Кримінальне право

УДК 343.2

Корогод Світлана Володимирівна
доктор філософії у галузі права,
старший викладач кафедри кримінального права та кримінології
Дніпровський державний університет внутрішніх справ
Korohod Svitlana
Doctor of Philosophy in Law,
Senior Lecturer at the Department of Criminal Law and Criminology
Dnipro State University of Internal Affairs
ORCID: 0000-0001-6696-6818

ЧИ ВІДПОВІДАЄ ЗАГАЛЬНА ЧАСТИНА ККУ СУЧАСНИМ ЦИФРОВИМ ВИКЛИКАМ (DEEPFAKE, БІОМЕТРИЧНІ ШАХРАЙСТВА, КІБЕРВПЛИВ)?
DOES THE GENERAL PART OF THE CCU MEET MODERN DIGITAL CHALLENGES (DEEPFAKE, BIOMETRIC FRAUD, CYBER INFLUENCE)?

Анотація. *Вступ. Цифрова трансформація суспільних відносин зумовила виникнення нових форм злочинності, які не знаходять належного відображення у чинному кримінальному законодавстві України. Технології deepfake, біометричні шахрайства, алгоритмічна шкода та різноманітні форми цифрової маніпуляції вказують на значний концептуальний розрив між положеннями Загальної частини Кримінального кодексу України та реальною цифровою дійсністю. Такий розрив створює загрозу безкарності, сприяє формуванню правового вакууму та знижує ефективність кримінально-правового захисту у сфері інформаційних відносин. Актуальність проблеми також підсилюється тим, що цифрова*

злочинність нерідко має транснаціональний характер, що ускладнює застосування традиційних механізмів відповідальності та міжнародного співробітництва.

Метою цієї наукової статті є виявлення ключових проблем функціонування кримінального права в умовах цифровізації суспільства, а також обґрунтування необхідності його концептуального оновлення.

Матеріали і методи. У дослідженні використано: 1) нормативноправові акти; 2) результати наукових досліджень щодо заходів запобігання кіберзлочинності. Використано методи порівняльно-правового аналізу для з'ясування світових підходів до боротьби з цифровими правопорушеннями, системний метод для узагальнення ключових проблем цифрової злочинності, формально-логічний метод для уточнення змісту дефініцій та кримінально-правових категорій, а також метод прогнозування для визначення можливих шляхів розвитку національного законодавства.

Результати. У результаті проведеного аналізу запропоновано низку напрямів оновлення кримінального законодавства. По-перше, доцільним є розширення поняття суб'єкта кримінального правопорушення з урахуванням можливості впливу на шкідливий результат через цифрових агентів, алгоритми та автоматизовані системи. По-друге, необхідним є оновлення дефініцій базових кримінально-правових категорій з урахуванням цифрової специфіки, що дозволить усунути прогалини у правозастосуванні. По-третє, пропонується розширення трактування вини у випадках опосередкованого цифрового впливу, де відповідальність особи може визначатися не лише за прямі дії, а й за керування або контроль над алгоритмами, які призвели до суспільно небезпечних наслідків. Нарешті, актуальною видається побудова цифрової парадигми кримінального права, яка забезпечить адаптацію правової системи до викликів глобального

кіберпростору, включаючи розвиток Metaverse та інших новітніх технологічних платформ.

Перспективи. Розробка цілісної системи кримінально-правових інструментів протидії цифровим правопорушенням, виробленні універсальних дефініцій у сфері інформаційної безпеки, адаптації національного законодавства до міжнародних стандартів, а також у створенні ефективних механізмів взаємодії між державами у боротьбі з транснаціональною цифровою злочинністю. Реалізація цих завдань дозволить подолати правовий вакуум, забезпечити ефективний захист цифрових прав особи та підвищити стійкість кримінально-правової системи до сучасних технологічних викликів.

Ключові слова: *цифрове правопорушення, deepfake, біометричні шахрайства, штучний інтелект, інформаційна ідентичність, цифрова особа, кібервплив.*

Summary. *Introduction. The digital transformation of social relations has led to the emergence of new forms of crime that are not adequately reflected in the current criminal legislation of Ukraine. Deepfake technologies, biometric fraud, algorithmic harm, and various forms of digital manipulation point to a significant conceptual gap between the provisions of the General Part of the Criminal Code of Ukraine and the reality of the digital world. This gap creates a threat of impunity, contributes to the formation of a legal vacuum, and reduces the effectiveness of criminal law protection in the field of information relations. The relevance of the problem is also exacerbated by the fact that digital crime is often transnational in nature, which complicates the application of traditional mechanisms of accountability and international cooperation.*

The purpose of this scientific article is to identify the key problems of the functioning of criminal law in the context of the digitalization of society, as well as to justify the need for its conceptual renewal.

Materials and methods. The study used: 1) regulatory acts; 2) results of scientific research on measures to prevent cybercrime. Comparative legal analysis was used to identify global approaches to combating digital offences, a systematic method was used to summarise the key problems of digital crime, a formal logical method was used to clarify the content of definitions and criminal law categories, and a forecasting method was used to identify possible ways of developing national legislation.

Results. As a result of the analysis, a number of areas for updating criminal legislation were proposed. First, it is advisable to expand the concept of a criminal offense, taking into account the possibility of influencing harmful results through digital agents, algorithms, and automated systems. Second, it is necessary to update the definitions of basic criminal law categories, taking into account digital specifics, which will eliminate gaps in law enforcement. Third, it is proposed to broaden the interpretation of guilt in cases of indirect digital influence, where a person's liability may be determined not only by direct actions, but also by the management or control of algorithms that have led to socially dangerous consequences. Finally, it seems relevant to build a digital paradigm of criminal law that will ensure the adaptation of the legal system to the challenges of global cyberspace, including the development of the Metaverse and other cutting-edge technological platforms.

Key words: *digital crime, deepfake, biometric fraud, artificial intelligence, information identity, digital identity, cyber influence.*

Постановка проблеми. Цифрова трансформація суспільства призвела до появи нових форм злочинності, які не мають належного відображення у чинному кримінальному законодавстві України. Зокрема, такі явища, як deepfake, алгоритмічна шкода, біометричні шахрайства та цифрова маніпуляція, вказують на значний концептуальний розрив між положеннями Загальної частини ККУ та об'єктивною цифровою

реальністю. Існуюча правова конструкція не передбачає можливості притягнення до відповідальності суб'єктів нової природи (автоматизованих систем, алгоритмів, цифрових агентів), а також не забезпечує належного захисту цифрових прав особи, що створює загрозу безкарності та правового вакууму.

Аналіз останніх досліджень і публікацій. Узагальнення наукових напрацювань вітчизняних і зарубіжних дослідників у сфері цифрових правопорушень дозволяє виокремити кілька ключових напрямів їхніх досліджень.

1. Проблематика визначення суб'єкта цифрового правопорушення та можливості притягнення до кримінальної відповідальності алгоритмів, автономних систем і штучного інтелекту (наприклад, Радутний О.Є. [2]).
2. Кримінологічний аналіз використання новітніх технологій deepfake та їх кримінально-правова оцінка (наприклад, Юртаєва К.В. [3]).
3. Біометричні шахрайства та загрози безпеці цифрової ідентичності особи, що стають основним об'єктом протиправних посягань (наприклад, Філіппов С.О. [4]).
4. Міжнародні стандарти протидії цифровим загрозам, що закріплені у Будапештській конвенції про кіберзлочинність та актах Європейського Союзу (наприклад, Конвенція про кіберзлочинність [6]; Директива ЄС NIS 2 [9]).

Перспективним концептуальним напрямом у розробці нової кримінально-правової парадигми є інтеграція традиційних положень кримінального права з сучасними підходами цифрового права та міждисциплінарними дослідженнями у сфері ІТ і кібербезпеки. Такий підхід дозволяє сформувати універсальні механізми протидії цифровим загрозам та адаптувати Загальну частину ККУ до викликів інформаційного суспільства.

Метою цієї наукової статті є виявлення ключових проблем функціонування кримінального права в умовах цифровізації суспільства, а також обґрунтування необхідності його концептуального оновлення.

Виклад основного матеріалу дослідження. У XXI столітті цифровізація трансформувала традиційні уявлення про об'єкти та суб'єкти правовідносин, породивши нові виклики для кримінального права. Однією з головних особливостей цього процесу є поява нових, раніше неіснуючих, категорій: цифрові особистості (аватари), електронні агенти, штучний інтелект (ШІ), смарт-контракти, NFT, віртуальні активи, автономні цифрові системи тощо. Водночас розвиток інформаційних технологій створив передумови для появи складних алгоритмічних конструкцій, що здатні вчиняти шкідливі дії без безпосередньої участі людини. До прикладу, технологія deepfake - це не просто інструмент генерації цифрових зображень, а механізм, що може створювати фальшиві свідчення, відео, які порушують честь, гідність та інші права, а також використовуються як засіб дискредитації в політичних, військових, кримінальних та особистих цілях. У подібних випадках виникає логічне запитання: хто є суб'єктом кримінального правопорушення – користувач, який скористався алгоритмом, чи розробник коду? Або, можливо, сама програма, якщо вона діє автономно?

Згідно зі статтею 11 Кримінального кодексу України (далі - ККУ), кримінальним правопорушенням є, передбачене цим Кодексом суспільно небезпечне винне діяння (дія або бездіяльність), вчинене суб'єктом кримінального правопорушення [1]. Ця норма побудована на традиційних уявленнях про фізичну дію особи, вольове її спрямування та наявність вини. Однак в умовах цифрового середовища, коли шкода може бути заподіяна автоматизованою системою, за допомогою самооновлюваного алгоритму, виникає правовий вакуум щодо притягнення до відповідальності.

Особливої актуальності ця проблема набуває у контексті застосування штучного інтелекту, який здатен до самонавчання, прийняття рішень, створення нових об'єктів або навіть взаємодії з іншими учасниками суспільних відносин без втручання людини. Алгоритм, який створює шкідливий deepfake без цільової вказівки людини, або біометричний сканер, який помилково ідентифікує особу і запускає ланцюг правових наслідків, формально не можуть бути притягнуті до відповідальності. Проте шкода заподіюється, і механізм відповідальності або профілактики такого типу шкоди відсутній.

Наявна редакція статті 18 КК України визначає, що суб'єктом кримінального правопорушення може бути лише фізична осудна особа, яка досягла встановленого віку кримінальної відповідальності. Таке положення виключає інші форми правосуб'єктності, зокрема юридичну, яка в умовах цифрової трансформації набуває все більшого значення. Разом із тим сучасні технології дозволяють автономним системам, алгоритмам і штучним агентам функціонувати у цифровому середовищі та метавсесвіті, створюючи реальну можливість заподіяння суспільно небезпечної шкоди [2, с.107]. Попри це, вони не можуть визнаватися самостійними суб'єктами кримінальної відповідальності. Натомість обґрунтованим видається розширення відповідальності юридичних осіб, а також запровадження конструкції «опосередкованої вини» фізичних чи юридичних осіб - розробників, користувачів або адміністраторів, які свідомо чи через грубу необережність допустили використання таких цифрових систем у протиправних цілях.

Відсутність механізмів притягнення до відповідальності або щонайменше ідентифікації винної сторони у випадку використання штучного інтелекту чи цифрових інструментів створює загрозу безкарності в межах нових форм злочинності. Це також актуалізує проблему притягнення до відповідальності осіб, які є лише посередниками -

наприклад, хостинги, онлайн-платформи або розробники відкритого коду, які не мали умислу, але створили інструмент, що став засобом правопорушення.

Складність посилюється у ситуаціях, коли правопорушення вчиняються в транскордонному режимі. Скажімо, бот, що генерує deepfake-контент, розміщений на сервері в одній країні, адмініструється з іншої, а шкода заподіюється третій стороні - громадянину України. У таких обставинах постає питання про застосовність норм ККУ в просторі, визначене в статті 6, і про юрисдикцію, особливо якщо шкода має нематеріальний характер (наприклад, репутаційна шкода, порушення приватності).

Окремої уваги потребує питання інтерпретації вини її розширення та правильного тлумачення у сфері цифрових правопорушень. Використання ШІ-систем, зокрема тих, що здатні до самонавчання, ускладнює традиційне розмежування умислу та необережності. Адже особа може запускати алгоритм, не маючи повного уявлення про всі потенційні наслідки його автономних дій. Проте це не свідчить про необхідність відмови від класичної чотиричленної моделі вини. Навпаки, її збереження забезпечує юридичну визначеність та стабільність кримінально-правової системи, а для цифрових деліктів доцільним є вироблення доктринальних орієнтирів, що дозволять правильно тлумачити прямий та непрямий умисел, самовпевненість і недбалість в умовах опосередкованого впливу людини на шкідливий результат. Таким чином, йдеться не про створення нових форм вини, а про адаптацію вже існуючих категорій шляхом уточнення критеріїв їх застосування у цифровому середовищі.

У традиційній кримінально-правовій доктрині вихідним є прямий причинно-наслідковий зв'язок між діянням особи та шкідливим результатом, однак у цифровому середовищі цей зв'язок часто опосередковується діями програмного коду, машинних алгоритмів або

роботизованих систем. За таких умов постає питання: якою мірою особа усвідомлювала можливі наслідки застосування технології та чи можна її поведінку віднести до умислу або необережності у класичному сенсі. Проте складність кваліфікації не означає, що необхідно конструювати нові, спеціально «цифрові» форми вини. Такий підхід міг би призвести до надмірної фрагментації кримінального права, ускладнити правозастосування та суперечити принципу юридичної визначеності. Саме тому принциповим є збереження класичної чотиричленної моделі вини - прямого умислу, непрямого умислу, самовпевненості та недбалості, яка забезпечує системність кримінально-правового регулювання і водночас дозволяє врахувати нові суспільні реалії.

Разом із тим, у цифровому середовищі кожна з форм вини потребує конкретизації. Прямий умисел матиме місце тоді, коли особа створює або використовує штучно-інтелектуальну систему чи алгоритм із чітким усвідомленням і бажанням досягти конкретного протиправного результату. Це може проявлятися у програмуванні алгоритму, що генерує шкідливе програмне забезпечення, або у створенні deepfake-матеріалів для шантажу чи дискредитації. У таких випадках цифровий інструмент виступає як своєрідне «знаряддя кримінального правопорушення», а особа діє з чітко визначеним наміром.

Непрямий умисел охоплює ситуації, коли суб'єкт усвідомлює високу ймовірність шкідливих наслідків автономних дій системи, але свідомо допускає їх. Типовим прикладом є запуск неконтрольованої бот-мережі, наслідком роботи якої може стати дезінформація, паніка чи дестабілізація суспільно-політичної ситуації. У цьому випадку особа не прагне безпосередньо досягти результату, але допускає його настання.

Самовпевненість виявляється тоді, коли суб'єкт розуміє ризики використання технології, проте легковажно вважає, що вони не реалізуються. Це може бути у випадках впровадження біометричних систем

без належного тестування чи сертифікації, коли розробник знає про можливі помилки алгоритму, але необґрунтовано сподівається, що проблеми не виникнуть.

Недбалість у цифровому контексті має місце тоді, коли особа не вживає заходів належного контролю за роботою системи, хоча повинна була й могла передбачити можливі негативні наслідки. Яскравим прикладом є розміщення у відкритому доступі програмного коду з відомими вразливостями, що створює ризик кібератак чи витоку даних.

Для правильного визначення форми вини у цифровій сфері необхідно спиратися на певні доктринальні орієнтири. Насамперед слід враховувати ступінь передбачуваності наслідків від використання конкретного алгоритму чи системи: чи існували відомості про потенційні збої, чи були зафіксовані аналогічні випадки раніше. Важливим є також обсяг можливостей і обов'язку контролю за функціонуванням системи, що покладається на розробника, адміністратора чи користувача. Крім того, визначальне значення має рівень професійної компетентності особи: спеціаліст у галузі ІТ чи кібербезпеки повинен мати вищий рівень обізнаності та передбачливості, ніж пересічний користувач. Не менш важливим є характер взаємодії людини з технологією – чи особа здійснювала програмування, налаштування чи запуск системи, чи лише користувалася нею.

Сучасні технологічні виклики - такі як deepfake, біометричні підробки, кіберманіпуляції, зловживання даними - вказують на наявну концептуальну і правову розривність між Загальною частиною ККУ та об'єктивною реальністю сучасного цифрового світу. Це потребує фундаментального перегляду таких базових положень, об'єкта кримінального правопорушення, форми вини, місця вчинення кримінального правопорушення та засобів його вчинення. Лише за умови такої ревізії кримінальне право здатне виконувати свої класичні функції -

охоронну, превентивну та регулятивну - в умовах цифрової трансформації суспільства.

У контексті порушеної проблеми доцільно зосередити увагу на окремих цифрових феноменах, що становлять реальну загрозу особистій безпеці та стабільному функціонуванню правової системи, проте залишаються поза межами належного кримінально-правового реагування у чинному законодавстві. Йдеться насамперед про deepfake-контент, біометричні шахрайські практики та технології кіберманіпуляції (інформаційного впливу). Ці явища не лише змінюють уявлення про суспільну небезпеку, а й наочно демонструють, що традиційне визначення складу кримінального правопорушення у національному кримінальному праві (зокрема, крізь призму умислу, суб'єкта та форми вини) потребує розширення чи переосмислення.

Технологія deepfake є результатом використання алгоритмів глибинного навчання (нейромереж) для створення фальшивих відео, аудіо або зображень, що імітують реальну особу. Її небезпека полягає у повній достовірності підробки, яка не дозволяє звичайному спостерігачу відрізнити фейк від реального контенту [3, с.32-33]. На практиці такі матеріали використовуються для шантажу, кібербулінгу, порушення честі й гідності особи, втручання у приватне життя. Частково ці дії можуть кваліфікуватися за статтями про наклеп, шахрайство, втручання в діяльність працівника правоохоронного органу або суду, але така кваліфікація є непрямою та складною для доведення. Суб'єктом таких правопорушень може бути фізична особа, власник або користувач алгоритму, а в деяких випадках - автоматизована система, яка вочевидь не охоплюється нормами статті 18 ККУ.

Не менш проблемною у цьому контексті є й сфера біометричних шахрайств. Йдеться про зловживання у сфері використання фізіологічних і генетичних характеристик особи (відбитки пальців, геометрія обличчя,

сітківка ока, ДНК, голос), що стали основним інструментом цифрової ідентифікації у багатьох системах: банківській, прикордонній, медичній, податковій тощо [4]. В Україні, як і в більшості інших держав, такі дії можуть кваліфікуватися через шахрайства (ст. 190 ККУ), незаконного збору персональних даних (ст. 182), порушення недоторканності приватного життя (ст. 145) або використання підроблених документів (ст. 358). Однак жодна з вказаних норм не враховує специфіку предмета посягання - біометричної інформації - як особливого різновиду персональних даних, який за своєю природою не підлягає відновленню чи зміні, що об'єктивно підвищує ступінь суспільної небезпеки. Відсутність чіткої дефініції поняття «біометрична інформація» у тексті ККУ унеможливлює її окрему кримінально-правову охорону, попри те, що в умовах розвитку штучного інтелекту такі дані стають основою для формування цифрових двійників, аватарів та інших ідентифікаційних моделей.

Особливої уваги потребує і категорія кібервпливу, під якою слід розуміти як цілеспрямовану маніпуляцію інформаційним середовищем, так і індивідуальне психологічне або соціальне програмування користувачів цифрових платформ. Зокрема, це виявляється у формуванні інформаційних атак (дезінформація, фейкові новини, алгоритмічне просування контенту), впливі на електоральні процеси (шляхом керованої реклами, бот-мереж, синтетичних новин), використанні нейролінгвістичного програмування через соціальні мережі тощо [5, с.80]. На відміну від класичного «інформаційного кримінального правопорушення» (розголошення державної таємниці, незаконне збирання інформації), кібервплив спрямований не на об'єкти, а на свідомість і поведінку мас. На рівні КК України подібні прояви не отримали жодної нормативної інтерпретації. Це обумовлює нагальну потребу в оновленні положень про об'єкт кримінального правопорушення (ст. 1, 11 ККУ), адже вказані дії вже сьогодні призводять до реальних деструктивних наслідків: політичної

дестабілізації, зростання рівня насильства, підриву правопорядку, мілітаризації суспільства.

У цьому контексті варто згадати і Будапештську конвенцію про кіберзлочинність 2001 року, яка була ратифікована Україною та стала основним міжнародно-правовим актом у сфері протидії кримінальним правопрушенням у кіберпросторі [6]. Її положення визначають базові стандарти криміналізації діянь, пов'язаних із неправомірним доступом до комп'ютерних систем, перехопленням даних, втручанням у роботу мереж, комп'ютерним шахрайством та порушенням авторських прав у цифровому середовищі. Разом з тим, попри фундаментальне значення цієї Конвенції, слід наголосити, що вона була розроблена понад два десятиліття тому і не охоплює новітні загрози, зокрема deepfake-технології, біометричні шахрайства чи системний кібервплив. Це вказує на потребу як у вдосконаленні національного законодавства, так і в ініціюванні оновлених міжнародних стандартів, здатних адекватно реагувати на сучасні форми цифрових загроз.

У перелічених випадках стає очевидною недостатність законодавства України як у концептуальному, так і в інструментальному вимірах. Ті цифрові виклики, що були розглянуті вище (deepfake, біометричні шахрайства, кібервплив), є лише окремими проявами більш глибоких проблем, що виникають у сфері загальноправової конструкції кримінального правопорушення. Найбільш системними серед них є відсутність сучасної термінології, обмеженість поняття суб'єкта кримінального правопорушення, негнучкість традиційного розуміння вини та нерозвинутість механізмів фіксації і оцінки електронних доказів у кримінальному провадженні.

Передусім, необхідно вказати на відсутність належних дефініцій ключових понять цифрової доби, що вже є не просто технічними, а соціально-правовими категоріями. У КК України повністю відсутні такі

терміни, як «кіберпростір», «цифровий контент», «віртуальна особа», «штучний агент», «алгоритмічна шкода», «інформаційна ідентичність». Це унеможливлює нормативну конкретизацію складу кримінальних правопорушеннь, об'єктів посягання, форм вини та способів вчинення діяння. Наприклад, вчинення правопорушення щодо цифрової репутації особи (шляхом розповсюдження deepfake-контенту чи штучної дискредитації в мережі) фактично не має об'єктивного вираження в термінах Загальної частини ККУ. Немає поняття «репутаційної шкоди в цифровому середовищі» як самостійної форми шкоди. Відповідно, не існує і правових механізмів її захисту в рамках кримінального права.

Друга фундаментальна прогалина полягає у звуженому визначенні суб'єкта кримінального правопорушення, яке закріплене у статті 18 ККУ. У такому підході абсолютно ігнорується цифрова реальність, де кримінальне правопорушення може бути вчинене за допомогою алгоритмічної системи (наприклад, бот-мережі, deepfake-генератора, нейромережі, яка сама змінює свій функціонал) або ж юридичною особою, яка цілеспрямовано запускає такі механізми. У правових системах низки держав уже активно впроваджується концепція деліктоздатності юридичних осіб або навіть «розширеного суб'єкта», коли відповідальність покладається не тільки на безпосереднього виконавця, а й на дизайнера цифрового середовища, розробника програмного забезпечення, системного адміністратора або замовника алгоритму [7]. В Україні ж навіть саме питання про відповідальність конструктора алгоритму залишається поза межами правового поля. Особливо небезпечним проявом цієї концептуальної прогалини є так звана алгоритмічна відповідальність - ситуація, коли шкідливі дії вчиняються автоматизованою системою без прямого втручання людини. Наприклад, алгоритм, що аналізує поведінку користувачів і на її основі генерує фейкові новини або обирає мішень для дискредитації, самостійно реалізує функцію, що має ознаки правопорушення. У той же час

кримінальне право не визнає алгоритм суб'єктом, а його творець може бути відстороненим у часі або в просторі від моменту заподіяння шкоди. Відтак відповідальність фактично «розчиняється» в системі - і виникає ефект безкарності, особливо якщо технологія функціонує на умовах відкритого коду або через децентралізовану платформу (наприклад, DAO - децентралізовану автономну організацію [8, с.45]).

Третім рівнем проблемності виступає питання форм вини та причинного зв'язку у цифрових правопорушеннях. Традиційна кримінально-правова парадигма розрізняє прямий і непрямий умисел, кримінально-протиправну самовпевненість та недбалість, і ці категорії залишаються універсальними. Водночас у випадках, коли протиправний результат настає внаслідок автономних дій алгоритму або штучної системи, виникає необхідність у більш гнучкому тлумаченні цих форм. Йдеться не про запровадження нових понять на кшталт «цифрової необережності» чи «технологічної халатності», що могло б призвести до надмірної фрагментації кримінально-правової матерії, а про уточнення критеріїв для правильного застосування вже існуючих доктринальних конструкцій. Так, у випадках використання нестабільного програмного забезпечення або неналежного тестування ШІ-системи перед її комерційним запуском, шкідливий результат може бути кваліфікований крізь призму самовпевненості чи недбалості залежно від того, чи особа свідомо розраховувала на відсутність негативних наслідків, чи взагалі не вжила належних заходів контролю. Аналогічно, навмисне створення алгоритму з потенційно шкідливим функціоналом може свідчити про прямий чи непрямий умисел. Важливо також враховувати питання причинного зв'язку: навіть якщо шкідливий наслідок реалізується через автономне рішення системи, відповідальність особи визначається її рівнем передбачуваності, можливістю контролю та професійною компетентністю у сфері цифрових технологій.

У світлі вже зазначених глибоких концептуальних прогалин у Загальній частині Кримінального кодексу України, особливо щодо термінології, доречно звернути увагу на підходи зарубіжних держав та міжнародної доктрини, що демонструють прагнення системно оновити кримінальне право відповідно до вимог цифрової епохи. В умовах стрімкої трансформації суспільних відносин під впливом штучного інтелекту, мета всесвітів, нейромереж та цифрових валют, дедалі більше країн вбачають за необхідне формулювати нову парадигму кримінально-правового реагування на цифрові виклики.

Зокрема, у провідних юрисдикціях - США, країнах Європейського Союзу, КНР, Південній Кореї, Японії - вже фіксується тенденція до кодифікації спеціальних кримінальних норм, що регулюють цифрові простори, віртуальну поведінку та кіберзлочини нової генерації. Наприклад, у низці штатів США (Каліфорнія, Техас, Нью-Йорк) прийнято норми, що прямо забороняють створення та розповсюдження deepfake-контенту, особливо з метою впливу на вибори або поширення порнографії. У ЄС розроблено Директиву щодо боротьби з кіберзлочинністю, яка вимагає криміналізувати доступ до ІТ-систем, втручання в дані, розповсюдження шкідливого програмного забезпечення, протиправне використання бот-мереж та інші форми кібервтручання [9]. Китай, зі свого боку, пішов шляхом створення спеціального законодавства, яке прирівнює цифрову ідентичність до особистих немайнових благ, захищених кримінальним законом, і встановлює кримінальну відповідальність за їх порушення [10, с.139-140].

Особливої уваги заслуговує концепція так званого «Модельного Кримінального кодексу для Metaverse», яка вже пропонується окремими українськими та зарубіжними науковцями як відповідь на стрімкий розвиток віртуальних світів і цифрових платформ, що функціонують автономно або з мінімальним людським втручанням. Цей підхід передбачає розробку нової редакції Загальної частини КК, адаптованої під

правовідносини у цифровому середовищі. Зокрема, в його межах пропонується [11]:

- формалізувати окрему категорію віртуального або електронного суб'єкта кримінального правопорушення - тобто розширити поняття суб'єкта за рахунок юридичних осіб, автоматизованих систем, децентралізованих агентів та осіб, які діють через них;
- оновити класифікацію форм вини, доповнивши її поняттями «цифрової необережності», «алгоритмічного умислу», «непрямого технологічного впливу»;
- запровадити механізми електронної ідентифікації правопорушника, які б дозволили встановлювати особу на підставі цифрового сліду, IP-ідентифікаторів, записів логів, блокчейн-активності, біометричних відбитків тощо;
- ввести окремі норми щодо кримінальних правопорушень у віртуальних середовищах, які б передбачали відповідальність за дії, спрямовані на цифрову власність (наприклад, віртуальні активи, NFT, токенізовані ресурси), цифрову особистість, психоемоційний стан особи внаслідок віртуального насильства, атак на віртуальні спільноти тощо;
- встановити особливий порядок визначення юрисдикції у випадках вчинення правопорушення у транскордонному цифровому середовищі (тобто коли правопорушник, потерпілий і платформа знаходяться в різних державах, а кримінальне правопорушення вчинено у віртуальному просторі).

Ця модельна концепція заснована на визнанні факту, що цифровий світ формує власні соціальні відносини, які за своєю суттю не є аналогами офлайн-дій, а відтак потребують оригінального кримінально-правового підходу, а не спроби формального розширення вже наявних норм. Вона орієнтована на технологічну нейтральність, тобто формулювання кримінально-правових приписів у спосіб, який не залежить від конкретного

цифрового носія чи програми, але дозволяє охопити широкий спектр сучасних та майбутніх технологій.

Водночас така ідея викликає дискусії у вітчизняній юридичній науці. З одного боку, існує аргумент про несумісність класичних принципів кримінального права (особистої вини, суб'єктивного ставлення до діяння, презумпції невинуватості) з феноменом штучного інтелекту та алгоритмічної поведінки. З іншого - очевидною є потреба знайти юридичну форму для реагування на реальні цифрові загрози, які спричиняють шкоду не менш значущу, ніж традиційні кримінальні правопорушення. Саме тому постає необхідність поєднати доктрину кримінального права з міждисциплінарними розробками у сфері IT-етики, кіберправа, цифрової політики, що дозволить сформувати гібридну нормативну матрицю, придатну до застосування у нових цифрових середовищах.

Зарубіжний досвід та наукові моделі, зокрема ідеї Модельного Кримінального кодексу для Metaverse, вказують на неминучість реформування Загальної частини КК України в бік її цифрової адаптації. Україна, яка активно рухається в напрямку цифрової держави (через ініціативи «Дія» [12], електронний суд, реєстри, смарт-контракти тощо), не може залишити поза увагою реформу кримінального законодавства як одного з ключових інструментів охорони прав і свобод у цифровому вимірі.

Висновки та перспективи подальших досліджень. Чинна Загальна частина Кримінального кодексу України потребує не точкових змін, а системного перегляду основоположних понять, структур і логіки її побудови. Проблеми, пов'язані з неврахуванням цифрових об'єктів, нових форм шкоди та технологічно зумовлених видів вини, свідчать про те, що традиційна кримінально-правова конструкція вже не відповідає реаліям інформаційного суспільства. Відтак, доцільно сформулювати конкретні пропозиції щодо модернізації Загальної частини ККУ, які дозволили б підвищити її ефективність в умовах цифрових трансформацій.

По-перше, у чинному Кримінальному кодексі України бракує чіткого врахування нових цифрових викликів. Проте доцільніше не перевантажувати його завдання та загальні положення складними і змінними технічними термінами, які з часом втрачатимуть актуальність. Натомість варто передбачити загальне положення про охорону прав та свобод особи від суспільно протиправних посягань у сфері цифрових технологій, залишивши деталізацію конкретних складів кримінальних правопорушень для Особливої частини КК. Це дозволить гнучко реагувати на появу нових явищ, таких як маніпулятивний алгоритмічний вплив, неправомірне використання біометричних даних чи створення шкідливих цифрових симуляцій (наприклад, дипфейків), без необхідності постійно змінювати Загальну частину.

По-друге, надзвичайно актуальним є розширення поняття суб'єкта кримінального правопорушення (ст. 18 КК України). Поряд із фізичними особами суб'єктами повинні визнаватися також юридичні особи, причому їхня відповідальність має бути чітко розширена в частині цифрових правопорушень. Крім того, доцільно закріпити положення про можливість притягнення до відповідальності осіб, які опосередковано реалізують кримінально-протиправну поведінку через використання автоматизованих систем чи децентралізованих структур (наприклад, DAO). У такому випадку мова може йти про введення доктрини «опосередкованої вини» розробників, користувачів чи адміністраторів програмних продуктів, які свідомо або з грубою необережністю допустили використання створених ними технологій у кримінально-протиправних цілях.

По-третє, актуальним є питання оновлення доктринальної класифікації форм вини, закріплених у статтях 23-25 КК України. Йдеться не про введення нових категорій, що могло б порушити цілісність кримінально-правової системи, а про конкретизацію існуючих понять умислу та необережності з урахуванням особливостей цифрового

середовища. Це дозволить правильно кваліфікувати дії розробників, операторів чи адміністраторів алгоритмічних систем, які можуть впливати на настання шкідливого результату навіть без їхньої прямої участі в момент вчинення правопорушення. У такому контексті прямий і непрямий умисел, самовпевненість і недбалість отримують цифрові виміри: від свідомого програмування системи для досягнення протиправного результату - до невжиття необхідних заходів контролю за її функціонуванням. Важливим є також запровадження додаткових доктринальних орієнтирів (передбачуваність наслідків, можливість і обов'язок контролю, рівень цифрової компетентності, характер взаємодії особи з технологією), що сприятиме більш точному встановленню форми вини у випадках опосередкованого впливу людини на алгоритмічний процес.

По-четверте, доцільним є доповнення статті 15 ККУ (готування до кримінального правопорушення) ознаками, що відображають специфіку дій у цифровому середовищі. Наприклад, до готування слід віднести написання коду, що дозволяє генерувати deepfake, створення бот-мережі з метою подальшої атаки, завантаження шкідливого програмного забезпечення для злому систем. Такий підхід дозволить виявляти і переслідувати цифрові кримінального правопорушення ще на стадії підготовки, що особливо важливо з огляду на швидкоплинність цифрових дій та їхню високу латентність.

По-п'яте, потрібно переглянути підхід до визначення причинного зв'язку між діянням і наслідками, адаптувавши його до складності цифрових процесів. Наприклад, у разі кримінально-протиправної поведінки штучного інтелекту слід оцінювати не лише «фактичний» причинний зв'язок, а й технологічно опосередкований, з урахуванням участі розробника, замовника, користувача тощо.

По-шосте, важливо врегулювати принципи визначення юрисдикції у випадках вчинення кримінальних правопорушень у цифровому середовищі,

особливо коли йдеться про транскордонні атаки, хакерські вторгнення, поширення шкідливого контенту через зарубіжні сервери. Доцільно у Загальній частині встановити правило, за яким місцем вчинення кримінального правопорушення вважатиметься не лише місце, де діяв правопорушник, а й місце, де було завдано шкоди або де перебуває потерпілий.

Окрім того, важливим кроком могла б стати розробка окремого розділу або додатку до Загальної частини ККУ, присвяченого особливостям кримінально-правового регулювання у цифровому середовищі - своєрідної «цифрової парадигми кримінального права», яка б враховувала особливості віртуальних просторів, взаємодії між людиною та ШІ, транснаціональної природи багатьох цифрових правопорушень.

Література

1. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : станом на 17 лип. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 03.08.2025).

2. Радутний О.Е. Штучний інтелект як суб'єкт злочину. *Інформація і право.* 2017. № 4. С. 106-115.

3. Юртаєва К.В. Кримінологічний аналіз використання технології Deepfake: коли фейк стає злочином. *Вісник кримінологічної асоціації України.* 2021. № 1(24). С. 31–42.

4. Філіппов С. О. Біометричні технології: значення для протидії транскордонній злочинності. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2018. Вип. 2.

5. Вдовенко С.Г., Даник Ю.Г. Проблеми та перспективи забезпечення кібероборони держави. *Збірник наукових праць військового інституту*

Київського Національного університету імені Тараса Шевченка. 2020. Вип. 66. С. 75-89.

6. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 25.08.2025).

7. Napieralska A., Kepczynski P. Redefining accountability: navigating legal challenges of participant liability in decentralized autonomous organizations. *ArXiv, abs/2408*. 2024. 04717. DOI: https://doi.org/10.48550/arXiv.2408.04717.

8. Бровченко Т. І., Білоус Д. Є. Децентралізована автономна організація: правові аспекти та міжнародний досвід. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Юридичні науки*. 2025. С. 44-50.

9. Директива європейського парламенту і ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території союзу, внесення змін до регламенту (ЄС) № 910/2014 та директиви (ЄС) 2018/1972 та скасування директиви (ЄС) 2016/1148 (директива NIS 2). *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text (дата звернення: 03.08.2025).

10. Завадський А. А. Підходи Китаю до регулювання технологій глибокого синтезу (DEEPFAKE). *Правові виклики сучасності:* Матеріали круглого столу (20 грудня 2022 р.). 2022. С. 139-142.

11. Костенко О.В., Журавльов Д.В., Дніпров О.С., Коротюк О.В. Нові горизонти права: від електронної юрисдикції до модельного кримінального кодексу Метавсесвіту. *Інформація і право.* 2024. № 2(49). С. 43-61.

12. Дія – Державні послуги онлайн. *Державні послуги онлайн. Дія*. URL: https://diia.gov.ua/ (дата звернення: 03.08.2025).

References

1. Kryminalnyi kodeks Ukrainy : Kodeks Ukrainy vid 05.04.2001 № 2341-III : stanom na 17 lyp. 2025 r. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text [in Ukrainian].

2. Radutnyi O.E. Shtuchnyi intelekt yak subiekt zlochynu. *Informatsiia i pravo.* 2017. № 4. S. 106-115 [in Ukrainian].

3. Yurtaieva K.V. Kryminolohichnyi analiz vykorystannia tekhnolohii Deepfake: koly feik staie zlochynom. *Visnyk kryminolohichnoi asotsiatsii Ukrainy.* 2021. № 1(24). S. 31–42 [in Ukrainian].

4. Filippov S. O. Biometrychni tekhnolohii: znachennia dlia protydii transkordonnii zlochynnosti. *Visnyk Natsionalnoi akademii Derzhavnoi prykordonnoi sluzhby Ukrainy. Yurydychni nauky*. 2018. Vyp. 2 [in Ukrainian].

5. Vdovenko S.H., Danyk Yu.H. Problemy ta perspektyvy zabezpechennia kiberoborony derzhavy. *Zbirnyk naukovykh prats viiskovoho instytutu Kyivskoho Natsionalnoho universytetu imeni Tarasa Shevchenka.* 2020. Vyp. 66. S. 75-89 [in Ukrainian].

6. Konventsiia pro kiberzlochynnist : Konventsiia Rady Yevropy vid 23.11.2001 : stanom na 7 veres. 2005 r. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text [in Ukrainian].

7. Napieralska A., Kepczynski P. Redefining accountability: navigating legal challenges of participant liability in decentralized autonomous organizations. *ArXiv, abs/2408.* 2024. 04717. DOI: https://doi.org/10.48550/arXiv.2408.04717

8. Brovchenko T. I., Bilous D. Ye. Detsentralizovana avtonomna orhanizatsiia: pravovi aspekty ta mizhnarodnyi dosvid. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Yurydychni nauky.* 2025. C. 44-50 [in Ukrainian].

9. Dyrektyva yevropeiskoho parlamentu i rady (IeS) 2022/2555 vid 14 hrudnia 2022 roku pro zakhody dlia vysokoho spilnoho rivnia kiberbezpeky na vsii terytorii soiuzu, vnesennia zmin do rehlamentu (IeS) № 910/2014 ta

dyrektyvy (IeS) 2018/1972 ta skasuvannia dyrektyvy (IeS) 2016/1148 (dyrektyva NIS 2). *Ofitsiinyi vebportal parlamentu Ukrainy.* URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text [in Ukrainian].

10. Zavadskyi A. A. Pidkhody Kytaiu do rehuliuvannia tekhnolohii hlybokoho syntezu (DEEPFAKE). *Pravovi vyklyky suchasnosti: Materialy kruhloho stolu* (20 hrudnia 2022 r.). 2022. S. 139-142 [in Ukrainian].

11. Kostenko O.V., Zhuravlov D.V., Dniprov O.S., Korotiuk O.V. Novi horyzonty prava: vid elektronnoi yurys-dyktsii do modelnoho kryminalnoho kodeksu Metavsesvitu. *Informatsiia i pravo.* 2024. № 2(49). S. 43-61 [in Ukrainian].

12. Diia - Derzhavni posluhy onlain. Derzhavni posluhy onlain. *Diia*. URL: https://diia.gov.ua/ [in Ukrainian].