DOI https://doi.org/10.30525/978-9934-26-686-7-9

КРИМІНАЛІСТИЧНІ ЗАСОБИ ОТРИМАННЯ ЗНАЧУЩОЇ ІНФОРМАЦІЇ ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У ЦИФРОВУ ЕПОХУ

Курман О. В.

ВСТУП

У сучасних умовах практично не існує сфер суспільного життя, у яких не застосовувалися б електронні засоби комунікації. Будь-яка діяльність, спрямована на збереження ефективності та конкурентоспроможності, об'єктивно потребує активного використання сучасних технічних комунікаторів, що забезпечують майже миттєве отримання, оброблення та передавання значних обсягів інформації.

Сфери державного управління, охорони здоров'я, науки, оборони, правоохоронної діяльності, виробництва та зв'язку зазнали глибокої цифрової трансформації, результатом якої стало широке впровадження електронного документообігу, цифрових методів обробки, зберігання й використання інформації. В Україні реєстри та бази даних органів державної влади й управління вже переведені або перебувають у процесі переведення на електронні носії з розміщенням інформації у локальних мережах або з доступом до неї через глобальну мережу Інтернет. Паралельно з цим стрімко зростає рівень цифрової активності населення: сотні мільйонів користувачів у різних країнах світу мають власні вебресурси або персональні сторінки в соціальних мережах, що формує новий інформаційний простір і нові соціальні зв'язки.

У нашій країні запущено онлайн-сервіс державних послуг «Дія» і проєкти електронної державної реєстрації речових прав на нерухоме майно та їхніх обтяжень; для юридичних і фізичних осіб (підприємців і громадських формувань) – е-Бізнес; для актів цивільного стану – е-ДРАЦС; для цифрової трансформації вищої, фахової передвищої і професійної (професійно-технічної) освіти – е-Університет; для системи управління запасами лікарських засобів і медичних виробів – створення/модернізація Державного реєстру лікарських засобів і Державного реєстру медичних виробів, розвиток застосування електронних рецептів.

Загальновідоме прислів'я про те, що хто володіє інформацією, той володіє світом, характеризує роль інформації у сучасному суспільстві. На нинішньому етапі розвитку суспільства масштаби злочинних посягань на конфіденційні відомості різко зросли. Інформація про результати чужих прикладних і фундаментальних досліджень дає змогу заощадити власні сили й кошти та зосередити увагу на виробництві й маркетингу. Подальший розвиток науково-технічного прогресу, збільшення потоку патентів і жорсткість конкуренції роблять викрадення чужих таємниць особливо прибутковою, а тому дуже

перспективною справою[1]. Все більше видів інформації у сучасному суспільстві зберігається в електронному вигляді. Такі обставини зумовили широке поширення портативних комп'ютерів, смартфонів, планшетів в усіх галузях діяльності людини. Практично всі сучасні електронні пристрої мають постійне чи періодичне підключення до електронних комунікаційних мереж передачі та отримання інформації.

Така зручність у збиранні, обробці та використанні інформації створює велику спокусу незаконного отримання конфіденційних відомостей про конкретну особу, об'єднання громадян, підприємства, установи з метою використання у подальшому в протиправних цілях[2].

Сьогодні з'являються нові, раніше невідомі способи вчинення злочинів у сфері використання електронно-обчислюваних машин, систем та комп'ютерних мереж і мереж електрозв'язку, де предметом посягання виступає різного роду інформація, що зумовлює необхідність розроблення ефективних методик виявлення й розслідування цих злочинних деліктів.

1. Штучний інтелект у дослідженні цифрових слідів: інноваційні перспективи та проблеми використання

Популярність мережі Інтернет та її суцільне проникнення у повсякденне життя суспільства зумовили формування принципово нового інформаційного середовища. У цьому середовищі практично будь-яка діяльність людини – від перегляду вебсторінок до активної взаємодії в соціальних мережах – супроводжується створенням і накопиченням цифрових слідів. Такі сліди містять інформацію, яка може бути повністю відкритою для необмеженого кола осіб, так і частково або повністю закритою у доступі.

Значну та перспективну роль на сучасному етапі відіграють методики, спрямовані на аналіз цифрового сліду користувачів. За їх допомогою спеціалісти можуть реконструювати послідовність дій злочинців навіть у випадках навмисного знищення доказів або використання засобів анонімізації. Застосовуються методи зворотного аналізу, що включають відновлення видаленої інформації, дослідження історії браузера, системних логів і мережевої активності. Це дає змогу встановлювати не лише автора забороненого контенту, а й осіб, причетних до його поширення або співучасті у цифрових злочинах.

На сучасному етапі розвитку криміналістичної науки відбувається переосмислення тактичних підходів до організації та проведення слідчих (розшукових) дій. Використання новітніх досягнень науки й техніки створює

[1] Курман О.В. Типізація способів учинення злочинних посягань на відомості, що становлять комерційну або банківську таємницю. *Теорія та практика судової експертизи і криміналістики*: збірник наукових праць. Вип. 10 / ред. кол.: М.Л. Цимбал, В.Ю. Шепітько, Л.М. Головченко та ін. Харків: Право, 2010. С. 62.

[2] Курман О.В. Способи несанкціонованого втручання в роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Право і суспільство*. 2017. № 4. С. 245. URL: http://pravoisuspilstvo.org.ua/archive/2017/4_2017/part_1/44.pdf

передумови для підвищення результативності роботи органів досудового розслідування та посилення рівня захисту прав і безпеки громадян[3].

З кожним роком зростають потреби правоохоронних органів в ефективних інструментах виявлення, вилучення, дослідження та використання в доказуванні цифрових доказів. У криміналістичній науці останніх десятиліть цифрова криміналістика є одним із найбільш актуальних напрямів розвитку[4]. Сучасна цифрова криміналістика розвивається в умовах стрімкого технологічного прогресу, що зумовлює радикальні зміни в підходах до розслідування правопорушень.

Сучасна злочинна діяльність дедалі частіше характеризується утворенням значних масивів цифрової інформації, зокрема лог-файлів, електронних повідомлень, графічних і відеоматеріалів, метаданих, а також відомостей, що зберігаються на мобільних та інших електронних пристроях. За наявності такого обсягу й різноманіття цифрових слідів використання традиційних аналітичних підходів не забезпечує належної оперативності та результативності й потребує значних ресурсних витрат. У цьому контексті застосування технологій штучного інтелекту для обробки та аналізу цифрових слідів постає як перспективний науково-практичний напрям, здатний суттєво вплинути на організацію досудового розслідування та процес доказування у кримінальному провадженні.

Водночас на сучасному етапі поняття «цифрові сліди» не відзначається єдністю підходів до його визначення та змістовного наповнення. У межах криміналістичної техніки триває наукова дискусія щодо сутності цифрових слідів, їх характерних ознак, а також можливих підстав для класифікації.

Так, І. Колеснікова наводить визначення цифрових слідів через сукупність їх характерних властивостей. Зокрема: 1) цифрові сліди – це інформація, що міститься на матеріальних цифрових пристроях; 2) для аналізу такої інформації необхідні спеціальні криміналістичні знання із застосуванням комп'ютерних технологій; 3) цифрові сліди як інформаційний ресурс містять відомості про вчинені кримінальні правопорушення. До основних властивостей цифрових слідів, за авторкою, належать: відсутність нерозривного зв'язку з матеріальним носієм; динамічність, тобто здатність до просторового переміщення; можливість їх миттєвого знищення, а також здатність створювати ідентичні копії без втрати змісту[5].

---

[3] Курман О. Правові та практичні аспекти використання поліграфа у кримінальному провадженні України. *Сучасний досвід використання поліграфа у сфері національної безпеки і оборони України в умовах воєнних загроз*: зб. матеріалів панел. дискусії: IX Харків. міжнар. юрид. форум, м. Харків, 26 верес. 2025 р. / [редкол.: А. Гетьман, В. Журавель, В. Шевчук та ін.] ; Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. криміналістики; Нац. акад. прав. наук України; Всеукр. асоц. поліграфологів [та ін.]. Харків: Право, 2025. С. 76. URL: https://dspace.nlu.edu.ua/jspui/handle/123456789/20575

[4] Степанюк Р. Л., Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник ЛДУВС ім. Е. О. Дідоренка*. 2022. Вип. 3 (99). С. 283. URL: https://dspace.univd.edu.ua/items/b174d57a-bf4b-47f9-9211-aeb715b61844

[5] Колеснікова І. А. Цифрові сліди: поняття та їх значення при розслідуванні кримінальних правопорушень. *Юридичний науковий електронний журнал*. 2023. № 10. С. 473. URL: http://lsej.org.ua/10_2023/114.pdf

Г. Авдєєва визначає цифрові сліди як матеріальні невидимі сліди, що містять криміналістично значущу інформацію (відомості, дані), зафіксовану в цифровій формі на матеріальних носіях, які можуть бути виявлені, зафіксовані та досліджені із застосуванням відповідних цифрових пристроїв[6].

Є. Демидова подає визначення цифрових слідів через перелік їх ознак, а саме: 1) наявність цифрової форми існування (відсутність традиційної матеріальної форми); 2) виникнення внаслідок взаємодії певного об'єкта з цифровими пристроями, технологіями або інформаційними мережами; 3) локалізація в цифровому просторі (сервері, комп'ютері, смартфоні тощо); 4) можливість їх виявлення та дослідження з використанням відповідного обладнання та/або спеціалізованого програмного забезпечення; 5) здатність до копіювання (виготовлення дублікатів) без втрати якості, у тому числі дистанційно; 6) можливість дистанційного модифікування або знищення[7].

Цифрова трансформація суспільних процесів і способів учинення кримінальних правопорушень супроводжується інтенсивним збільшенням кількості та різновидів цифрових слідів, що об'єктивно вимагає залучення сучасних інтелектуальних технологій, спроможних здійснювати аналіз значних за обсягом і різнорідних інформаційних масивів у стислих часових межах.

У сучасних реаліях в галузі криміналістичної техніки простежується тенденція активних пошуків щодо розроблення та впровадження інноваційних криміналістичних продуктів, спрямованих на оптимізацію розслідування злочинів та судового розгляду. Як зазначається, до таких інноваційних продуктів можна віднести нові розроблені або прилаштовані до потреб слідчої (судової) практики техніко-криміналістичні засоби, сучасні інформаційні технології, електронні бази знань, методи фіксації, аналізу та оцінки доказової інформації та ін[8].

У розв'язанні таких завдань саме ШІ може відіграти ключову роль. Проблематиці використання штучного інтелекту в судовій та правоохоронній діяльності приділяється значна увага з боку науковців-правознавців. Свої наукові праці цій тематиці присвятили такі дослідники, як Бєлова М. В., Бєлов Д. М., Рущак І. В[9]., Карчевський М. В.,

---

[6] Авдєєва Г. Сутність цифрових слідів у криміналістиці. *Актуальні питання судової експертизи та криміналістики*. 2018. С. 91. URL: https://dspace.nlu.edu.ua/bitstream/123456789/15677/1/Avdeeva_90-93.pdf

[7] Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського національного університету. Серія Право*. 2024. Вип. 85, ч. 4. С. 75. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/11/12-3.pdf

[8] Шепітько В. Ю., Журавель В. А., Авдєєва Г. К. Інновації в криміналістиці та їх впровадження в діяльність органів досудового слідства. *Питання боротьби зі злочинністю*: зб. наук. праць. Харків: Право, 2011. Вип. 21. С. 40.

[9] Бєлова М. В., Бєлов Д. М., Рущак І. В. Штучний інтелект у досудовому розслідуванні кримінальних справ: окремі питання міжнародної практики. *Аналітично порівняльне правознавство*. 2025. № 1. С. 818-824. URL: https://doi.org/10.24144/2788-6018.2025.01.136

Куковинець Д. О.[10], Негребецький В. В.[11], Плахотнік О. В[12]., Червеко К. О[13]. та інші. З огляду на стрімку динаміку розвитку штучного інтелекту, його активне впровадження у практику діяльності правоохоронних та експертних органів, а також пов'язані з цим виклики та проблеми, цей напрям наукових криміналістичних досліджень потребує постійного вивчення, оновлення та вдосконалення. В. Шевчук справедливо наголошує на необхідності активізації зусиль щодо застосування штучного інтелекту з метою розв'язання практичних завдань як у сфері правозастосування, так і в боротьбі зі злочинністю в умовах війни[14].

Технології штучного інтелекту можуть використовуватися для здійснення автоматизованого виявлення цифрових слідів у різноманітних інформаційних середовищах, зокрема на мобільних пристроях, персональних комп'ютерах, у хмарних сховищах, соціальних мережах і месенджерах. Застосування інтелектуальних алгоритмів пошуку та фільтрації забезпечує можливість визначення потенційно значущих файлів, електронних повідомлень, графічних матеріалів і журналів подій на підставі аналізу ключових слів, часових характеристик, геолокаційних відомостей та особливостей контексту їх використання. Цифрові сліди переважно характеризуються неструктурованістю та представлені у різних інформаційних форматах, зокрема у вигляді текстових документів, мультимедійних матеріалів і системних журналів. Використання алгоритмів машинного навчання й технологій обробки природної мови дає змогу системам штучного інтелекту здійснювати класифікацію таких даних за визначеними ознаками, встановлювати взаємозв'язки між окремими об'єктами (зокрема IP-адресами, обліковими записами та діями користувачів), а також формувати впорядковані інформаційні структури, придатні для подальшого аналітичного опрацювання.

Використання технологій штучного інтелекту, зокрема алгоритмів часової аналітики, створює можливості для реконструкції послідовності дій певної особи, виявлення нетипових або потенційно протиправних форм активності та відтворення причинно-наслідкового зв'язку між окремими подіями, такими як авторизація в системі, копіювання інформаційних ресурсів і подальші спроби

[10] Карчевський М. В., Куковинець Д. О. Використання технологій штучного інтелекту правоохоронними та судовими органами: світовий досвід та напрями розвитку національного законодавства. *Питання боротьби зі злочинністю*. 2023. Вип. 46. С. 21-31. URL: http://pbz.nlu.edu.ua/issue/view/17882

[11] Негребецький В. В. Використання систем штучного інтелекту у боротьбі зі злочинністю: огляд та перспективи. *Українська поліцеїстика: теорія, законодавство, практика*. 2024. № 1 (9). С. 66-70. URL: DOI: https://doi.org/10.32782/2709-9261-2024-1-9-13

[12] Плахотнік О. В. Практичне застосування штучного інтелекту у кримінальному провадженні. *Вісник кримінального судочинства*. 2019. № 4. С. 45-57. URL: https://vkslaw.com.ua/index.php/journal/article/view/222

[13] Черевко К. О., Луценко І. Г. Штучний інтелект як інструмент протидії злочинності. *Вісник Кримінологічної асоціації України*. 2023. № 1. С. 124-133. URL: DOI: https://vca.univd.edu.ua/index.php/vca/article/view/43

[14] Shevchuk V. M. Development trends in criminalistics in the era of digitalization. *Modern knowledge: research and discoveries: I International Scientific and Practical Conference* (May 19–20, 2023; Vancouver, Canada). 2023. Pp. 198. URL: https://archive.interconf.center/index.php/2709-4685/issue/view/19-20.05.2023/165

приховування цифрових слідів. Зазначений підхід набуває особливої значущості під час розслідування кримінальних правопорушень у сфері інформаційних технологій, витоків конфіденційної інформації, а також фактів несанкціонованого доступу до інформаційних систем.

Використання технологій комп'ютерного зору в системах штучного інтелекту забезпечує можливість автоматизованого розпізнавання облич, реєстраційних номерів транспортних засобів, окремих об'єктів і моделей поведінки на фото- та відеоматеріалах, отриманих у ході досудового розслідування. Застосування таких інструментів сприяє встановленню місцезнаходження особи, аналізу її дій у певний проміжок часу, зіставленню зовнішніх ознак із відомостями з інших інформаційних джерел, а також виявленню ознак можливого втручання в цифрові відеодані, у тому числі шляхом детекції технологій deepfake.

Окрім цього, штучний інтелект може залучатися до аналізу значних обсягів текстової інформації, зокрема електронного листування, повідомлень у месенджерах і матеріалів, оприлюднених у соціальних мережах, з метою виокремлення ключових смислових тем, встановлення можливих намірів та ідентифікації осіб, причетних до злочинної діяльності. Застосування методів семантичного аналізу дає змогу оцінювати емоційне наповнення повідомлень, виявляти використання умовних або кодованих позначень, а також фіксувати приховані комунікативні загрози

Системи штучного інтелекту можуть бути інтегровані з наявними криміналістичними інформаційними ресурсами, зокрема дактилоскопічними та генотипічними обліками, відеоархівами, реєстрами викрадених транспортних засобів, зброї, мобільних пристроїв та іншими спеціалізованими базами даних, з метою здійснення автоматизованого порівняльного аналізу цифрових слідів із вже накопиченою інформацією. Застосування такого підходу забезпечує скорочення строків ідентифікації особи, сприяє встановленню серійності кримінальних правопорушень, а також створює підґрунтя для формування профілю правопорушника.

Під час використання штучного інтелекту у роботі з цифровими слідами виникає низка проблем і викликів, які можуть істотно вплинути на допустимість, достовірність та ефективність застосування таких технологій у кримінальному судочинстві.

Сучасні системи штучного інтелекту, зокрема побудовані на основі методів глибокого навчання, характеризуються високою результативністю та точністю під час оброблення значних масивів цифрових даних. Разом із тим однією з ключових проблем їх використання залишається недостатній рівень пояснень отриманих результатів, що набуває особливої ваги у контексті кримінального провадження. Обмежена прозорість функціонування алгоритмів унеможливлює належне обґрунтування причин, з яких система дійшла певного висновку або сформувала відповідне рішення, що, своєю чергою, ускладнює перевірку достовірності та обґрунтованості таких висновків і безпосередньо впливає на питання допустимості та належності доказів у судовому розгляді. Додатково відсутність чітко визначених критеріїв і процедур контролю створює ризики зловживань, у тому числі шляхом свідомого коригування параметрів алгоритмів з

метою отримання наперед заданого результату, що суперечить принципам змагальності, об'єктивності та справедливості кримінального процесу.

Незважаючи на значні технічні можливості, застосування систем штучного інтелекту супроводжується низкою обмежень, здатних позначатися на точності й надійності аналізу цифрових слідів у межах кримінального провадження. Одним із ключових ризиків є формування хибнопозитивних або хибнонегативних результатів, що може проявлятися, зокрема, у помилковому тлумаченні змісту текстових повідомлень, неточній ідентифікації облич чи інших цифрових об'єктів. Подібні похибки потенційно спотворюють висновки органів досудового розслідування та істотно впливають на подальшу оцінку доказів під час дослідження в суді.

Окремий блок проблем пов'язаний з обмеженою здатністю систем штучного інтелекту адекватно враховувати комунікативний і ситуаційний контекст повідомлень, особливо у випадках використання неструктурованої лексики, професійного сленгу, іронічних або двозначних висловлювань. За таких умов існує ймовірність суттєвого викривлення змісту аналізованої інформації, що, своєю чергою, підвищує ризик формування помилкових або необґрунтованих висновків.

Додатково системи штучного інтелекту характеризуються вразливістю до цілеспрямованого зовнішнього впливу, зокрема шляхом застосування так званих *adversarial examples* – спеціально модифікованих вхідних даних, які за мінімальних і практично непомітних для людини змін можуть призводити до істотних викривлень результатів аналізу. Наявність таких уразливостей ставить під сумнів надійність використання технологій штучного інтелекту під час роботи з цифровими слідами, особливо в умовах змагальності судового процесу.

Аналіз чинного законодавства України засвідчує відсутність комплексного та системного нормативного регулювання ключових питань застосування систем штучного інтелекту у сфері кримінального провадження. Подібна правова невизначеність спостерігається й у суміжних галузях права, що зумовлює міждисциплінарний характер зазначеної проблематики та потребу у виробленні узгоджених підходів до її вирішення.

По-перше, на законодавчому рівні відсутнє визначення правового статусу результатів, отриманих із використанням систем штучного інтелекту. Така обставина формує правову невизначеність щодо можливості визнання відповідної інформації належними, допустимими, достовірними та достатніми доказами у кримінальному провадженні. Неврегульованість критеріїв оцінки фактично унеможливлює повноцінне процесуальне використання відомостей, сформованих або оброблених із застосуванням технологій штучного інтелекту.

По-друге, чинне законодавство не передбачає уніфікованих процедур перевірки (верифікації) цифрових слідів, які були зібрані, ідентифіковані чи проаналізовані за допомогою автоматизованих систем на основі штучного інтелекту. Це істотно ускладнює оцінку їх достовірності та створює ризики використання доказів, що не відповідають вимогам наукової обґрунтованості, відтворюваності й об'єктивності.

По-третє, законодавчо не врегульовано питання розподілу юридичної відповідальності у випадках помилок або технічних збоїв, що виникають під

час використання систем штучного інтелекту у процесі прийняття рішень. У зв'язку з цим залишається відкритим питання щодо суб'єкта відповідальності за наслідки такого використання – розробника програмного забезпечення, оператора системи, експерта, який застосовував інструменти штучного інтелекту, чи слідчого, який покладався на відповідні результати при ухваленні процесуальних рішень. Подібна невизначеність має безпосередній вплив на забезпечення гарантій справедливого судового розгляду, реалізацію прав сторін кримінального провадження та ефективний захист від можливих технічних або процедурних зловживань.

Використання систем штучного інтелекту у кримінальному провадженні за відсутності належного контролю або чітко визначених процесуальних гарантій може призводити до істотних порушень прав учасників кримінального процесу. Насамперед це стосується ризиків, пов'язаних із дотриманням фундаментальних принципів кримінального судочинства та стандартів справедливого правосуддя. У ситуаціях, коли стороні захисту не забезпечено доступ до інформації про архітектуру алгоритму, параметри його навчання чи методи оброблення цифрових слідів, виникає реальна загроза обмеження права на захист, зокрема можливості ефективного оскарження доказів, покладених в основу обвинувачення.

Додатковим джерелом ризиків є застосування алгоритмів, навчання яких здійснювалося на упереджених або нерепрезентативних масивах даних, що може зумовлювати формування дискримінаційних чи стереотипних висновків. Подібні проблеми вже знаходили відображення у міжнародній правозастосовній практиці, зокрема у випадках, коли системи штучного інтелекту демонстрували статистичну схильність до формування обвинувальних результатів стосовно представників окремих етнічних, соціальних або демографічних груп. Так, у ході журналістських розслідувань було задокументовано щонайменше вісім фактів неправомірних арештів у різних штатах США, спричинених хибними результатами алгоритмів розпізнавання облич, причому переважна більшість постраждалих належала до афроамериканської спільноти, що свідчить про наявність системної алгоритмічної упередженості[15].

Оскільки функціонування систем штучного інтелекту ґрунтується на аналізі наявних масивів даних, використання спотворених, фальсифікованих або отриманих із порушенням вимог законодавства цифрових слідів неминуче зумовлює формування хибних або недостовірних висновків. Водночас можливості сучасних систем штучного інтелекту щодо відмежування автентичних цифрових слідів від штучно створених чи модифікованих залишаються обмеженими, особливо у випадках застосування високотехнологічних методів фальсифікації, у тому числі із залученням тих самих алгоритмів штучного інтелекту. За таких умов виникають суттєві ризики для забезпечення точності, достовірності та процесуальної допустимості доказів, отриманих у результаті автоматизованого аналізу цифрової інформації.

[15] MacMillan D. Arrested by AI: Police ignore standards after facial recognition matches. *The Washington Post.* 13 січня 2025. URL: https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/ (дата звернення: 20.01.2026).

Використання технологій штучного інтелекту у криміналістичній діяльності становить перспективний напрям розвитку, який розширює можливості підвищення ефективності розкриття та розслідування кримінальних правопорушень, автоматизації типових аналітичних і технічних процедур, прогнозування злочинної активності, а також опрацювання значних за обсягом масивів інформації. Різні варіації штучного інтелекту, зокрема методи машинного й глибокого навчання, обробки природної мови та комп'ютерного зору, вже активно впроваджуються у низці напрямів криміналістичних досліджень[16].

Системи штучного інтелекту створюють можливості для автоматизації процесів виявлення, систематизації та аналітичного тлумачення цифрових слідів із високим рівнем точності. Вони спроможні встановлювати приховані взаємозв'язки між окремими об'єктами, фіксувати аномальні прояви у поведінці осіб, реконструювати послідовність подій і формувати обґрунтовані доказові гіпотези на основі комплексного аналізу цифрової інформації. Окрім цього, технології штучного інтелекту можуть інтегруватися у процедури судово-експертних досліджень, істотно скорочуючи строки опрацювання та інтерпретації цифрових доказів.

Водночас, попри значний потенціал застосування штучного інтелекту у сфері аналізу цифрових слідів, його впровадження супроводжується низкою істотних ризиків і проблем, що зумовлюють необхідність комплексного нормативно-правового регулювання, формування етичних стандартів використання відповідних технологій, а також підвищення рівня цифрової компетентності всіх учасників кримінального провадження.

Упровадження технологій штучного інтелекту в практичну діяльність супроводжується комплексом суттєвих ризиків і проблем, серед яких особливе місце посідають алгоритмічна упередженість, обмежена прозорість процесів ухвалення рішень, етичні та правові виклики, а також наявні технічні обмеження й рівень готовності правничого середовища до використання таких інструментів. З метою мінімізації зазначених ризиків і підвищення результативності застосування штучного інтелекту в криміналістичній практиці необхідним є формування чітких етичних і правових стандартів, забезпечення прозорості та підзвітності алгоритмічних рішень, а також удосконалення якості й репрезентативності навчальних даних.

Доцільним вбачається поетапне та виважене впровадження систем штучного інтелекту у криміналістичну практику за умови збереження визначальної ролі людини у прийнятті остаточних процесуальних рішень і з урахуванням потенційного впливу відповідних технологій на права людини та принципи справедливого судочинства. За відсутності належного нормативного й інституційного врегулювання необґрунтоване та широкомасштабне використання штучного інтелекту у сфері кримінального судочинства здатне поставити під загрозу фундаментальні засади кримінального процесу, що є апріорі неприпустимим.

[16] Черваньова Д. А., Курман О. В. Застосування штучного інтелекту в криміналістиці: перспективи та ризики. *Аналітично-порівняльне правознавство*. 2025. № 3. Ч.3. С.215. https://app-journal.in.ua/wp-content/uploads/2025/06/33-2.pdf

2. Цифрові сліди мобільних засобів зв'язку у криміналістичній практиці

Розвиток науково-технічного прогресу, використання штучного інтелекту, упровадження сучасних досягнень науки і техніки в практику вчинення кримінальних правопорушень зумовлює необхідність вдосконалення науково-методичного та техніко-криміналістичного забезпечення розслідування злочинів, одним із пріоритетних напрямів якого стає використання спеціальних знань і спеціальної криміналістичної техніки.

Одним із найпоширеніших видів технічних засобів, що використовуються злочинцями під час вчинення правопорушень, є мобільні телефони (смартфони), за допомогою яких узгоджуються та координуються злочинні дії співучасників, висуваються погрози і здійснюється вимагання грошових коштів або майна, підшукують та вербують нових виконавців, визначають дії спільників із підготовки та приховування злочинної діяльності, збирають інформацію щодо майбутніх жертв, фіксують результати своїх дій для звітування, реалізують шахрайські схеми заволодіння чужим майном тощо. Сучасні можливості засобів мобільного зв'язку дають змогу здійснювати дзвінки та обмінюватися повідомленнями за допомогою стільникового зв'язку, проводити фото та відео зйомку, спілкуватися та передавати великі об'єми інформації через месенджери (Telegram, WhatsApp, Viber, Signal тощо), моніторити соціальні мережі та інтернет-простір.

Механізм слідоутворення під час використання засобів мобільного зв'язку має свою специфіку, оскільки утворені ними сліди, маючи інформаційний характер, не відображаються у зовнішній матеріальній обстановці. Використання спеціальних знань під час розслідування кримінальних правопорушень дає змогу не тільки виявити й зафіксувати залишені за допомогою мобільних засобів стільникового зв'язку сліди злочинної діяльності, але й встановити місцезнаходження злочинця або потерпілого, визначити маршрут їхнього переміщення, відновити текстову й мультимедійну інформацію, передану за допомогою мобільного пристрою, з'ясувати приналежність переданих даних конкретній особі.

Сліди, що утворюються під час вчинення злочинів із використанням мобільних засобів зв'язку – це інформація, яка зафіксована в цифрову форматі, міститься в різного роду цифрових пристроях зі створення, оброблення, збереження та передачі цієї інформації, причинно пов'язана з подією кримінального правопорушення, та дає змогу встановити як обставини вчиненого злочину, так і особу злочинця. Іншими словами такі сліди отримали назву цифрових, під якими розуміють дані, що залишаються в цифровому просторі внаслідок використання цифрових пристроїв, технологій та інформаційних мереж, які можуть бути використані в кримінальному провадженні й судочинстві[17].

Інформація (цифрові сліди), яка зберігається у операторів та провайдерів телекомунікацій, відіграє важливу роль у процесі кримінального провадження.

[17] Криміналістика: підручник / В. М. Шевчук, В. А. Журавель, В. Ю. Шепітько та ін.; за ред. В. М. Шевчука. Харків: Право, 2024. С. 396.

Встановлення особи, що користувалася послугами мобільного зв'язку, надає можливість органам досудового розслідування отримати відомості про ймовірного правопорушника, його соціальні зв'язки, а також характер і обставини протиправної діяльності. Будь-які дії злочинця, потерпілого чи інших осіб, які користуються послугами мобільного зв'язку, знаходять відображення на серверах оператора.

Такий процес збирання, аналіз та систематизації інформації отримав назву – білінг. В сучасних телекомунікаційних компаніях білінг – це складний комплекс програм, який дозволяє реалізувати процес збору інформації про використання телекомунікаційних послуг, тарифікацію, виставлення рахунків й обробку платежів споживачів послуг фіксованого і мобільного зв'язку, доступу до мережі Інтернет, інтернет-телефонії[18].

Оператори мобільного зв'язку в процесі надання телекомунікаційних послуг здійснюють безперервну фіксацію технічних параметрів функціонування мобільних пристроїв абонентів шляхом використання реєстрів місцезнаходження та переміщення. У результаті такої діяльності на серверах оператора формується база білінгових даних, яка містить відомості про ідентифікаційні характеристики абонента та параметри з'єднань, зокрема: 1) номер SIM-картки абонента; 2) міжнародний ідентифікаційний номер мобільного обладнання (IMEI); 3) дату, час та тривалість телекомунікаційного з'єднання; 4) номер абонента, який ініціює виклик; 5) номер абонента, з яким встановлюється з'єднання; 6) ім'я абонента, закріплене за відповідним номером у разі його верифікації; 7) вартість наданих послуг зв'язку; 8) ідентифікатор базової станції, через яку здійснено початок з'єднання; 9) ідентифікатор базової станції, через яку завершено з'єднання.

Встановлення місцезнаходження підозрюваного, потерпілого або будь-якої іншої особи може здійснюватися за допомогою можливостей технічних засобів операторів стільникового зв'язку або ж із використанням слідчими спеціалізованої криміналістичної техніки. Як правило, на етапі відкриття кримінального провадження підозрюваний невідомий і, запросивши дані білінгу, слідчий отримує масив даних про здійснені з'єднання абонентів за вказаний період часу в межах відповідної базової станції біля місця вчинення кримінального правопорушення. У подальшому, слідчий, аналізуючи отримані дані, виділяє збіги за датою, місцем і часом, після чого здійснюється перевірка конкретних SIM- та IMEI-номерів.

Зазначені відомості можуть бути отримані слідчим під час проведення такого заходу забезпечення кримінального провадження, як тимчасовий доступ до речей і документів. Відповідна ухвала слідчого судді надсилається оператору мобільного зв'язку, у володінні якого перебуває необхідна інформація, після чого уповноважена службова особа зобов'язана забезпечити тимчасовий доступ до неї з метою вилучення або виготовлення належним чином засвідчених копій. Надалі отриманий масив даних щодо конкретного абонентського номера оператора

[18] Сертифікація білінгових систем в Україні. URL: http://oniis.org/ukr/poslugi/sertifikaciya-obladnannya-zvyazku/sertifikaciya-bilingovih-sistem-v-ukraini (дата звернення: 20.01.2026)

мобільного зв'язку підлягає аналітичному опрацюванню. У разі виникнення потреби в одержанні додаткових відомостей, що мають значення для кримінального провадження, можливе проведення негласних слідчих (розшукових) дій, зокрема зняття інформації з електронних комунікаційних мереж відповідно до статті 263 КПК України або встановлення місцезнаходження радіообладнання (радіоелектронного засобу) згідно зі статтею 268 КПК України[19]. Положеннями статей 159 та 162 КПК України передбачена можливість отримання слідчим або прокурором відомостей про телекомунікаційні з'єднання, що мали місце у минулому (постфактум), зокрема інформації щодо місцезнаходження радіоелектронного засобу у визначений проміжок часу. Відповідно до частини першої статті 165 КПК України особа, яка зазначена в ухвалі слідчого судді або суду про надання тимчасового доступу до речей і документів як їх володілець, зобов'язана забезпечити надання такого доступу до визначених в ухвалі об'єктів особі, зазначеній у відповідному судовому рішенні, або іншій уповноваженій особі, яка діє на підставі доручення слідчого[20].

Відповідно до п. 1 ст. 159 КПК тимчасовий доступ до електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку здійснюється шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення. Відповідно до п. 2 ч.2, 3 ст. 168 КПК тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку не допускається, за винятком випадків, коли надання відповідних об'єктів разом з інформацією, що на них зберігається, є необхідною умовою проведення експертного дослідження, або коли такі об'єкти були отримані внаслідок вчинення кримінального правопорушення чи використовувалися як засіб або знаряддя його вчинення, а також у ситуаціях, коли доступ до них обмежується власником, володільцем чи утримувачем або пов'язаний із необхідністю подолання систем логічного захисту. У разі потреби слідчий або прокурор здійснює копіювання інформації, що міститься в інформаційних (автоматизованих), телекомунікаційних чи інформаційно-телекомунікаційних системах, а також у їх невід'ємних складових частинах. Копіювання такої інформації проводиться із залученням спеціаліста з метою забезпечення належної повноти, точності та збереження цілісності цифрових даних[21].

Оброблення цифрових доказів здійснюється з урахуванням вимог, викладених в ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи

[19] Кузубова Т. О. Розвиток законодавчих положень, що регламентують тимчасовий доступ до речей і документів в України. *Вісник ЛДУВС ім. Е.О. Дідоренка*. 2017. № 2. С. 118. URL: https://dspace.univd.edu.ua/items/d6ab6f17-2a01-407a-a288-d51d5ee4488b

[20] Використання інформації, що знаходиться в операторів та провайдерів телекомунікацій у кримінальному провадженні: метод. рек. / О.В. Таран, О.М. Брисковська, О.С. Тарасенко, А.А. Вознюк та ін. Київ: Нац. акад. внутр. справ, 2021. С. 13. URL: https://elar.naiau.kiev.ua/bitstreams/28ffc35c-c1e5-4583-8e16-2954c8bdd641/download

[21] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651 – VI URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів»[22].

Процес ідентифікації складається з пошуку, розпізнавання та документування потенційного цифрового доказу. В процесі ідентифікації працівники правоохоронного органу повинні визначити носій інформації, цифрові дані на якому потрібно зберегти у якості доказу, а також пристрої обробки інформації, які можуть містити потенційні цифрові докази, що стосуються кримінального правопорушення. Збирання передбачає вилучення пристроїв, які можуть містити цифрові докази з метою їх подальшого огляду та проведення експертних досліджень[23].

На стадії вчинення кримінального правопорушення та безпосереднього приховування його слідів і наслідків причетна особа може здійснювати дії, спрямовані на знищення, модифікацію або унеможливлення доступу до цифрової інформації, що зберігається на мобільному пристрої. До таких дій, зокрема, належать видалення електронного листування, фото- й відеоматеріалів, очищення історії вебперегляду, застосування засобів шифрування, а також блокування доступу до відповідних даних на мобільному телефоні.

З метою забезпечення своєчасного та належного вилучення електронно-цифрових слідів у криміналістичній практиці застосовуються спеціалізовані апаратно-програмні комплекси мобільної криміналістики. Для отримання та аналізу інформації з мобільних терміналів підрозділи правоохоронних органів України широко використовують відповідні технічні засоби, зокрема апаратно-програмні комплекси «Cellebrite UFED Touch 2 Ultimate» та «Cellebrite UFED 4 PC Physical Analyzer». Зокрема, такі комплекси використовують у своїй роботі оперативно-технічні підрозділи Національної поліції України та ДНДЕКЦ МВС України[24] під час проведення: 1) відповідних оперативно-технічних заходів та негласних слідчих (розшукових) дій зі зняття інформації з електронних інформаційних систем; 2) слідчої (розшукової) дії як-то: огляд місцевості, приміщення, речей, документів та комп'ютерних даних (ст. 237 КПК України), для огляду мобільного терміналу (стільникового радіотелефону) та/або SIM-картки, виявлених на місці вчинення кримінального правопорушення;

[22] Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів: ДСТУ ISO/IEC 27037:2017. На заміну ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT); Чинний від 2019-01-01. Київ: УкрНДНЦ, 2018. VI, 31 с. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU_ISO_IEC_27037-2017.pdf

[23] Міжнародні стандарти та правова регламентація цифрових (електронних) доказів у кримінальному аналізі: науково-методичні рекомендації / розробн. Манжай О.В., Носов В.В., Мальцев В.В., Роговий А.П./ за ред. Бутко Р.Ю. Харків: ХНУВС, 2024. С. 29. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/10ad6bf2-b7d4-45d1-9923-34e9acc0d785/content?trackerId=5e9e04034bf21dff

[24] Кобець М. В. Апаратно-програмний комплекс «Cellebrite UFED» як засіб отримання інформації з мобільних терміналів. *Актуальні питання та перспективи використання оперативно-розшукових засобів у розкритті злочинів в умовах воєнного стану*: матер. міжвідоч. наук.-практ. конференції (м. Київ, 30 берез. 2023 р.). Київ: Нац. акад. внутр. справ. 2023. С. 71. URL: https://elar.navs.edu.ua/items/71ba959b-a48b-468d-a611-cad52e202482

3) обшуку житла чи іншого володіння особи, обшуку особи (ст. 236 КПК України) для доступу до комп'ютерних систем або їх частин, мобільних терміналів (стільникових радіотелефонів) та/або SIM-карток[25].

Зазначені апаратно-програмні комплекси забезпечують можливість пошуку, вилучення та аналізу інформації, що зберігається на мобільних і комп'ютерних пристроях, а також у хмарних сховищах даних (зокрема iCloud, Google, Dropbox), у тому числі у випадках, коли відповідний пристрій перебуває у заблокованому стані. Програмні засоби дозволяють отримувати дані як безпосередньо з мобільних терміналів, так і з їх резервних копій незалежно від особливостей встановленої операційної системи. У результаті застосування такого програмного забезпечення формується повний цифровий образ досліджуваного пристрою, включно з інформацією із зашифрованих застосунків, яка виявляється та, за наявності технічної можливості, розшифровується у максимально повному обсязі й відповідає даним, що містилися на оригінальному пристрої.

Вагомою перевагою зазначених апаратно-програмних комплексів є можливість дослідження мобільних пристроїв, що перебувають у неробочому стані, зокрема внаслідок тривалого впливу води або механічних ушкоджень. Окрім смартфонів на базі операційних систем iOS та Android, програмне забезпечення підтримує також менш поширені платформи, такі як Windows Phone, BlackBerry OS тощо. Пріоритетним напрямом функціонування UFED є виявлення та вилучення інформації з прихованих або видалених джерел, зокрема електронного листування у месенджерах, контактних даних, фотографій і відеозаписів. Крім того, програмні інструменти дозволяють відновлювати та аналізувати геолокаційні дані, що зберігалися на пристрої під час його використання, з метою встановлення маршруту переміщення користувача.

Розкриття та розслідування кримінальних правопорушень, що вчиняються з використанням мобільних засобів зв'язку, вимагає наявності спеціальних знань і навичок у дослідженні інформаційного простору вилученого пристрою. Якщо слідчий приймає рішення здійснити огляд самостійно, він повинен дотримуватися певних криміналістичних рекомендацій.

Слідчий огляд мобільного засобу зв'язку передбачає дві стадії – статичну та динамічну[26]. Проведення слідчої дії починається із загального огляду мобільного пристрою, результати якого підлягають обов'язковій фіксації у протоколі. У ньому, зокрема, зазначаються модель смартфона, його конструктивні особливості (форма, колір, габарити), найменування та наявність ідентифікаційних позначень (логотипів), а також інформація про оснащення пристрою вбудованими фото- чи відеокамерами з лицьового та тильного боку.

[25] Тіхонов С. В., Кобець М. В. Застосування апаратно-програмного комплексу «Cellebrite UFED» під час виявлення та розслідування кримінальних правопорушень: метод. рекомендації. Київ: Нац. акад. внутр. справ, 2023. С. 6. URL: https://elar.navs.edu.ua/items/eb658e56-3060-413b-9e01-6f797ce3e731

[26] Курман О.В. Мобільні телекомунікаційні засоби як носії важливої доказової інформації: перспективність та проблеми дослідження. *Аналітично-порівняльне правознавство.* 2023. № 5. С. 533. URL: https://app-journal.in.ua/wp-content/uploads/2023/10/APP_05_2023_FINAL.pdf

Крім того, у протоколі відображається розташування функціональних і сенсорних елементів керування, а також наявність технічних роз'ємів, зокрема micro-USB або Type-C, призначених для підключення зарядних пристроїв, стереонавушників, а також отворів для динаміків і мікрофона.

За наявності технічної можливості та з урахуванням конкретної слідчої ситуації слідчому доцільно залучати спеціаліста й використовувати відповідні техніко-криміналістичні засоби для розблокування мобільного пристрою у випадках, коли на ньому застосовано один із засобів захисту, зокрема буквено-цифровий пароль, PIN-код, графічний ключ, біометричну ідентифікацію за обличчям (Face ID) або інші подібні механізми.

У протоколі огляду слідчий зобов'язаний детально зафіксувати процедуру розблокування мобільного пристрою (смартфона), а також усі подальші дії у чіткій хронологічній послідовності. Після отримання доступу до пристрою здійснюється опис графічних і текстових елементів інтерфейсу, що відображаються у центральному вікні екрана та додаткових системних або прикладних вікнах.

Виявлення криміналістично значущої інформації здійснюється шляхом аналізу вмісту мобільного пристрою, зокрема журналу вхідних і вихідних дзвінків, SMS-повідомлень, електронної та голосової пошти, історії користування вебброузером (у тому числі вмісту каталогів «Вибране», «Журнал», «Cookies», «Temporary Internet Files»), даних месенджерів (WhatsApp, Viber, Telegram тощо), фото- й відеоматеріалів, аудіозаписів диктофона, а також інформації, що міститься в органайзері, з урахуванням технічних особливостей конкретної моделі смартфона.

Під час огляду вмісту мобільного засобу зв'язку спеціаліст за дорученням слідчого здійснює поетапну детальну фотозйомку зображень, що відображаються на екрані мобільного пристрою, з метою фіксації відомостей, які мають значення для кримінального провадження.

У випадках, коли обсяг інформації, що міститься в пам'яті технічного пристрою, є значним, доцільним є застосування методів і прийомів криміналістичного відеозапису для забезпечення повної та наочної фіксації відповідних даних. За таких умов слідчий зобов'язаний здійснювати усний коментар усіх дій і маніпуляцій, спрямованих на одержання конкретних відомостей із мобільного пристрою (смартфона), що забезпечує належну процесуальну фіксацію ходу та результатів огляду.

Водночас слід констатувати наявність низки технічних обмежень і проблем, пов'язаних із застосуванням криміналістичних програмно-технічних комплексів мобільної криміналістики. Одним із основних завдань слідчого за участю спеціаліста є отримання доступу до інформації, що зберігається на захищених мобільних пристроях або перебуває у зашифрованому вигляді. Однак засоби захисту сучасних смартфонів постійно удосконалюються, що, у свою чергу, істотно ускладнює процес їх розблокування та вилучення цифрових даних. У разі впровадження виробниками нових або оновлених протоколів безпеки операційних систем iOS та Android і їх встановлення на мобільні пристрої виникають труднощі з реалізацією повного функціоналу відповідних програмно-апаратних комплексів, а в окремих випадках – і повна

неможливість розшифрування даних. За таких умов від розробників криміналістичних програмно-технічних засобів вимагається постійне оновлення знань щодо характеристик нових моделей пристроїв, особливостей операційних систем та сучасних методів шифрування. Водночас на практиці інструментарій, що пропонується, не завжди є сумісним з останніми поколіннями мобільних пристроїв або з численними варіаціями їх регіональних чи операторських модифікацій.

ВИСНОВКИ

Цифровізація суспільних відносин і масове використання електронних технологій комунікації зумовили формування принципово нового інформаційного середовища, у межах якого майже кожна дія людини залишає цифрові сліди. Особливе місце серед технічних засобів, що використовуються як у повсякденному житті, так і в злочинній діяльності, посідають мобільні телефони (смартфони). Їх багатофункціональність, постійне підключення до мереж електрозв'язку та здатність акумулювати значні обсяги різнорідної інформації роблять ці пристрої одним із ключових джерел криміналістично значущих даних. Саме через мобільні засоби зв'язку здійснюється координація злочинних дій, передавання вказівок, погроз, реалізація шахрайських схем, а також фіксація та приховування результатів протиправної діяльності.

Механізм слідоутворення під час використання мобільних пристроїв має специфічний інформаційний характер і не проявляється у традиційній матеріальній формі. Цифрові сліди локалізуються у внутрішній пам'яті пристроїв, хмарних сховищах, а також у базах даних операторів і провайдерів телекомунікацій. Їх виявлення, фіксація та дослідження можливі виключно за умови застосування спеціальних криміналістичних знань і сучасних техніко-криміналістичних засобів. Аналіз таких слідів дозволяє встановлювати обставини вчинення кримінального правопорушення, ідентифікувати осіб, причетних до нього, відновлювати маршрути переміщення, часову послідовність подій, коло контактів і характер комунікацій.

Важливе місце у процесі доказування займає інформація білінгу, що накопичується на серверах операторів мобільного зв'язку. Відомості про SIM-картки, IMEI-номери, параметри з'єднань і дані базових станцій дають змогу реконструювати події, які відбувалися у конкретний час і в певному місці, а також звузити коло ймовірних підозрюваних. Процесуальні механізми отримання такої інформації, передбачені кримінальним процесуальним законодавством України, створюють необхідні правові умови для її використання як доказу за умови дотримання вимог законності, належності та допустимості.

Водночас стрімке зростання обсягів цифрових даних і їх неструктурований характер істотно ускладнюють застосування традиційних методів аналізу. У цьому контексті штучний інтелект постає як перспективний інструмент оптимізації процесів виявлення, систематизації та інтерпретації цифрових слідів. Використання алгоритмів машинного навчання, обробки природної мови та комп'ютерного зору дозволяє автоматизувати аналіз великих масивів інформації, відновлювати хронологію подій, виявляти приховані взаємозв'язки між об'єктами та формувати обґрунтовані доказові гіпотези. Інтеграція таких

технологій у діяльність слідчих і експертних підрозділів здатна суттєво підвищити ефективність розслідування злочинів, учинених із використанням інформаційних технологій.

У той же час впровадження штучного інтелекту та сучасних апаратно-програмних комплексів мобільної криміналістики супроводжується низкою суттєвих проблем і ризиків. Серед них – складність встановлення причинно-наслідкових зв'язків між вхідними даними та отриманими результатами аналізу, імовірність помилкових результатів, уразливість до технічних атак, а також постійне вдосконалення засобів захисту операційних систем і методів шифрування, що ускладнює доступ до даних. Крім того, відсутність чіткого нормативно-правового врегулювання статусу результатів, отриманих із використанням інтелектуальних технологій, створює ризики порушення прав учасників кримінального провадження та принципів справедливого судочинства.

Узагальнюючи викладене, можна дійти висновку, що ефективне розслідування кримінальних правопорушень у цифровому середовищі можливе лише за умови комплексного поєднання процесуальних механізмів, спеціальних знань, сучасних техніко-криміналістичних засобів і контрольованого використання технологій штучного інтелекту. Подальший розвиток криміналістичної науки в цьому напрямі має бути спрямований на вдосконалення методик роботи з цифровими слідами, адаптацію технічних інструментів до нових технологічних викликів, формування чітких правових і етичних стандартів застосування ШІ та забезпечення балансу між ефективністю розслідування й дотриманням прав і свобод людини.

АНОТАЦІЯ

У науковій роботі досліджено сучасні криміналістичні засоби отримання значущої інформації для розслідування кримінальних правопорушень в умовах цифровізації суспільних відносин. Розкрито сутність і особливості формування цифрових слідів як результату використання інформаційно-комунікаційних технологій у повсякденній та злочинній діяльності. Проаналізовано наукові підходи до визначення поняття, ознак і класифікації цифрових слідів у криміналістиці. Окрему увагу приділено дослідженню ролі мобільних засобів зв'язку як одного з ключових джерел цифрових доказів. Висвітлено механізми слідоутворення під час використання мобільних пристроїв та можливості їх дослідження з застосуванням спеціальних криміналістичних знань і технічних засобів. Розглянуто потенціал використання штучного інтелекту для автоматизованого виявлення, аналізу та інтерпретації цифрових слідів. Проаналізовано основні технічні, правові та етичні проблеми впровадження інтелектуальних технологій у криміналістичну діяльність. Окреслено ризики, пов'язані з достовірністю, допустимістю та законністю результатів, отриманих за допомогою систем штучного інтелекту. Запропоновано напрями вдосконалення криміналістичних методик роботи з цифровими слідами з урахуванням сучасних технологічних викликів.

Література

1. MacMillan D. Arrested by AI: Police ignore standards after facial recognition matches. *The Washington Post.* 13 січня 2025. URL: https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/ (дата звернення: 20.01.2026).
2. Shevchuk V. M. Development trends in criminalistics in the era of digitalization. *Modern knowledge: research and discoveries: I International Scientific and Practical Conference* (May 19–20, 2023; Vancouver, Canada). 2023. Pp. 198–219. URL: https://archive.interconf.center/index.php/2709-4685/issue/view/19-20.05.2023/165
3. Авдєєва Г. Сутність цифрових слідів у криміналістиці. *Актуальні питання судової експертизи та криміналістики*. 2018. С. 90–93. URL: https://dspace.nlu.edu.ua/bitstream/123456789/15677/1/Avdeeva_90-93.pdf
4. Бєлова М. В., Бєлов Д. М., Рущак І. В. Штучний інтелект у досудовому розслідуванні кримінальних справ: окремі питання міжнародної практики. *Аналітично порівняльне правознавство*. 2025. № 1. С. 818-824. URL: https://doi.org/10.24144/2788-6018.2025.01.136
5. Використання інформації, що знаходиться в операторів та провайдерів телекомунікацій у кримінальному провадженні: метод. рек. / О.В. Таран, О.М. Брисковська, О.С. Тарасенко, А.А. Вознюк та ін. Київ: Нац. акад. внутр. справ, 2021. 50 с. URL: https://elar.naiau.kiev.ua/bitstreams/28ffc35c-c1e5-4583-8e16-2954c8bdd641/download
6. Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського національного університету. Серія Право*. 2024. Вип. 85, ч. 4. С. 71–75. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/11/12-3.pdf
7. Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі: монографія / В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін.; за заг. ред. В. Ю. Шепітька. Харків: Право, 2024. 208 с. URL: https://ivpz.kh.ua/wp-content/uploads/2025/01/%D0%9C%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F-%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%D1%96%D1%81%D1%82%D1%96%D0%B2-2024.pdf
8. Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів: ДСТУ ISO/IEC 27037:2017. На заміну ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT); Чинний від 2019-01-01. Київ: УкрНДНЦ, 2018. VI, 31 с. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU_ISO_IEC_27037-2017.pdf
9. Карчевський М. В., Куковинець Д. О. Використання технологій штучного інтелекту правоохоронними та судовими органами: світовий досвід та напрями розвитку національного законодавства. *Питання боротьби зі злочинністю*. 2023. Вип. 46. С. 21-31. URL: http://pbz.nlu.edu.ua/issue/view/17882
10. Кобець М. В. Апаратно-програмний комплекс «Cellebrite UFED» як засіб отримання інформації з мобільних терміналів. *Актуальні питання та перспективи використання оперативно-розшукових засобів у розкритті злочинів в умовах воєнного стану*: матер. міжвідоч. наук.-практ. конференції (м. Київ, 30 берез. 2023 р.). Київ: Нац. акад. внутр. справ. 2023. С. 70-73. URL: https://elar.navs.edu.ua/items/71ba959b-a48b-468d-a611-cad52e202482

11. Коваленко А. В. Класифікація електронних (цифрових слідів кримінального правопорушення. *Проблеми законності*. 2023. Вип. 161. С. 202–214. URL: http://plaw.nlu.edu.ua/issue/view/16823

12. Колеснікова І. А. Цифрові сліди: поняття та їх значення при розслідуванні кримінальних правопорушень. *Юридичний науковий електронний журнал*. 2023. № 10. С. 472–475. URL: http://lsej.org.ua/10_2023/114.pdf

13. Криміналістика: підручник / В. М. Шевчук, В. А. Журавель, В. Ю. Шепітько та ін.; за ред. В. М. Шевчука. Харків: Право, 2024. 1008 с.

14. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651–VI. URL:https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.01.2026)

15. Кузубова Т. О. Розвиток законодавчих положень, що регламентують тимчасовий доступ до речей і документів в України. *Вісник ЛДУВС ім. Е.О. Дідоренка*. 2017. № 2. С. 117-123. URL: https://dspace.univd.edu.ua/items/d6ab6f17-2a01-407a-a288-d51d5ee4488b

16. Курман О. В. Мобільні телекомунікаційні засоби як носії важливої доказової інформації: перспективність та проблеми дослідження. *Аналітично-порівняльне правознавство.* 2023. № 5. С. 532-536. URL: https://app-journal.in.ua/wp-content/uploads/2023/10/APP_05_2023_FINAL.pdf

17. Курман О. Правові та практичні аспекти використання поліграфа у кримінальному провадженні України. *Сучасний досвід використання поліграфа у сфері національної безпеки і оборони України в умовах воєнних загроз*: зб. матеріалів панел. дискусії: IX Харків. міжнар. юрид. форум, м. Харків, 26 верес. 2025 р. / редкол.: А. Гетьман, В. Журавель, В. Шевчук та ін.; Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. криміналістики; Нац. акад. прав. наук України; Всеукр. асоц. поліграфологів [та ін.]. Харків: Право, 2025. С. 76-80. URL: https://dspace.nlu.edu.ua/jspui/handle/123456789/20575

18. Курман О. В. Способи несанкціонованого втручання в роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Право і суспільство*. 2017. № 4. С. 245-249. URL: http://pravoisuspilstvo.org.ua/archive/2017/4_2017/part_1/44.pdf

19. Курман О. В. Типізація способів учинення злочинних посягань на відомості, що становлять комерційну або банківську таємницю. *Теорія та практика судової експертизи і криміналістики*: збірник наукових праць. Вип. 10 / ред. кол.: М.Л. Цимбал, В.Ю. Шепітько, Л.М. Головченко та ін. Харків.: Право, 2010. С. 62-68.

20. Латиш К. В. Криміналістичний аналіз кіберінструментів вчинення злочинів. *Проблеми законності*. 2021. Вип. 153. С. 165-172. URL: http://nbuv.gov.ua/UJRN/Pz

21. Міжнародні стандарти та правова регламентація цифрових (електронних) доказів у кримінальному аналізі: науково-методичні рекомендації / розробн. Манжай О.В., Носов В.В., Мальцев В.В., Роговий А.П./ за ред. Бутко Р.Ю. Харків: ХНУВС, 2024. 36 с. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/10ad6bf2-b7d4-45d1-9923-34e9acc0d785/content?trackerId=5e9e04034bf21dff

22. Негребецький В. В. Використання систем штучного інтелекту у боротьбі зі злочинністю: огляд та перспективи. *Українська поліцеїстика: теорія, законодавство, практика*. 2024. № 1 (9). С. 66-70. URL: DOI: https://doi.org/10.32782/2709-9261-2024-1-9-13

23. Плахотнік О. В. Практичне застосування штучного інтелекту у кримінальному провадженні. *Вісник кримінального судочинства*. 2019. № 4. С. 45-57. URL: https://vkslaw.com.ua/index.php/journal/article/view/222

24. Сертифікація білінгових систем в Україні. URL: http://oniis.org/ukr/poslugi/sertifikaciya-obladnannya-zvyazku/sertifikaciya-bilingovih-sistem-v-ukraini (дата звернення: 20.01.2026)

25. Степанюк Р. Л., Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник ЛДУВС ім. Е. О. Дідоренка*. 2022. Вип. 3 (99). С. 283-284. URL: https://dspace.univd.edu.ua/items/b174d57a-bf4b-47f9-9211-aeb715b61844

26. Тіхонов С. В., Кобець М. В. Застосування апаратно-програмного комплексу «Cellebrite UFED» під час виявлення та розслідування кримінальних правопорушень: метод. рекомендації. Київ : Нац. акад. внутр. справ, 2023. 41 с. URL: https://elar.navs.edu.ua/items/eb658e56-3060-413b-9e01-6f797ce3e731

27. Черваньова Д. А., Курман О. В. Застосування штучного інтелекту в криміналістиці: перспективи та ризики. *Аналітично-порівняльне правознавство.* 2025. № 3. Ч.3. С. 211-215. URL: https://app-journal.in.ua/wp-content/uploads/2025/06/33-2.pdf

28. Черевко К. О., Луценко І. Г. Штучний інтелект як інструмент протидії злочинності. *Вісник Кримінологічної асоціації України*. 2023. № 1. С. 124-133. URL: DOI: https://vca.univd.edu.ua/index.php/vca/article/view/43

29. Шевчук В. Перспективні напрями використання технологій штучного інтелекту в розслідуванні кримінальних правопорушень. *Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі: монографія* / В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін. Харків: Право, 2024. С. 83–106. URL: https://ivpz.kh.ua/wp-content/uploads/2025/01/Монорафія-Криміналістів-2024.pdf

30. Шевчук В. М. Криміналістичне забезпечення розслідування воєнних злочинів: цифровізація, інновації, перспективи. *Військові правопорушення та воєнні злочини: історія, теорія та практика*. Колективна монографія. “Izdevnieciba “Baltija Publishing” (м. Рига, Латвія), 2023. С. 795-822. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/view/322/8791/18392-1

31. Шепітько В. Ю., Журавель В. А., Авдєєва Г. К. Інновації в криміналістиці та їх впровадження в діяльність органів досудового слідства. *Питання боротьби зі злочинністю*: зб. наук. праць. Харків: Право, 2011. Вип. 21. С. 39-46.

Information about the autho:
Kurman Oleksandr Vasylyovych,
Candidate of Law,
Associate Professor of the Department of Forensic Science
Yaroslav the Wise National Law University
77, Hryhoriya Skovoroda St., Kharkiv, 61024, Ukraine