УДК 343.98

Гринько Лариса Петрівна –
кандидат юридичних наук,
доцент кафедри кримінального права
та кримінально-правових дисциплін
Полтавського юридичного інституту
Національного юридичного університету
імені Ярослава Мудрого, м. Полтава, Україна;
ORCID id 0000-0003-1861-8354
email: gull_ukr@ukr.net

Larysa P. Grynko –
PhD, Associated Professor of the Department of Criminal Law
and Criminal Law Disciplines
Poltava Law Institute of The Yaroslav Mudryi
National Law University, Poltava, Ukraine
(5 Hrytsayenka Vitalii Avenue, Poltava, 36011, Ukraine)
ORCID id 0000-0003-1861-8354
email: gull_ukr@ukr.net

Криміналістичний аналіз діпфейків: виявлення аномалій, аудіовізуальна атрибуція та ланцюг збереження доказів

У статті досліджено криміналістичні аспекти виявлення, фіксації та дослідження діпфейк-контенту, створеного з використанням технологій штучного інтелекту, а також їх вплив на сучасну практику доказування у кримінальному процесі. Зазначено, що діпфейки – синтетичні аудіо- чи відеоматеріали, створені генеративно-змагальними мережами (GAN), стають інструментом нової хвилі інтернет-шахрайств, інформаційних маніпуляцій і порушення приватності. На основі аналізу сучасних наукових джерел і міжнародних стандартів окреслено основні криміналістичні проблеми, пов'язані з використанням ШІ у злочинній діяльності: високий рівень латентності, труднощі у визначенні автентичності цифрових доказів, а також ризики фальсифікації особистих даних під час фінансових операцій і процедур верифікації.

Розглянуто основні напрями криміналістичного аналізу deepfake-контенту: дослідження цифрових артефактів і метаданих, перевірка частоти кадрів і часових аномалій, візуальний аналіз ознак синтетичного відео (освітлення, тіней, кольорової гами, міміки), аудіоаналіз синхронності звуку й відео, а також застосування алгоритмів машинного навчання для виявлення прихованих закономірностей. Наголошено на необхідності дотримання ланцюга збереження цифрових доказів і забезпечення їх допустимості в суді.

*Окрему увагу приділено етичним і правовим аспектам використання штучного інтелекту у криміналістиці, зокрема питанням упередженості алгоритмів, конфіденційності персональних даних та контролю за достовірністю автоматизованих систем. Підкреслено, що розвиток діпфейк-технологій демонструє дуалізм ШІ як інструмента вчинення і водночас виявлення злочинів. Зазначено, що впровадження сучасних методів цифрової експертизи, міжнародна співпраця, правове регулювання та розвиток цифрової грамотності є ключовими умовами ефективної протидії злочинності у цифрову епоху. Зроблено висновок, що формування нової криміналістичної парадигми – **«криміналістики діпфейків»,** є невід'ємною складовою забезпечення справедливості, інформаційної безпеки та захисту прав людини.*

Ключові слова: *штучний інтелект; діпфейк; цифрові докази; аудіовізуальна атрибуція; ланцюг збереження доказів; цифрова експертиза; генеративно-змагальні мережі (GAN); кіберзлочинність; машинне навчання; етичні та правові ризики; фальсифікація даних; судова експертиза; інформаційна безпека.*

L.P. Grynko Forensic Analysis of Deepfakes: Anomalies Detection, Audiovisual Attribution, and Chain of Evidence Preservation

The article examines the forensic aspects of the detection, fixation, and examination of deepfake content created using artificial intelligence technologies, as well as their impact on current evidence practice in criminal proceedings. It is noted that deepfakes – synthetic audio or video materials created by Generative Adversarial Networks (GANs) – are becoming a tool for a new wave of internet fraud, information manipulation, and privacy violations. Based on the analysis of modern scientific sources and international standards, the main forensic challenges associated with the use of AI in criminal activities are outlined: a high level of latency, difficulties in determining the authenticity of digital evidence, and the risks of falsification of personal data during financial transactions and verification procedures.

The main directions of the forensic analysis of deepfake content are considered: examination of digital artifacts and metadata, verification of frame rate and time anomalies, visual analysis of synthetic video features (lighting, shadows, color scheme, facial expressions), audio analysis of sound and video synchronization, as well as the application of machine learning algorithms to detect hidden patterns. Emphasis is placed on the need to comply with the chain of custody of digital evidence and ensure its admissibility in court.

Particular attention is paid to the ethical and legal aspects of using artificial intelligence in forensics, including the issues of algorithmic bias, personal data confidentiality, and control over the reliability of automated systems. It is emphasized that the development of deepfake technologies demonstrates the dualism of AI as a tool for committing and, simultaneously, detecting crimes. It is noted that the implementation of modern methods of digital expertise, international cooperation, legal regulation, and the development of digital literacy are key conditions for effectively countering crime in the digital age. It is concluded that the formation of a new forensic paradigm – the "forensics of deepfakes" – is an integral part of ensuring justice, information security, and the protection of human rights.

Keywords: *artificial intelligence; deepfake; digital evidence; audiovisual attribution; chain of custody of evidence; digital expertise; Generative Adversarial Networks (GAN); cybercrime; machine learning; ethical and legal risks; data falsification; forensic examination; information security.*

Постановка проблеми. За даними Sensity AI, кількість діпфейк-відео в інтернеті зростає щороку, що свідчить про безпрецедентне поширення технологій маніпуляції аудіо- та відеоконтентом у цифровому середовищі [1]. Водночас, за оцінками компанії McAfee, лише у 2023 році глобальні втрати від шахрайства, пов'язаного із застосуванням штучного інтелекту, перевищили 10 мільярдів доларів і більшість таких злочинів були здійснені за допомогою імітації голосу чи зображення людини [2]. Ці дані вказують на масштабну кризу довіри до цифрової інформації, адже дедалі важче відрізнити реальні матеріали від підроблених, що створює сприятливе середовище для кіберзлочинців. Використання діпфейків у шахрайських схемах, шантажі, маніпулюванні громадською думкою або навіть у судових процесах становить не лише технологічну, а й правову загрозу. У таких умовах криміналістика стикається з потребою розроблення нових методів виявлення, фіксації та аналізу цифрових підробок, здатних забезпечити достовірність і допустимість доказів. Водночас ситуацію ускладнює відсутність у чинному кримінально-процесуальному законодавстві України належного рівня нормативного регулювання електронних доказів, зокрема їх класифікації, механізмів перевірки автентичності та процесуальної оцінки. Ігнорування цих аспектів призводить до правової невизначеності, знижує ефективність досудового розслідування та створює ризики порушення прав учасників процесу. Тому, нагальною постає потреба у модернізації криміналістичної теорії та практики, розробка та впровадження методик розслідування інтернет-шахрайств, вчинених з використанням діпфейків.

Аналіз останніх досліджень і публікацій. Проблематика використання технологій штучного інтелекту у злочинній діяльності, зокрема у сфері інтернет-шахрайств та створення діпфейків активно досліджується як вітчизняними, так і зарубіжними науковцями. І. Чайка аналізує сучасний стан наукової розробки питань запобігання шахрайству в Україні, акцентуючи на необхідності оновлення

кримінально-правових підходів [3]; З. Демидов і О. Колмик визначають фішинг як окрему форму шахрайства в онлайн-середовищі [4]. Зарубіжні автори, зокрема C. Roux, S. Willis, C. Weyermann та R. Stoykova, досліджують вплив цифрових технологій на судову експертизу, підкреслюючи ризики для справедливості й презумпції невинуватості [5; 6]. Питання ідентифікації та виявлення deepfake-контенту розглядаються у працях A. Ismail, S. ST, A. Raza, які пропонують моделі глибинного навчання для автоматизованої детекції фальсифікацій [7; 8; 9; 10]. Українські дослідники В. Теремецький, О. Ковальчук, Ю. Бурило, С. Бандурка, С. Албул та Ю. Рябченко розглядають штучний інтелект як чинник цифрової трансформації системи правосуддя [11; 12]. К. Юртаєва, О. Подобний, В. Слатвінська та О. Макарова висвітлюють кримінологічні, правові й практичні аспекти використання діпфейків, наголошуючи на необхідності комплексної протидії цим явищам у контексті цифрової трансформації суспільства [13; 14; 15].

Мета статті полягає у комплексному аналізі стану розвитку криміналістичних технологій, що використовуються при розслідуванні інтернет-шахрайств з використанням діпфейків.

Виклад основного матеріалу. Шахрайство є одним із найпоширеніших кримінальних правопорушень проти власності як в Україні, так і в інших країнах, що завдає значних фінансових збитків та може сягати десятків і навіть сотень тисяч гривень. З огляду на зростання кількості таких злочинів, боротьба з шахрайством залишається пріоритетним напрямом діяльності правоохоронних органів, адже воно становить загрозу не лише для майнових прав громадян, а й для стабільності економічної системи держави [3].

Масова цифровізація, спричинена стрімким поширенням Інтернету, створила нове сприятливе середовище для реалізації шахраями своїх протиправних дій. Відсутність безпосереднього контакту з потерпілими спонукає зловмисників до створення нових схем заволодіння чужим майном, коштами чи іншими цінностями. Основними рисами інтернет-шахрайства є високий рівень латентності, різноманіття способів вчинення (через широкий спектр онлайн-послуг), глобальний характер злочинів та складність їх виявлення й попередження. Найпоширенішими є фішингові атаки, створення підроблених онлайн-платформ, маніпуляції з електронними платежами, шахрайські інвестиційні схеми, а також використання діпфейків та інших ШІ-технологій для введення потерпілих в оману [4, с. 449].

Сучасні технології штучного інтелекту (ШІ) відкрили нові можливості не лише для інноваційного розвитку суспільства, а й для злочинної діяльності у сфері інтернет-шахрайств. Застосування генеративних моделей, нейромереж та алгоритмів машинного навчання дозволяє створювати надзвичайно реалістичні візуальні та аудіо- матеріали, автоматизувати процеси соціальної інженерії й розробляти високоефективні інструменти для введення користувачів в оману.

Одним із найнебезпечніших напрямів ШІ-злочинності є використання технологій deepfake, що базуються на генеративно-змагальних мережах (GAN). За їх допомогою створюються відео- та аудіозаписи, у яких відомі особи нібито рекламують інвестиційні проекти, фінансові платформи чи «вигідні» токен-роздачі. Такі матеріали мають високий рівень правдоподібності, що сприяє маніпуляції довірою користувачів. Крім того, діпфейки дедалі частіше застосовуються для проходження процедур верифікації особи (KYC) на криптовалютних біржах або фінансових сервісах, що створює передумови для відмивання коштів та вчинення масштабних фінансових махінацій.

Іншим поширеним різновидом є фішинг із використанням ШІ, який набув персоналізованого характеру. Завдяки алгоритмам обробки великих даних злочинці створюють тисячі індивідуалізованих повідомлень електронною поштою, у месенджерах або через чат-ботів, імітуючи природне людське спілкування. Такі повідомлення враховують інтереси, поведінкові особливості та історію онлайн-активності потенційної жертви, що істотно підвищує ефективність шахрайських дій.

Значного поширення набули також фейкові криптоплатформи, створені за допомогою ШІ-технологій. Такі вебресурси або мобільні застосунки імітують легальні торговельні майданчики: мають професійний

дизайн, підроблені аналітичні панелі, «позитивні» відгуки та симульовану активність користувачів. Проте їхня єдина мета – викрадення персональних даних і коштів вкладників.

Штучний інтелект активно застосовується і для маніпуляцій на ринку криптовалют. Зокрема, за допомогою ботів програмуються масові транзакції, що створюють штучний ажіотаж навколо певних токенів. Така схема, відома як pump-and-dump, полягає у штучному підвищенні курсу активу з подальшим його різким продажем, що призводить до обвалу ціни та значних збитків для інших інвесторів.

Окрему загрозу становить соціальна інженерія, підсилена технологіями клонування голосу. Алгоритми ШІ здатні аналізувати відкриту інформацію з соціальних мереж і формувати детальні психологічні профілі користувачів. На цій основі злочинці створюють індивідуальні сценарії обману: здійснюють дзвінки, у яких зімітовано голос працівників банку чи фінансової установи, переконливо просячи розкрити конфіденційні дані або здійснити переказ коштів.

Отже, технології штучного інтелекту суттєво змінили характер і масштаби інтернет-шахрайства. Вони забезпечують злочинцям анонімність, автоматизацію процесів та високий рівень правдоподібності фальсифікованого контенту, що ускладнює виявлення і розслідування таких злочинів. Це вимагає переосмислення традиційних криміналістичних підходів та впровадження нових методів цифрової експертизи, спрямованих на ідентифікацію й нейтралізацію загроз, пов'язаних із використанням ШІ у шахрайських схемах [16].

Окрему небезпеку становить генеративний ШІ у створенні діпфейків — відео чи аудіо з імітацією голосів і зовнішності відомих осіб. Такі підробки можуть використовуватися для шахрайства чи маніпуляцій у судових процесах. З цією метою вже розроблено спеціалізовані засоби автентифікації, зокрема FakeCatcher від Intel, який у реальному часі відрізняє справжнє відео від синтетичного з високою точністю. Таким чином, упровадження штучного інтелекту в криміналістику потребує поєднання технічного прогресу з етичними й правовими гарантіями, щоб використання інтелектуальних систем підсилювало, а не спотворювало процес доказування у кримінальному судочинстві [17].

Програми FakeApp і DeepFaceLab істотно знизили поріг входу для виготовлення підроблених відеоматеріалів, унаслідок чого відповідні посягання поширилися з інформаційного простору публічних осіб на масові атаки проти пересічних громадян, створюючи підвищені ризики дезінформації, викрадення ідентифікаційних даних та порушення приватності. У відповідь на такі виклики сформовано еталонні масиви даних для потреб судово-цифрової експертизи, зокрема FaceForensics++, що акумулює 1 000 автентичних та 5 000 штучно модифікованих відео й використовується для тестування та валідації алгоритмів виявлення підробок [7].

Сьогодні штучний інтелект (ШІ) уже став невід'ємним елементом судових наук, що потребує глибшого усвідомлення його впливу на процес доказування та криміналістичну практику. Технології ШІ офіційно включено до Європейського бачення розвитку судової науки до 2030 року (European Forensic Science Area 2030), однак, з огляду на стрімку цифровізацію, їхнє впровадження набуває актуальності вже зараз.

Сучасна цифрова криміналістика забезпечує ефективне розслідування завдяки спеціальним методам виявлення та дослідження цифрових доказів, розширюючи можливості класичних галузей судової експертизи [5]. Проте технічні інструменти є лише частиною системи: цифрові сліди часто розподілені між різними платформами, пристроями чи хмарними сервісами, можуть бути зашифрованими, фрагментованими або дублюватися з різними часовими мітками, що ускладнює процес їх виявлення та оцінки. Тому з огляду на постійне оновлення цифрових технологій, правоохоронним органам необхідно своєчасно адаптувати методики розслідування. Обсяг і різноманітність цифрових доказів у кримінальних провадженнях стрімко зростають, а сама цифрова криміналістика стає ключовим інструментом протидії кіберзлочинності. Водночас активне використання персональних даних породжує етичні та правові дилеми, пов'язані з приватністю, захистом даних і дотриманням прав людини. Важливо

гарантувати, що такі системи є безпечними, достовірними та захищеними від втручання. Окремої уваги потребує проблема упередженості (bias), адже моделі ШІ часто відтворюють соціальні диспропорції, закладені у навчальні бази даних, що може впливати на об'єктивність результатів. Тому необхідні постійна валідація, аудит і моніторинг алгоритмів із урахуванням демографічних особливостей об'єктів розслідування.

У процесі криміналістичного аналізу цифрові сліди – відбитки пальців, ДНК, аудіо- чи відеофрагменти перетворюються на вектори даних, які обробляються алгоритмами класифікації для ідентифікації особи або події. У межах прогнозувального ШІ (Predictive AI) система навчається за допомогою маркованих даних, тоді як генеративний ШІ (Generative AI) виконує зворотну функцію – створює новий контент (зображення, текст, відео, код) на основі наявних шаблонів. Саме такі технології використовуються у великомовних моделях (LLM), зокрема ChatGPT, що дедалі частіше застосовуються не лише у наукових, а й у злочинних цілях. Зокрема, розроблений хакерами WormGPT призначений для створення шкідливого програмного забезпечення, що піднімає питання надійності та контрольованості ШІ-систем. Очікується, що подальший розвиток приведе до появи ШІ-асистентів і мультимодальних моделей, які поєднуватимуть мовні, візуальні та біометричні дані у криміналістичних дослідженнях.

У сучасних умовах ключовим завданням криміналістики є поширення знань про цифрові докази, вдосконалення методів їх виявлення, фіксації та дослідження, а також забезпечення прозорості експертних висновків. Це сприятиме підвищенню довіри суспільства, зміцненню міжнародного співробітництва та формуванню нової культури цифрового розслідування.

Стрімка еволюція технологій діпфейків підвищує етичні та безпекові ризики, а відтак обумовлює потребу у створенні надійних інструментів цифрової криміналістики, здатних гарантувати достовірність медіаконтенту та запобігати маніпуляціям. Ядром таких посягань є використання глибоких нейронних мереж (DNN) і генеративно-змагальних мереж (GAN), причому глибинне навчання застосовується як для механізму вчинення (створення підробок), так і для механізму виявлення (ідентифікації протиправних модифікацій). Переважаючі підходи спрямовані на криміналістичне розрізнення автентичних і фальсифікованих зображень, текстів, відео та результатів розпізнавання обличчя, із покладанням на формалізовані ознаки та їхні просторово-часові кореляції.

Комплексне застосування алгоритмів глибинного навчання забезпечило суттєвий поступ у детекції. Так, на прикладі набору даних fisher-face продемонстровано доцільність використання Deep Belief Networks (DBN) та Local Binary Pattern Histogram (FF-LPBH) для відмежування оригінальних і змінених ознак [18]. Паралельно CRNN у поєднанні з YOLO дозволяє фіксувати просторово-часові патерни відеоряду, релевантні для виявлення діпфейків [19]. З урахуванням криміналістичної характеристики наслідків, поширення підробленого контенту спричиняє шкоду репутаційним благам, приватності та інформаційній безпеці суспільства.

З огляду на масштаб даних, методики виявлення адаптовано до великих вибірок: застосування FCC-GAN, RCNN і PGGAN до DFDC для наближеного до реального часу виявлення підкреслило потребу в підвищенні точності шляхом модернізації моделей [8]. Поруч із автоматизованими підходами у практиці доведення зберігається значення й ручних прийомів ідентифікації; при цьому емоційні та поведінкові нюанси відеоряду створюють окремі прикладні труднощі для експертного аналізу.

У сегменті виявлення аномалій низка досліджень класифікує відхилення за просторово-часовими критеріями, що додатково ілюструє складність відмежування підробок від автентичного контенту. Інтеграція блокчейн-та хмарних технологій із DL-архітектурами (зокрема VGG16, CNN) розглядається як шлях до підвищення надійності систем засвідчення походження та цілісності мультимедіа [9].

Також еволюціонують засоби протидії аудіо-діпфейкам: перетворення мовних сигналів у спектральні ознаки та їх класифікація ML/DL-моделями демонструють високу точність, що важливо для доказування у справах про шахрайство, пов'язане з телефонними дзвінками та віддаленою аутентифікацією. Ефективність

ансамблевих підходів, які поєднують кілька глибинних моделей для підвищення стійкості до різних способів маніпулювання, підтверджена інтегрованими стратегіями [10].

Для цілей досудового розслідування ключовим є формування належної доказової бази шляхом фіксації просторових і темпоральних артефактів, подальшого здійснення їх кореляційного аналізу та обов'язкової експертної верифікації. Водночас необхідно враховувати фізіологічні обмеження окремих індикаторів (наприклад, частота моргання), які можуть варіюватися залежно від стану здоров'я та спричиняти хибні спрацьовування чи пропуски, а отже потребують підтвердження комплексом незалежних ознак та методів дослідження.

До основних методів криміналістичного аналізу deepfake-контенту належать кілька ключових напрямів. По-перше, аналіз цифрових артефактів – дослідження метаданих, ознак редагування, особливостей стиснення та інших технічних параметрів, що можуть свідчити про втручання у файл. По-друге, перевірка частоти кадрів і часових аномалій, тобто виявлення різких змін темпу, відсутності кадрів або неузгодженостей у відеоряді, які часто виникають під час монтажу. По-третє, візуальний аналіз – оцінка освітлення, тіней, кольорової гами, відображень, асиметрії обличчя та нетипових мімічних рухів, що свідчать про штучне відтворення обличчя. Як зазначає О. Макарова, ідентифікація змін у динаміці міміки є складним завданням, яке потребує поєднання технічних інструментів із розумінням психологічних особливостей людини [13]. Важливою складовою є також аудіо аналіз, який дозволяє виявляти не синхронність між звуком і відео, штучні паузи, обриви чи ознаки синтетичного голосу. Останнім етапом є застосування алгоритмів машинного навчання, навчених на великих наборах справжніх і підроблених відео, що здатні виявляти малопомітні закономірності та аномалії, невидимі людському оку [14]. Ефективність експертизи забезпечує комплексний підхід, який поєднує технічний аналіз із розумінням людської поведінки. Поєднання технологічних та гуманітарних методів підвищує об'єктивність і достовірність висновків експерта. Процес дослідження deepfake-контенту має відповідати загальним принципам судової експертизи – допустимості, достовірності та обґрунтованості [15]. Експертиза може бути призначена слідчим, прокурором або судом у справах, де deepfake є речовим доказом. Критично важливим є дотримання ланцюга збереження цифрових доказів, адже порушення процедури збору або зберігання може зробити результати експертизи недопустимими у суді.

Отже, криміналістична експертиза deepfake-контенту виступає ключовим інструментом протидії кіберзлочинності та інформаційним маніпуляціям. Її ефективність залежить від постійного вдосконалення технічних методів, міжнародної співпраці, розвитку законодавства й підвищення рівня цифрової грамотності населення. Забезпечення справедливості, захист прав людини та інформаційна безпека держави безпосередньо пов'язані з успішним розвитком криміналістичної експертизи deepfake-технологій.

Майбутнє судової експертизи у цифрову епоху вже настало – воно поєднує нові можливості з новими викликами для системи кримінальної юстиції. Сучасна криміналістична наука потребує переосмислення своїх засад, щоб уникнути хибних інтерпретацій і відповідати темпам технологічного розвитку суспільства. Важливі орієнтири для цього визначено у Сіднейській декларації, де підкреслено, що будь-яка діяльність і присутність залишають сліди – носії інформації, які стають об'єктом криміналістичного дослідження. До таких слідів належать і цифрові, які можна виявляти, вилучати, аналізувати та інтерпретувати як інформаційні вектори [20].

Для ефективного реагування на виклики цифровізації необхідно реформувати систему судово-експертного забезпечення, впроваджуючи сучасні методики цифрового аналізу, вдосконалюючи управління, ризик-менеджмент і міжвідомчу взаємодію [6]. Узгодження цифрової криміналістики з методами оцінки доказів сприяє підвищенню повноти та достовірності розслідування, що є основою для формування якісної доказової бази у кримінальному процесі. Зокрема, стандарт ISO/IEC 21043 визначає оцінку доказів як невід'ємний елемент процесу цифрової криміналістики.

Висновок. Результати дослідження свідчать, що стрімкий розвиток штучного інтелекту суттєво змінив характер і масштаби інтернет-шахрайств, ускладнивши їх виявлення та доведення у судовому процесі. Технології deepfake, засновані на генеративно-змагальних мережах, створюють реалістичні відео- та аудіоматеріали, що здатні вводити в оману навіть досвідчених користувачів, тому боротьба з ними вимагає нових криміналістичних підходів. Ефективне розслідування таких злочинів потребує поєднання технічних методів аналізу цифрових артефактів, темпоральних і візуальних аномалій із психологічними знаннями про поведінкові реакції людини. Важливу роль відіграють алгоритми машинного навчання, здатні виявляти невидимі для людського ока закономірності та забезпечувати об'єктивну ідентифікацію фальсифікацій. Водночас дотримання принципів ланцюга збереження цифрових доказів та вимог допустимості є ключовими для визнання результатів експертизи у суді. Впровадження міжнародних стандартів, зокрема ISO/IEC 21043, сприяє уніфікації процедур оцінки цифрових доказів і підвищенню достовірності судових висновків. Подальший розвиток цифрової криміналістики має ґрунтуватися на міжвідомчій співпраці, удосконаленні анти-deepfake технологій, регулярному моніторингу упередженостей штучного інтелекту та етичних ризиків. У сукупності ці чинники формують основу для побудови надійної системи протидії AI-зумовленим шахрайствам, забезпечення справедливого судового розгляду й ефективного захисту прав людини в умовах цифрової епохи.

Список використаних джерел:

1. Reports - Sensity AI. *Sensity*. URL: https://sensity.ai/reports/.
2. As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public. *Federal Trade Commission*. URL: https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public.
3. Чайка І. Стан наукового розроблення проблем запобігання шахрайству в кримінологічній та кримінально-правовій науці України. URL: http://pravoisuspilstvo.org.ua/ archive/2022/1_2022/30.pdf.
4. Демидов З.Г., Колмик О.О. Фішинг-як шахрайство у мережі. *Study of modern problems of civilization*. 2020. С. 448-450.
5. Roux C., Willis S., Weyermann C. Shifting forensic science focus from means to purpose: A path forward for the discipline?. *Science & Justice*. 2021. Vol. 61, no. 6. P. 678–686. URL: https://doi.org/10.1016/j.scijus.2021.08.005.
6. Stoykova R. Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*. 2021. Vol. 42. P. 105575. URL: https://doi.org/10.1016/j.clsr.2021.105575.
7. Korshunov P., Marcel S. DeepFakes: a New Threat to Face Recognition? Assessment and Detection. *arXiv.org*. URL: https://arxiv.org/abs/1812.08685.
8. Chauhan S., Jain N., Pandey S., Chabaque A. Deepfake Detection in Videos and Picture: Analysis of Deep Learning Models and Dataset. *IEEE Xplore*. URL: https://ieeexplore.ieee.org/abstract/document/9915885.
9. Raza A., Munir K., Almutairi M. A Novel Deep Learning Approach for Deepfake Image Detection. *Applied Sciences*. 2022. Vol. 12, no. 19. P. 9820. URL: https://doi.org/10.3390/app12199820.
10. Rana S., Sung A. DeepfakeStack: A Deep Ensemble-based Learning Technique for Deepfake Detection. *IEEE Xplore*.URL: https://ieeexplore.ieee.org/abstract/document/9171002.
11. Teremetskyi, V. I., & Kovalchuk, O. Ya. Artificial Intelligence as a Factor in the Digital Transformation of the Justice System [Штучний інтелект як чинник цифрової трансформації системи правосуддя]. *Forum Prava*. 2024. 78(1). 106–115. http://doi.org/10.5281/zenodo.10870779. URL: http://forumprava.pp.ua/files/106-115-2024-1-FP-Teremetskyi,Kovalchuk_13.pdf.
12. Teremetskyi, V., Burylo, Y., Bandurka, S., Albul, S., & Riabchenko, Y. Application of artificial intelligence as a way of digitalizing the system of justice: legal, economic and social issues [Застосування

штучного інтелекту як спосіб цифровізації системи правосуддя: правові, економічні та соціальні питання]. *Via Inveniendi Et Iudicandi*. 2025. 20(1). 172-186. https://doi.org/10.15332/19090528.11118.

13. Макарова О.П. Використання цифрових технологій в діяльності поліції для боротьби зі злочинністю. *Правова наука і державотворення в Україні в контексті правової інтеграції*: матеріали XIII Міжнародної науково-практичної конференції Сумська філія Харківського національного університету внутрішніх справ. Суми: Видавничий дім «Ельдорадо», 2021. С. 173-176.

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

15. Подобний О.О., Слатвінська В.М. Діпфейк в контексті декларації про майбутнє інтернету. *Юридичний науковий електронний журнал.* № 5. 2022. С. 594-596. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/ 6555a817-3832-492e-b340-b832c1d2dbef/content.

16. Шахрайство в епоху штучного інтелекту: виклики, ризики та шляхи протидії. *Juscutum*. URL: https://www.juscutum.com/news/shahraystvo-v-epohu-shtuchnogo-intelektu-vikliki-riziki-ta-shlyahi-protidiyi.

17. Klasén L., Fock N., Forchheimer R. The Invisible Evidence: Digital Forensics as Key to Solving Crimes in the Digital Age. *Forensic Science International*. 2024. P. 112133. URL: https://doi.org/10.1016/j.forsciint.2024.112133.

18. Suganthi S., Ayoobkhan M., Kumar V., Nebojsa B., Venkatachalam K., Hubálovský Š., Trojovský P. Deep learning model for deep fake face recognition and detection. *PeerJ Computer Science*. 2022. Vol. 8. P. e881. URL: https://doi.org/10.7717/peerj-cs.881.

19. Ismail A., Elpeltagy M., Zaki M., ElDahshan K. Deepfake video detection: YOLO-Face convolution recurrent approach. *PeerJ Computer Science*. 2021. Vol. 7. P. e730. URL: https://doi.org/10.7717/peerj-cs.730.

20. Reedy P. Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy*. 2023. Vol. 6. P. 100313. URL: https://doi.org/10.1016/j.fsisyn.2022.100313.

References:

1. Reports - Sensity AI. Sensity. URL: https://sensity.ai/reports/.

2. As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public. *Federal Trade Commission*. URL: https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public.

3. Chaika I. Stan naukovoho rozroblennia problem zapobihannia shakhraistvu v kryminolohichnii ta kryminalno-pravovii nautsi Ukrainy. URL: http://pravoisuspilstvo.org.ua/ archive/2022/1_2022/30.pdf.

4. Demydov Z.H., Kolmyk O.O. Fishynh-iak shakhraistvo u merezhi. *Study of modern problems of civilization*. 2020. S. 448-450.

5. Roux C., Willis S., Weyermann C. Shifting forensic science focus from means to purpose: A path forward for the discipline?. *Science & Justice*. 2021. Vol. 61, no. 6. P. 678–686. URL: https://doi.org/10.1016/j.scijus.2021.08.005.

6. Stoykova R. Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*. 2021. Vol. 42. P. 105575. URL: https://doi.org/10.1016/j.clsr.2021.105575.

7. Korshunov P., Marcel S. DeepFakes: a New Threat to Face Recognition? Assessment and Detection. arXiv.org. URL: https://arxiv.org/abs/1812.08685.

8. Chauhan S., Jain N., Pandey S., Chabaque A. Deepfake Detection in Videos and Picture: Analysis of Deep Learning Models and Dataset. *IEEE Xplore*. URL: https://ieeexplore.ieee.org/abstract/document/9915885.

9. Raza A., Munir K., Almutairi M. A Novel Deep Learning Approach for Deepfake Image Detection. *Applied Sciences*. 2022. Vol. 12, no. 19. P. 9820. URL: https://doi.org/10.3390/app12199820.

10. Rana S., Sung A. DeepfakeStack: A Deep Ensemble-based Learning Technique for Deepfake Detection. IEEE Xplore. URL: https://ieeexplore.ieee.org/abstract/document/9171002.

11. Teremetskyi, V. I., & Kovalchuk, O. Ya. Artificial Intelligence as a Factor in the Digital Transformation of the Justice System [Shtuchnyi intelekt yak chynnyk tsyfrovoi transformatsii systemy pravosuddia].

Forum Prava. 2024. 78(1). 106–115. http://doi.org/10.5281/zenodo.10870779. URL: http://forumprava.pp.ua/files/106-115-2024-1-FP-Teremetskyi,Kovalchuk_13.pdf.

12. Teremetskyi, V., Burylo, Y., Bandurka, S., Albul, S., & Riabchenko, Y. Application of artificial intelligence as a way of digitalizing the system of justice: legal, economic and social issues [Zastosuvannia shtuchnoho intelektu yak sposib tsyfrovizatsii systemy pravosuddia: pravovi, ekonomichni ta sotsialni pytannia]. *Via Inveniendi Et Iudicandi*. 2025. 20(1). 172-186. https://doi.org/10.15332/19090528.11118.

13. Makarova O.P. Vykorystannia tsyfrovykh tekhnolohii v diialnosti politsii dlia borotby zi zlochynnistiu. *Pravova nauka i derzhavotvorennia v Ukraini v konteksti pravovoi intehratsii*: materialy XIII Mizhnarodnoi naukovo-praktychnoi konferentsii Sumska filiia Kharkivskoho natsionalnoho universytetu vnutrishnikh sprav. Sumy: Vydavnychyi dim "Eldorado", 2021. S. 173-176.

14. Yurtaieva K.V. Kryminolohichnyi analiz vykorystannia tekhnolohii Deepfake: koly feik staie zlochynom. *Visnyk kryminolohichnoi asotsiatsii Ukrainy*. 2021. № 1(24). S. 31-42.

15. Podobnyi O.O., Slatvinska V.M. Dipfeik v konteksti deklaratsii pro maibutnie internetu. *Yurydychnyi naukovyi elektronnyi zhurnal*. № 5. 2022. S. 594-596. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/ 6555a817-3832-492e-b340-b832c1d2dbef/content.

16. Shakhraistvo v epokhu shtuchnoho intelektu: vyklyky, ryzyky ta shliakhy protydii. *Juscutum*. URL: https://www.juscutum.com/news/shahraystvo-v-epohu-shtuchnogo-intelektu-vikliki-riziki-ta-shlyahi-protidiyi.

17. Klasén L., Fock N., Forchheimer R. The Invisible Evidence: Digital Forensics as Key to Solving Crimes in the Digital Age. *Forensic Science International*. 2024. P. 112133. URL: https://doi.org/10.1016/j.forsciint.2024.112133.

18. Suganthi S., Ayoobkhan M., Kumar V., Nebojsa B., Venkatachalam K., Hubálovský Š., Trojovský P. Deep learning model for deep fake face recognition and detection. *PeerJ Computer Science*. 2022. Vol. 8. P. e881. URL: https://doi.org/10.7717/peerj-cs.881.

19. Ismail A., Elpeltagy M., Zaki M., ElDahshan K. Deepfake video detection: YOLO-Face convolution recurrent approach. *PeerJ Computer Science*. 2021. Vol. 7. P. e730. URL: https://doi.org/10.7717/peerj-cs.730.

20. Reedy P. Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy*. 2023. Vol. 6. P. 100313. URL: https://doi.org/10.1016/j.fsisyn.2022.100313.