УДК 343.98:004.056
DOI https://doi.org/10.32782/2078-3566-2026-2-20

Едуард РИЖКОВ
кандидат юридичних наук, професор
(Дніпровський державний університет внутрішніх справ,
м. Дніпро, Україна)
ORCID ID: https://orcid.org/0000-0002-6661-4617
eduard.ryzhkov@dduvs.edu.ua

ПРИКЛАДНІ АСПЕКТИ ВПРОВАДЖЕННЯ У ПРАВООХОРОННУ ДІЯЛЬНІСТЬ МЕТОДИКИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ЗА КЛАВІАТУРНИМ ПОЧЕРКОМ (ЗА МАТЕРІАЛАМИ ПАТЕНТУ № 130372)

У статті досліджено прикладні аспекти використання поведінкової біометрії, зокрема клавіатурного почерку, в оперативно-розшуковій, слідчій та експертно-криміналістичній діяльності. Базуючись на архітектурі патенту України № 130372 «Пристрій біометричної ідентифікації особи по клавіатурному почерку», автор розглядає потенціал трансформації апаратно-програмного рішення у дієвий правоохоронний інструмент. У роботі структуровано ключові напрями застосування методики: як засобу безперервної багатофакторної автентифікації для захисту відомчих інформаційних ресурсів; як інструменту профілювання для складання психоемоційного та соціально-демографічного портрета користувача; як негласного засобу оперативно-розшукової діяльності (для деанонімізації організаторів шахрайських кол-центрів та злочинів у сфері віртуальних активів); як основи для створення новітнього криміналістичного комплексу з метою формування електронної доказової бази відповідно до вимог КПК України. Окрему увагу приділено питанням трансферу технологій – алгоритму запровадження наукової розробки у практичну площину підрозділів Національної поліції України, зокрема Департаменту кіберполіції. Зроблено висновок, що клавіатурна динаміка є високоефективним, безперервним цифровим слідом, який за умови правильної процесуальної фіксації здатен суттєво підвищити ефективність протидії організованій кіберзлочинності.

Ключові слова: *клавіатурний почерк, поведінкова біометрія, кіберзлочинність, оперативно-розшукова діяльність, електронні докази, багатофакторна автентифікація, патент № 130372, криміналістична ідентифікація.*

Постановка проблеми. Стрімка цифровізація суспільства та перехід організованої злочинності у кіберпростір ставлять перед правоохоронною системою України безпрецедентні виклики. Традиційні методи ідентифікації злочинців дедалі частіше виявляються неефективними через масове використання зловмисниками анонімайзерів, VPN-сервісів, криптографічного захисту та підроблених цифрових ідентифікаторів. Особливої гостроти набуває проблема деанонімізації операторів тіньових ринків, адміністраторів шахрайських кол-центрів та осіб, причетних до злочинів із використанням віртуальних активів (блокчейн-технологій). За цих умов критичного значення набуває пошук нових, невідірваних від фізичної особи цифрових слідів. Одним із таких маркерів є поведінкова біометрія, зокрема клавіатурний почерк. Розроблення та патентування вітчизняними науковцями інноваційних рішень у цій сфері (зокрема, патенту України № 130372) створюють міцне технологічне

підґрунтя. Однак виникає нагальна науково-практична проблема: як саме трансформувати інженерно-технічний винахід у легітимний, ефективний та доказовий інструмент поліцейської діяльності.

Аналіз публікацій, у яких започатковано вирішення цієї проблеми. Питання використання цифрових слідів та біометричної автентифікації у криміналістиці активно досліджуються у працях вітчизняних та зарубіжних учених. Правовим аспектам кібербезпеки та електронних доказів присвячено роботи В. Білоуса, М. Карчевського, В. Носова, Ю. Орлова, В. Шепітька, П. Біленчука, О. Хахановського. Технічні та алгоритмічні засади ідентифікації за клавіатурним почерком глибоко розкрито у дослідженнях А. Грєхова, С. Євсєєва, О. Кузнецова, В. Лахно, В. Хорошко, І. Цимперідіса (I. Tsimperidis), Р. Джойса (R. Joyce), Г. Гупти (G. Gupta), а також у попередніх працях автора цієї статті у співавторстві з В. Мирошниченком. Разом із тим комплексне бачення імплементації конкретного запатентованого апаратно-програмного рішення у цілісну систему оперативно-розшукової та криміналістичної практики в Україні потребує окремого ґрунтовного аналізу.

Метою статті є визначення та наукове обґрунтування прикладних аспектів і напрямів використання можливостей методики ідентифікації за клавіатурним почерком (на базі патенту України № 130372) у практичній діяльності правоохоронних органів, а також розроблення алгоритму її технологічного трансферу.

Виклад основного матеріалу. На початку 2026 р. колективом науковців Дніпровського державного університету внутрішніх справ було отримано патент України на винахід № 130372 «Пристрій біометричної ідентифікації особи по клавіатурному почерку» [5]. Запропонована архітектура вирішує фундаментальну проблему «перекриття» клавіш (коли друга клавіша натискається до відпускання першої), створюючи безперервний потік високоточних часових інтервалів: часу утримання (DT) та інтервалу між натисканнями (FT) [5; 15]. Аналіз тактико-технічних можливостей методики дає змогу виокремити чотири магістральні напрями її впровадження в діяльність Національної поліції України.

По-перше, як інструмент багатофакторної ідентифікації та забезпечення внутрішньої кібербезпеки. Захист відомчих баз даних та державних реєстрів (таких як інформаційно-комунікаційна система «Інформаційний портал Національної поліції») є питанням національної безпеки. Традиційна система «логін-пароль» або навіть апаратні токени не захищають від ситуації, коли авторизований користувач залишає робоче місце (компрометація сесії) або коли пароль передається третім особам (корупційний ризик). Прикладом такої ситуації може слугувати одна з наймасштабніших кібератак на критичну інфраструктуру України під час повномасштабної війни – атаки на національного оператора «Київстар», яка відбулася у грудні 2023 р. Доступ до віртуальних серверів та баз даних національного мобільного оператора «Київстар» було реалізовано ворогом саме через заволодіння паролем до облікового запису одного з адміністраторів системи оператора. За даними Служби безпеки України (СБУ), до атаки причетна російська хакерська група «Solntsepyok» («Сонцепек»), яка вважається пов’язаною з Головним управлінням Генштабу ЗС РФ (ГРУ) [2]. Використання алгоритмів патенту № 130372 дає змогу впровадити парадигму Zero Trust (Нульової довіри) через механізм безперервної автентифікації. Система фоново аналізує мілісекундні затримки друку вільного тексту оперативником, аналітиком, слідчим або працівником інформаційно-аналітичного підрозділу. У разі виявлення аномалії (інша людина сіла працювати за клавіатуру) система миттєво блокує доступ до бази даних [17]. Це робить неможливим несанкціонований виток інформації навіть за наявності легітимних облікових даних.

По-друге, як інструмент складання психоемоційного та соціально-демографічного портрета особи. У ситуаціях, коли правоохоронці не мають еталонного зразка почерку підозрюваного (наприклад, анонімні мінування, кібербулінг, погрози в месенджерах), методика дає змогу здійснювати непряме профілювання [16, с. 15]. Сучасні системи

машинного навчання, що аналізують вектори затримок ($T_{press}, T_{release}$), здатні з високою часткою ймовірності визначати демографічні маркери: вікову групу, стать, домінуючу руку (правша/шульга) та навіть рівень освіти [18]. Окрім цього, клавіатурна динаміка є чутливим індикатором психоемоційного стану. Ритміка друку кардинально змінюється під впливом стресу, страху або когнітивного навантаження (наприклад, під час конструювання брехні). Отже, програмний комплекс може виконувати функцію дистанційного «поліграфа» при аналізі онлайн-листування під час проведення оперативної комбінації.

По-третє, як оперативно-розшуковий інструмент деанонімізації. Найбільш перспективним є використання методики як засобу отримання орієнтуючої інформації під час проведення негласних слідчих (розшукових) дій (НСРД) та оперативної розробки. Клавіатурний почерк є ідеальним пасивним цифровим фінгерпринтом. У протидії шахрайським кол-центрам організатори використовують віртуальні машини, проксі-сервери та підставні акаунти. Однак якщо оперативний підрозділ (наприклад, Департамент кіберполіції або Департамент стратегічних розслідувань) інтегрує алгоритми патенту у вигляді прихованого скрипта-обробника на фішинговий сайт, підконтрольний оперативникам, або у вигляді легалізованого «трояна» на етапі контролю за вчиненням злочину, з'являється можливість збирати біометричні профілі зловмисників. Згодом ці профілі порівнюються з активністю тих самих осіб у легальних сегментах мережі (або під час їх затримання та вилучення техніки), що дає змогу беззаперечно пов'язати анонімний крипто-гаманець чи Telegram-акаунт із конкретною фізичною особою [8].

По-четверте, як криміналістичний комплекс для формування доказової бази за КПК України. Отримані дані повинні мати доказову силу. Запровадження методики вимагає створення апаратно-програмного комплексу для експертних установ МВС (НДЕКЦ). Згідно зі ст. 99 КПК України, електронні документи є джерелом доказів [3]. Механізм формування доказової бази включає: а) перехоплення сирих логів клавіатури з жорсткого диску (або дампу оперативної пам'яті); б) криптографічне хешування вилучених логів для забезпечення їх незмінності; в) проведення слідчого експерименту (ст. 240 КПК), під час якого підозрюваний на імітаторі пристрою набирає текст; г) призначення судової комп'ютерно-технічної експертизи (а в перспективі – судово-біометричної), яка шляхом математичного порівняння доведе ідентичність патернів [4, с. 215]. Важливим аспектом є здатність систем на базі клавіатурного почерку відрізняти текст, набраний людиною, від тексту, згенерованого штучним інтелектом (наприклад, ChatGPT та ін.) або вставленого з буфера обміну [14]. Це руйнує типову лінію захисту підозрюваних: «Це писав не я, це діяв вірус або бот». У результаті отримуємо якісний емпіричний матеріал доказового характеру, що має своє електронне походження [12].

У науковому та прикладному аспекті для нас найбільший інтерес становить алгоритм трансферу технологій у практичну площину. Щоб перетворити патент № 130372 з наукового здобутку на звичайний інструмент поліцейського, необхідний чіткий механізм трансферу технологій [10; 11]. На нашу думку, алгоритм дій має включати в себе декілька етапів. Етап перший – програмна інкапсуляція. Спільно з фахівцями Департаменту кіберполіції та ДП «ІНФОТЕХ» необхідно перекласти апаратну логіку роботи пристрою (зсувні регістри, таймери) на мову програмного забезпечення. Потрібно створити: а) системні драйвери для endpoint-контролю (для внутрішньої безпеки); б) мережеві payload-модулі на JS/Python (для ОРД). Етап другий – валідація та сертифікація. Проведення закритих відомчих випробувань комплексу на базі ДНДІ МВС. Отримання експертних висновків ДССЗЗІ щодо відповідності КСЗІ (для захисту реєстрів). Етап третій – легалізація методик експертизи. Розроблення та реєстрація у Реєстрі методик проведення судових експертиз Міністерства юстиції України «Методики встановлення особи за динамічними параметрами клавіатурного вводу». Етап четвертий – нормативне врегулювання. Внесення доповнень до відомчих

наказів МВС, що регламентують порядок збору електронних доказів та використання засобів аналітичної розвідки (OSINT/SOCMINT).

Запропонований нами підхід повністю корелюється з положеннями стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 рр. та переходу Національної поліції на сучасну концепцію Intelligence-Led Policing (ILP) як поліцейської діяльності, керованою аналітикою, у частині використання новітніх інформаційно-аналітичних засобів у діяльності поліцейських підрозділів [6; 7]. Своєю чергою, такий широкий спектр трансферу наукової розробки відповідає сучасним інформаційно-технічним викликам у проявах організованої злочинності та зумовлює доцільність реалізації ефективних засобів протидії у рамках використання наукових знань із поведінкової біометрії [1; 9; 13].

Висновки. Таким чином, методика біометричної ідентифікації за клавіатурним почерком, архітектура якої розкрита у патенті № 130372, є потужним інноваційним ресурсом для правоохоронної діяльності. Її прикладний потенціал охоплює як сферу превенції (захист критичної інформаційної інфраструктури від внутрішніх загроз), так і сферу реакції (деанонімізація кіберзлочинців, профілювання та збір електронних доказів). Ураховуючи відносну простоту впровадження програмних аналогів цього пристрою (через відсутність потреби у складному специфічному апаратному забезпеченні на стороні підозрюваного), інтеграція цієї технології в арсенал Національної поліції України здатна кардинально змінити баланс сил у протидії організованій злочинності у цифровому середовищі. Реалізація запропонованого алгоритму трансферу технологій дасть змогу у стислі терміни перетворити наукову ідею на дієвий правоохоронний стандарт.

Список використаних джерел

1. Білоус В. В. Використання поведінкової біометрії у кіберкриміналістиці. *Теорія і практика судової експертизи і криміналістики*. 2022. № 3. С. 45–52.

2. Васьків О. СБУ ідентифікувала хакерів російського ГРУ, які атакували «Київстар»: матеріали справи передадуть у Гаагу. URL: https://suspilne.media/720596-sbu-identifikuvala-hakeriv-rosijskogo-gru-aki-atakuvali-kiivstar-peredast-materiali-spravi-v-gaagu/

3. Кримінальний процесуальний кодекс України від 13.04.2012. *Відомості Верховної Ради України*. 2013. № 9–10. Ст. 88.

4. Пащенко Є. М., Чалий М. Г. Організаційно-правові засади протидії корупції у секторі безпеки і борони України на відомчому рівні. *Південноукраїнський правничий часопис*. 2022. Ч. 3. С. 213–216.

5. Пристрій біометричної ідентифікації особи по клавіатурному почерку / В. О. Мирошниченко та ін. Патент України на винахід № 130372, опубліковано 04.02.2026, Бюл. № 5/2026.

6. Про затвердження Концепції запровадження моделі поліцейської діяльності, керованої аналітикою (ILP) у діяльність Національної поліції України : Наказ Національної поліції України від 10.06.2020 № 424.

7. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки : Указ Президента України від 11.05.2023 № 273/2023. URL: https://zakon.rada.gov.ua/laws/show/273/2023#Text

8. Про оперативно-розшукову діяльність : Закон України від 18.02.1992. *Відомості Верховної Ради України*. 1992. № 22. Ст. 303.

9. Рижков Е. В. Інноваційні методи біометричної ідентифікації за клавіатурним почерком у системі заходів протидії організованій злочинності (за матеріалами патенту № 130372). *Актуальні питання діяльності Національної поліції як суб'єкта протидії організованій злочинності* : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 02.04.2026. Кропивницький : ДонДУВС, 2026. С. 286–290.

10. Рижков Е. В., Мирошниченко В. О. Патентна діяльність як предмет трансферу технологій (на прикладі патенту на корисну модель «Пристрій радіолокаційного розпізнавання об'єктів»). *Сучасні інформаційні технології у діяльності Національної поліції України* : матеріали Всеукр. наук.-практ. семінару, м. Дніпро, 26.11.2020. Дніпро : ДДУВС, 2020. С. 32–33.

11. Рижков Е. В., Мирошниченко В. О. Трансфер технологій у частині патентної діяльності як запорука успіху відомчої науки та освіти. *Інформаційні технології в освіті та практиці* : матеріали Всеукр. наук.-практ. конф., м. Львів, 18.12.2020. Львів : ЛьвДУВС, 2020. С. 13–14.

12. Хахановський В. Г. Електронні докази: проблеми теорії та практики використання у кримінальному судочинстві. Київ : Нац. акад. внутр. справ, 2021. 240 с.

13. Continuous Authentication using Behavioral Biometrics. *IEEE Access*, 2023. Vol. 11. P. 11245–11260.

14. Keystroke Dynamics for User Identification – IDEAS/RePEc. URL: https://ideas.repec.org/h/spr/sprchp/978-3-031-83157-7_21.html

15. Keystroke Dynamics for User Identification. *ResearchGate.* URL: https://www.researchgate.net/publication/391594241_Keystroke_Dynamics_for_User_Identification

16. Tsimperidis I. Classifying Users through Keystroke Dynamics. *Democritus University of Thrace*. URL: http://tsimperidis.cs.duth.gr/wp-content/uploads/pdfs/Classifying%20Users%20through%20Keystroke%20Dynamics.pdf

17. US8332932B2 – Keystroke dynamics authentication techniques. Google Patents. URL: https://patents.google.com/patent/US8332932B2/en

18. Users' identification through keystroke dynamics based on vibration parameters and keyboard pressure. *ResearchGate.* URL: https://www.google.com/search?q=https://www.researchgate.net/publication/325341000_users_identification_through_keystroke_dynamics_based_on_vibration_parameters_and_keyboard_pressure

References

1. Bilous, V. V. (2022) Vykorystannya povedinkovoyi biometriyi v kiberkryminalistytsi [The use of behavioral biometrics in cybercriminology]. *Teoriya i praktyka sudovoyi ekspertyzy i kryminalistyky*. № 3, pp. 45–52. [in Ukr.].

2. Vaskiv, O. SBU identyfikuvala khakeriv rosiyskoho HRU, yaki atakuvaly «Kyyivstar»: materialy spravy peredadut v Haahu [SSU identified hackers of the Russian GRU who attacked Kyivstar: case materials will be transferred to The Hague]. Retrieved from: https://suspilne.media/720596-sbu-identifikuvala-hakeriv-rosijskogo-gru-aki-atakuvali-kiivstar-peredast-materiali-spravi-v-gaagu/ [in Ukr.].

3. Kryminalnyy protsesualnyy kodeks Ukrayiny vid 13.04.2012 [Criminal Procedure Code of Ukraine of 13.04.2012]. *Vidomosti Verkhovnoyi Rady Ukrayiny*. 2013. № 9–10, art. 88. [in Ukr.].

4. Pashchenko, Ye. M., Chalyy, M. H. (2022) Orhanizatsiyno-pravovi zasady protydiyi koruptsiyi v sektori bezpeky i borony Ukrayiny na vidomchomu rivni [Organizational and legal principles of combating corruption in the security and defense sector of Ukraine at the departmental level]. *Pivdennoukrayinskyy pravnychyy chasopys.* Part 3, pp. 213–216. [in Ukr.].

5. Prystriy biometrychnoyi identyfikatsiyi osoby po klaviaturnomu pocherku [Device for biometric identification of a person by keyboard handwriting] / V. O. Myroshnychenko, E. V. Ryzhkov, Yu. P. Synytsina, S. O. Prokopov et al. Patent Ukrayiny na vynakhid № 130372, opublikovano 04.02.2026, Byul. № 5/2026. [in Ukr.].

6. Pro zatverdzhennya Kontseptsiyi zaprovadzhennya modeli politseyskoyi diyalnosti, kerovanoyi analitykoyu (ILP) u diyalnist Natsionalnoyi politsiyi Ukrayiny [On approval of the Concept of introducing the model of policing guided by analytics (ILP) into the activities of the National Police of Ukraine] : nakaz Natsionalnoyi politsiyi Ukrayiny vid 10.06.2020 № 424. [in Ukr.].

7. Pro Kompleksnyy stratehichnyy plan reformuvannya orhaniv pravoporyadku yak chastyny sektoru bezpeky i oborony Ukrayiny na 2023–2027 roky [On the Comprehensive Strategic Plan for Reforming Law Enforcement Agencies as Part of the Security and Defense Sector of Ukraine for 2023–2027] : zatv. Ukazom Prezydenta Ukrayiny vid 11.05.2023 № 273/2023. Retrieved from: https://zakon.rada.gov.ua/laws/show/273/2023#Text [in Ukr.].

8. Pro operatyvno-rozshukovu diyalnist [On Operational-Search Activities] : Zakon Ukrayiny vid 18.02.1992. *Vidomosti Verkhovnoyi Rady Ukrayiny*. 1992. № 22, art. 303. [in Ukr.].

9. Ryzhkov, E. V. (2026) Innovatsiyni metody biometrychnoyi identyfikatsiyi za klaviaturnym pocherkom u systemi zakhodiv protydiyi orhanizovaniy zlochynnosti (za materialamy patentu № 130372) [Ryzhkov E. V. Innovative methods of biometric identification by keyboard handwriting in the system of measures to combat organized crime (based on patent No. 130372)]. *Aktualni pytannya diyalnosti Natsionalnoyi politsiyi yak subyekta protydiyi orhanizovaniy zlochynnosti* : materialy Vseukr. nauk.-prakt. konf. (m. Kropyvnytskyy, 02.04.2026). Kropyvnytskyy : DonDUVS, pp. 286–290. [in Ukr.].

10. Ryzhkov, E. V., Myroshnychenko, V. O. (2020) Patentna diyalnist yak predmet transferu tekhnolohiy (na prykladi patentu na korysnu model «Prystriy radiolokatsiynoho rozpiznavannya obyektiv») [Patent activity as a subject of technology transfer (on the example of a patent for a utility model "Device for radar recognition of objects")]. *Suchasni informatsiyi tekhnolohiyi v diyalnosti Natsionalnoyi politsiyi Ukrayiny* : materialy Vseukr. nauk.-prakt. seminaru (m. Dnipro, 26.11.2020). Dnipro : DDUVS, pp. 32–33. [in Ukr.].

11. Ryzhkov, E. V., Myroshnychenko, V. O. (2020) Transfer tekhnolohiy v chastyni patentnoyi diyal′nosti yak zaporuka uspikhu vidomchoyi nauky ta osvity [Technology transfer in the part of patent activity as a guarantee of the success of departmental science and education]. *Informatsiyni tekhnolohiyi v osviti ta praktytsi* : materialy Vseukr. nauk.-prakt. konf. (m. Lviv, 18.12.2020). Lviv : LvDUVS, pp. 13–14. [in Ukr.].

12. Khakhanovskyy, V. H. (2021) Elektronni dokazy: problemy teoriyi ta praktyky vykorystannya u kryminalnomu sudochynstvi [Electronic evidence: problems of theory and practice of use in criminal proceedings]. Kyiv : Nats. akad. vnutr. sprav, 240 p. [in Ukr.].

13. Continuous Authentication using Behavioral Biometrics. IEEE Access, 2023. Vol. 11. P. 11245–11260.

14. Keystroke Dynamics for User Identification – IDEAS/RePEc. Retrieved from: https://ideas.repec.org/h/spr/sprchp/978-3-031-83157-7_21.html

15. Keystroke Dynamics for User Identification. ResearchGate. Retrieved from: https://www.researchgate.net/publication/391594241_Keystroke_Dynamics_for_User_Identification

16. Tsimperidis I. Classifying Users through Keystroke Dynamics. Democritus University of Thrace. Retrieved from: http://tsimperidis.cs.duth.gr/wp-content/uploads/pdfs/Classifying%20Users%20through%20Keystroke%20Dynamics.pdf

17. US8332932B2 – Keystroke dynamics authentication techniques. Google Patents. Retrieved from: https://patents.google.com/patent/US8332932B2/en

18. Users' identification through keystroke dynamics based on vibration parameters and keyboard pressure. ResearchGate. Retrieved from: https://www.google.com/search?q=https://www.researchgate.net/publication/325341000_users_identification_through_keystroke_dynamics_based_on_vibration_parameters_and_keyboard_pressure

ABSTRACT

Eduard Ryzhkov. Applied aspects of implementing biometric identification methods based on keyboard handwriting in law enforcement activities (based on the patent No. 130372)

The article deals with applied aspects of the use of behavioral biometrics, in particular keyboard handwriting, in operational-search, investigative and expert-forensic activities. Based on the architecture of the patent of Ukraine No. 130372 "Device for biometric identification of a person by keyboard handwriting", the author considers the potential for transforming a hardware-software solution into an effective law enforcement tool.

The paper structures the key areas of application of the methodology: as a means of continuous multi-factor authentication to protect departmental information resources; as a profiling tool for compiling a psycho-emotional and socio-demographic portrait of the user; as a covert means of operational-search activities (for de-anonymization of organizers of fraudulent call centers and crimes in the field of virtual assets); as well as the basis for creating a new forensic complex for the purpose of forming an electronic evidence base in accordance with the requirements of the Code of Criminal Procedure of Ukraine. Special attention is paid to the issues of technology transfer – the algorithm for introducing scientific development into the practical plane of the units of the National Police of Ukraine, in particular the Cyber Police Department. It is concluded that keyboard dynamics is a highly effective, continuous digital trace, which, provided that it is correctly procedurally recorded, can significantly increase the effectiveness of combating organized cybercrime.

Keywords*: keyboard handwriting, behavioral biometrics, cybercrime, operational and investigative activities, electronic evidence, multi-factor authentication, patent No. 130372, forensic identification.*

Дата першого надходження статті до видання: 07.04.2026
Дата прийняття статті до друку після рецензування: 03.05.2026
Дата публікації (оприлюднення) статті: 28.08.2026