Денисенко Дмитро Миколайович,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Резнік Ю. С., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВЧИНЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ: ВИКЛИКИ ДЛЯ КРИМІНАЛЬНОГО ПРАВА

Стрімкий розвиток технологій штучного інтелекту (ШІ) суттєво трансформував багато сфер суспільного життя – від економіки, освіти та медицини до систем безпеки. Однак разом із позитивними змінами виникають і нові загрози: сьогодні злочинні суб'єкти дедалі активніше застосовують ШІ як інструмент для вчинення кримінальних правопорушень. Це явище являє собою не просто еволюцію існуючих злочинних схем, але і якісно новий фронт ризиків для кримінального права, правоохоронних органів та суспільства в цілому [1].

Зокрема, одним із найпомітніших трендів є використання технологій deepfake – створення надзвичайно реалістичних відео- або аудіоматеріалів, які можуть бути використані для шантажу, вимагання коштів, дискредитації публічних осіб чи приватних громадян. У відомих випадках шахраї імітували голоси керівників компаній або державних службовців, змушуючи працівників переводити значні кошти на підконтрольні шахраям рахунки [2]. Паралельно з цим формуються нові моделі фішингових атак: ШІ дозволяє генерувати високоперсоналізовані повідомлення, адаптовані під конкретну особу, що робить їх значно ефективнішими, ніж традиційні розсильні листи [3]. Додатково ШІ використовується у кіберзлочинності для створення шкідливого програмного забезпечення, пошуку вразливостей або проведення атак без прямої участі людини.

Автоматизація в цій сфері дозволяє злочинцям одночасно атакувати тисячі жертв по всьому світу, що раніше було технічно значно складніше. Генеративні моделі глибокого навчання також сприяють фальсифікації доказів – створенню зображень, аудіо чи відео, які практично не вирізняються від справжніх, і це істотно ускладнює кримінальне переслідування та доведення провини [4].

Використання ШІ у злочинній діяльності породжує низку серйозних викликів для традиційної системи кримінального права. По-перше, алгоритм як такий не має умислу (mens rea), і тому класичні підходи до визначення вини або відповідальності стають недостатніми. Хто має нести відповідальність – розробник алгоритму, провайдер, хостинг-платформа чи кінцевий користувач – часто не визначено чітко, що створює правову невизначеність. По-друге, збору та перевірці цифрових доказів потрібна спеціалізована експертиза та ретельне логування, що не завжди забезпечується на рівні правоохоронних органів. По-третє, злочини із застосуванням ШІ часто мають транскордонний характер, що ускладнює розслідування: юрисдикції перетинаються, обмін доказами та співпраця між країнами – не завжди налагоджені.

Додатково автоматизація та масштабність атак (наприклад, одночасне застосування ШІ-базованих схем на тисячі жертв) роблять традиційні правові механізми – реагування, переслідування, санкції – малоефективними. Нарешті, законодавство значною мірою відстає від технологічного прогресу: нові форми злочинів вже реалізуються, тоді як нормативна база часто ще не адаптована до них [5].

У міжнародному контексті можна виділити приклади нормативної та практичної відповіді на виклики, пов’язані із ШІ. У межах AI Act Європейського Союзу встановлено рамки щодо ризикованих систем ШІ та передбачено відповідальність за зловживання ними [6]. У США правоохоронні органи видають рекомендації та попередження щодо використання технологій deepfake у шахрайських схемах, а також обговорюються кримінальні санкції за створення чи розповсюдження deepfake без згоди особи. У сукупності міжнародна практика демонструє, що ефективна протидія злочинам із застосуванням ШІ потребує системного підходу: узгодження нормативної бази, технологічних стандартів і міжнародного співробітництва.

До заходів, які вже вживаються або обговорюються, належать: обов'язкове збереження логів та метаданих платформ, що надають доступ до систем ШІ; розробка стандартів цифрової криміналістики для верифікації AI-контенту; створення міжнародних каналів співпраці для розслідування транскордонних злочинів; залучення експертів із кібербезпеки та технологій ШІ до кримінальних проваджень; розробка методик доказування вини та атрибуції у справах, пов'язаних із ШІ.

Окрім цього, обговорюється введення окремого складу злочину «використання технологій ШІ з метою вчинення кримінальних правопорушень», адміністративна та кримінальна відповідальність для провайдерів, які не забезпечують адекватні механізми безпеки, обов'язок розробників зберігати історію використання ШІ, маркування контенту, створеного алгоритмами, та система оперативного реагування на шкідливий контент.

Крім вищезгаданих правових і технологічних заходів, ключове місце належить і просвітницьким ініціативам з підвищення цифрової грамотності суспільства. Навіть найсучасніші технології захисту виявляються недостатніми, якщо користувачі не здатні розпізнати шахрайські схеми чи ознаки маніпуляцій. Освітні програми та тренінги для працівників державних установ, приватних компаній і громадськості повинні включати навчання щодо потенційних ризиків ШІ, методів безпечної взаємодії з цифровими системами та ознак активних атак. Водночас важливо розвивати міждисциплінарну співпрацю – поєднувати зусилля юристів, правоохоронців, фахівців із технологій, етиків та соціологів, щоб адекватно аналізувати та реагувати на злочини XXI століття.

Отже, використання ШІ у кримінальній діяльності становить одну з найсерйозніших загроз для системи кримінального права сьогодні. Злочини із застосуванням ШІ важко розслідувати, важко довести і ще важче попередити, що вимагає від правової системи, технологічного сектору та суспільства оновлення підходів. Необхідна модернізація законодавства, підвищення технічної грамотності правоохоронців, впровадження технічних стандартів і міжнародна координація. Штучний інтелект – потужний

інструмент, який може бути використаний як на благо, так і на шкоду; лише взаємодія держави, технологічного сектору, правової системи та суспільства дозволить мінімізувати ризики його зловживання та зберегти потенціал для розвитку науки, економіки й соціальних сфер.

Список використаних джерел

1. Gupta et al. (2024). *Digital deception: generative artificial intelligence in social engineering and phishing*. Artificial Intelligence Review, 57:324. SpringerLink

2. Chenchi Reddy, K., & Saleem, M. (2025). *The dark side of AI: How criminals leverage machine learning for illicit activities in the context of assault*. International Journal of Intelligent Systems and Applications in Engineering, 13(1). IJISAE

3. Riurean, P., Bolog, G., & Riurean, S. (2024). *The rise of sophisticated phishing. How AI fuels cybercrime*. Journal of Digital Science, 6(2), 15-25. Institute of Cited Scientists

4. Seidlitz, S., Dittmann, J. (2024). *Media forensic considerations of the usage of artificial intelligence using the example of DeepFake detection*. J. Imaging, 10(2):46. MDPI

5. «AI and Serious Online Crime». Centre for Emerging Technology and Security report. cetas.turing.ac.uk

6. «AI-deepfake scams and the importance of a holistic communication security strategy». International Cybersecurity Law Review, 6:53-61 (2025). SpringerLink