ускладнює обходи захисних стратегій злочинців і дозволяє оперативно реагувати на зміни у кримінальній ситуації, ефективніше запобігаючи можливим загрозам [4, с. 103].

Список використаних джерел

1. King T. C. Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and engineering ethics*. 2020. №. 1. С. 89-120. URL: https://link.springer.com/article/10.1007/s11948-018-00081-0

2. Hallevy G. When robots kill: Artificial intelligence under criminal law. UPNE, 2013.

3. Kan C. H. Criminal liability of artificial intelligence from the perspective of criminal law: An evaluation in the context of the general theory of crime and fundamental principles. *International Journal of Eurasia Social Sciences*. 2024. № 55. URL: http://dx.doi.org/10.35826/ijoess.4434

4. Макаренко В. І., Кисельов А. Інтегрування системи штучного інтелекту в кримінальний аналіз. *International scientific journal «Grail of Science*. 2024. № 35. URL: 10.36074/grail-of-science.19.01.2024.017

Мягких Софія Вікторівна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Шопіна Ю. О., доцент кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

ПРОБЛЕМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВЧИНЕННЯ КІБЕЗЛОЧИНІВ

Штучний інтелект стає потужним інструментом не лише для розвитку економіки та науки, а й для вчинення кіберзлочинів. Його використання у кримінально-протиправних цілях зумовлює новий рівень загроз, оскільки алгоритми здатні автоматизувати

злам систем, створювати реалістичні фішингові повідомлення, генерувати шкідливий код та здійснювати масові атаки без значних ресурсних витрат, що підвищує ефективність кіберзлочинців і ускладнює виявлення кримінальних правопорушень традиційними методами. Актуальність дослідження полягає в тому, що розвиток технологій штучного інтелекту випереджає темпи формування правових механізмів їхнього регулювання та протидії такому застосуванню. В умовах зростання цифрових ризиків необхідно аналізувати потенційні загрози, розробляти нормативно-правові та технічні засоби захисту, а також формувати міжнародне співробітництво у сфері кібербезпеки, що дозволить мінімізувати небезпеку використання ШІ у протиправних цілях і забезпечити баланс між інноваціями та безпекою.

Штучний інтелект – це сукупність теоретичних та практичних підходів у галузі інформаційних технологій, які передбачають створення систем, що можуть функціонувати розумно та незалежно, подібно до механізму прийняття рішень у мозку людини [1, с. 6].

Штучний інтелект є дуже корисним в багатьох галузях діяльності. В тому числі він може бути використаний для покращення ефективності роботи правоохоронних органів та забезпечення публічної безпеки. Але є і незаконні методи застосування ChatGPT. Протиправне застосування ШІ є важливою проблемою, яка вимагає уваги як з боку суспільства, так і з боку влади. Наприклад, злочинці легко обходять вбудований розробниками ChatGPT захист: заборону на створення шкідливого коду. Для цього вони просто розбивають завдання на кілька частин, щоб запити виглядали нейтральними. А потім за інструкціями від самого ж штучного інтелекту збирають їх в одну програму. Навіть ті, хто нічого не тямлять у програмуванні, створюють шкідливі програмні засоби під свої потреби, використовуючи ChatGPT як інструктора. Ще одна популярна ніша незаконного використання нейромережі – соціальна інженерія. ChatGPT здатний без зусиль написати переконливий текст для фішингового сайту або листування, без помилок і з такими деталями, які введуть в оману користувача. Він може вести діалоги та переконувати людей у своїй правоті, створювати привабливі пропозиції для розсилок і наслідувати конкретну манеру спілкування, щоб видати себе за реально існуючу людину.

ШІ може створювати дуже реалістичні фішингові листи, повідомлення чи навіть телефонні дзвінки за допомогою голосових ботів. Наступний спосіб застосування ChatGPT – можливість безпосередньо запитати його, як скоїти кримінальне правопорушення з найбільшою вигодою, дізнатися про нові афери, схеми обману, отримати статистику щодо скоєних кримінальних правопорушень, щоб не конкурувати з іншими злочинцями, а також отримати розуміння, які помилки роблять інші шахраї, на чому їх ловить поліція, як цього уникнути. Можливе використання технологій відтворення голосу людини з метою шахрайського отримання грошей або інформації. Також за допомогою ШІ можливо генерувати підроблені документи, підписи чи фото. У процесі нелегальної діяльності у фінансовій сфері за допомогою ШІ можливе зловживання біржовими алгоритмами для маніпуляцій на фінансових ринках та аналізу схем відмивання грошей та пошуку способів їх оптимізації [2, с. 32].

Кримінальні правопорушення у сфері сучасних інформаційних та інших технологій набувають міжнародного, транснаціонального характеру, до того ж потерпілі від таких дій і самі злочинці можуть перебувати в різних країнах світу (наприклад, злочинці, навіть у місцях позбавлення волі). Для протидії таким видам кримінальних правопорушень особливе значення насамперед має посилення й удосконалення міжнародного співробітництва в цій сфері, підвищення його ефективності [3, с. 41].

Водночас впровадження штучного інтелекту у правоохоронну сферу викликає дискусії щодо конфіденційності та захисту персональних даних. Масове збирання й зберігання інформації про громадян може створити ризик зловживань і порушень прав людини. Отже, необхідно розробити чіткі та прозорі регуляторні норми, які забезпечать безпеку особистої інформації, а також запобігатимуть неправомірному використанню цих технологій. Окремим викликом стає захист персональних та, зокрема, біометричних даних. Ризик несанкціонованого доступу до таких даних або їх використання для прихованого спостереження вимагає розроблення суворих стандартів і правил [4, с. 32].

Оскільки з протиправною метою все активніше використовують інформаційні, телекомунікаційні, цифрові й інші технології, а також мережі кіберпростору, різноманітні види

засобів зв'язку, штучний інтелект та інші сучасні досягнення науки й техніки, то нагальною стає необхідність відбору, застосування й адаптування всіх цих засобів до потреб криміналістики, експертології й досудового слідства, а саме розроблення відповідних методик розслідування, які б передбачали застосування єдиних методів, засобів і прийомів для вирішення типових завдань досудового розслідування на різних його етапах [3, с. 42].

Що стосується правового регулювання, законодавчі органи повинні розробляти та впроваджувати нормативно-правові акти, що будуть в повній мірі регулювати використання штучного інтелекту в сфері прав людини та боротьби з протиправністю. Вони мають включати в себе правила щодо захисту приватності, заборони дискримінації, етичного використання алгоритмів тощо. Закони повинні вимагати від компаній, що використовують ШІ, надавати прозору та доступну інформацію про алгоритми, дані та вплив ШІ на права людини. Також мають створюватися групи для моніторингу за дотриманням прав людини та боротьби з протиправністю в контексті ШІ [5, с. 191].

Європейський комітет з проблем протиправності Ради Європи (із метою підвищення ефективності протидії таким видам кримінальних правопорушень і правового визначення в Європі групи кримінальних правопорушень, пов'язаних із комп'ютерами й інформаційними технологіями) підготував рекомендації про включення до законодавств європейських країн кримінальних норм «мінімального списку» і «необов'язкового списку» комп'ютерних кримінальних правопорушень. На початку 2002 р. ухвалено Протокол № 1 до Конвенції, який додав до цього переліку кримінальні правопорушення із поширення інформації расистського, ксенофобного й іншого характеру, що підбурює до насильницьких дій, ненависті чи дискримінації окремої особи або групи осіб і/або ґрунтується на расовій, національній, релігійній або етнічній належності. Згаданий Протокол також ратифіковано Верховною Радою України. Згідно з Конвенцією кримінальні правопорушення класифіковано за чотирма групами, а саме: 1) спрямовані проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), вплив на комп'ютерні дані (протиправне навмисне пошкодження, знищення, погіршення якості, зміна або блокування комп'ютерних даних) (ст. 4) або

системи (ст. 5)), протизаконне використання спеціальних технічних пристроїв (ст. 6) і комп'ютерних програм, розроблених або адаптованих для скоєння кримінальних правопорушень, передбачених у ст. 25, а також комп'ютерних паролів, кодів доступу, їх аналогів, за допомогою яких можна отримати доступ до комп'ютерної системи загалом або будь-якої її частини (норми ст. 6 застосовують тільки в разі, якщо використання (поширення) спеціальних технічних пристроїв спрямовано на скоєння протиправних діянь); 2) пов'язані з використанням комп'ютерних засобів (підроблення та шахрайство з використанням комп'ютерних технологій (ст. 7, 8): зловмисні й протиправні введення, зміна, видалення або блокування комп'ютерних даних, що тягнуть за собою порушення автентичності даних із наміром, щоб їх розглядали або використовували з юридичною метою як автентичні); 3) здійснювані з метою розповсюдження за допомогою комп'ютерних систем (надання пропозицій для користування, поширення та придбання різних видів дитячої порнографії, а також наявність дитячої порнографії в пам'яті комп'ютера певної особи; ст. 9); 4) пов'язані з порушенням авторського права й суміжних прав на програмне забезпечення (ст. 10; в Україні – ст. 176 Кримінального кодексу) [3, с. 42].

Отже, робимо висновок, що використання штучного інтелекту у сфері кіберзлочинності створює новий рівень небезпеки для інформаційної безпеки держави, бізнесу та громадян. Алгоритми здатні значно підвищувати ефективність протиправних дій, робити їх менш помітними та більш масштабними, що ускладнює їх своєчасне виявлення та формує серйозний виклик для правоохоронних органів і потребує постійного удосконалення механізмів протидії. Таким чином, виникла необхідності своєчасного оновлення законодавчої бази, розвитку сучасних засобів кіберзахисту та активного міжнародного співробітництва, бо тільки комплексний підхід дозволить мінімізувати ризики протиправного використання штучного інтелекту та зберегти баланс між технологічним прогресом і безпекою суспільства.

Список використаних джерел

1. Савченко В. А., Шаповаленко О. Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. *Сучасний захист інформації.* 2020. С. 6–11. URL: https://surl.li/mgyeej (дата звернення: 25.09.2025).

2. Зачек О. І. Проблеми злочинного застосування штучного інтелекту. 2025. С. 32–34. URL: https://surl.li/cynjgl (дата звернення: 25.09.2025).

3. Юхно О. Генезис і проблемні питання використання новітніх технологій та штучного інтелекту в криміналістиці, експертній діяльності й досудовому розслідуванні. *Теорія та практика судової експертизи і криміналістики.* 2021. С. 40–59.

4. Кириченко В. В. Вплив штучного інтелекту на злочинність в Україні. 2025. С. 30–32. URL: https://surl.li/gwvrbs (дата звернення: 25.09.2025).

5. Андрущенко О. П. Захист прав людини в умовах розвитку штучного інтелекту. *Наукові дослідження*. 2024. С. 186–193.

Насальська Анна Олексіївна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Шопіна Ю. О., доцент кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ВИЯВЛЕННІ ТА ПОПЕРЕДЖЕННІ КІБЕРЗЛОЧИНІВ: ПЕРСПЕКТИВИ ТА ВИКЛИКИ ДЛЯ КРИМІНАЛЬНОГО ПРАВА

Штучний інтелект (ШІ) займає провідне місце у розвитку сучасних технологій, зокрема у сфері кібербезпеки. Збільшення обсягів цифрової інформації та ускладнення видів кіберзлочинів вимагають впровадження ефективних інструментів для їх виявлення та попередження. Завдяки своїй здатності аналізувати великі масиви даних, розпізнавати закономірності та прогнозувати потенційні загрози, ШІ відкриває нові горизонти у боротьбі з кіберзлочинністю.