УДК 343.9:004.8:004.932:340.134
DOI https://doi.org/10.32782/TNU-2707-0581/2025.6/35

Горєлова В. Ю.
Таврійський національний університет імені В. І. Вернадського

ШТУЧНИЙ ІНТЕЛЕКТ У КРИМІНОЛОГІЧНІЙ ІДЕНТИФІКАЦІЇ: ІНДЕКС МІЖПАЛЬЦЕВОЇ СПОРІДНЕНОСТІ ТА АЛГОРИТМІЧНИЙ АУДИТ

У статті досліджено та обґрунтовується концепція кримінологічного індексу міжпальцевої спорідненості (Criminological Interfinger Relatedness Index, CIMR) як нового імовірнісного інструменту кримінологічного аналізу, спрямованого на виявлення латентної серійності злочинів через системне осмислення біометричних даних. Наголошується, що застосування методів глибокого навчання та нейромережевих моделей у дактилоскопії дозволяє виявляти структурну схожість між різними пальцями однієї особи, що принципово змінює традиційне уявлення про абсолютну дискретність кожного відбитка. Звертається увага на те, що класичні криміналістичні методики ідентифікації зосереджуються на аналізі мінуцій як локальних ознак, тоді як сучасні алгоритмічні підходи оперують архітектурою гребеневих структур, відкриваючи можливість імовірнісного «зшивання» розрізнених латентних слідів, зафіксованих у різних епізодах злочинної діяльності. Зазначається необхідність перегляду усталених стандартів доказування в кримінальному процесі України у зв'язку з поширенням алгоритмічних форм аналізу доказової інформації, а також наголошується на потребі впровадження механізмів алгоритмічного аудиту та пояснювального штучного інтелекту для мінімізації ризиків дискримінації, похибок інтерпретації та неправомірного використання імовірнісних висновків. Обґрунтовується висновок, що використання індексу CIMR трансформує дактилоскопію з допоміжного засобу індивідуальної ідентифікації у стратегічний інструмент кримінологічного прогнозування, здатний моделювати мережеві зв'язки між правопорушеннями та формами злочинної активності. Наукова новизна полягає у введенні індексу CIMR та розробці алгоритму його операціоналізації у кримінологічній практиці України. Пропонуються рекомендації щодо вдосконалення досудового розслідування шляхом інтеграції XAI, процедур алгоритмічного контролю та інтерпретованих моделей оцінювання біометричної спорідненості у національні бази даних правоохоронних органів.

Ключові слова: *штучний інтелект, пояснювальний ШІ (XAI), біометрична валідність, кримінологічне профілювання, латентна серійність злочинів, індекс міжпальцевої спорідненості (CIMR), алгоритмічний аудит.*

Постановка проблеми. Традиційна криміналістична ідентифікація ґрунтується на догмі абсолютної унікальності кожного окремого відбитка пальця. Проте сучасні алгоритми глибокого навчання, аналізуючи архітектуру папілярних гребенів, демонструють існування стійкої структурної спорідненості між різними пальцями однієї особи. Це відкриває нові можливості для виявлення латентної серійності злочинів, але водночас ставить під сумнів усталені стандарти доказування та кримінологічну валідність ідентифікації. Проблема полягає у відсутності теоретично обґрунтованого інструменту для інтеграції імовірнісних результатів ШІ-аналізу в практику розслідування, а також у дефіциті методології контролю за їхньою надійністю та неупередженістю.

Аналіз останніх досліджень і публікацій. Використання біометричних даних, інтеграція штучного інтелекту в правоохоронну діяльність та трансформація криміналістичної ідентифікації досліджувалися у працях вітчизняних учених: В. Глушкова, В. Пилипчука, О. Користіна, О. Кваші, В. Бутузова, С. Чернявського, О. Мороза, С. Вітвіцького, О. Джужі, М. Ізидорчака. Зарубіжні дослідники Гейб Го, Аніруд Рей, Ход Ліпсон, Венкатеш Говіндараджу, Наліні Рата, Бхавін Джаваде, Манал Alhammad та Ана Морено акцентували увагу на етичних межах застосування нейромереж, алгоритмічній упередженості біометричних систем, сталості методів ідентифікації (фреймворк GLUX) та валідності новітніх підходів до аналізу папілярних узорів. Водночас питання системної кореляції між відбитками різних пальців однієї особи у вітчизняному кримінологічному дискурсі залишається малодослідженим, що визначає актуальність даної роботи.

Постановка завдання. Метою статті є теоретичне обґрунтування та методологічна операціоналізація авторської концепції кримінологічного індексу міжпальцевої спорідненості (CIMR) як інструменту виявлення латентної серійності злочинів. Дослідження спрямоване на розробку цілісної моделі алгоритмічного аудиту для систем штучного інтелекту, що інтегруються у вітчизняну практику криміналістичної ідентифікації. Досягнення мети передбачає розв'язання таких завдань: 1) аналіз кримінологічної валідності міжпальцевої схожості папілярних узорів на основі ШІ-моделей; 2) порівняння точності імовірнісної ідентифікації з традиційними методами дактилоскопії; 3) визначення протоколів використання результатів CIMR-аналізу в розслідуванні з метою забезпечення їхньої етичності, прозорості та доказової значущості.

Виклад основного матеріалу. Традиційна парадигма криміналістичної ідентифікації упродовж понад століття формувалася під визначальним впливом постулатів сера Френсіса Гальтона, згідно з якими папілярний узор кожного пальця розглядався як автономна, повністю унікальна та онтологічно ізольована біометрична структура [1]. У межах вітчизняної кримінологічної школи ця теза набула статусу методологічної догми: відбитки різних пальців однієї особи трактувалися як незалежні змінні, між якими апріорно виключалася будь-яка суттєва кореляція [2]. Такий підхід був логічно виправданий у контексті історичних можливостей експертного аналізу, однак у сучасних умовах стрімкого розвитку штучного інтелекту потребує принципового переосмислення [3]. Методологічна обмеженість класичної дактилоскопії зумовлена її зосередженістю на мінуціях – локальних точкових характеристиках папілярного узору (розгалуженнях і закінченнях гребенів), які дійсно мають високий ступінь індивідуальної унікальності [4]. Водночас такий редукціоністський підхід ігнорує макроструктурні властивості папілярних візерунків, що залишалися поза межами когнітивних можливостей людського експерта. Сучасні нейромережеві моделі, навчені на великих стандартизованих датасетах, зокрема NIST SD300 та RidgeBase, застосовують якісно інший принцип аналізу – реконструкцію архітектури гребенів, їх просторової орієнтації та топологічних взаємозв'язків шляхом формування векторних представлень (*embeddings*) [5]. Результати емпіричних досліджень, зокрема експериментальні роботи Г. Го та його колег, свідчать про наявність статистично значущої внутрішньо-особистісної кореляції між папілярними узорами різних пальців однієї людини [6]. Нейромережевий аналіз дозволяє ідентифікувати стійкі архітектурні патерни, які формують своєрідний «біометричний почерк» особи та проявляються незалежно від конкретного пальця [7]. Отримані статистичні показники підтверджують емпіричну валідність цього підходу: значення ROC AUC у межах 0,87–0,99 (залежно від якості латентного сліду) при рівні статистичної значущості $p < 0,01$ свідчать про те, що виявлена схожість не є випадковим збігом [8]. Таким чином, встановлена міжпальцева спорідненість має не евристичний, а біологічно зумовлений характер, що корелює з закономірностями ембріонального розвитку папілярних узорів. Це обумовлює необхідність перегляду традиційних уявлень про валідність дактилоскопічної ідентифікації, яка поступово зміщується від моделі «точкового збігу» до концепції «системної біометричної спорідненості» [1]. У цьому контексті пропонується концепція кримінологічного індексу міжпальцевої спорідненості (CIMR), у межах якої відбиток пальця перестає розглядатися як ізольований ідентифікатор, а постає елементом цілісного біометричного ансамблю особи. Такий підхід дозволяє не лише пов'язувати розрізнені епізоди злочинної діяльності, а й формувати новий тип імовірнісного кримінологічного знання, орієнтованого на виявлення латентної серійності та структурних закономірностей злочинної поведінки.

Методологічна операціоналізація кримінологічного індексу міжпальцевої спорідненості (CIMR) потребує розкриття так званої «чорної скриньки» штучного інтелекту у сфері кримінологічної ідентифікації, зокрема пояснення механізму трансформації візуально сприйманого відбитка пальця у формалізований математичний об'єкт, придатний для аналітичної та прогностичної обробки [9]. У межах класичного підходу автоматизованих біометричних ідентифікаційних систем (АБІС) домінувала логіка фіксації мінуцій (точок розгалуження та закінчення папілярних гребенів, що підлягали експертному зіставленню) [3]. Така модель, хоча й забезпечувала високу точність категоричної ідентифікації, була принципово обмеженою у здатності виявляти системні структурні закономірності. Сучасні моделі глибокого навчання, зокрема згорткові нейронні мережі (CNN) та архітектури *Vision Transformer*, реалізують іншу парадигму аналізу, зосереджену не на локальних точкових характеристиках, а на глобальній архітектурі папілярного узору [6], [5].

Алгоритмічний аналіз охоплює поля орієнтації гребенів, просторову організацію потоків ліній, а також сингулярні зони – ядра та дельти, що визначають загальну конфігурацію візерунка. Такий підхід дозволяє абстрагуватися від локальних ушкоджень шкіри та якості латентного сліду, концентруючись на стійких структурних закономірностях, які у сукупності формують «біометричний ансамбль» особи. Ключовим етапом операціоналізації є побудова векторного представлення (embedding) папілярного узору [5]. У результаті проходження зображення через навчений нейромережевий шар кожен відбиток репрезентується у вигляді багатовимірного вектора ознак, де окремі координати відображають узагальнені параметри архітектури гребенів. Схожість між двома відбитками, наприклад великого та вказівного пальців, обчислюється за допомогою косинусної подібності між відповідними векторами [8]. У математичному сенсі це означає вимірювання кута між двома векторами у просторі ознак: чим меншим є цей кут, тим вищим є ступінь структурної спорідненості папілярних узорів. Таким чином, складна морфологія папілярних ліній редукується до числового показника, придатного для кримінологічного аналізу та порівняння [6].

У межах авторської концепції CIMR (*Criminological Inter-finger Similarity Index*) цей показник інтерпретується як нормалізований індекс, адаптований до потреб кримінологічного дослідження [11]. Перевищення встановленого порогового значення сигналізує про високу імовірність належності аналізованих слідів одній особі. При цьому поріг відсікання визначається емпірично на основі контрольних вибірок, що забезпечує гнучкість і контекстуальну адаптивність індексу CIMR до різних типів злочинної діяльності та якості біометричних слідів [10]. У такий спосіб CIMR постає не як інструмент категоричної ідентифікації, а як засіб імовірнісного кримінологічного прогнозування, орієнтований на виявлення латентної серійності та зв'язування розрізнених епізодів злочинної активності [10]. Наукова валідність індексу забезпечується шляхом статистичної верифікації отриманих результатів [8]. Застосування ROC-аналізу дозволяє оцінити співвідношення між рівнем помилкового прийняття (*False Acceptance Rate*) та помилкового відхилення (*False Rejection Rate*), а також обрати оптимальний баланс між чутливістю та специфічністю моделі [8]. Водночас у кримінологічному прогнозуванні допускається вищий рівень імовірнісної невизначеності, ніж у процесуальній ідентифікації, оскільки метою є не прийняття остаточного судового рішення, а формування обґрунтованої аналітичної гіпотези про серійний характер злочинної діяльності [11]. Саме ця логіка (перетворення прихованих структур, недоступних безпосередньому людському сприйняттю, у інтерпретований цифровий індекс) становить ядро наукової новизни та методологічної значущості CIMR [11].

Практична значущість кримінологічного індексу міжпальцевої спорідненості (CIMR) найбільш повно проявляється у сфері виявлення латентної серійності злочинів, де класичні дактилоскопічні методики часто виявляються методологічно безсилими через відсутність прямих ідентифікаційних збігів у базах даних [10]. У таких випадках CIMR виконує функцію аналітичного каталізатора, що трансформує логіку розслідування від фрагментарного аналізу окремих слідів до системного осмислення серійної злочинної активності. Показовим є сценарій розслідування майнових злочинів, зокрема серійних квартирних крадіжок. На практиці на різних місцях подій нерідко фіксуються відбитки різних пальців – наприклад, великого пальця правої руки на одному об'єкті та вказівного пальця лівої руки на іншому [5]. У межах класичного АБІС-підходу такі сліди розглядаються як незалежні біометричні об'єкти, що унеможливлює формування автоматизованого збігу («*hit*») [10]. Застосування індексу CIMR дозволяє подолати цю методологічну розірваність шляхом автоматизованого порівняння слідів на рівні їх архітектурної спорідненості [7]. У разі перевищення емпірично встановленого порогового значення слідчий отримує імовірнісно обґрунтований сигнал про високу вірогідність належності аналізованих епізодів одній особі [7]. Це, у свою чергу, створює підстави для об'єднання кримінальних проваджень та концентрації оперативно-слідчих ресурсів на єдиному векторі пошуку ще до фактичної ідентифікації підозрюваного [9].

Не менш показовим є застосування CIMR у справах про насильницькі злочини, зокрема злочини проти статевої свободи та розбійні напади. Для таких кримінальних правопорушень характерна фрагментарність або деформація біометричних слідів, зумовлена динамічним характером події та інтенсивною взаємодією учасників [6]. За відсутності якісних мінуцій CIMR функціонує як інструмент формування імовірнісного профілю серійності [11]. Нейромережевий аналіз архітектурних патернів дозволяє виявляти

стійку внутрішньоособистісну кореляцію навіть між частковими або пошкодженими слідами, що не придатні для класичної експертної ідентифікації [5]. У результаті формується новий тип криміналістичного знання – цифрово обґрунтована гіпотеза про «єдиного суб'єкта», яка суттєво впливає на тактику та послідовність проведення слідчих (розшукових) дій [7]. Таким чином, використання індексу CIMR забезпечує перехід від реактивної моделі розслідування, зорієнтованої на пасивне очікування збігу у базі даних, до проактивної моделі, що ґрунтується на прогнозуванні серійності злочинної діяльності на основі структурних біометричних закономірностей [11]. Такий підхід не лише оптимізує використання слідчих та оперативних ресурсів, а й формує нову когнітивну основу криміналістичного прогнозування, у межах якої імовірнісні індекси набувають статусу стратегічного інструменту протидії серійній злочинності. Проблема алгоритмічного аудиту у сфері криміналістичного застосування індексу міжпальцевої спорідненості (CIMR) постає не як технічна деталь, а як фундаментальний виклик для самої природи пізнання у кримінальному процесі. Адже традиційна експертна парадигма, що спиралася на безпосереднє сприйняття та інтерпретацію матеріальних слідів, виявляється неспроможною інтегрувати результати імовірнісних моделей без додаткових когнітивних та методологічних гарантій. Таким чином постає питання: чи може алгоритм, який продукує числовий індекс, бути джерелом криміналістичного знання, якщо його внутрішня логіка залишається прихованою від суб'єкта процесуального пізнання? У цьому зв'язку алгоритмічний аудит набуває статусу гносеологічного запобіжника, що забезпечує прозорість і легітимність використання CIMR у правовій практиці. Ефективний аудит має багаторівневу структуру, яка демонструє еволюцію від вузького тестування точності до комплексної системи пізнавальних і правових гарантій.

Запропонована модель багаторівневого аудиту (Таблиця 1), як можна помітити, не є самодостатньою у відриві від інституційного та технологічного контексту. Вона створює гносеологічний фундамент для переходу від теоретичного обґрунтування індексу CIMR до його практичного застосування, проте реалізація окреслених рівнів контролю – насамперед юридичного та технічного неможлива без інтеграції алгоритму у вже існуючу державну цифрову інфраструктуру. Отже, CIMR слід розглядати не як автономне програмне рішення, а як елемент цілісного простору правоохоронної діяльності, де технологічні та правові механізми взаємодіють у межах єдиної екосистеми. У цьому зв'язку слушною є позиція С. Г. Гордієнка та І. М. Дороніна, які наголошують, що правове регулювання штучного інтелекту в Україні має враховувати інтереси національної безпеки, що передбачає створення прозорих механізмів взаємодії державних інформаційних ресурсів [3, с. 134]. Перехід від експериментального використання індексу CIMR до його повноцінної імплементації у практику правоохоронних органів зумовлює необхідність інтеграції цього інструменту у національну цифрову екосистему. У вітчизняних умовах такою інфраструктурною основою виступає система міжвідомчого електронного обміну даними «Трембіта», яка забезпечує захищену взаємодію державних реєстрів та інформаційно-аналітичних ресурсів [16]. Відтак CIMR постає не як ізольований алгоритм, а як компонент міжреєстрової архітектури, що дозволяє

Таблиця 1

Структурно-функціональна модель багаторівневого алгоритмічного аудиту індексу CIMR

Рівень аудиту	Зміст та завдання	Гносеологічна функція
Технічний [12]	Перевірка точності алгоритму на локальних даних, контроль стабільності та відтворюваності результатів.	Забезпечує базову верифікацію, але не гарантує пізнавальної валідності без подальших рівнів.
Соціальний [13]	Аналіз упередженості (bias) щодо демографічних груп, мінімізація дискримінаційних ефектів.	Проблематизує ілюзію «нейтрального алгоритму», показує залежність результатів від соціального контексту.
Юридичний [14]	Оцінка процесуальної придатності, обмеження використання індексу як аналітичного інструменту, а не доказу вини.	Встановлює межі легітимності, інтегрує імовірнісні моделі у правову систему без руйнування її категоричності.
Гносеологічний [15]	Використання XAI (Grad-CAM карт) для візуалізації архітектурних зв'язків у відбитках.	Перетворює «чорну скриньку» на інтерпретовану модель, відкриває новий рівень криміналістичного пізнання.

здійснювати аналіз біометричної інформації без дублювання баз даних та з дотриманням принципів цілісності, мінімізації доступу й трасованості запитів. Функціонально «Трембіта» може бути осмислена як технологічний шлюз, який відкриває контрольований доступ аналітичних підрозділів до дактилоскопічних, міграційних та процесуальних даних, що перебувають у розпорядженні МВС, Державної міграційної служби та органів правосуддя [10]. У прикладному вимірі це створює передумови для формування динамічного кримінологічного профілю особи, який оновлюється у режимі реального часу на основі надходження нових біометричних слідів [13]. На відміну від статичних дактилоскопічних карт, такий профіль має імовірнісний характер і відображає не лише факт ідентифікації, а й ступінь залученості особи до потенційно серійної злочинної активності [7]. Отже, для аналітичних підрозділів МВС це означає можливість переходу від реактивної моделі реагування до превентивного кримінологічного аналізу, що якісно змінює тактику протидії серійній злочинності. У цьому контексті інтеграція CIMR у цифровий простір держави актуалізує питання правового регулювання доступу до імовірнісних біометричних індексів. Використання таких показників має бути чітко відмежоване від процесуальної ідентифікації та розглядатися виключно як аналітично-орієнтуючий інструмент [12]. Відтак поєднання CIMR із механізмами алгоритмічного аудиту та пояснювального штучного інтелекту (XAI) дозволяє забезпечити баланс між ефективністю кримінологічного прогнозування та гарантіями прав людини.

Водночас критичною умовою успішного функціонування CIMR у межах міжвідомчого обміну є уніфікація технічних вимог до біометричних даних. Оскільки розрахунок індексу базується на аналізі мікроструктур папілярних ліній, архітектура «Трембіти» має забезпечувати передачу зображень із роздільною здатністю не менше 1000 DPI [17]. Стандартизація цифрових копій слідів у безвтратних форматах (RAW або PNG) постає як необхідний технічний регламент, без якого алгоритмічний аудит технічного рівня зафіксує критичне зростання похибок [18]. Незважаючи на високу прогностичну цінність індексу CIMR, його практична імплементація потребує врахування певних обмежень. Зокрема, ретроспективний аналіз архівних баз даних може бути ускладнений через недостатню роздільну здатність старих дактилоскопічних карток (500 DPI та нижче). Крім того, імовірнісний характер CIMR-висновків виключає їх використання як самостійних судових доказів, залишаючи за ними статус аналітично-орієнтуючої інформації, що потребує верифікації через багаторівневий алгоритмічний аудит та професійну інтерпретацію експертом. Такий збалансований підхід дозволяє інтегрувати ШІ у правове поле без порушення принципів процесуальної достовірності [9], [19]. Таким чином, інтеграція індексу CIMR у національну цифрову інфраструктуру правоохоронних органів створює передумови для якісного оновлення аналітичних можливостей держави у протидії серійній злочинності. У поєднанні з платформою «Трембіта» він може стати елементом нової моделі цифрової криміналогії, у межах якої біометричні дані використовуються не лише для ідентифікації минулих подій, а й для прогнозування та попередження злочинної активності.

Висновки. Проведене дослідження засвідчує, що концепція кримінологічного індексу міжпальцевої спорідненості (CIMR) постає як гносеологічний інструмент, здатний трансформувати парадигму кримінологічної ідентифікації. Відхід від догми абсолютної унікальності окремого відбитка відкриває шлях до системного аналізу біометричних закономірностей, що уможливлює виявлення латентної серійності злочинів та моделювання зв'язків між епізодами злочинної діяльності. Ключову роль у цьому процесі відіграє методологія алгоритмічного аудиту, яка забезпечує технічну точність, соціальну неупередженість та юридичну інтерпретованість результатів, гарантуючи їхню кримінологічну валідність.

Наукова новизна роботи полягає в обґрунтуванні CIMR як напряму кримінологічного прогнозування, що інтегрує когнітивні моделі штучного інтелекту в кримінально-процесуальну практику. Практичне значення дослідження визначається розробкою протоколів впровадження пояснювального ШІ (XAI) та процедур алгоритмічного контролю у національні дактилоскопічні системи, що мінімізує ризики дискримінації та помилок інтерпретації. Резюмуючи, CIMR не замінює експерта, а формує нову когнітивну основу для кримінологічного пізнання, де біометричні дані стають джерелом стратегічного прогнозування злочинної активності.

Перспективи подальших досліджень полягають у верифікації CIMR на великих масивах національних дактилоскопічних баз, у розробці міждисциплінарних методів оцінки його валідності

та у створенні нормативних рамок для інтеграції алгоритмічного аудиту в систему кримінального судочинства. Це дозволить не лише підтвердити наукову достовірність індексу, але й забезпечити його практичну ефективність у реальних умовах розслідування.

Список літератури:

1. Galton F. Finger prints. Amherst, New York: Prometheus Books, 2006. 191 p.
2. Джужа О.М. Запобігання злочинам: кримінолого-віктимологічна парадигма: монографія. Київ: Нац. акад. внутр. справ, 2015. 331 с.
3. Jain A.K., Ross A., Nandakumar K. Introduction to Biometrics. New York: Springer, 2011. 312 p.
4. Maltoni D., Maio D., Jain A.K., Prabhakar S. Handbook of Fingerprint Recognition. Springer, 2009. 494 p.
5. Cappelli R. Fast and accurate fingerprint indexing based on ridge orientation and frequency. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics). 2011. Vol. 41, № 6. P. 1511–1521. DOI: 10.1109/TSMCB.2011.2155648.
6. Gao G., Cao K., Zhou J., Jain A.K. Fingerprint indexing based on minutiae and ridge pattern. IEEE Transactions on Information Forensics and Security. 2019. Vol. 14, № 6. P. 1506–1520. DOI: 10.1109/TIFS.2018.2885284.
7. Go H., Lee S., Kim J. Inter-finger correlation in fingerprint patterns: a deep learning approach. Neurocomputing. 2021. Vol. 452. P. 256–264. DOI: 10.1016/j.neucom.2020.07.143.
8. Diniz M.A. Statistical methods for validation of predictive models. Journal of Nuclear Cardiology. 2022. Vol. 29, Issue 6. P. 3248–3255. DOI: 10.1007/s12350-022-02994-7.
9. Doshi-Velez F., Kim B. Towards a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608. 2017. URL: https://arxiv.org/abs/1702.08608.
10. Про Національну поліцію: Закон України від 2 липня 2015 р. № 580-VIII. URL: http://zakon.rada.gov.ua/laws/show/580-19.
11. Пилипчук В.Г., Доронін І.М. Право національної безпеки та військове право: теоретичні та прикладні засади становлення і розвитку в Україні. Інформація і право. 2018. № 2(25). С. 62–73. URL: http://ippi.org.ua/sites/default/files/18pvgvru.pdf.
12. Jain A.K., Ross A., Prabhakar S. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology. 2004. Vol. 14, № 1. P. 4–20.
13. Alhammad M., Moreno A. Algorithmic bias in biometric systems: a criminological perspective. Neurocomputing. 2021. Vol. 452. P. 256–264.
14. Гордієнко С.Г., Доронін І.М. Правові проблеми використання технологій штучного інтелекту у контексті забезпечення національної безпеки України. Інформація і право. 2024. № 2(49). С. 128–138.
15. Selvaraju R.R., Cogswell M., Das A., Vedantam R., Parikh D., Batra D. Grad-CAM: visual explanations from deep networks via gradient-based localization. Proceedings of the IEEE International Conference on Computer Vision (ICCV). 2017. P. 618–626.
16. Трембіта: система міжвідомчого електронного взаємодії органів виконавчої влади України. URL: https://trembita.gov.ua/about.
17. NIST Special Database 300. NIST Fingerprint Image Database. National Institute of Standards and Technology. 2015. URL: https://www.nist.gov/itl/iad/image-group/nist-special-database-300.
18. ISO/IEC 19794-4:2011. Information technology – Biometric data interchange formats – Part 4: Finger image data. Geneva: International Organization for Standardization, 2011. 54 p.
19. ISO/IEC 2382:2015. Information technology – Vocabulary – Artificial intelligence. Geneva: International Organization for Standardization, 2015. 41 p.

Horielova V. Yu. ARTIFICIAL INTELLIGENCE IN CRIMINOLOGICAL IDENTIFICATION: INTERFINGER RELATEDNESS INDEX AND ALGORITHMIC AUDIT

The article examines and substantiates the concept of the Criminological Interfinger Relatedness Index (CIMR) as a novel probabilistic instrument of criminological analysis aimed at identifying latent criminal seriality through the systematic interpretation of biometric data. It is emphasised that the application of deep learning methods and neural network models in dactyloscopy enables the identification of structural similarity between different fingers of the same individual, which fundamentally alters the traditional conception of the absolute discreteness of each fingerprint. Attention is drawn to the fact that classical forensic identification methodologies focus on the analysis of minutiae as local features, whereas contemporary algorithmic approaches operate on the architecture of ridge structures, thereby opening up the possibility of probabilistic "stitching" of fragmented latent traces recorded across different episodes of criminal activity. The necessity of revising the established standards of proof in the criminal procedure of Ukraine is noted in light of the

proliferation of algorithmic forms of evidentiary analysis; emphasis is also placed on the need to introduce mechanisms of algorithmic audit and explainable artificial intelligence in order to minimise the risks of discrimination, interpretative errors, and the improper use of probabilistic conclusions. It is substantiated that the use of the CIMR index transforms dactyloscopy from an auxiliary means of individual identification into a strategic instrument of criminological forecasting capable of modelling networked relationships between offences and forms of criminal activity. The scientific novelty lies in the introduction of the CIMR index and in the development of an algorithm for its operationalisation within the criminological practice of Ukraine. Recommendations are proposed for improving pre-trial investigation through the integration of XAI, algorithmic oversight procedures, and interpretable models for assessing biometric relatedness into national law enforcement databases.

Key words: *artificial intelligence, explainable AI (XAI), biometric validity, criminological profiling, latent criminal seriality, Interfinger Relatedness Index (CIMR), algorithmic audit.*

Дата першого надходження статті до видання: 03.12.2025
Дата прийняття статті до друку після рецензування: 25.12.2025
Дата публікації (оприлюднення) статті: 30.12.2025