Малород Анастасія Андріївна,
студент Київського національного
економічного університету
імені Вадима Гетьмана
Науковий керівник:
Рощина Інна Олександрівна,
професор кафедри публічного
та міжнародного права Київського
національного економічного університету
імені Вадима Гетьмана, кандидат
юридичних наук, доцент

ПРОБЛЕМИ КВАЛІФІКАЦІЇ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ: ПОРІВНЯЛЬНИЙ АНАЛІЗ УКРАЇНИ ТА СІНГАПУРУ

Сучасні технології відіграють ключову роль у процесах оновлення та модернізації світового порядку, і одне з провідних місць серед них належить штучному інтелекту. Актуальність штучного інтелекту у сучасних умовах є надзвичайно високою, що зумовлює не лише розвиток різних сфер суспільного життя [1, с. 298], а й формування нових викликів для кримінального права.

Водночас його стрімкий розвиток призводить до появи нових форм суспільно небезпечної поведінки, які потребують адекватного правового реагування. Створення діпфейків, кібератак, автоматичне генерування та опрацювання великої кількості тексту, стає ефективним засобом для вчинення кримінальних правопорушень. Україна не є виключенням та застосовує вже існуючі кримінально-правові норми до ШІ-злочинів, у той час як Сінгапур впроваджує нові закони для попередження таких зловживань. Порівняння підходів цих двох країн, дозволяє оцінити реагування на сучасні виклики пов'язані з використанням штучного інтелекту.

Слід зазначити, що сучасний стан правового регулювання штучного інтелекту суттєво відстає від темпів його технологічного розвитку. Станом на 2024 рік у більшості держав майже відсутні комплексні закони, які б охоплювали весь спектр відносин, пов'язаних із розробкою, впровадженням та використанням систем штучного інтелекту. Одними з найбільш значущих нормативних досягнень у цій сфері є Загальний регламент Європейського Союзу про захист даних (GDPR), оновлений 13 червня 2024 року, та Закон Каліфорнії про захист прав споживачів.

Особливе значення в контексті регулювання новітніх технологій має Закон ЄС про штучний інтелект, який передбачає формування єдиного комплексного підходу до регулювання ШІ незалежно від галузі застосування чи типу технології. Дія цього закону поширюється на всіх операторів систем штучного інтелекту – постачальників, імпортерів,

дистриб'юторів та виробників – як на території Європейського Союзу, так і за його межами у випадку, якщо відповідні системи експлуатуються в ЄС. Нормативна модель, закладена в основу акта, має багатовимірний характер і поєднує централізовані та децентралізовані механізми регулювання, а також інструменти державного та приватного управління. Такий підхід обумовлений необхідністю забезпечення узгодженої взаємодії між різними інститутами та суб'єктами на рівні Європейського Союзу й держав-членів [2, с. 89].

Україна також розпочала формування власної нормативної бази у сфері штучного інтелекту. Першими кроками в цьому напрямі стали Концепція розвитку штучного інтелекту в Україні [3] та План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки [4], які визначають стратегічні орієнтири державної політики у сфері розробки, впровадження та використання технологій ШІ.

Попри це, головною проблемою у кваліфікації кримінальних правопорушень, пов'язаних з використанням штучного інтелекту, залишається відсутність у Кримінальному кодексі України чітких і спеціальних норм, які б безпосередньо регулювали такі діяння.

Прикладом може послугувати злочинна група, яку було викрито у 2024 році. Зловмисники застосовували штучний інтелект для схем з викраденими даними українців. Вони копіювали голос та обличчя потерпілих з використанням deepfake-технологій, через які їм вдавалося обходити верифікацію у банках та оформлювати кредити на понад 280 осіб на загальну суму понад 4 мільйони гривень [10]. Відповідно до законодавства України, а саме статті 190 Кримінального кодексу України, дії цієї групи кваліфікуються, як шахрайство, оскільки вони заволоділи чужим майном шляхом обману. Також використання штучного інтелекту дає підстави на застосування статті 361 Кримінального кодексу України, як несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку [5]. Ця ситуація вказує на прогалини у кримінальному законодавстві України, які потребують термінового вирішення. З'являється необхідність запровадження спеціальних правових норм, які б регулювали питання використання ШІ-технологій у вчиненні злочинів. Хоча Україна вже рухається в бік європейської моделі регулювання і вже 24 жовтня 2025 року команда ШІ Міністерства цифрової трансформації України, вперше взяла участь у засіданні високого рівня Європейської ради зі штучного інтелекту [9]. Це стало важливим кроком до європейської інтеграції. EU AI Act – перший у світі наднаціональний регламент (звід законів та правил) про штучний інтелект [7].

У Сінгапурі питання стосовно злочинів з використанням штучного інтелекту, зокрема діпфейків, регулюються законом. З лютого 2024 року набув чинності закон про кримінальну шкоду в інтернеті під назвою «Online Criminal Harms Act 2023», який надає повноваження уряду Сінгапуру видавати вказівки для онлайн-

платформ щодо блокування, обмеження доступу чи видалення контенту, який пов'язаний з шахрайством та злочинною діяльністю. Закон включає в себе превентивні заходи, спрямовані на швидке припинення онлайн-шахрайства, що дозволяє суттєво зменшити масштаб і темпи розповсюдження шкідливого контенту. Сінгапур також активно впроваджує заходи для протидії діпфейкам та покращує технології через діяльність Центру передових технологій онлайн-безпеки «CATOS», який створює інструменти для розпізнавання неправдивого контенту, а саме цифрові водяні знаки та криптоавтентифікацію, співпрацюючи з світовими експертами. Також існує Закон «POFMA», він встановлює відповідальність за навмисне розповсюдження фейків та надає міністру права блокувати чи виправляти хибну інформацію[6]. У свою чергу, модель керування генеративним ШІ, створена Управлінням з розвитку інфокомунікаційних медіа Сінгапуру (IMDA), наголошує на підзвітності розробників, прозорості даних і безпеці контенту, щоб результативно реагувати на виклики, пов'язані з розвитком штучного інтелекту. Уряд організовує навчальні заходи для зростання цифрової обізнаності та кібербезпеки, формуючи уміння ідентифікувати фейки[8]. Я вважаю, що своїми діями, Сінгапур доводить, що штучний інтелект можна тримати під контролем, якщо норми чіткі та діють на практиці. Для України це є прикладом того, як правильно класифікувати та регулювати злочинність пов'язану з новітніми складними технологіями.

Отже, бачимо, що проблема кваліфікація кримінальних правопорушень пов'язаних із використанням штучного інтелекту, є актуальною як для України, так і для Сінгапуру. В Україні такі протиправні діяння змушені регулюватися статтями Кримінального кодексу, які не включають в себе цифрові алгоритми та самостійні інструменти. Сінгапур же навпаки, завдяки технологіям IMDA та спеціальним нормам намагається попередити ризики, але також зіштовхується з проблемами, які пов'язані зі стрімким прогресом технологій. Зрештою, обидві країни зустрічаються з тим, що ШІ стрімко трансформує сутність кіберзлочинів, а законодавство має пристосовуватись набагато оперативніше.

Список використаних джерел

1. Курман О.В. П. Переваги та проблемні питання використання штучного інтелекту при дослідженні цифрових слідів. Науковий вісник Ужгородського Національного Університету: Серія Право. Вип. 90, ч. 4. 2025. С. 298–302. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/340161/328209

2. Підгородинський В. М. Штучний інтелект та кримінальне право: сучасні грані досліджень. Кримінально-виконавча система: Вчора. Сьогодні. Завтра № 2 (16), 2024. С. 84–94.

3. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядж. Кабінету Міністрів України від 02.12.2020

№ 1556-р: станом на 29 груд. 2021 р. URL: https://zakon.rada.gov.ua /laws/show/1556– 2020-р#Text
4. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки: Розпорядж. Кабінету Міністрів України від 9 травня 2025 р. № 457-р: https://zakon.rada.gov.ua/laws/show/457-2025-%D1%80#Text
5. Кримінальний кодекс України: Закон України від 5 квіт. 2001 р. № 2341-III URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
6. CNPLaw. Generative AI and deepfakes. URL: https://www.cnplaw.com/generative-ai-and-deepfakes/?print-posts=pdf
7. DeNovo. Що принесе європейському ринку EU AI Act. URL: https://denovo.ua/blog/eu-ai-act-into-force
8. IMDA. 3 things Singapore is doing to take action against deepfakes. URL: https://www.imda.gov.sg/resources/blog/blog-articles/2024/07/3-things-sg-do-to-take-action-against-deepfakes
9. The Digital. Україна приєдналася до Європейської ради зі штучного інтелекту. URL: https://thedigital.gov.ua/news/progress/ ukrayina-pryyednalasia-do-yevropeyskoyi-rady-zi-shtuchnoho-intelektu
10. Шахраї за допомогою штучного інтелекту оформили кредити на українців – Нацполіція. URL: https://unn.ua/news/shakhrai-za-dopomohoiu-shtuchnoho-intelektu-oformliuvaly-kredyty-na-ukraintsiv-natspolitsiia

Манжус Богдан Олегович,
курсант Національної академії
внутрішніх справ
Науковий керівник:
Федорюк Людмила Василівна,
доцент кафедри оперативно-розшукової
діяльності та національної безпеки
Національної академії внутрішніх справ,
доктор філософії

ВПЛИВ МІЖНАРОДНОГО ДОСВІДУ НА ВДОСКОНАЛЕННЯ КРИМІНАЛЬНОГО ЗАКОНОДАВСТВА УКРАЇНИ ЩОДО ЗАХИСТУ ДАНИХ

Актуальність дослідження впливу міжнародного досвіду на вдосконалення кримінального законодавства України щодо захисту даних зумовлена стрімким розвитком цифрових технологій, зростанням кількості кіберзлочинів і необхідністю забезпечення ефективного правового механізму захисту персональної інформації. Вивчення міжнародного досвіду дозволяє удосконалити кримінально-правові норми, підвищити ефективність розслідування кримінальних правопорушень у сфері інформаційної безпеки й забезпечити баланс між правом на приватність і потребами національної безпеки, що є