ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ТЕХНІЧНОЇ ДІЯЛЬНОСТІ ПОЛІЦІЇ

УДК 004.89:351.74:342.7
DOI https://doi.org/10.32782/2709-9261-2024-3-11-9

Гудзь Тетяна Іванівна,
кандидат юридичних наук, доцент
(Харківський національний університет внутрішніх справ, м. Харків)
ORCID: https://orcid.org/0000-0002-6950-6136

Синжерян Андрій Андрійович,
курсант
(Харківський національний університет внутрішніх справ, м. Харків)
ORCID: https://orcid.org/0009-0001-6063-4254

ІНТЕГРАЦІЯ ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ У ДІЯЛЬНІСТЬ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ: ПЕРСПЕКТИВИ ТА ВИКЛИКИ

Статтю присвячено інтеграції штучного інтелекту у діяльність Національної поліції України. Розглянуто можливості використання штучного інтелекту поліцією для підвищення ефективності її діяльності, автоматизації процесів та моніторингу Інтернету з метою запобігання та розкриття правопорушень. Акцентовано на ризиках порушення приватності громадян України. Відзначено необхідність ухвалення нормативних актів для регулювання використання штучного інтелекту. Наведено приклади сучасних технологій, таких як розпізнавання обличчя і прогнозування злочинності.

Ключові слова: *штучний інтелект, Національна поліція, автоматизація, кібербезпека, персональні дані.*

Постановка проблеми. Стрімкий розвиток науково-технічного прогресу, зокрема в галузі інформаційних технологій, призвів до створення та вдосконалення штучного інтелекту (ШІ), який наразі активно впроваджується у різні сфери суспільного життя. Використання технологій ШІ здатне радикально змінити способи обробки інформації, автоматизувати процеси та значно підвищити ефективність діяльності державних органів.

Однак впровадження таких технологій у правоохоронну діяльність, зокрема в діяльність Національної поліції України, ставить перед суспільством нові виклики. Основними проблемами є питання правового регулювання використання ШІ, необхідність захисту персональних даних та забезпечення приватності громадян. Окрім цього, виникає потреба в адаптації ШІ для специфічних потреб поліції, таких як моніторинг великих обсягів даних, розпізнавання облич і боротьба з кіберзлочинністю. Поряд із технічними аспектами залишається невирішеним питання етичності використання ШІ, щоб уникнути можливих зловживань та дискримінаційних практик у правоохоронній діяльності.

Аналіз останніх досліджень і публікацій. Попри невеликий строк існування штучного інтелекту, в Україні вже проведено низку досліджень, спрямованих на його впровадження в державні органи. Зокрема, актуальні проблеми застосування ШІ в правоохорон-

ній діяльності та його роль у підвищенні ефективності боротьби зі злочинністю були предметом дослідження О. Зачека, Ю. Дмитрика та В. Сеника. Використання ШІ у протидії злочинності також досліджували Т. Шевчук та Я. Свистун. Колективом авторів монографії «Стратегія розвитку штучного інтелекту в Україні» під загальною редакцією А. Шевченка було розглянуто передумови та наукові засади створення стратегії розвитку ШІ в Україні, а також засоби й шляхи її ефективної імплементації. Ці дослідження заклали важливу науково-теоретичну базу для розуміння можливостей і викликів, пов'язаних із впровадженням ШІ в українських реаліях. Однак, незважаючи на ці напрацювання, реальне практичне використання ШІ в правоохоронних органах, зокрема в Національній поліції України, перебуває на початковому етапі. Досвід інших країн доводить, що ШІ може значно підвищити ефективність правоохоронної діяльності через аналіз великих обсягів даних, прогнозування злочинності та автоматизацію операційних процесів. Важливим є використання технологій ШІ для аналізу відеоспостереження, моніторингу інтернет-активності та створення аналітичних звітів, що вже активно застосовується в міжнародній практиці.

Отже, перспективи впровадження штучного інтелекту в діяльність Національної поліції України мають величезний потенціал, але потребують подальших досліджень, законодавчого регулювання та практичного тестування. Тому **метою статті** є дослідження можливостей інтеграції штучного інтелекту у діяльність Національної поліції України з урахуванням потенційних ризиків, викликів та правових аспектів, а також розробка рекомендацій щодо впровадження технологій ШІ з урахуванням специфічних потреб цієї сфери.

Виклад основного матеріалу. Штучний інтелект (ШІ) останніми роками стає невіддільною частиною технологічного прогресу, глибоко впливаючи на всі аспекти суспільного життя, включаючи правоохоронну діяльність. Завдяки здатності ШІ обробляти великі обсяги даних та аналізувати інформацію в реальному часі, він визнаний ефективним інструментом у боротьбі зі злочинністю [1, с. 149]. Особливого значення надається використанню ШІ для прогнозування кримінальних дій, профілювання злочинців та поліпшення процесів розслідування правопорушень, що дозволяє правоохоронним органам діяти більш оперативно та ефективно.

Згідно з дослідженнями Європейського парламенту, впровадження ШІ в правоохоронні органи Європейського Союзу вже показало позитивні результати. У 2022 році технології ШІ сприяли зниженню рівня злочинності на 15% завдяки точнішому моніторингу правопорушень, прогнозуванню потенційних інцидентів і вдосконаленню процедур розслідування [2]. Ці результати підтверджують ефективність ШІ як одного з ключових елементів цифрової трансформації правоохоронної системи.

В Україні також починається поступове впровадження технологій ШІ. Одним із найбільш перспективних напрямків є автоматизація відеоспостереження. Наприклад, технології розпізнавання облич на основі машинного навчання дозволяють у реальному часі відстежувати підозрюваних, аналізувати поведінку людей на масових заходах та виявляти потенційні загрози безпеці. Такі технології вже використовуються у великих містах, таких як Київ, для підвищення рівня громадської безпеки та моніторингу публічних місць [3, с. 130].

Проте впровадження ШІ в Україні стикається з інфраструктурними та технічними обмеженнями, зокрема через пошкодження комунікаційних мереж, нестабільне енергопостачання та обмежені інформаційно-технічні ресурси. Ці виклики ускладнюють ефективне використання ШІ для аналізу великих масивів даних, моніторингу кіберзлочинів та оперативної роботи поліції в реальному часі. В умовах війни та повоєнної відбудови необхідно враховувати ці обмеження під час планування впровадження ШІ, розвиваючи технічну базу та адаптуючи новітні технології до реалій української інфраструктури.

Незважаючи на технологічні досягнення, існують важливі правові та етичні виклики, пов'язані з використанням ШІ в правоохоронній діяльності. Зокрема, це питання захисту прав людини, особливо права на приватність і захист персональних даних. Європейські дослідження наголошують на необхідності балансування між ефективністю правоохоронних заходів та дотриманням прав людини, особливо при обробці великих масивів конфіденційної інформації громадян [4].

Науковий підхід до розвитку ШІ зосереджується на кількох ключових технологіях, зокрема на машинному навчанні (ML) та глибокому навчанні (DL), що становлять основні підсистеми штучного інтелекту [5]. Машинне навчання – це один із напрямів розвитку ШІ, який дозволяє алгоритмам самостійно навчатися, обробляючи великі обсяги даних без явного програмування на кожен конкретний сценарій. Основним підходом у ML є нейронні мережі – математичні моделі, що імітують структуру і функції людського мозку [6, с. 80]. Вони складаються з кількох шарів нейронів: вхідного, прихованого та вихідного шару. Цей підхід дозволяє ШІ вчитися шляхом зворотного поширення помилки та оптимізації параметрів для досягнення бажаного результату [7, с. 34]. Наприклад, для задачі розпізнавання зображень може бути використана конволюційна нейронна мережа (CNN), яка здатна аналізувати візуальні дані, класифікуючи об'єкти на основі шаблонів, виявлених у навчальному датасеті. Такі системи особливо корисні для поліції при автоматизації аналізу відео та розпізнавання підозрюваних за допомогою камер відеоспостереження.

Глибоке навчання (DL) є підвидом машинного навчання, що використовує багатошарові нейронні мережі для обробки даних, дозволяючи системам ШІ виконувати складні завдання, які раніше вимагали участі людини [8]. Це включає розпізнавання обличчя, аналіз великих масивів текстової інформації, розробку прогнозних моделей для передбачення злочинної активності та інші завдання, які є важливими для правоохоронних органів. Наприклад, у США використання технологій ШІ дозволило значно покращити ефективність пошуку злочинців через аналіз відео з камер спостереження на основі CNN [9].

Проте питання етичної та правової відповідності таких технологій продовжують бути предметом активних наукових дискусій [10; 11; 12]. Наприклад, мовні моделі, такі як ChatGPT, які спеціалізуються на обробці природної мови, використовують алгоритми ML, але не є повноцінними системами ШІ [13]. Попри їхню потужність, вони мають обмеження, що пов'язані з недостатньою прозорістю процесів прийняття рішень та можливими упередженнями в результатах роботи.

З огляду на це, науковці активно досліджують можливості вдосконалення алгоритмів ШІ для забезпечення етичності та законності їхнього використання у правоохоронних органах [14]. Зокрема, дослідження в галузі права й технологій наголошують на необхід-

ності розробки правових механізмів, що забезпечують прозорість процесів прийняття рішень ШІ та відповідальність за їх наслідки. Питання про контроль за використанням ШІ стає ще більш актуальним в умовах глобальної політичної напруженості та підвищеного рівня кіберзлочинності.

Отже, наукове дослідження штучного інтелекту як інструмента у правоохоронній діяльності включає не лише технологічні аспекти, але й глибоке вивчення етичних та правових викликів, пов'язаних із його застосуванням. Створення регуляторних рамок, які забезпечують дотримання прав людини при використанні ШІ, є одним із найважливіших завдань сучасної наукової спільноти.

Використання ШІ у діяльності поліції охоплює різні напрями, які дозволяють значно підвищити ефективність правоохоронних органів. Серед ключових прикладів застосування ШІ можна виділити наступні:

1. *Формування стенограм*. ШІ активно використовується для автоматизації створення стенограм, що дозволяє значно зекономити час на підготовку документів у правоохоронних органах. Такі сервіси, як Google Speech-to-Text та Otter.ai, забезпечують швидке перетворення аудіозаписів допитів, судових слухань або брифінгів у текстові документи [15]. Ці системи використовують алгоритми машинного навчання для підвищення точності розпізнавання мовлення, що допомагає зменшити кількість помилок у стенограмах. ШІ також може інтегруватися з іншими інструментами, такими як системи управління документами, для автоматичного збереження та класифікації стенограм.

2. *Моніторинг активностей в мережі.* ШІ здатен проводити моніторинг активностей у мережі Інтернет, включаючи соціальні мережі, форуми, новинні сайти та блоги. Використовуючи інструменти, такі як DataMiner або спеціалізовані системи аналізу контенту, правоохоронні органи можуть відстежувати ключові теми обговорення, прогнозувати злочинні дії та виявляти потенційні загрози [16]. Алгоритми ШІ здатні автоматично виділяти важливу інформацію, фільтрувати фейкові новини та виявляти зловмисників, що діють в Інтернеті. Цей процес допомагає кіберполіції швидко ідентифікувати загрози та зменшити час на обробку інформації.

3. *Оптимізація роботи з ІКС ІПНП («Армор»).* Інформаційно-пошукові системи, такі як ІКС ІПНП «Армор», використовуються для управління розслідуваннями, зберігання та обробки даних [17, с. 182–183]. Впровадження ШІ в такі системи дозволяє автоматизувати рутинні процеси, такі як обробка та класифікація доказів. ШІ здатен швидко аналізувати великі обсяги даних, виявляти закономірності або аномалії, що допомагає правоохоронцям ухвалювати оперативні рішення на основі реальних даних. Крім того, ШІ може використовуватися для прогнозування розвитку подій або для створення сценаріїв, що дозволяють запобігати злочинам.

4. *Розпізнавання облич і відеоаналітика*. Одним із найпоширеніших застосувань ШІ в поліції є використання систем розпізнавання облич. За допомогою нейронних мереж, таких як YOLO (You Only Look Once) [18], поліцейські можуть автоматично розпізнавати підозрюваних або виявляти правопорушників на відеозаписах. Системи відеоаналітики дозволяють в режимі реального часу аналізувати потоки відео з камер спостереження, що підвищує ефективність розшуку злочинців. Такі технології вже застосовуються у багатьох країнах для забезпечення громадської безпеки на масових заходах або в місцях з великим скупченням людей.

5. *Прогнозування злочинів.* ШІ може бути використаний для прогнозування злочинів на основі аналізу історичних даних. Такі системи, як PredPol, використовують алгоритми машинного навчання для визначення зон з підвищеним ризиком злочинності на основі патернів поведінки [19]. Правоохоронні органи можуть використовувати ці дані для планування патрулювання та превентивних заходів у потенційно небезпечних районах. Прогнозування дозволяє поліції не тільки реагувати на злочини, але й запобігати їм.

6. *Аналіз великих даних і кіберзлочинність.* В умовах чимраз більшої кіберзлочинності ШІ допомагає поліції аналізувати великі обсяги даних, зокрема зламані бази даних, лог-файли та цифрові докази. Такі інструменти, як Splunk та IBM Watson, можуть обробляти величезні масиви даних, виявляючи кіберзагрози або аномальні дії в комп'ютерних мережах. ШІ-системи також можуть автоматично визначати атаки за підозрілими патернами та негайно попереджати правоохоронні органи про потенційні зломи [20].

7. *Робота з безпілотниками та сенсорними системами.* Безпілотні літальні апарати (БПЛА), оснащені системами ШІ, стають важливим інструментом для правоохоронних органів. Вони можуть використовуватися для моніторингу ситуації на місцях злочину, пошуку підозрюваних або спостереження за великими територіями [21]. Крім того, БПЛА можуть оснащуватися датчиками та камерами, які передають інформацію в режимі реального часу для подальшого аналізу за допомогою ШІ-систем [22].

Актуальність використання таких технологій ще більше зросла у зв'язку з російською агресією, що триває. В умовах війни, яка супроводжується зростанням рівня злочинності, військовими та гібридними загрозами, БПЛА з ШІ здатні виконувати критично важливі завдання щодо моніторингу порушень на окупованих або небезпечних територіях, виявлення та фіксації доказів воєнних злочинів, а також забезпечення безпеки мирних громадян. Використання таких інструментів дозволяє українським правоохоронним органам оперативно реагувати на загрози, підвищуючи ефективність дій у надзвичайних ситуаціях, що виникають у результаті збройного конфлікту [23].

8. *Аналіз поведінки підозрюваних.* ШІ може допомогти поліції у вивченні поведінкових патернів підозрюваних або осіб, що знаходяться під слідством. За допомогою алгоритмів, що аналізують фізіологічні показники, вирази обличчя та жести, можна оцінити ймовірність причетності особи до злочину. Такі системи вже використовуються в деяких країнах для проведення співбесід з підозрюваними. Наприклад, такі платформи, як CrowdStrike, застосовують аналіз поведінкових патернів для виявлення відхилень від норм і прогнозування можливих загроз безпеці [24].

Впровадження технологій штучного інтелекту в правоохоронній діяльності несе певні ризики, особливо в контексті захисту персональних даних та інформаційної безпеки. Одним із найбільших ризиків є потенційний витік даних, що може статися через вразливості у ШІ-системах. Наприклад, випадки кібератак на державні системи показують, що навіть передові технології не завжди гарантують повний захист інформації [25].

Ще одним викликом є зловживання інформацією. Оскільки системи ШІ часто використовуються для обробки великих обсягів даних, зокрема біометричних та персональних, існує ризик, що ці дані можуть бути використані неправомірно або без згоди громадян

[26, с. 20]. Юридичні наслідки таких порушень можуть бути значними, включаючи штрафи за недотримання норм захисту даних відповідно до українського законодавства та міжнародних стандартів.

Крім того, необхідно встановити відповідальність за прийняття рішень на основі ШІ-систем. На міжнародному рівні триває дискусія щодо того, хто несе відповідальність за помилки або порушення, які можуть виникнути внаслідок використання алгоритмів ШІ – розробники, правоохоронні органи чи безпосередньо держава [27].

Це питання набуває особливої актуальності в умовах дедалі більшого використання ШІ для обробки персональних даних. Наприклад, Закон України «Про захист персональних даних», регламентує збирання, зберігання та обробку біометричних та інших персональних даних громадян [28]. Важливо відзначити, що ШІ-технології, такі як системи розпізнавання обличчя або аналіз поведінкових патернів, часто використовують саме ці дані, що створює ризики для конфіденційності громадян. Зокрема одне з найбільших порушень пов'язане з використанням ШІ для негласних слідчих (розшукових) дій (НСРД) без належного дозволу судових органів або без належного інформування осіб, чиї дані обробляються. Таке застосування технологій є порушенням статті 31 Конституції України, яка гарантує право на приватність і захист від втручання в приватне життя без законних підстав [29].

Щобільше, використання систем для моніторингу Інтернет-активностей, соціальних мереж або комунікацій, хоча і може бути корисним для кіберполіції, інколи викликає сумніви з погляду законності таких дій. Це може розглядатися як порушення права людини на свободу та особисту недоторканність, закріпленого у статті 8 Конвенції про захист прав людини і основоположних свобод [30]. Для уникнення таких правопорушень ми вважаємо необхідним здійснити низку конкретних кроків. По-перше, слід розробити та впровадити нормативно-правові акти, які регулюватимуть використання технологій моніторингу відповідно до міжнародних стандартів, таких як Конвенція про захист прав людини і основоположних свобод та Загальний регламент захисту даних (GDPR). Важливо, щоб ці акти чітко визначали умови, за яких допускається використання подібних систем, включно з обов'язковим отриманням судових рішень або інших легітимних підстав для проведення моніторингу. По-друге, необхідно створити незалежний механізм нагляду, який здійснюватиме постійний аудит дій правоохоронних органів щодо використання систем моніторингу. Це може бути спеціальний орган або громадська комісія, що забезпечуватимуть прозорість процесів і захист прав громадян. По-третє, державі слід активно сприяти впровадженню новітніх технологій захисту даних, таких як шифрування, а також інших технічних рішень, які мінімізують ризики незаконного використання особистої інформації.

Отже, комплексний підхід, що включає удосконалення законодавства, впровадження незалежних механізмів нагляду та використання сучасних технологій захисту даних, дозволить забезпечити ефективний захист прав людини в умовах чимраз більшого використання систем моніторингу та інших інструментів ШІ.

З розвитком ШІ та нових технологій Україна стикається з новими викликами у сфері захисту персональних даних. Адаптація до стандартів GDPR (Загальний регламент захисту даних) стає необхідною для забезпечення відповідності міжнародним вимогам. Це включає організаційні зміни, підготовку спеціалістів, проведення інформаційних кампаній та зміцнення технічних засобів захисту. Тому Україні потрібно не лише вдосконалювати свої нормативні акти, але й впроваджувати ефективні механізми захисту даних у відповідь на нові виклики, що з'являються з розвитком технологій [31, с. 689]. Україна також повинна адаптувати своє законодавство до нових технологій, щоб забезпечити належний контроль за використанням ШІ у правоохоронній діяльності та уникнути зловживань, які можуть призвести до порушення прав людини.

Щодо міжнародного досвіду, то варто зазначити, що у країнах Європейського Союзу вже впроваджуються законодавчі обмеження щодо використання ШІ у діяльності правоохоронних органів. Так, законопроєкт «Акт про штучний інтелект», запропонований Європейською комісією, встановлює суворі правила щодо захисту прав громадян і обмежень на використання технологій, що можуть втручатися у приватне життя [32].

Висновки. Впровадження штучного інтелекту в діяльність Національної поліції України відкриває значні можливості для підвищення ефективності боротьби зі злочинністю, зокрема у профілактиці та розслідуванні правопорушень. Здатність ШІ обробляти великі обсяги даних у реальному часі, автоматизувати рутинні процеси та покращувати моніторинг дозволяє правоохоронним органам діяти більш швидко й ефективно.

Проте, разом із новими можливостями, впровадження ШІ супроводжується серйозними викликами. Один із ключових аспектів – це необхідність законодавчого регулювання, яке б забезпечувало баланс між ефективністю використання ШІ та захистом прав громадян, зокрема права на приватність. Особливого значення також набуває питання безпеки даних через ризики витоків конфіденційної інформації та можливі зловживання. Крім того, впровадження ШІ пов'язане з низкою етичних питань, зокрема щодо прозорості ухвалення рішень і відповідальності за їх наслідки.

Для успішного впровадження штучного інтелекту в правоохоронну діяльність України необхідно розробити чіткі правові механізми, які регулюватимуть його використання, та забезпечити ефективний нагляд за застосуванням цих технологій. Одним із ключових завдань є визначення відповідальності за рішення, ухвалені з використанням ШІ, а також дотримання етичних стандартів.

Подальші дослідження в цій сфері мають бути спрямовані не лише на вдосконалення технологічних аспектів ШІ, але й на розробку чітких нормативно-правових актів, які регулюватимуть його використання в українських реаліях і забезпечуватимуть захист прав людини.

Список використаних джерел

1. Зачек О. І., Дмитрик Ю. І., Сеник В. В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2023. № 3. С. 148–156. DOI: https://doi.org/10.32782/2311-8040/2023-3-19

2. Police use of AI: A Force for good or a public threat? Eviden. 18.09.2023. URL: https://eviden.com/insights/blogs/police-use-of-ai-a-force-for-good-or-a-public-threat/ (дата звернення: 20.09.2024).

3. Шевчук Т. А., Свистун Я. В. Використання штучного інтелекту у протидії злочинності. *Вісник кримінологічної асоціації України*. 2021. № 2 (25). С. 128–134.

4. Artificial Intelligence. Wikipedia : сайт. URL: https://en.wikipedia.org/wiki/Artificial_intelligence (дата звернення: 20.09.2024).

5. Що таке штучний інтелект: історія, види та складові. *GIGACLOUD* : сайт. 16.05.2023. URL: https://gigacloud.ua/blog/navchannja/scho-take-shtuchnij-intelekt-istorija-vidi-ta-skladovi (дата звернення: 20.09.2024).

6. Іванотчак О., Кеденко І., Куліш С., Глібчук А., Дмитренок С. Концептуалізація нейромоделей задач підтримки прийняття рішень. *Вісник Хмельницького національного університету. Технічні науки*. 2024. № 3, т. 1 (335). С. 78–87. DOI: 10.31891/2307-5732-2024-335-3-11

7. Інтелектуальні системи автоматизації : монографія / Аврунін О. Г., Владов С. І., Петченко М. В., Семенець В. В., Татарінов В. В., Тельнова Г. В., Філатов В. О., Шмельов Ю. М., Шушляпіна Н. О. Кременчук : Вид-во «НОВАБУК», 2021. 322 с.

8. Neural Network. *Wikipedia* : сайт. URL: https://en.wikipedia.org/wiki/Artificial_neural_network (дата звернення: 20.09.2024).

9. Deep Learning. *Wikipedia* : сайт. URL: https://en.wikipedia.org/wiki/Deep_learning (дата звернення: 20.09.2024).

10. Каткова Т. Г. Штучний інтелект в Україні: правові аспекти. *Право і суспільство*. 2020. № 6. С. 46–55. DOI: https://doi.org/10.32842/2078-3736/2020.6.1.8

11. Турута О. В., Турута О. П. Штучний інтелект крізь призму фундаментальних прав людини. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2022. № 71. С. 49–54. DOI: https://doi.org/10.24144/2307-3322.2022.71.7

12. Яровой Т. С. Можливості та ризики використання штучного інтелекту в публічному управлінні. *Economic Synergy*. 2023. № 2. С. 36–47. DOI: https://doi.org/10.53920/ES-2023-2-3

13. OpenAI. ChatGPT Model. URL: https://openai.com/chatgpt (дата звернення: 20.09.2024).

14. Використання технологій штучного інтелекту у протидії злочинності : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. 112 с.

15. Google Speech-to-Text. *GoogleCloud* : сайт. URL: https://cloud.google.com/speech-to-text (дата звернення: 20.09.2024).

16. Real-time information – reimagined. *DataMiner* : сайт. URL: https://www.dataminr.com (дата звернення: 20.09.2024).

17. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції : навч. посібник / А. В. Мовчан. Львів : ЛьвДУВС, 2017. 244 с.

18. Real-Time Object Detection. *YOLO* : сайт. URL: https://pjreddie.com/darknet/yolo/ (дата звернення: 20.09.2024).

19. Predictive Policing Technology. *PredPol* : сайт. URL: https://www.predpol.com (дата звернення: 20.09.2024).

20. Data-to-Everything Platform. *Splunk* : сайт. URL: https://www.splunk.com (дата звернення: 20.09.2024).

21. Мовчан А. В., Мовчан М. А. Використання безпілотних літальних апаратів у діяльності правоохоронних органів. *Соціально-правові студії*. 2020. Вип. 3 (9). С. 104–110.

22. Demonstrating Autonomous Operations in the Public Safety & Security Sector. *The Drone Centre* : сайт. URL: https://thedronecentre.ae/autonomous-drones-in-the-police-force/ (дата звернення: 20.09.2024).

23. Особливості застосування безпілотних літальних апаратів органами та підрозділами поліції: метод. рек. / А. А. Саковський, С. М. Науменко, С. І. Кравченко, І. М. Єфіменко та ін. Київ : Нац. акад. внутр. справ. 2022. 72 с.

24. CrowdStrike: We Stop Breaches with AI-native Cybersecurity. *CrowdStrike* : сайт. URL: https://www.crowdstrike.com/en-us/ (дата звернення: 20.09.2024).

25. Україна з 14 січня 2022 року залишається на першому місці у світі за кількістю кібератак проти неї – заступник голови Держспецзв'язку. *Interfax – Україна* : сайт. 23.05.2023. URL: https://interfax.com.ua/news/interview/911979.html (дата звернення: 20.09.2024).

26. Права людини в епоху штучного інтелекту: виклики та правове регулювання. 2024. 44 с. URL: https://eu4digitalua.eu/wp-content/uploads/2024/02/guia_ukr_5.pdf (дата звернення: 20.09.2024).

27. Artificial intelligence liability directive. BRIEFING EU Legislation in Progress. *European Parliament* : сайт. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf (дата звернення: 20.09.2024).

28. Про захист персональних даних : Закон України від 1 червня 2010 року № 2297-VI (із змін.) // БД «Законодавство України» / ВР України. URL: http://zakon5.rada.gov.ua/laws/show/2297-17 (дата звернення: 20.09.2024).

29. Конституція України від 28 червня 1996 р. (із змін.) // БД «Законодавство України» / ВР України. URL: http://zakon1.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 20.09.2024).

30. Конвенція про захист прав людини і основоположних свобод: прийнята Радою Європи 4 листопада 1950 р. // БД «Законодавство України» / ВР України URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 20.09.2024).

31. Синжерян А. А. Історія становлення законодавства Україні про захист персональних даних. *European scientific congress* : The 12th International scientific and practical conference (Madrid, Spain, December 25–27, 2023). Madrid, 2023. P. 687–690.

32. Proposal for a Regulation laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act). *European Commission* : сайт. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (дата звернення: 20.09.2024).

References

1. Zachek, O., Dmytryk, Y., & Senyk, V. (2023). Rol shtuchnoho intelektu v pidvyshchenni efektyvnosti pravookhoronnoi diialnosti [The Role of Artificial Intelligence in Increasing Efficiency in Law Enforcement Activities]. *Naukovyi visnyk Lvivsko-*

ho derzhavnoho universytetu vnutrishnikh sprav. Seriia yurydychna, 3, 148–156. DOI: doi.org/10.32782/2311-8040/2023-3-19 [in Ukrainian].

2. Police use of AI: A Force for good or a public threat? *Eviden* (September 18, 2023). Retrieved from: https://eviden.com/insights/blogs/police-use-of-ai-a-force-for-good-or-a-public-threat/ (date of application: 20.09.2024) [in English].

3. Shevchuk, T.A., & Svystun, Y.V. (2021). Vykorystannia shtuchnoho intelektu u protydii zlochynnosti [Use of Artificial Intelligence in Crime Combating]. *Visnyk kryminolohichnoi asotsiatsii Ukrainy*, 2(25), 128–134 [in Ukrainian].

4. Artificial Intelligence. Retrieved from: https://en.wikipedia.org/wiki/Artificial_intelligence (date of application: 20.09.2024) [in English].

5. Shcho take shtuchnyi intelekt: istoriia, vydy ta skladovi [What is artificial intelligence: history, types and components]. *GIGACLOUD* (May 16, 2023). Retrieved from: https://gigacloud.ua/blog/navchannja/scho-take-shtuchnij-intelekt-istorija-vidi-ta-skladovi (date of application: 20.09.2024) [in Ukrainian].

6. Ivanotchak, O., Kedenko, I., Kulish, S., Hlibchuk, A., & Dmytrenok, S. (2024). Kontseptualizatsiia neiromodelei zadach pidtrymky pryiniattia rishen [Conceptualization of Neural Models for Decision Support Tasks]. *Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky*, 3(335), 78–87. DOI: doi.org/10.31891/2307-5732-2024-335-3-11 [in Ukrainian].

7. Avrunin, O.G., Vladov, S.I., Petchenko, M.V., Semenets, V.V., Tatarinov, V.V., Telnova, H.V., Filatov, V.O., Shmelyov, Y.M., & Shushlyapina, N.O. (2021). *Intelektualni systemy avtomatyzatsii [Intellectual automation systems]:* monohrafiia / Kremenchuk : Vyd-vo «NOVABUK», 2021. 322 s. [in Ukrainian].

8. Neural Network. Retrieved from: https://en.wikipedia.org/wiki/Artificial_neural_network (date of application: 20.09.2024) [in English].

9. Deep Learning. Retrieved from: https://en.wikipedia.org/wiki/Deep_learning (date of application: 20.09.2024) [in English].

10. Katkova, T.H. (2020). Shtuchnyi intelekt v Ukraini: pravovi aspekty [Artificial intelligence in Ukraine: Legal aspects]. *Pravo i suspilstvo*, 6, 46–55. DOI: doi.org/10.32842/2078-3736/2020.6.1.8 [in Ukrainian].

11. Turuta, O.V., & Turuta, O.P. (2022). Shtuchnyi intelekt kriz pryzmu fundamentalnykh prav liudyny [Artificial intelligence through the lens of fundamental human rights]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo,* (71), 49–54. DOI: doi.org/10.24144/2307-3322.2022.71.7 [in Ukrainian].

12. Yarovoi, T.S. (2023). Mozhlyvosti ta ryzyky vykorystannia shtuchnoho intelektu v publichnomu upravlinni [Opportunities and risks of using artificial intelligence in public administration]. *Economic Synergy,* (2), 36–47. DOI: https://doi.org/10.53920/ES-2023-2-3 [in Ukrainian].

13. OpenAI. ChatGPT Model. Retrieved from: https://openai.com/chatgpt (date of application: 20.09.2024) [in English].

14. Vykorystannia tekhnolohii shtuchnoho intelektu u protydii zlochynnosti (2020). [Use of artificial intelligence technologies in combating crime]: materialy nauk.-prakt. onlain-seminaru, m. Kharkiv, 5 lystop. 2020 r. Kharkiv : Pravo. 112 s. [in Ukrainian].

15. Google Speech-to-Text. Retrieved from: https://cloud.google.com/speech-to-text (date of application: 20.09.2024) [in English].

16. Real-time information – reimagined. Retrieved from: https://www.dataminr.com (date of application: 20.09.2024) [in English].

17. Movchan, A.V. (2017). Informatsiino-analitychna robota v operatyvno-rozshukovii diialnosti Natsionalnoi politsii [Information and analytical work in the operational-search activity of the National Police]: navch. posibnyk. Lviv: LvDUVS. 244 s. [in Ukrainian].

18. Real-Time Object Detection. Retrieved from: https://pjreddie.com/darknet/yolo/ (date of application: 20.09.2024) [in English].

19. Predictive Policing Technology. Retrieved from: https://www.predpol.com (date of application: 20.09.2024) [in English].

20. Data-to-Everything Platform. Retrieved from: https://www.splunk.com (date of application: 20.09.2024) [in English].

21. Movchan, A., Movchan, M. (2020). Vykorystannia bezpilotnykh litalnykh aparativ u diialnosti pravookhoronnykh orhaniv [Use of Unmanned Aerial Vehicles in the Activities of Law Enforcement Agencies]. *Sotsialno-pravovi studii*, 3 (9), 104–110 [in Ukrainian].

22. Demonstrating Autonomous Operations in the Public Safety & Security Sector. Retrieved from: https://thedronecentre.ae/autonomous-drones-in-the-police-force/ (date of application: 20.09.2024) [in English].

23. Sakovskyi, A.A., Naumenko, S.M., Kravchenko, S.I., & Yefimenko, I.M., et al. (2022). *Osoblyvosti zastosuvannia bezpilotnykh litalnykh aparativ orhanamy ta pidrozdilamy politsii [Features of the use of unmanned aerial vehicles by police bodies and units]:* metod. rek. Kyiv : Nats. akad. vnutr. Sprav. 72 s. [in Ukrainian].

24. CrowdStrike: We Stop Breaches with AI-native Cybersecurity. Retrieved from: https://www.crowdstrike.com/en-us/ (date of application: 20.09.2024) [in English].

25. Ukraina z 14 sichnia 2022 roku zalyshaietsia na pershomu mistsi u sviti za kilkistiu kiberatak proty nei – zastupnyk holovy Derzhspetszviazku. *Interfax – Ukraina* (May 23, 2023). Retrieved from: https://interfax.com.ua/news/interview/911979.html (date of application: 20.09.2024) [in Ukrainian].

26. Prava liudyny v epokhu shtuchnoho intelektu: vyklyky ta pravove rehuliuvannia. 2024. 44 s. Retrieved from: https://eu4digitalua.eu/wp-content/uploads/2024/02/guia_ukr_5.pdf (date of application: 20.09.2024) [in Ukrainian].

27. Artificial intelligence liability directive. BRIEFING EU Legislation in Progress. Retrieved from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf (date of application: 20.09.2024) [in English].

28. Zakon Ukrainy "Pro zakhyst personalnykh danykh" [Law of Ukraine "On the protection of personal data] vid 1 chervnia 2010 roku № 2297-VI (iz zmin.). Retrieved from: http://zakon5.rada.gov.ua/laws/show/2297-17 (date of application: 20.09.2024) [in Ukrainian].

29. Konstytutsiia Ukrainy [Constitution of Ukraine] vid 28 chervnia 1996 r. (iz zmin.). Retrieved from: http://zakon1.rada.gov.ua/laws/show/254к/96-вр (date of application: 20.09.2024) [in Ukrainian].

30. Konventsiia pro zakhyst prav liudyny i osnovopolozhnykh svobod [Convention for the Protection of Human Rights and Fundamental Freedoms] pryiniata Radoiu Yevropy 4 lystopada 1950 r. Retrieved from: https://zakon.rada.gov.ua/laws/show/995_004 (date of application: 20.09.2024) [in Ukrainian].

31. Synzherian, A.A. (2023). Istoriia stanovlennia zakonodavstva Ukraini pro zakhyst personalnykh danykh [The history of the formation of legislation in Ukraine on the protection of personal data]. European scientific congress : The 12th International scientific and practical conference, Madrid, Spain, December 25–27, 2023. Madrid, 2023. S. 687–690 [in Ukrainian].

32. Proposal for a Regulation laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act). Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (date of application: 20.09.2024) [in English].

Gudz Tetyana,
Candidate of Juridical Sciences, Associate Professor
(Kharkiv National University of Internal Affairs, Kharkiv)
ORCID: 0000-0002-6950-6136

Synzherian Andrii,
Cadet
(Kharkiv National University of Internal Affairs, Kharkiv)
ORCID: 0009-0001-6063-4254

INTEGRATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGY INTO THE ACTIVITIES OF THE NATIONAL POLICE OF UKRAINE: PROSPECTS AND CHALLENGES

The article is dedicated to the integration of artificial intelligence (AI) into the activities of the National Police of Ukraine. It emphasizes that the use of AI can significantly transform information processing, automate processes, and enhance police efficiency, particularly in monitoring the Internet and social networks to prevent and solve crimes. However, one of the key challenges in implementing AI in law enforcement is the lack of proper legal regulation. The use of AI-based systems, such as facial recognition technologies or crime prediction tools, may lead to violations of citizens' privacy and even discrimination if these systems are employed without appropriate oversight and transparency. The need to protect personal data in the context of increasing AI usage is especially pressing, as Ukraine must comply with international standards such as the General Data Protection Regulation (GDPR) to ensure adequate information protection.

In addition, overcoming technical limitations related to infrastructure, unstable power supply, and insufficient resources is essential for the effective use of AI.

The article proposes the introduction of legal acts to regulate AI use and ensure its controlled application. The creation of an independent oversight mechanism, as well as the implementation of modern data protection technologies such as encryption, will help minimize the risks of unauthorized access to personal information. Thus, the combination of legislative regulation, technical modernization, and process transparency will contribute to enhancing police efficiency and protecting human rights in the context of digital transformation.

Key words: *artificial intelligence, National Police, automation, cybersecurity, personal data.*