; 2) запобігання розвитку будь-якої дискримінації окремих осіб чи груп осіб; 3) безпека та якість обробки судових рішень і даних у безпечному технологічному середовищі; 4) «під контролем користувача», тобто поінформованість людини зрозумілою мовою про всі процесуальні аспекти, можливості й функції штучного інтелекту відповідно до статті 6 ЄКПЛ; 5) прозорість, неупередженість та справедливість[4]. Перелічені принципи мають безпосереднє відношення до запобіжної діяльності, адже правосуддя є ключовим елементом у системі запобігання злочинності, оскільки саме через правосуддя суспільство реалізує заходи для забезпечення закону, справедливості й безпеки.

У свою чергу, слід навести й перелік етичних принципів, які проголошуються у Регламенті ЄС про штучний інтелект і які є загальними вимогами запровадження діджитал-інструментів у будь-якій сфері людського життя. До таких принципів, що покликані, з одного боку, допомогти забезпечити надійність та етичність використання, а, з другого, – сприяти розробці орієнтованого на людину штучного інтелекту відповідно до Хартії та цінностей, на яких засновано ЕС, належать: нагляд людини; технічна надійність і безпека; конфіденційність і управління даними; прозорість; різноманітність, відсутність дискримінації та справедливість; суспільне та екологічне благополуччя і відповідальність[5]. Наведені вище принципи є відправними положеннями й для визначення засадничих позицій щодо організації та реалізації діяльності із запобігання злочинності в цілому та окремим її проявам, зокрема.

Що стосується національної площини, то у Концепції розвитку штучного інтелекту в Україні 2020 р. одним із принципів використання технологій штучного інтелекту є, зокрема, підвищення рівня безпеки суспільства шляхом застосування технологій штучного інтелекту під час розроблення заходів ресоціалізації засуджених осіб та визначення ризику скоєння повторного правопорушення[6]. Як бачимо, у документі робиться осо-

[1] Бусол О Ю 'Потенційна небезпека штучного інтелекту' (2015) 2 (14) Інформація і право 127

[2] Голіна В В, Головкін Б М (ред) *Кримінологія: підручник* (Право, 2014) 167.

[3] Шапар В Б *Сучасний тлумачний психологічний словник* (Прапор, 2007) 364.

[4] European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment: Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3–4 December 2018) / (CEPEJ). Strasbourg: European Commission for the Efficiency of Justice, 2018. P. 7

[5] Artificial Intelligence Act: Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024. *Official Journal (OJ) of the European Union.* 12/07/2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689. (дата звернення: 13.10.2024)

[6] Концепція розвитку штучного інтелекту в Україні: схвал. розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. *Урядовий кур'єр.* 2020. 18 груд. № 247

бливий наголос лише на невеликий сегмент «прикладання сили» нових можливостей, які людство отримало у зв'язку із науково-технічним прогресом. Вважаємо, що треба вести мову про поширення відповідних засадничих положень на всю різноманітну діяльність з убезпечення соціуму від злочинних проявів.

З урахуванням наведеного, застосовуючи методи аналізу і синтезу, розкриємо зміст тих засадничих положень використання можливостей штучного інтелекту, що обрані нами як орієнтири для такого роду діяльності.

Принцип законності. Це є базовий принцип, що висувається до будь-якої сфери життєдіяльності людини та набуває характеру правової «оболонки». Використання штучного інтелекту у практиці боротьби зі злочинністю повинно так само відповідати положенням національного та міжнародного законодавства. Це передбачає дотримання всіх правових норм й обмежень, що, з одного боку, гарантують захист прав людини, приватності та конфіденційності даних, рівність та свободу від дискримінації, а, з другого боку, забезпечують прозорість і підзвітність процесів, тим самим запобігаючи зловживанням або дискримінаційним рішенням. Іншими словами, будь-яке збирання, обробка, зберігання даних та ін. для цілей запобігання злочинності має здійснюватися лише у правовій площині та з урахуванням обмежень щодо конфіденційності інформації, отриманої під час такої діяльності. Водночас у відповідності до ч. 1 ст. 7 Закону України «Про захист персональних даних»[1] «забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних». Однак із цього загального правила є виключення, що має безпосереднє відношення до досліджуваної нами сфери. Справа в тому, що наведене положення не застосовується, «якщо обробка персональних даних стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом у межах його повноважень, визначених законом» (п. 7 ч. 2 ст. 7 Закону України «Про захист персональних даних»).

Цей принцип уявляється важливим з огляду на значну кількість випадків неправомірного використання технологій штучного інтелекту у протидії злочинності. Як приклад можна навести випадки надмірного контролю та втручання у приватне життя, дискримінацію окремих груп населення, непрозорість алгоритмів і зловживання доступом до певних даних. Тут знов нагадаємо про практику запобігання злочинам із використанням деяких систем штучного інтелекту, що містять приховану дискримінацію за расовими, етнічними або соціальними ознаками, коли алгоритми системи можуть визначати осіб із певних районів або груп як більш схильних до вчинення правопорушень лише на підставі місця їх проживання, зовнішнього вигляду, якогось знання про історичні події, що характеризували у минулому представників цих груп як, так би мовити, неблагонадійних. Це призводить до дискримінаційних рішень і потенційного переслідування невинних осіб. Крім того, у деяких випадках правоохоронні органи не надають інформацію про те, як працюють застосовані системи штучного інтелекту та які алгоритми використовуються для виявлення підозрюваних або прогнозування вчинення правопорушень. Відсутність пояснень або доступу до механізму ухвалення рішень штучним інтелектом робить неможливим оскарження помилкових висновків, що порушує, у тому числі, й принцип законності.

Принцип прозорості і пояснюваності. Сутність цього принципу, пов'язаного в цілому з коректністю використання систем штучного інтелекту у запобіжній діяльності, полягає в тому, щоб алгоритми і методи, задіяні у запобіганні злочинності, є зрозумілими та підзвітними. Громадськість і правозахисні організації повинні мати можливість розуміти, як приймаються рішення з використанням штучного інтелекту, та перевіряти, чи дотримуються застосувачі відповідних законодавчих вимог у процесі, про який йдеться. При цьому прозорість означає, по-перше, відкритість інформації щодо того, як працює система штучного інтелекту та які алгоритми використовуються; по-друге, знання про те, в який спосіб приймаються рішення та чи можна отримати пояснення щодо функцій і завдань застосовуваних технологій штучного інтелекту; по-третє, які дані для цього

[1] Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI. *Відомості Верховної Ради України.* 2010. № 34. Ст. 481.

використовуються та як відстежується походження необхідних даних, щоб уникнути прихованого використання дискримінаційних практик чи особистої інформації у протиправних цілях. У свою чергу, пояснюваність є важливою для зрозумілості прийнятих штучним інтелектом рішень, тобто їх раціональної оцінки та перевірки. Ключові моменти пояснюваності полягають в тому, що: 1) будь-яке рішення штучного інтелекту, припустимо, у кримінальних провадженнях, повинне супроводжуватися поясненнями, які можуть бути зрозумілі не лише розробникам, а й суддям, адвокатам, обвинуваченим та громадськості; 2) правоохоронці повинні мати відповідні вміння й навички щодо інтерпретації результатів, згенерованих такими системами, щоб уникнути помилок чи упереджених висновків під час прийняття рішень щодо вживання тих чи інших запобіжних заходів.

Ризики, що можуть призвести до порушення принципу прозорості та пояснюваності під час використання штучного інтелекту у запобіганні злочинності, вбачають у тому, що відповідні технології працюють на основі доволі складних алгоритмів, які не завжди зрозумілі навіть розробникам, не кажучи вже про громадськість. Якщо правоохоронці приймають рішення, ґрунтуючись на таких непрозорих алгоритмах, то громадськість може почати сумніватися в справедливості та об'єктивності цих рішень. Ще одним прикладом – ілюстрацією до порушення аналізованого принципу – можна вважати ті випадки, коли алгоритми штучного інтелекту збирають та аналізують особисту інформацію, таку як дані із соціальних мереж, без пояснення, як саме ці дані впливають на рішення системи.

Принцип недопущення дискримінації. Це засадниче положення використання технологій штучного інтелекту у сфері запобігання злочинності випливає з двох попередніх принципів та означає, що останній не повинен створювати ситуацію нерівності або дискримінації. Тому алгоритми повинні бути налаштовані у такий спосіб, щоб уникати упередженого ставлення до людей на основі раси, статі, національності чи інших ознак, адже забезпечення рівного ставлення до всіх громадян є важливим етичним аспектом використання подібних систем у будь-якій сфері людського буття, включаючи й сферу убезпечення суспільства від правопорушень. Порушення цього принципу може призводити, зокрема, до: упередженості алгоритмів щодо певних расових або етнічних (національних) груп населення, помилково класифікуючи представників цих груп як більш схильних до вчинення правопорушень, навіть якщо це не відповідає дійсності; дискримінації за соціально-економічних статусом чи районом проживання з таким самим результатом; непропорційного використання технології розпізнавання облич для певних груп населення (наприклад, для осіб з темним кольором шкіри); упередженості аналізованих технологій з огляду на стать та вік особи (особливо під час прогнозних розрахунків щодо схильності чоловіків молодого віку до вчинення правопорушень) та ін. Так, у 2016 р. штучний інтелект у США звинуватили у расизмі, оскільки комп'ютерна програма під назвою «Виправлення правопорушників з профілювання альтернативних санкцій» (COMPAS), яка використовується американським судом для оцінки ризику, була упереджена щодо афроамериканців. Справа в тому, що зазначена програма була більш схильною помилково маркувати афроамериканських підсудних як таких, що здатні вчинювати повторні правопорушення вдвічі частіше, ніж білі особи (45% до 24%)[1].

Принцип безпеки. Сутність зазначеного принципу пов'язується з тим, що використання штучного інтелекту в боротьбі зі злочинністю повинно гарантувати безпеку як самих систем, так й оброблюваних за допомогою таких систем даних. У зв'язку із цим виникає завдання – забезпечити захист інформації від кібератак, несанкціонованого доступу та маніпуляцій інформацією, а так само від знищення та викривлення останньої. Водночас є важливим й унеможливлення таких ситуацій, при яких алгоритми можуть бути зламані або використані для вчинення нових злочинів. Теоретично нескладно уявити ситуацію, в якій зловмисники використовують шкідливі програми, спеціально створені для обходу систем безпеки та виявлення загроз, шляхом адаптування своїх алгоритмів й кодів для того, щоб вони виглядати як законний трафік або файли. Це дозволяє злочинцям непомітно проникати в мережі та отримувати доступ до конфіденційних даних. З огляду на це безпека технологій штучного інтелекту, використання яких має місце у запобіжній діяльності, сьогодні підноситься до неабиякого методологічного принципу діа-

[1] Плахотнік О В 'Практичне застосування штучного інтелекту у кримінальному провадженні' (2019) 4 Вісник кримінального судочинства 49–50.

логу людини з новітніми інструментами свого буття.

Захист приватності. Зазначений принцип при використанні штучного інтелекту у запобіганні злочинності уявляється вельми важливим, оскільки, з одного боку, він стосується дотримання широкої палітри прав людини, а, з другого, – сама по собі така діяльність часто вимагає обробки великої кількості особистих даних, таких як дані з камер спостереження, відомості про онлайн-активність, записи з телефонів, соціальних мереж, різних платформ тощо. Щоб не порушувати цей принцип, треба мати на увазі, що для реалізації завдань із запобігання правопорушенням збираються лише ті дані, які є критично необхідними саме для реалізації поставлених завдань, тобто без «перевантаження» системи зайвою у даному випадку інформацією. Наприклад, якщо метою є аналіз поведінкових моделей для виявлення ризику вчинення будь-якого правопорушення вперше або вчинення рецидиву, не потрібно зберігати додаткову персональну інформацію, таку як адреса, споживацькі уподобання особи та ін. І знов таки цей принцип корелює із принципом безпеки, адже ті персональні відомості, які обробляються й зберігаються для цілей запобігання злочинності, повинні бути надійно захищені, аби попередити несанкціонований доступ до персональних даних. Так само слід пам'ятати про те, що системи штучного інтелекту, котрі використовуються для запобігання злочинності, повинні піддаватися регулярному аудиту з метою перевірки їх відповідності стандартам приватності.

Принцип адаптивності та оновлюваності. Цей принцип є своєрідною антитезою тому факту, що злочинці постійно вдосконалюють свої методи. У таких ситуаціях технології штучного інтелекту мають бути здатними до адаптації і самовдосконалення, що передбачає постійне оновлення баз даних, навчання алгоритмів на нових зразках злочинних схем і модернізацію технологічної інфраструктури, що відповідало б сучасним викликам і загрозам. Лише при умові здатності системи штучного інтелекту, що використовується для зниження тиску злочинних проявів на суспільство, «підлаштовуватися» під змінюване середовище та реагувати на будь-які зміни в ньому, вона залишатиметься актуальною, точною й ефективною. Це досягається за допомогою широкого спектру дій, як-от: автоматичне оновлення алгоритмів системи штучного інтелекту у відповідності до нових тенденцій у розвитку злочинності; самонавчання системи на основі нових даних, власних помилок, припустимо, щодо неправильного прогнозу розвитку ситуації або упередженого ставлення до будь-якої особи; швидка інтеграція нових баз даних, які можуть допомогти покращити точність і релевантність вживаної у запобіганні злочинності системи штучного інтелекту; врахування змін у законодавстві стосовно приватності, захисту даних, кримінально-правової оцінки тих чи інших діянь тощо.

Принцип етичності. Сутність цього принципу, на наш погляд, полягає у забезпеченні балансу між необхідністю дотримання громадської безпеки та захистом основоположних прав людини, таких як приватність, право на забуття, свобода, рівність та ін. Тим самим відповідне засадниче положення спрямовується на уникнення зловживань технологіями штучного інтелекту. Фактично принцип етичності вбирає в себе всі попередні вимоги до практики застосування останніх під час запобігання злочинності, що повністю відповідає законам, котрі регулюють права людини, захист даних від протиправного використання, а так само запобігання злочинності як вид людської діяльності в цілому.

На підставі викладеного можна зробити низку висновків, що матимуть не лише теоретичну, а й практичну спрямованість.

1. Використання штучного інтелекту у запобіганні злочинності створює нові можливості для підвищення ефективності соціальних інституцій, задіяних у зазначеній діяльності. Разом із тим подібна практика вимагає суворого дотримання принципів, що є визначальними для правомірності використання у відповідній царині досягнень науково-технічного прогресу. У противному разі такі технології можуть викликати серйозні соціальні й правові ризики, тому їх впровадження у запобіжну діяльність потребує ретельного регулювання та контролю.

2. Під принципами запобігання злочинності з використанням технологій штучного інтелекту слід розуміти засадничі положення, що ставляться теорією і практикою боротьби зі злочинністю до організації і реалізації системи відповідних заходів із застосуванням можливостей штучного інтелекту, спрямованих на зниження ризику вчинення кримінально караних правопорушень і формування безпекового середови-

ща з огляду на необхідність суворого дотримання законних інтересів і прав людини, суспільства та держави.

3. До основних принципів, що висуваються до вживання запобіжних заходів із використанням технологій штучного інтелекту, належать такі засадничі положення, як: законність, прозорість і пояснюваність, недопущення дискримінації, безпека, захист приватності, адаптивність та оновлюваність, етичність. Цей перелік, звісно ж, не є вичерпним, оскільки час і практика постійно вноситиме свої корективи стосовно вимог, яких слід дотримуватися під час вживання заходів із запобігання злочинності.

REFERENCES

List of legal documents

Legislation

1. Artificial Intelligence Act: Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024. *Official Journal (OJ) of the European Union.* 12/07/2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689. (in English)
2. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment: Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3–4 December 2018) / (CEPEJ). Strasbourg: European Commission for the Efficiency of Justice, 2018. P. 7 (in English)
3. Kontseptsiia rozvytku shtuchnoho intelektu v Ukraini: skhval. rozporiadzhenniam Kabinetu Ministriv Ukrainy vid 2 hrudnia 2020 r. № 1556-r. Uriadovyi kurier. 2020. 18 hrud. № 247 (in Ukrainian)
4. Polozhennia pro Yedynyi derzhavnyi vebportal elektronnykh posluh: zatv. postanovoiu Kabinetu Ministriv Ukrainy vid 4 hrudnia 2019 r. № 1137 (v redaktsii postanovy Kabinetu Ministriv Ukrainy vid 16 serpnia 2022 r. № 937. URL: https://zakon.rada.gov.ua/laws/show/1137–2019-%D0%BF#n15. 247 (in Ukrainian)
5. Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 1 chervnia 2010 roku № 2297-VI. Vidomosti Verkhovnoi Rady Ukrainy. 2010. № 34. St. 481. 247 (in Ukrainian)
6. Stratehiia kiberbezpeky Ukrainy: zatv. Ukazom Prezydenta Ukrainy vid 26 serpnia 2021 r. № 4447/2021. Ofitsiinyi visnyk Ukrainy. 2021. № 70. St. 4417. 247 (in Ukrainian)

Bibliography

Authored books

1. Shapar V B *Suchasnyi tlumachnyi psykholohichnyi slovnyk* [Modern explanatory psychological dictionary] (Prapor, 2007) 364 (in Ukrainian)

Edited books

2. Holina V V (red) *Zmenshennia mozhlyvostei vchynennia zlochyniv: stratehichnyi pidkhid: monohraf*iia [Reducing the Opportunities to Commit Crime: A Strategic Approach: Monograph] (Pravo, 2020) 166 (in Ukrainian)
3. Holina V V, Holovkin B M (red) *Kryminolohiia: pidruchnyk* [Criminology: textbook] (Pravo, 2014) 167 (in Ukrainian)

Journal articles

4. Busol O Yu 'Potentsiina nebezpeka shtuchnoho intelektu' [The potential danger of artificial intelligence] (2015) 2 (14) Informatsiia i pravo 127 (in Ukrainian)
5. Plakhotnik O V 'Praktychne zastosuvannia shtuchnoho intelektu u kryminalnomu provadzhenni'[Practical application of artificial intelligence in criminal proceedings] (2019) 4 Visnyk kryminalnoho sudochynstva 49–50 (in Ukrainian)
6. Turuta O. V., Turuta O. P. 'Shtuchnyi intelekt kriz pryzmu fundamentalnykh prav liudyny' [Artificial intelligence through the prism of fundamental human rights] (2022) 71 Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu 50 (in Ukrainian)
7. Zachek O. I., Dmytryk Yu. I., Senyk V. V. 'Rol shtuchnoho intelektu v pidvyshchenni efektyvnosti pravookhoronnoi diialnosti' [The role of artificial intelligence in increasing the effectiveness of law enforcement activities] (2023) 3 Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav 149 (in Ukrainian)

Conference paper

8. Avdieieva H. V., Konovalova V. O. 'Shtuchnyi intelekt u borotbi zi zlochynnistiu: napriamy vykorystannia ta problemy zakonodavchoho vrehuliuvannia' *Tsyfrova transformatsiia kryminalnoho provadzhennia v umovakh voiennoho stanu*: materialy kruhloho stolu, prysviach. Vseukr. tyzhniu prava (m. Kharkiv, 23 hrud. 2022 r.) 36–37 (in Ukrainian)

Журавель В. В.

Принципи запобігання злочинності з використанням технологій штучного інтелекту

Статтю присвячено виділенню і розкриттю принципів, на яких має будуватися діяльність із запобігання правопорушенням із використанням технологій штучного інтелекту. При цьому дається визначення зазначеним принципам, під якими розуміються засадничі положення, що опрацьовані, зокрема, теорією кримінологічної науки та ставляться до організації і реалізації системи відповідних заходів із застосуванням можливостей штучного інтелекту. Метою таких заходів є зниження ризику вчинення кримінально караних правопорушень, а так само створення безпекового середовища з огляду на необхідність суворого дотримання законних інтересів і прав людини, суспільства та держави.

Автором аналізується низка європейських документів, в яких наводяться принципи використання штучного інтелекту в людській діяльності, включаючи й сферу відправлення правосуддя. Робиться висновок, що принципи, які містяться в Європейській етичній хартії про використання штучного інтелекту в судових системах та Регламенті Європейського Союзу про штучний інтелект виявляються відправними положеннями й для генерації засадничих позицій щодо організації та здійснення діяльності із запобігання злочинності в цілому та окремим її проявам, зокрема.

До переліку основних принципів, що висуваються до вживання запобіжних заходів із використанням технологій штучного інтелекту, сьогодні доцільно віднести такі засадничі положення, як: законність, прозорість і пояснюваність, недопущення дискримінації, безпека, захист приватності, адаптивність та оновлюваність, етичность. Водночас у статті підкреслюється, що цей перелік не є вичерпним, адже практика постійно вноситиме свої корективи стосовно вимог, яких слід дотримуватися, вживаючи заходи із запобігання злочинності.

Ключові слова: *запобігання злочинності, штучний інтелект, принципи запобігання злочинності з використанням технологій штучного інтелекту, законнність, приватність.*

Zhuravel V. V.

The Principles of Crime Prevention Using Artificial Intelligence Technologies

The article is devoted to the selection and disclosure of the principles on which crime prevention activities with the use of artificial intelligence technologies should be based. At the same time, the specified principles are defined, which are understood as the basic provisions developed, in particular, by the theory of criminological science and related to the organization and implementation of the system of appropriate measures using the capabilities of artificial intelligence. The purpose of such measures is to reduce the risk of committing criminal offenses, as well as to create a safe environment in view of the need for strict observance of the legitimate interests and rights of man, society and the state.

The author analyzes a number of European documents, which state the principles of using artificial intelligence in human activities, including the sphere of administration of justice. It is concluded that the principles contained in the European Ethical Charter on the use of artificial intelligence in judicial systems and their environment and the Artificial Intelligence Act are the starting points for the generation of basic positions regarding the organization and implementation of activities for the prevention of crime in general and its individual manifestations, in particular .

To the list of basic principles put forward for the use of preventive measures using artificial intelligence technologies, it is appropriate today to include such basic provisions as: legality, transparency and explainability, non-discrimination, security, privacy protection, adaptability and updateability, ethics. At the same time, the article emphasizes that this list is not exhaustive, because the practice will constantly make its own corrections regarding the requirements that should be followed when taking measures to prevent crime.

Key words: *crime prevention, artificial intelligence, principles of crime prevention using artificial intelligence technologies, legality, privacy.*

Стаття надійшла до редакції:15.10.2024 р.
Прийнята до друку: 20.11.2024 р.