УДК 343.9:004.8]:347.9
DOI https://doi.org/10.24144/2788-6018.2026.02.2.72

КІБЕРЗЛОЧИНИ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ: ВИКЛИКИ ДЛЯ КРИМІНАЛЬНОГО ПРАВА ТА ГОСПОДАРСЬКОГО ПРОЦЕСУ УКРАЇНИ

Хом'яченко С.І.,
кандидат юридичних наук, доцент,
Вінницький торговельно-економічний інститут ДТЕУ
ORCID: 0000-0002-1223-5881

Дроздов М.Є.,
магістр права,
Дніпровський національний університет імені Олеся Гончара
ORCID: 0009-0003-1179-6315

Хом'яченко С.І., Дроздов М.Є. Кіберзлочини з використанням штучного інтелекту: виклики для кримінального права та господарського процесу України.

Досліджено проблематику кваліфікації кіберзлочинів, вчинених із використанням технологій штучного інтелекту, за чинним законодавством України. Проаналізовано способи застосування нейронних мереж, генеративних моделей та алгоритмів машинного навчання у злочинній діяльності, зокрема для створення дипфейків, автоматизації фішингових атак, підбору паролів та генерації шкідливого програмного забезпечення. Встановлено, що технології штучного інтелекту дозволяють злочинцям здійснювати масштабні кібератаки з високим рівнем автоматизації, що ускладнює їх виявлення та розслідування правоохоронними органами.

Встановлено істотні прогалини у кримінально-правовій охороні інформаційної безпеки, зокрема відсутність спеціальних норм про відповідальність за створення та поширення дипфейків у злочинних цілях, використання автономних систем для здійснення кібератак на критичну інфраструктуру, а також застосування генеративних моделей для виготовлення синтетичних матеріалів сексуального характеру. Досліджено проблеми використання ШІ у кіберзлочинності як чинника дестабілізації господарського процесу. Визначено, що генерування дипфейків створює загрозу для належного функціонування правосуддя через підрив інституту електронних доказів.

Констатовано, що положення Розділу XVI Кримінального кодексу України не враховують специфіку злочинів, вчинених за допомогою технологій штучного інтелекту, що створює труднощі при їх кваліфікації. Сформульовано пропозиції щодо вдосконалення матеріальних норм шляхом впровадження у КК України нової кваліфікуючої ознаки – вчинення злочину з використанням штучного інтелекту, а також процесуальних норм у частині модернізації ст. 96 ГПК України для запровадження спеціальних фільтрів перевірки автентичності електронних доказів.

Окрему увагу приділено аналізу складнощів доказування у кримінальних провадженнях щодо злочинів, вчинених за допомогою штучного інтелекту. Розглянуто проблеми збереження цифрових доказів, встановлення причинно-наслідкового зв'язку між діями особи та результатом роботи автономної системи, а також ідентифікації осіб, причетних до злочину.

Ключові слова: електронні докази, господарський процес, штучний інтелект, кіберзлочини, дипфейк, нейронні мережі, кримінальна відповідальність, кіберполіція.

Khomiachenko S.I., Drozdov M.Y. Cybercrimes using artificial intelligence: challenges for criminal law and economic process in Ukraine.

The issue of qualification of cybercrimes committed using artificial intelligence technologies under the current legislation of Ukraine was studied. Methods of using neural networks, generative models and machine learning algorithms in criminal activity were analyzed, in particular for creating deepfakes, automating phishing attacks, selecting passwords and generating malicious software. It was established that artificial intelligence technologies allow criminals to carry out large-scale cyberattacks with a high level of automation, which complicates their detection and investigation by law enforcement agencies. Significant gaps in the criminal law protection of information security were identified, in particular the lack of special norms on liability for the creation and distribution of deepfakes for criminal purposes, the use of autonomous systems to carry out cyberattacks on critical infrastructure, as well as the use of generative models for the production of synthetic materials of a sexual nature.

The problems of using AI in cybercrime as a factor in destabilizing the economic process were studied. It was determined that the generation of deepfakes poses a threat to the proper functioning of justice by undermining the institution of electronic evidence.

It was found that the provisions of Chapter XVI of the Criminal Code of Ukraine do not take into account the specifics of crimes committed using artificial intelligence technologies, which creates difficulties in their qualification. Proposals were formulated to improve substantive norms by introducing a new qualifying feature in the Criminal Code of Ukraine – committing a crime using artificial intelligence, as well as procedural norms in terms of modernizing Article 96 of the Code of Criminal Procedure of Ukraine to introduce special filters for verifying the authenticity of electronic evidence.

Special attention was paid to the analysis of the difficulties of proving in criminal proceedings regarding crimes committed using artificial intelligence. The problems of preserving digital evidence, establishing a causal relationship between a person's actions and the result of the work of an autonomous system, as well as identifying persons involved in a crime were considered.

Key words: human rights, constitutional principles, constitutionalism, humanism.

Постановка проблеми. Стрімкий розвиток технологій штучного інтелекту (надалі – ШІ) створює нові можливості для вчинення злочинів у кіберпросторі. І якщо раніше кіберзлочинність асоціювалася переважно з несанкціонованим доступом до комп'ютерних систем або поширенням шкідливого програмного забезпечення, то сьогодні правопорушники активно використовують алгоритми машинного навчання, нейронні мережі та генеративні моделі для досягнення злочинних цілей.

Понад те, сучасна трансформація кіберзлочинності під впливом технологій штучного інтелекту створює виклики, що виходять далеко за межі традиційного кримінального права, формуючи складну систему міжгалузевих деструктивних наслідків. Зокрема, використання ШІ для вчинення злочинів у цифровій сфері – від маніпуляцій із фінансовими активами до генерації високоточних дипфейків – не лише потребує перегляду підходів до кваліфікації діянь за Кримінальним кодексом України, а й безпосередньо дестабілізує господарський оборот. Це зумовлює виникнення нових категорій спорів у господарському процесі, де матеріали кримінальних проваджень стають ключовим елементом доказової бази, а питання преюдиційності вироків суду та правової ідентифікації ШІ-генерованих правочинів ставлять під загрозу принцип юридичної визначеності та захисту прав суб'єктів господарювання. Отже, розв'язання проблеми ШІ-кіберзлочинів вимагає комплексного аналізу, який поєднує кримінально-правову превенцію з механізмами ефективного процесуального захисту економічних інтересів у господарських судах».

Метою дослідження є теоретичне обґрунтування та розробка практичних рекомендацій щодо адаптації кримінального та процесуального законодавства України до умов стрімкого розвитку технологій штучного інтелекту задля подолання правової невизначеності та зміцнення кібербезпеки держави.

Стан опрацювання проблематики. Питання правового регулювання кіберзлочинності традиційно привертає увагу вітчизняних науковців. Значний внесок у розробку цієї проблематики зробили такі вчені, як: В.Д. Гавловський, Б.М. Головкін, М.В. Гуцалюк, І.І. Липкан, В.В. Луцик, М.В. Карчевський, В.Г. Хахановський, В.С. Цимбалюк, та інші. Зокрема, Неділько Я.В. у дисертації комплексно дослідив генезу «комп'ютерних злочинів» [1]. Втім, його робота не охоплює специфіку використання ШІ як знаряддя вчинення злочинів. Думчиков М.О. у дисертації систематизував зарубіжний досвід правового регулювання відповідальності за вчинення кримінальних правопорушень шляхом використання інформаційно-телекомунікаційних технологій [2].

Лугівська Л.Р., Яцишин О.О. та Любавіна В.П. у науковій праці 2024 року розглянули тенденції розвитку кримінальної відповідальності за кіберзлочини в умовах цифровізації суспільства [3]. Науковці наголошують на необхідності врахування нових технологічних реалій у формуванні кримінально-правової політики держави. Однак їхній аналіз залишає поза увагою конкретні механізми використання ШІ злочинцями та відповідні прогалини у законодавстві.

Іванцов В. та Зелінський В. у дисертаційному дослідженні 2024 року вивчали вплив цифровізації на розвиток кримінологічних досліджень [4]. Автори переконливо доводять, що традиційні кримінологічні методи потребують переосмислення в епоху цифрових технологій. Вони пропонують нові підходи до вивчення детермінант кіберзлочинності, проте питання застосування ШІ у злочинній діяльності розглядається ними фрагментарно.

Аналіз наукової літератури свідчить про наявність певного дослідницького інтересу до проблематики кіберзлочинності загалом. Водночас спеціалізованих праць, присвячених саме використанню технологій штучного інтелекту у злочинних цілях та відповідним викликам для кримінального права України, бракує. Наявні публікації не дають відповіді на запитання про кримінально-правову кваліфікацію діянь, вчинених за допомогою автономних систем, або про межі відповідальності розробників та користувачів таких систем.

Виклад основного матеріалу. Кіберзлочини охоплюють широкий спектр протиправних діянь: від банального шахрайства з банківськими картками до складних атак на критичну інфраструктуру держави. Їхня особливість полягає у високій латентності, транснаціональному характері та використанні складних технологічних інструментів, що ускладнює процес виявлення, фіксації та доведення вини конкретних осіб [5, с. 4]. Водночас, чинне кримінальне законодавство України формувалося в період, коли подібні технології або не існували, або перебували на початковій стадії розвитку. Виникає запитання: чи спроможні наявні норми Кримінального кодексу України адекватно реагувати на нові форми злочинної поведінки? Проблема ускладнюється тим, що застосування ШІ розмиває традиційні уявлення про суб'єкта злочину та його вину. Коли автономна система вирішує без безпосереднього втручання людини, встановлення причинно-наслідкового зв'язку між діями особи та злочинним результатом стає нетривіальним завданням. Законодавець опиняється перед дилемою: або адаптувати класичні інститути кримінального права до нових реалій, або створювати принципово сучасні правові конструкції.

Технології штучного інтелекту істотно розширюють інструментарій, доступний суб'єктам протиправної діяльності, що зумовлює появу нових форм та способів вчинення правопорушень у цифровому середовищі. Одним із найбільш поширених напрямів їх використання є створення дипфейків – високореалістичних відео– та аудіоматеріалів, у яких відтворюється поведінка або мовлення особи щодо подій, які фактично не мали місця. Застосування таких технологій створює суттєві ризики для інформаційної безпеки, репутаційних прав та належного функціонування правосуддя.

З огляду на це особливу небезпеку для господарського процесу становить генерування дипфейків, яке дає змогу з високою точністю фальсифікувати волевиявлення сторін або зміст електронних доказів. Така деформація цифрової реальності безпосередньо загрожує дотриманню принципу змагальності та об'єктивному встановленню обставин справи, адже чинна редакція ст. 96 ГПК України (Електронні докази) наразі не містить специфічних критеріїв для перевірки автентичності контенту, створеного за допомогою штучного інтелекту. Відтак, кримінально-правова загроза використання ШІ-інструментарію трансформується у складну процесуальну проблему, де підроблені цифрові образи можуть бути подані як належні докази, що вимагає негайної адаптації інституту судової експертизи до нових реалій кіберзлочинності.

Генеративні мовні моделі гарантують можливість автоматизації фішингових атак шляхом формування персоналізованих повідомлень, стилістично та змістовно наближених до легітимної комунікації. Системи штучного інтелекту здійснюють аналіз відкритих даних і профілів потенційних жертв у соціальних мережах, адаптують мовні конструкції та комунікативні стратегії до індивідуальних особливостей адресатів, що суттєво підвищує ефективність методів соціальної інженерії. Автоматизація таких процесів дозволяє здійснювати масштабні кібернетичні атаки за мінімальних часових і ресурсних витрат, що значно ускладнює їх своєчасне виявлення та нейтралізацію.

Алгоритми машинного навчання набувають щораз більшого використання щодо пошуку та аналізу вразливостей у програмному забезпеченні супроти темпів, що перевищують можливості традиційних методів тестування безпеки. У межах організованої кіберзлочинної діяльності штучний інтелект може застосовуватися для автоматизованого дослідження захисних механізмів інформаційних систем і розробки експлойтів без безпосередньої участі людини на кожному етапі. Нейронні мережі, здатні моделювати поведінкові патерни легітимних користувачів, створюють додаткові труднощі для функціонування систем виявлення аномалій та біометричних засобів захисту, що підвищує латентність відповідних правопорушень та рівень їх суспільної небезпеки.

Окремої уваги потребують проблеми кваліфікації за чинним законодавством правопорушень, вчинених із застосуванням штучного інтелекту, позаяк чинні конструкції Кримінального кодексу України не повною мірою враховують специфіку цифрової трансформації злочинної діяльності.

Розділ XVI Кримінального кодексу України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» встановлює кримінальну відповідальність за несанкціоновані дії з інформацією, створення та використання шкідливих програмних засобів, а також за інші суміжні посягання у сфері інформаційної безпеки [6]. Водночас аналіз положень цього розділу свідчить про відсутність норм, які б безпосередньо враховували використання технологій штучного інтелекту як кваліфікуючої ознаки злочину або як самостійного елемента складу кримінального правопорушення, що обмежує можливості адекватної правової оцінки відповідних діянь.

Стаття 361 КК України передбачає відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. З формально-юридичного погляду дії особи, яка застосовує систему штучного інтелекту для автоматизованого підбору паролів або обходу механізмів автентифікації, можуть бути кваліфіковані за цією нормою, тому що містять ознаки об'єктивної сторони злочину.

При цьому законодавче регулювання не відображає специфічних характеристик таких посягань, зокрема їх масштабності, високої швидкості реалізації та автономності інтелектуальних систем, що істотно підвищує рівень суспільної небезпеки відповідних діянь.

Згідно зі статтею 361-1 КК України кримінально караним визнається створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів [6]. У контексті застосування штучного інтелекту постає питання щодо можливості віднесення до таких засобів нейронних мереж, спеціально навчених для генерації фішингових повідомлень або здійснення інших форм маніпулятивного впливу. З технічного погляду подібні системи не завжди спрямовані на порушення функціонування комп'ютерних систем, знищення інформації чи блокування процесів її обробки, що ускладнює їх кваліфікацію в межах чинної редакції норми. Водночас цілеспрямований характер створення таких інструментів для вчинення злочинів свідчить про наявність підвищеної суспільної небезпеки, яка й досі є недостатньо відображеною у кримінальному законі.

Окрему проблему становить кримінально-правова оцінка створення та використання дипфейків, які фактично перебувають поза межами традиційних складів кіберзлочинів. Залежно від спрямованості та наслідків відповідних дій вони можуть кваліфікуватися як шахрайство (наприклад, використання дипфейків для маніпулювання корпоративними активами змушено кваліфікуються за загальними статтями про шахрайство ст. 190 КК або втручання в роботу ЕОМ ст. 361 КК), порушення недоторканності приватного життя (стаття 182 КК України) або як ввезення, виготовлення, збут і розповсюдження порнографічних предметів (стаття 301 КК України). Проте жодна із зазначених норм не відображає технологічної специфіки використання штучного інтелекту та не враховує зумовлений ним рівень суспільної небезпеки, що актуалізує необхідність подальшого вдосконалення кримінально-правового регулювання у цій сфері.

З огляду на викладене вище, пропонуємо запровадити нову кваліфікуючу ознаку: доповнити частину другу статей 190 (Шахрайство) та 361 (Несанкціоноване втручання в роботу ІС) КК України ознакою «вчинення діяння з використанням технологій штучного інтелекту». Це дозволить диференціювати відповідальність залежно від технологічної складності злочину, позаяк ШІ багаторазово підвищує ефективність та масштаби шкоди.

Окрім того, криміналізувати створення шкідливого ШІ-контенту: розглянути можливість доповнення КК України спеціальною нормою, яка б передбачала відповідальність за виготовлення, збут або розповсюдження дипфейків (неправдивого аудіо– чи відеоконтенту) з метою маніпуляції ринковими активами або дискредитації суб'єктів господарювання. До того ж, задля гарантування належного функціонування правосуддя та захисту від цифрових фальсифікацій, вбачається за необхідне: впровадити «презумпцію сумнівності» цифрового контенту: уточнити положення ст. 96 ГПК України правилом, за яким у разі обґрунтованого сумніву щодо автентичності електронного доказу (наявність ознак генерації ШІ), тягар доказування (onus probandi) покладається на сторону, яка подає такий доказ.

Базовим інструментом державної політики у цифровій сфері є Закон України «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи гарантування захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із гарантування кібербезпеки [7]. Попри те, що Закон оперує фундаментальними поняттями, такими як «кіберзагроза», «кіберзахист» та «кіберінцидент», він демонструє суттєву статичність щодо стрімкого розвитку високих технологій. Наразі закон не містить жодних спеціальних положень, які б регулювали використання штучного інтелекту, що створює ситуацію невизначеності: алгоритми ШІ залишаються поза межами нормативного поля як у контексті їхнього застосування у злочинних цілях, так і як потенційного інструментарію для гарантування національного кіберзахисту.

Варто відзначити, що Стратегія кібербезпеки України [8], яка діяла протягом 2021–2025 років, визначала ключові пріоритети захисту цифрового простору, проте була розроблена без урахування масштабного впровадження технологій генеративного штучного інтелекту. Хоча серед її основних завдань було названо розбудову системи виявлення та реагування на кіберінциденти, вона фактично не передбачала конкретних інструментів для протидії загрозам, пов'язаним із використанням ШІ. Це зумовило певну інертність державної системи кіберзахисту перед появою нових високотехнологічних способів вчинення правопорушень наприкінці терміну дії документа.

Тим часом, відсутність спеціального регулювання породжує невизначеність як для правоохоронних органів, так і для розробників технологій. Компанії, що створюють системи ШІ, не мають чітких орієнтирів щодо допустимих меж функціональності своїх продуктів. Правоохоронці стикаються із труднощами у кваліфікації діянь та доказуванні вини.

Висновки. У результаті проробленого дослідження встановлено, що швидка еволюція технологій штучного інтелекту (ШІ) призвела до суттєвого розриву між динамікою розвитку цифрової злочинності та статичністю кримінально-правового регулювання в Україні. Використання ШІ (дипфейків, генеративних мовних моделей, автономних систем пошуку вразливостей) змінює характер загрози, перетворюючи атаки на масштабовані, персоналізовані та високоавтономні. Це розмиває класичне розуміння причинно-наслідкового зв'язку між діями суб'єкта та злочинним результатом. Основні положення чинного КК України (зокрема Розділ XVI та ст. 190) не враховують специфічну суспільну небезпеку щодо використання інтелектуальних систем. Кваліфікація дій із використанням ШІ за «традиційними» статтями не відображає технологічної складової злочину та не дає змоги диференціювати відповідальність належним чином.

Можливість високоточної фальсифікації волевиявлення та електронних доказів із використанням технології дипфейків ставить під загрозу принципи змагальності та об'єктивності судового процесу. Чинне процесуальне законодавство (зокрема ст. 96 ГПК України) потребує адаптації до умов «деформації цифрової реальності». Для розв'язання окреслених проблем пропонується: доповнити ч. 2 ст. 190 та ч. 2 ст. 361 КК України новою кваліфікуючою ознакою – «вчинення діяння з використанням технологій штучного інтелекту»; криміналізувати створення та розповсюдження шкідливого ШІ-контенту (дипфейків), спрямованого на маніпулювання ринками або дискредитацію суб'єктів; запровадити у процесуальне право «презумпцію сумніву» щодо цифрового контенту, переклавши тягар доказування автентичності на сторону, що надає такий доказ у разі обґрунтованих сумнівів у його справжності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Неділько Я.В. Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій. Дисерт. на здобуття наук. ступеня доктора філософії за спеціальністю 081 Право. Київський національний університет ім. Тараса Шевченка, Київ, 2023. https://scc.knu.ua/upload/iblock/6a9/hz4scjc31amo5xndta6ny22 koszxyw73BE.pdf.
2. Думчиков М.О. Концептуальні засади кримінально-правової охорони кіберпростору в Україні. Дисерт. на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. Сумський державний університет https://dduvs.edu.ua/wp-content/uploads/files/Structure/science/ rada/new_ d0872702/2024/1/3/d.pdf.
3. Лугівська Л.Р., Яцишин О.О., Любавіна В.П. Тенденції розвитку кримінальної відповідальності за кіберзлочини в умовах цифровізації суспільства. *Dictum Factum.* 2024. № 2 (16). С. 258–264. URL: https://df.duit.in.ua/index.php/dictum/article/view/363.
4. Іванцов В., Зелінський В. Вплив цифровізації на розвиток кримінологічних досліджень: нові виклики та можливості: дис. Чернігів: Пенітенціарна академія України, 2024. URL: https:// dspace.univd.edu.ua/items/33a805aa-6e5c-43c3-a5a0-e44518a53847.
5. Попович М.В., Продан Т.В. Розслідування кіберзлочинів: сучасні виклики та криміналістичні особливості*. Науковий вісник Ужгородського Національного Університету.* 2025. Серія ПРАВО. Випуск 92: частина 4. С.397-402.file:///C:/Users/Professional/Desktop/%D0%A5%D0%20(1).pdf.
6. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. База даних «Законодавство України». ВР України. URL: https://zakon.rada.gov.ua/laws/show/2341-14.
7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. База даних «Законодавство України». ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
8. Стратегія кібербезпеки України: Указ Президента України від 26.08.2021 № 447/2021. База даних «Законодавство України». ВР України. URL: https://zakon.rada.gov.ua/laws/show/447/2021.

Дата першого надходження рукопису до видання: 2.03.2026
Дата прийняття до друку рукопису після рецензування: 20.03.2026
Дата публікації: 3.04.2026