Для ефективної профілактики насильства необхідно впроваджувати освітні програми в школах та університетах, навчати молодь повазі до прав людини і ненасильницькому спілкуванню. Підготовка поліцейських та суддів до специфіки таких справ також є важливим кроком на шляху до зниження рівня насильства.

Таким чином, необхідно не тільки удосконалювати законодавство, але й реорганізовувати систему правосуддя для створення належних умов для захисту жертв домашнього насильства. Лише комплексний підхід до цієї проблеми забезпечить реальні зміни у боротьбі з домашнім насильством в Україні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Антонюк Н., Ліхолєтова Ю. Домашнє насильство: практика Касаційного кримінального суду у складі Верховного Суду. *Судово-юридична газета – Блог.* URL: https://sud.ua/uk/news/blog/265517-domashnye-nasilstvo-praktika-kasatsiynogo-kriminalnogo-sudu-u-skladi-verkhovnogo-sudu (дата звернення: 12.05.2025)

2. Гловюк І.В., Гутник А.В., Коць Є.П. Варіативність доказування домашнього насильства: праксеологічний аспект. *Аналітично-порівняльне правознавство.* 2024. № 4. С. 598–605. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/8116 (дата звернення: 12.05.2025)

3. Кримінальний кодекс України. Стаття 126-1. Домашнє насильство. *Протокол.ua (Юридичний інтернет ресурс).* URL: https://protocol.ua/ua/kriminalniy_kodeks_ukraini_stattya_126_1/ (дата звернення: 12.05.2025)

4. Про запобігання та протидію домашньому насильству : Закон України від 7 грудня 2017 р. № 2229-VIII : станом на 19 грудня 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2229-19#Text (дата звернення: 12.05.2025)

5. Суддя ВС розповіла про особливості застосування кримінального процесуального законодавства під час розгляду кримінальних проваджень, пов'язаних із домашнім насильством. *Верховний Суд.* URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1641873/ (дата звернення: 12.05.2025)

Велігурська О. А.
Науковий керівник: Острогляд О. В., к.ю.н., доц.,
доцент кафедри права та правоохоронної діяльності,
Державний університет «Житомирська політехніка»,
м. Житомир

КРИМІНАЛЬНО-ПРАВОВА КВАЛІФІКАЦІЯ ШАХРАЙСТВА ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Сучасний етап розвитку суспільства характеризується тотальною цифровізацією, ключовим рушієм якої є технології штучного інтелекту (ШІ). Поряд із позитивним економічним та соціальним ефектом, динамічна інтеграція ШІ в інформаційні, фінансові та комунікаційні системи створила нові, раніше невідомі, механізми вчинення злочинів. Зокрема, у сфері шахрайства (ст. 190 КК України), де ШІ виступає як високоточний та масштабний засіб обману, що значно ускладнює процес виявлення та доведення злочинного умислу і вимагає нових підходів до розслідування.

У контексті кримінального права, технології штучного інтелекту необхідно розглядати як високотехнологічне знаряддя або засіб вчинення злочину. Це означає, що ШІ не є суб'єктом кримінальної відповідальності, але слугує інструментом для людини-виконавця з метою реалізації її злочинного умислу, спрямованого на заволодіння чужим майном.

Відповідно до чинного законодавства України, зокрема статті 190 Кримінального кодексу України, шахрайство визначається як заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою. Однак розвиток технологій штучного інтелекту створює нові форми обману, які не завжди можуть охопити традиційне розуміння цієї норми [2].

Наприклад, об'єктивна сторона шахрайства обов'язково передбачає наявність обману (повідомлення неправдивих відомостей чи приховування істини) як основного способу вчинення. Однак, застосування технологій штучного інтелекту викликає суттєву трансформацію об'єктивної сторони шахрайства, особливо у частині способу вчинення – обману. Основний виклик тут пов'язаний з технологіями Deepfake, які генерують синтетичні відео- та аудіоматеріали, імітуючи голос або зовнішність конкретної особи (наприклад, керівника компанії, фінансового директора або близького родича). Такий високотехнологічний обман спрямований на повне придушення критичного сприйняття потерпілого, змушуючи його "добровільно" здійснити транзакцію чи передати дані під впливом ілюзії автентичності [6].

Deepfake є технологічно посиленою формою обману, оскільки високий рівень правдоподібності згенерованого контенту здатний повністю приспати здатність потерпілого до критичної оцінки, створюючи ілюзію абсолютної автентичності. По суті, Deepfake є імітацією особистості, що підриває довіру в критично важливих соціальних та фінансових комунікаціях [5].

Штучний інтелект виступає як потужний інструмент масової автоматизації та масштабування шахрайства. Якщо традиційне шахрайство вимагало від виконавця індивідуальної роботи з жертвою, то агентивні ШІ-системи можуть одночасно генерувати тисячі унікальних фішингових листів або повідомлень у чатах. Ці системи здатні аналізувати великі обсяги персональних даних жертви (професію, інтереси, попередню кореспонденцію) для створення обманного контенту, що значно підвищує відсоток успішних атак та багаторазово збільшує розмір заподіяної шкоди. Таким чином, ШІ трансформує шахрайство з точкового злочину в масштабну кіберкампанію [4].

Подальше застосування ШІ включає маніпуляцію автоматизованими фінансовими системами та обхід біометричного захисту. Наприклад, ШІ може бути застосований для внесення несанкціонованих змін у великі масиви фінансових чи корпоративних даних, що спричинить автоматичне перерахування коштів чи придбання майнових прав на користь злочинця без прямого контакту з людиною-бухгалтером чи менеджером.

Особливе значення для аналізу кіберзлочинів, зокрема тих, що вчиняються із застосуванням штучного інтелекту (ШІ), є кваліфікуюча ознака «шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ЕОТ)», яка зазначена у частині 4 статті 190 Кримінального кодексу України як підстава для посиленої кримінальної відповідальності [1].

Під незаконними операціями з використанням електронно-обчислювальної техніки як ознакою шахрайства слід розуміти такі спрямовані на заволодіння чужим майном або придбання права на майно операції, в основі яких лежать обман чи зловживання довірою.

При цьому вказану обставину утворюють лише операції, здійснення яких без використання електронно-обчислювальної техніки є неможливим. Якщо ж з використанням такої техніки здійснюються операції, які цілком можуть здійснюватись за допомогою іншої техніки, то розглядуваний склад шахрайства відсутній. Електронно-обчислювальна техніка у такому випадку виступає засобом вчинення злочину, а здійснювані з використанням неї операції становлять зміст шахрайського заволодіння чужим майном чи правом на нього [3].

Наведене тлумачення ознаки «шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ЕОТ)» (ч. 4 ст. 190 КК України) повністю охоплює та обґрунтовує підвищену небезпеку шахрайства, вчиненого із застосуванням штучного інтелекту (ШІ). Ключовим моментом є те, що під незаконними операціями слід розуміти такі, що спрямовані на заволодіння майном і неможливі без використання ЕОТ – як-от здійснення електронних платежів або інших операцій з безготівковими коштами. Шахрайство з ШІ ідеально підпадає під це визначення, оскільки технології ШІ (наприклад, Deepfake, агентні системи) використовуються для здійснення високошвидкісних, масованих та технічно складних операцій, які є невід'ємними частинами функціонування цифрових фінансових систем.

Штучний інтелект виступає у ролі високотехнологічного засобу автоматизації незаконних операцій. Наприклад, застосування ШІ для маніпуляції фінансовими системами через несанкціоноване внесення змін у цифрові бази даних, що призводить до автоматичного перерахування безготівкових коштів, є прямим прикладом такої операції. Так само, використання генеративних моделей для створення правдоподібних Deepfake-матеріалів з метою обходу біометричних систем чи автоматизованих верифікаційних протоколів є технічним втручанням, спрямованим на отримання доступу до чужого майна. У цих випадках ЕОТ (у широкому розумінні, включаючи мережі, програмне забезпечення та алгоритми ШІ) виступає засобом вчинення злочину, а ШІ трансформує шахрайство з обману людини на обман автоматизованої системи.

Якщо ШІ використовується не для обману людини, а для безпосереднього впливу на цифрову систему, він діє як інструмент автоматизації «незаконних операцій з ЕОТ». Наприклад, алгоритми машинного навчання можуть бути використані для автоматичного сканування вразливостей системи, підбору паролів, або масової розсилки фішингових повідомлень, які ініціюють несанкціоновану транзакцію в банківській чи платіжній мережі.

Використання автоматизованих систем, як-от боти, для здійснення масових або цільових несанкціонованих дій з даними (спам-атаки, маніпуляція алгоритмами), також відповідає змісту ознаки «незаконних операцій з ЕОТ», оскільки це є неправомірним впливом на процес обробки даних, що призводить до заволодіння чужим майном.

Таким чином, технології штучного інтелекту кардинально трансформують шахрайство (ст. 190 КК України), перетворюючи його з точкового злочину на масштабну кіберкампанію за допомогою автоматизації обману (зокрема, через Deepfake). Ключовим для кваліфікації є визначення ШІ як високотехнологічного засобу вчинення «незаконних операцій з використанням електронно-обчислювальної техніки» (ч. 4 ст. 190 КК України), оскільки саме ШІ автоматизує ці операції, спрямовані на маніпуляцію цифровими фінансовими системами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Драгоненко А. О. Наколенко М. І. Проблеми кваліфікаці шахрайства з використанням електронно-обчислювальних машин. Порівняльно-аналітичне право. 2018. с. 256-259.
2. Кримінальний кодекс України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
3. Мельник М. І., Хавронюк М. І. Науково-практичний коментар Кримінального кодексу України. 2018. С. 596-597.
4. Новий рівень онлайн-шахрайства: в Україні зростає кількість афер з ШІ та QR-кодами. Новини України - останні новини України сьогодні - УНІАН. URL: https://www.unian.ua/economics/other/shahraystvo-v-ukrajini-ukrajinciv-poperedili-pro-novi-metodi-zlochinciv-13063125.html
5. Штучний інтелект і діпфейки: як країни реагують на загрози - Центр демократії та верховенства права. Центр демократії та верховенства права -. URL: https://cedem.org.ua/analytics/shtuchnyi-intelekt-i-dipfeiky/
6. Deepfake. Кібер Брама. URL: https://stopfraud.gov.ua/cybersecurity-in-communication/deepfake-i1016