УДК 342.7
DOI https://doi.org/10.32782/ln.2024.24.22

Мазепа С.О.,
кандидат юридичних наук, доцент,
доцент кафедри кримінального права та процесу
Західноукраїнський національний університет,
міжнародний дослідник,
Оснабрюцький університет
ORCID ID: 0000-0003-1282-9089

ВИКЛИКИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Вступ. Штучний інтелект – це інструмент, який не лише полегшує життя людей в різних сферах, але й несе в собі потенційну загрозу. На останніх наукових і практичних конференціях у світі піднімаються питання етичного використання ШІ, його регулювання та контролю. Інструменти ШІ все активніше використовуються і для покращення ефективності правоохоронних органів, особливо у сфері аналізу великих даних, ідентифікації підозрюваних, прогнозування злочинності, ідентифікації крадіїв у магазинах, виявлення підроблених авто, підтримки слідчих при інтерв'ю, аналітики соцмереж, виявлення експлуатації дітей та ін [1]. Наукові роботи Басистої І., Дуфенюк О., Карчевського М., Сови М., Стрільцової О. та інших присвячені використанню штучного інтелекту у правоохоронній діяльності. Але існуючі розробки переважно піднімають питання проблем регулювання та використання ШІ, але мало висвітлюють саме виклики для забезпечення інформаційної безпеки у правоохоронній сфері.

Мета статті полягає у аналізі певних видів правоохоронної діяльності та потенційних ризиків в контексті забезпечення інформаційної безпеки під час застосування штучного інтелекту.

Виклад основного матеріалу. Сьогодні Україна активно готується до підписання Рамкової конвенції Ради Європи про штучний інтелект, права людини, демократію та верховенство права. Питання відповідального використання ШІ та відповідальності будуть центральними найближчі кілька років. З основних ризиків, які можуть виникнути під час застосування ШІ це порушення прав людини та витік персональних даних [4]. Як зазначає О. П. Андрущенко, важливо, щоб система ШІ, яка застосовується для боротьби зі злочинністю, була прозорою і підлягала громадському контролю [5, с. 189].

У сучасних умовах України кіберзагрози становлять серйозну небезпеку. Системи на основі ШІ, особливо пов'язані з державними реєстрами чи критичною інфраструктурою, можуть стати об'єктами хакерських атак. Несанкціонований доступ до них відкриває можливості для витоку, передачі або маніпулювання даними з метою компрометації чи вербування. Особливу тривогу викликає використання ШІ у судових рішеннях – навіть незначне втручання в алгоритм може мати фатальні наслідки для підозрюваних.

Сучасна поліція дедалі частіше має справу з величезними обсягами складних даних, які неможливо ефективно обробити звичайними засобами. Для цього використовуються потужні бази даних, хмарні сервіси та штучний інтелект, зокрема технології машинного навчання. Основна мета -швидке отримання важливої інформації. Наприклад:

– автоматичне виявлення прізвищ, імен, номерів телефонів, адрес та інших деталей

у текстах без повного перегляду повідомлень;

– виявлення повторюваних злочинних схем, залежностей між злочинами та такими чинниками, як місцевість, погода чи сезонність;

– прогнозування потреб у силах поліції залежно від часу доби, пори року чи району [2].

Ці технології допомагають поліції діяти швидше й ефективніше, зменшуючи обсяг обробки персональних даних і зберігаючи конфіденційність. Із розвитком цифрових технологій таких інструментів у поліцейській практиці ставатиме дедалі більше. Впровадження штучного інтелекту в діяльність органів внутрішніх справ здатне суттєво підвищити їхню ефективність, оперативність і прозорість. Технології ШІ дозволяють автоматизувати рутинні процеси, пришвидшити аналіз даних, поліпшити якість прийняття рішень та виявлення загроз, а також сприяють підвищенню довіри громадськості завдяки прозорості алгоритмів.

Однак ефективне застосування таких технологій вимагає врахування національних і регіональних особливостей – зокрема, стану цифрової інфраструктури, рівня правової культури, специфіки роботи правоохоронних органів і суспільного сприйняття технологій. Крім того, ключовим чинником є підготовка персоналу – впровадження ШІ не матиме бажаного ефекту без належного навчання кадрів, здатних користуватись цими системами, розуміти їхні межі та ризики.

Також необхідно розвивати законодавчу базу: правове регулювання повинно чітко визначати межі використання ШІ, гарантувати захист персональних даних, забезпечувати алгоритмічну прозорість і контроль над прийняттям рішень, що впливають на права і свободи людини. Таким чином, впровадження ШІ у правоохоронну сферу – це не лише технологічне, а й організаційне, правове та етичне завдання, яке вимагає комплексного підходу. Незважаючи на те, що концепція предиктивної поліцейської діяльності є потужною, дуже важливо вирішувати проблеми, пов'язані з упередженістю даних та потенційними порушеннями громадянських свобод. Керівники правоохоронних органів повинні забезпечити навчання алгоритмів ШІ на різноманітних та об'єктивних наборах даних, щоб запобігти збереженню існуючої соціальної нерівності.

Штучний інтелект (ШІ) має потенціал радикально змінити діяльність поліції, зокрема через:

– аналітику даних – ШІ дозволяє ефективно аналізувати великі обсяги інформації, виявляти закономірності та приймати швидкі рішення у критичних ситуаціях (наприклад, під час рейдів чи захоплень заручників).

– кримінальний аналіз – завдяки машинному навчанню системи ШІ здатні ідентифікувати аномалії (зокрема у фінансових операціях), підтримувати міжнародні розслідування та розробляти цільові стратегії.

– глибинний аналіз – на відміну від традиційної аналітики, ШІ виявляє приховані зв'язки та причини злочинності, що залишаються непоміченими при ручній обробці.

– обробка цифрових доказів – у випадках, пов'язаних із цифровими пристроями, ШІ є критично важливим для аналізу обсягів даних, які неможливо опрацювати вручну.

– інструменти майбутнього – перспективними напрямами є використання OSINT/SOCMINT, обробка природної мови (NLP) і робота з великими наборами даних, що дозволяють модернізувати правоохоронну діяльність [2].

Йде активна робота щодо впровадження від концепцій до вже затверджених до використання систем (наприклад, системи передбачення злочинів або виявлення конфіденційної інформації) [4; с. 82].

У контексті інформаційної безпеки, використання штучного інтелекту (ШІ) в правоохоронних органах створює як нові можливості, так і ризики, які потребують системної оцінки та реагування. Мова йде про діяль-

ність поліції, прокуратури та Служби Безпеки України, які пов'язана із розслідуваннями правопорушень та їх привенцією.

Вважаємо за необхідне, деталізувати, що ми розглядаємо під поняттям «інформаційної безпеки в правоохоронній сфері». Наприклад, Шевчук М. Розглядає інформаційну безпеку як постійний процес діяльності компетентних органів, спрямований на попередження, протидію загрозам в інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються і здатні контролюватися тривалий час [9; с. 134]. Сопілко І. переконана, що інформаційна безпека та кібербезпека нерозривні, і інформаційна безпека орієнтована на захист від будь-яких загроз важливих даних, як у цифровій, так і в аналоговій формі. А кібербезпека, зосереджена на цифровій інформації, також нерозривно пов'язана із такими категоріями як кіберзлочини, кібератаки тощо [10; с. 113]. Ми, у свою чергу, можемо сказати, що інформаційна та кібербезпека співвідносяться як ціле і частина. І якщо говорити про інформаційну безпеку в правоохоронній сфері, то визначимо її як стан захищеності інформації, що використовується або створюється в процесі діяльності правоохоронних органів, її змісту та форм подання – від несанкціонованого доступу, витоку, пошкодження або знищення; а також забезпечення захисту працівників правоохоронних органів від деструктивного інформаційного впливу та гарантування інформаційних прав і свобод громадян, які у той чи інший спосіб вступають у правові відносини з цими органами. В умовах застосування штучного інтелекту, що потребує особливої уваги та надійного контролю за обробкою даних, прозорості алгоритмів і недопущення маніпулятивного чи неправомірного впливу на процеси правозастосування.

Основні ризики можна згрупувати за такими категоріями:

1. Компрометація конфіденційних даних

Витік персональних даних: обробка великих масивів даних про громадян (включаючи відео, біометрику, соцмережі) через AI-системи збільшує ймовірність витоків. Недостатня безпека моделей: моделі ШІ, навчені на чутливих даних, можуть бути об'єктом атак.

2. Залежність від непрозорих (black-box) алгоритмів. Відсутність пояснень рішень системи може призвести до невиправданих затримань, обшуків або дискримінації. Системні помилки в розпізнаванні облич, прогнозуванні злочинності тощо можуть мати наслідки для громадської довіри.

3. Вразливість до маніпуляцій. Атаки на моделі: зловмисники можуть отруїти навчальні дані або використовувати «adversarial examples» для обману систем. Підміна або спуфінг даних (наприклад, у системах розпізнавання облич або голосу) може призвести до помилкових рішень.

4. Порушення права на приватність

Масове стеження із використанням ШІ може виходити за межі необхідного та пропорційного втручання. Відсутність нормативно визначених меж використання сенсорів, камер, трекерів, аналізу соцмереж тощо.

5. Залежність від сторонніх постачальників. Використання комерційних AI-продуктів без повного контролю над кодом або даними може створити ризики бекдорів, втрати суверенітету над інформацією, витоку у треті країни.

6. Недостатній рівень захисту цифрової інфраструктури. AI-системи можуть бути підключені до старих або вразливих мереж правоохоронних органів, що відкриває шлях для кібератак на критичну інфраструктуру.

7. Зниження громадської довіри. У разі неправомірного або непрозорого використання ШІ суспільство може втратити довіру до правоохоронних органів, особливо в умовах гібридної війни та інформаційних атак.

8. Галюцінації. Використання інструментів штучного інтелекту для складання документів може спричинити викривлення даних, тому необхідно достонала перевірка усієї документації працівником із врахуванням можливості галюцинацій.

Висновки. Впровадження штучного інтелекту в роботу органів внутрішніх справ може суттєво підвищити їхню ефективність і відкритість. Водночас для успішного застосування необхідно враховувати специфіку національного контексту, забезпечити підготовку персоналу та удосконалити нормативно-правове регулювання. Інформаційна безпека в правоохоронній сфері, є невідємною частиною національної безпеки, тому регулювання відносин у сфері захисту інформації має бути першочерговим. В ході аналізу певних видів діяльності у правоохоронній сфері виявлено ряд ризиків, рекомендації щодо їх мінімізації будуть надані у наступній публікації.

Анотація

Стаття присвячена аналізу потенціалу та ризиків впровадження штучного інтелекту (ШІ) у діяльність правоохоронних органів у контексті забезпечення інформаційної безпеки. Автор звертає увагу на широке застосування ШІ для обробки великих масивів даних, ідентифікації підозрюваних, прогнозування злочинності та автоматизації оперативно-розшукової діяльності. Водночас наголошується на недостатньому висвітленні питань інформаційної безпеки в правоохоронних органах в наукових працях, що присвячені правовим аспектам використання ШІ. У статті визначено, що інформаційна безпека в правоохоронній сфері – це стан захищеності інформації та учасників правовідносин від деструктивного впливу, витоку, несанкціонованого доступу, маніпуляцій і технічних збоїв, з урахуванням зростаючої ролі ШІ. Розглянуто ключові ризики, зокрема: витік персональних даних, непрозорість алгоритмів, технологічна вразливість, порушення приватності, залежність від зовнішніх постачальників і загроза втрати громадської довіри. Автор підкреслює необхідність правового регулювання, етичного контролю, якісної підготовки кадрів та розвитку цифрової інфраструктури. У підсумку ШІ визнається потужним інструментом трансформації правоохоронної діяльності, але за умови дотримання принципів законності, пропорційності, відповідальності й захисту основоположних прав людини.

Ефективне застосування нових технологій вимагає врахування національних і регіональних особливостей – зокрема, стану цифрової інфраструктури, рівня правової культури, специфіки роботи правоохоронних органів і суспільного сприйняття технологій. Міжнародний обмін досвідом також має важливе значення. Крім того, ключовим чинником є підготовка персоналу – впровадження ШІ не матиме бажаного ефекту без належного навчання кадрів, здатних користуватись цими системами, розуміти їхні межі та ризики.

Ключові слова: правоохоронна діяльність, інформаційна безпека, штучний інтелект, виклики, загрози

Mazepa S.O. Challenges of using artificial intelligence in law enforcement

Summary

The article analyzes the potential and risks of implementing artificial intelligence (AI) in law enforcement activities in the context of ensuring information security. The author highlights the increasing use of AI for processing large data sets, identifying suspects, predicting crime, and automating investigative processes. At the same time, the paper notes that current academic research insufficiently addresses the challenges of information security in the law enforcement domain. Information security in this context is defined as a state of protection of data and participants in legal relations from destructive influence, unauthorized access, data leakage, manipulation, and technical failures, especially in light of the growing use of AI. The article outlines key risks, including personal data breaches, algorithmic opacity, technological vulnerabilities, violations of privacy, dependency on third-party vendors, and the potential loss of public trust. The author emphasizes the need for legal regulation, ethical oversight,

high-quality personnel training, and the development of digital infrastructure. In conclusion, AI is recognized as a powerful tool for transforming law enforcement, but only if the principles of legality, proportionality, accountability, and the protection of fundamental human rights are upheld.

The effective application of new technologies requires consideration of national and regional characteristics, including the state of digital infrastructure, the level of legal culture, the specifics of law enforcement agencies' work, and public perception of technologies. International exchange of experience is also important. In addition, staff training is a key factor – the introduction of AI will not have the desired effect without proper training of personnel capable of using these systems and understanding their limitations and risks.

Key words: law enforcement, information security, artificial intelligence, challenges, threats.

Список використаних джерел:

1. INTERPOL, UNICRI. Artificial Intelligence and Robotics for Law Enforcement: Global Meeting Report. Singapore, 2018. 77 p.
2. EUROPOL. AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement. Люксембург, 2024. 56 с.
3. Зачек О. І., Йосифович Д. І. Перспективи та проблеми застосування штучного інтелекту в діяльності правоохоронних органів. Аналітико-порівняльне законодавство. 2024. С. 680–689.
4. Бугера О. І. Використання штучного інтелекту для запобігання злочинності. Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки. 2021. Т. 32, № 71. С. 82–86.
5. Андрущенко О. П. Вплив штучного інтелекту на захист прав людини: проблеми, прогнози та перспективи боротьби зі злочинністю. Питання боротьби зі злочинністю. 2024. Т. 1, № 47. С. 186–193.
6. Пядишев В. Г. Перспективи розвитку проактивної діяльності поліції: зарубіжний погляд. Право і суспільство. 2024. Т. 1. С. 403–412.
7. Using OSINT to Improve Your Competitive Intelligence Strategy. Medium. 2023. URL: https://goldenowl.medium.com/using-osint-to-improve-your-competitive-intelligence-strategy-eeb6114f9c71 (дата звернення: 10.05.2024).
8. Use of AI in Online Content Moderation. Cambridge Consultants. 2019. URL: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf (дата звернення: 10.05.2024).
9. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. Серія Право. 2023. № 78. С. 134–139.
10. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник*. Повітряне і космічне право. 2021. № 2. С. 110–115
11. Mazepa S., Dostálek L., Křivan V., Banakh S. Cybercrime in Ukraine and Cyber Security Game. 10th International Conference on Advanced Computer Information Technologies (ACIT). Deggendorf, Germany, 2020. Pp. 787–791. DOI: 10.1109/ACIT49673.2020.9208972.
12. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII Відом. Верховної Ради України. 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 2.05.2024).
13. Біла книга з регулювання штучного інтелекту в Україні. Мінцифра України. Київ : Міністерство цифрової трансформації України, 2021. 48 с. URL: https://thedigital.gov.ua/storage/uploads/files/page/community/docs/Біла_книга_з_регулювання_ШІ_в_Україні_АНГЛ.pdf_ (дата звернення: 2.05.2024).