ПРОБЛЕМИ ПРАВООХОРОННОЇ ТА ПРАВОЗАХИСНОЇ ДІЯЛЬНОСТІ

УДК 343.98
DOI https://doi.org/10.32782/2521-6473.2026-1.13

Л. І. Аркуша, доктор юридичних наук, професор,
професор кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»
ORCID: 0000-0002-0422-6416

О. В. Чернов, доктор філософії в галузі права,
доцент кафедри криміналістики, судових експертиз та поліграфології
Національного університету «Одеська юридична академія»
ORCID: 0009-0002-6038-9479

О. В. Дикий, кандидат юридичних наук, доцент,
доцент кафедри кримінального процесу
Національного університету «Одеська юридична академія»
ORCID: 0000-0001-9659-9350

ІДЕНТИФІКАЦІЯ СУБ'ЄКТІВ КІБЕРЗЛОЧИНІВ ШЛЯХОМ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ПОВЕДІНКОВИХ ЦИФРОВИХ СЛІДІВ

У статті здійснено комплексний науково-теоретичний та прикладний аналіз проблем ідентифікації суб'єктів кіберзлочинів шляхом інтелектуального аналізу поведінкових цифрових слідів у контексті сучасних викликів криміналістики та кримінального процесу. Обґрунтовано, що стрімка цифровізація суспільних відносин, зростання латентності кіберзлочинності, масове використання засобів анонімізації та багаторівнева інфраструктура кібератак істотно знижують ефективність традиційних підходів до встановлення особи правопорушника, орієнтованих переважно на технічні або матеріальні сліди. У зв'язку з цим акцентовано увагу на поведінкових цифрових слідах як особливому різновиді криміналістично значущої інформації, що відображає стійкі патерни взаємодії суб'єкта з інформаційно-комунікаційними системами та здатна виконувати індивідуалізуючу функцію навіть за умов технічної деанонімізації.

Розкрито сутність поведінкових цифрових слідів, їх місце у слідовій картині кіберзлочину та значення для побудови профілю невстановленого суб'єкта, розмежування ролей співучасників і формування обґрунтованих слідчих версій. Проаналізовано можливості застосування інтелектуального аналізу, зокрема методів машинного навчання, кластеризації, аналізу послідовностей, стилометрії та кореляції подій, для виявлення прихованих закономірностей у масивах цифрових даних і моделювання цифрової поведінки правопорушників. Наголошено, що алгоритмічні результати мають ймовірнісний характер і потребують криміналістичної інтерпретації, експертної верифікації та інтеграції з іншими видами доказів.

Окрему увагу приділено проблемам надійності, пояснюваності та процесуальної допустимості результатів інтелектуального аналізу поведінкових цифрових слідів, а також ризикам хибної атрибуції, упередженості моделей і порушення прав людини. Обґрунтовано необхідність формування уніфікованих криміналістичних підходів і методичних рекомендацій щодо використання поведінкової аналітики у кримінальному провадженні з метою забезпечення балансу між ефективністю розслідування та дотриманням принципів законності, змагальності й справедливого судового розгляду. Зроблено висновок про перспективність подальшого розвитку цього напряму як складової модернізації криміналістичного інструментарію протидії кіберзлочинності.

Ключові слова: *кіберзлочинність, ідентифікація суб'єкта злочину, злочинна поведінка, цифрові сліди, кримінальне провадження, версії, організована злочинність, інтелектуальний аналіз, машинне навчання, криміналістична атрибуція, докази, злочин.*

L. I. Arkusha, O. V. Chernov, O. V. Dykyi. Identification of cybercriminals through intellectual analysis of behavioural digital trails

The article provides a comprehensive scientific, theoretical and applied analysis of the problems of identifying cybercriminals through intelligent analysis of behavioural digital traces in the context of contemporary challenges in criminalistics and criminal procedure. It is argued that the rapid digitalisation of social relations, the growth of latent cybercrime, the widespread use of anonymisation tools and the multi-level infrastructure of cyberattacks significantly reduce the effectiveness of traditional approaches to identifying offenders, which are mainly focused on technical or material traces. In this regard, attention is focused on behavioural digital traces as a special type of criminally significant information that reflects stable patterns of interaction between the subject and information and communication systems and is capable of performing an individualising function even under conditions of technical de-anonymisation.

The essence of behavioural digital traces, their place in the trace pattern of cybercrime and their significance for building a profile of an unidentified subject, distinguishing the roles of accomplices and forming reasonable investigative versions are revealed. The possibilities of applying intelligent analysis, in particular machine learning methods, clustering, sequence analysis, stylometry and event correlation, to identify hidden patterns in digital data arrays and model the digital behaviour of offenders are analysed. It is emphasised that algorithmic results are probabilistic in nature and require forensic interpretation, expert verification and integration with other types of evidence.

Particular attention is paid to the issues of reliability, explainability and procedural admissibility of the results of intellectual analysis of behavioural digital traces, as well as the risks of misattribution, model bias and human rights violations. The need to develop unified forensic approaches and methodological recommendations for the use of behavioural analytics in criminal proceedings is justified in order to ensure a balance between the effectiveness of investigations and compliance with the principles of legality, adversarial proceedings and fair trial. It is concluded that further development of this area is promising as part of the modernisation of forensic tools for combating cybercrime.

Key words: *cybercrime, identification of the perpetrator, criminal behaviour, digital traces, criminal proceedings, investigative hypotheses, organized crime, intellectual analysis, machine learning, forensic attribution, evidence, crime.*

Постановка проблеми. Стрімке зростання кіберзлочинності, її транскордонний характер, високий рівень технологічної адаптивності правопорушників та масове використання засобів анонімізації істотно ускладнюють встановлення конкретних фізичних осіб, причетних до вчинення кримінальних правопорушень у кіберпросторі. Традиційні криміналістичні підходи до ідентифікації суб'єкта злочину, зорієнтовані переважно на матеріальні сліди або на прямі технічні індикатори (IP-адреси, пристрої, облікові записи), у цифровому середовищі часто не забезпечують належної доказової визначеності, оскільки такі індикатори легко піддаються підміні, делегуванню, використанню через скомпрометовані ресурси або фрагментації внаслідок багаторівневої інфраструктури атак. За цих умов особливого значення набувають поведінкові цифрові сліди як відносно стійкі патерни взаємодії суб'єкта з інформаційними системами, які відображають його навички, стиль діяльності, типові сценарії ухвалення рішень і можуть виконувати індивідуалізуючу функцію навіть тоді, коли технічна атрибуція є неповною або суперечливою.

Водночас науково-практична проблема полягає в тому, що використання поведінкових цифрових слідів для ідентифікації суб'єктів кіберзлочинів наразі не має достатньо усталеного криміналістичного й процесуального забезпечення. Відсутні уніфіковані критерії відбору та оцінки поведінкових ознак, не сформовано загальновизнаних методик їх інтелектуального (алгоритмічного) аналізу з позицій відтворюваності, верифікованості та пояснюваності результатів, а також не визначено межі доказової сили й допустимості висновків, отриманих на основі моделей машинного навчання та аналітики великих даних. Додаткову складність становлять ризики хибної кореляції, упередженості моделей, залежності результатів від якості та повноти даних, а також необхідність забезпечення балансу між ефективністю розслідування і гарантіями прав людини (приватність, захист персональних даних, справедливий суд).

Отже, проблематика полягає у наявності об'єктивної потреби в інтелектуалізації криміналістичного інструментарію ідентифікації кіберзлочинців на основі поведінкових цифрових слідів, за одночасної недостатності теоретико-методологічних та процесуально-правових засад, які б забезпечували надійність, перевірюваність і юридичну легітимність застосування таких підходів у кримінальному провадженні. Саме розв'язання цієї суперечності – між зростаючими можливостями поведінкової аналітики та вимогами криміналістичної доказовості й процесуальної допустимості – визначає актуальний напрям сучасних наукових пошуків і практичних розробок у сфері протидії кіберзлочинності.

Мета статті полягає у комплексному обґрунтуванні криміналістично значущих можливостей інтелектуального аналізу поведінкових цифрових слідів для ідентифікації суб'єктів кіберзлочинів, а також у визначенні концептуальних, методологічних і прикладних засад їх використання в кримінальному провадженні. Зазначена мета конкретизується через висвітлення сутності та структури поведінкових цифрових слідів, окреслення алгоритмічних підходів до їх виявлення, формалізації, порівняння та верифікації, встановлення критеріїв надійності й пояснюваності отриманих результатів, а також формулювання пропозицій щодо інтеграції таких результатів у систему доказування з урахуванням вимог процесуальної допустимості, забезпечення прав людини та мінімізації ризиків хибної атрибуції.

Виклад основного матеріалу. Інтенсифікація цифровізації суспільних відносин, стрімке зростання обсягів інформаційних потоків і трансформація соціальної взаємодії в онлайн-середовище зумовили якісно нові виклики для системи протидії злочинності. Кіберзлочинність, як одна з найбільш динамічних і латентних форм кримінальної діяльності, характеризується високим рівнем адаптивності, транскордонністю, технологічною складністю та специфічною конфігурацією слідів злочинної поведінки. У таких умовах класичні криміналістичні підходи до ідентифікації особи правопорушника виявляються недостатніми, що актуалізує потребу в розробленні та впровадженні інноваційних методів встановлення суб'єктів кіберзлочинів на основі аналізу цифрових поведінкових проявів. Особливого значення набуває інтелектуальний аналіз поведінкових цифрових слідів як міждисциплінарний напрям, що поєднує досягнення криміналістики, інформаційних технологій, кібербезпеки, психології, теорії штучного інтелекту, а також процесуальної доктрини доказування. Визначальним є те, що у кіберпросторі поведінкова активність суб'єкта набуває статусу інформаційного феномена, який підлягає вимірюванню, формалізації та інтерпретації, а відтак може бути використаний для побудови слідчих версій і доведення причетності конкретної особи до кримінального правопорушення.

Кіберзлочини відрізняються від традиційних форм кримінальної діяльності не лише способом вчинення, а й характером слідової картини, механізмом утворення слідів і структурою доказової інформації. Якщо у «класичних» злочинах домінують матеріальні відображення (сліди рук, взуття, знарядь, мікрочастинки тощо), то у кіберзлочинності ключовий масив відомостей формується в цифровому середовищі: це журнали подій (logs) операційних систем і прикладних сервісів, мережеві записи, телеметрія, метадані файлів і повідомлень, історія авторизацій, транзакційні ланцюги, резервні копії, дані мобільних пристроїв, артефакти браузерів, сліди взаємодії з хмарною інфраструктурою та іншими віддаленими ресурсами [1]. Такі сліди мають високу динамічність і мінливість: вони можуть автоматично перезаписуватися, знищуватися системними механізмами ротації, змінюватися внаслідок оновлень програмного забезпечення або мережевих перебоїв, а також навмисно піддаватися маніпуляції суб'єктом злочину. Водночас цифрові сліди характеризуються потенційною масовістю та багатоканальністю: одна дія в системі може породжувати одразу низку записів у різних джерелах, що, за умови належного збору й кореляції, підвищує вірогідність реконструкції подій і зменшує ризик хибних інтерпретацій.

Поведінкові цифрові сліди є особливим різновидом цифрових слідів, оскільки вони відображають не стільки «факт події», скільки спосіб діяльності, притаманний конкретному суб'єкту або групі суб'єктів. У цьому сенсі вони виступають функціональним аналогом криміналістично значущих навичок і звичок, які проявляються у стійких патернах дій. Поведінковий слід утворюється там, де цифрова активність набуває повторюваних ознак: типові часові інтервали входу в систему; регулярність звернень до певних сервісів; манера створення паролів або використання менеджерів паролів; спосіб організації файлів і директорій; характер командного рядка; вибір конкретних програм, утиліт, бібліотек; «почерк» програмування (іменування змінних, стиль коментарів, форматування, притаманна граматика повідомлень про помилки); лінгвістичні особливості спілкування у чатах; реакція на фактори ризику (наприклад, на появу попереджень безпеки, капчі, блокування акаунтів). Навіть якщо суб'єкт намагається приховати ідентичність через підміну IP-адрес, використання TOR, VPN або зламаних облікових записів, поведінкова складова часто залишається відносно стабільною, адже вона зумовлена рівнем компетентності, особистісними установками, професійним досвідом, «комфортними» інструментами та сформованими сценаріями роботи.

З криміналістичної позиції доцільно розглядати поведінкові цифрові сліди як систему ознак, що має часово-просторову прив'язку у цифровому середовищі, механізм утворення, носії фіксації та потенційні інформаційні «мішені». Така система підлягає ідентифікаційному аналізу, оскільки містить як загальні (родові) ознаки, що характеризують клас суб'єктів (наприклад, «новачок / професіонал», «скрипт-кідді / оператор ботнету», «інсайдер / зовнішній атакувальник»), так і індивідуалізуючі (видові) ознаки, що підвищують ймовірність прив'язки конкретних дій до конкретної особи. У практичній площині це означає, що результати аналізу поведінкових слідів можуть використовуватися у двох взаємодоповнювальних напрямах: по-перше, для побудови профілю невстановленого суб'єкта та формування слідчих версій; по-друге, для порівняльної ідентифікації, коли наявні відомості про підозрюваного зіставляються з цифровим «почерком», зафіксованим у матеріалах провадження.

Інтелектуальний аналіз поведінкових цифрових слідів становить сукупність методів і процедур, спрямованих на автоматизоване або напівавтоматизоване виявлення закономірностей у великих масивах даних. У традиційній логіці криміналістичного дослідження, слідчий або експерт здатен проаналізувати обмежену кількість артефактів, але у кіберінцидентах обсяги даних часто вимірюються гігабайтами та терабайтами: журнали подій, дампи пам'яті, пакети трафіку, записи SIEM-систем, дані з хмарних провайдерів. Тому виникає необхідність інтелектуалізації аналізу, тобто використання алгоритмів, які можуть швидко обробляти дані, виділяти значущі ознаки, будувати моделі поведінки та оцінювати ймовірність належності певного набору дій конкретному суб'єкту. Водночас «інтелектуальний аналіз» не зводиться лише до машинного навчання; він включає також експертні правила, графовий аналіз, кореляцію подій, семантичну обробку текстів, а за потреби – комбінування різних підходів (гібридні моделі), що підвищує стійкість результатів у складних слідчих ситуаціях.

Методологічною передумовою застосування інтелектуального аналізу є правильне визначення того, що саме виступає об'єктом моделювання. У контексті цієї теми об'єктом є цифрова поведінка суб'єкта – тобто послідовність його взаємодій із цифровими системами, відображена у множині подій. Подія у кіберсередовищі може розумітися як елементарний акт: спроба входу, створення процесу, виконання команди, звернення до API, запит до бази даних, відправлення повідомлення, зміна прав доступу, встановлення з'єднання, спроба ескалації привілеїв. Поведінка – це структурована послідовність таких подій, що має внутрішню логіку та цільову спрямованість. Для кіберзлочинів характерною є стадійність: розвідка, початкове проникнення, закріплення, розширення доступу, горизонтальне переміщення, ексфільтрація даних або шифрування (у випадку ransomware), маскування й утримання контролю. Виявлення поведінкових слідів передбачає, що кожна з цих стадій залишає специфічний набір ознак, а також переходи між стадіями мають певну повторюваність, пов'язану з навичками й «робочими звичками» суб'єкта.

У практиці розслідування кіберзлочинів особливе місце посідає встановлення співвідношення між технічною атрибуцією та персональною ідентифікацією [2]. Технічна атрибуція зазвичай спрямована на визначення джерела атаки на рівні інфраструктури: IP-адреси, домени, хости, мережеві маршрути, використані експлойти, відбитки шкідливого ПЗ, індикатори компрометації. Однак у багатьох випадках технічна атрибуція не дозволяє прямо назвати особу, оскільки інфраструктура може бути орендованою, скомпрометованою, підставною, а маршрутизація – багатоетапною. Саме тут поведінкова складова дозволяє «піднятися» на рівень суб'єктності: розпізнати стиль дій, оцінити рівень компетенції, виявити повторювані інструменти і робочі сценарії, які притаманні конкретному оператору чи групі. Таким чином, інтелектуальний аналіз поведінкових слідів виступає містком між технічним описом інциденту та криміналістичним завданням встановлення особи злочинця.

Змістовне наповнення поняття «поведінковий цифровий слід» доцільно деталізувати через його структурні компоненти. По-перше, це темпоральні ознаки: час активності, періодичність, часові вікна виконання операцій, затримки між діями, «ритм» сеансу. У багатьох випадках часові патерни можуть корелювати з часовим поясом, режимом роботи, навчальними чи професійними обов'язками, що опосередковано звужує коло пошуку. По-друге, це інструментальні ознаки: вибір операційної системи, мови програмування, фреймворків, засобів автоматизації, типових утиліт (сканери, експлойти, засоби підбору паролів, криптографічні бібліотеки). Навіть коли інструмент є загальнодоступним, спосіб його застосування, послідовність параметрів і налаштувань можуть мати індивідуалізуюче значення. По-третє, це комунікаційні та лінгвістичні ознаки: стиль повідомлень, типова лексика, граматичні конструкції, пунктуація, використання жаргону, мовні інтерференції. По-четверте, це стратегічні ознаки: характер ризик-менеджменту суб'єкта, ступінь обережності, наявність резервних планів, манера маскування, вибір цілей і критерії відбору жертв. По-п'яте, це структурно-логічні ознаки коду і сценаріїв: повторювані шаблони, улюблені конструкції, форматування, «почерк» документації. Сукупність таких компонентів дозволяє будувати багатовимірну модель, яка описує суб'єкта не тільки як технічну одиницю (джерело трафіку), а як носія певного стилю поведінки.

Ідентифікація суб'єктів кіберзлочинів на основі поведінкових слідів потребує розуміння того, які саме слідчі ситуації найбільш придатні для цього підходу. Найефективнішим він є у випадках серійності та повторюваності: багатоепізодні атаки на різні об'єкти, кампанії фішингу, розгортання шкідливого ПЗ, повторювані вторгнення в корпоративні мережі. У таких ситуаціях накопичується масив даних, що дозволяє виявити стійкі патерни. Водночас поведінковий аналіз цінний і при одиничних інцидентах, коли є потреба швидко класифікувати суб'єкта за рівнем компетенції та ймовірними мотивами, щоб спрямувати ресурс розслідування у правильному напрямі. Наприклад, атака може бути ініційована «внутрішнім» користувачем (інсайдером) або зовнішнім суб'єктом; поведінкові ознаки, такі як знання внутрішньої структури мережі, вибір критичних вузлів, специфічні облікові записи, можуть вказувати на інсайдерський характер, навіть якщо технічні параметри маскуються під зовнішнє вторгнення.

Окремої уваги потребує феномен групової суб'єктності у кіберзлочинності, коли протиправна діяльність здійснюється організованою групою з розподілом ролей. У таких випадках поведінкові сліди можуть належати різним операторам: один відповідає за первинний доступ, інший – за ескалацію привілеїв, третій – за ексфільтрацію, четвертий – за переговори з потерпілими. Інтелектуальний аналіз дозволяє здійснювати кластеризацію поведінкових патернів і відокремлювати активність різних осіб навіть у межах одного інциденту. Це має істотне значення для встановлення ролей співучасників, доведення організованості, а також визначення ступеня участі кожного суб'єкта. У криміналістичному сенсі це сприяє реконструкції механізму злочинної діяльності та підвищує точність процесуальної кваліфікації [3].

Технологічна реалізація інтелектуального аналізу поведінкових слідів передбачає використання різних класів алгоритмів. Методи навчання без учителя (кластеризація, виявлення аномалій) особливо корисні на початкових етапах, коли немає маркованих даних і треба виявити «підозрілу» активність серед великого потоку подій. Методи навчання з учителем (класифікація) застосовні тоді, коли існує база відомих профілів або коли в рамках конкретного провадження вже ідентифіковано частину дій як належні певному суб'єкту, і виникає потреба віднести інші дії до тієї ж особи. Графовий аналіз є ефективним для моделювання мережі зв'язків між об'єктами: акаунтами, IP-адресами, доменами, файлами, транзакціями, пристроями. Аналіз

послідовностей (зокрема методи, що враховують порядок подій) дозволяє розпізнавати типові сценарії атаки та індивідуальний «ритм» роботи оператора. Важливо, що у криміналістичній практиці алгоритм має не лише «видати результат», а й забезпечити можливість інтерпретації: слідчий і експерт повинні розуміти, які ознаки стали підставою для висновку, щоб оцінити його доказове значення та відтворити логіку у процесуальному документі.

Етап збору та фіксації даних у випадку поведінкових цифрових слідів має критичне значення, оскільки будь-які помилки на цьому етапі можуть призвести до втрати значущих ознак або до формування хибних кореляцій. Джерелами даних можуть бути як кінцеві пристрої (комп'ютери, сервери, мобільні телефони), так і мережеві вузли (маршрутизатори, фаєрволи, проксі), системи моніторингу та безпеки (EDR, SIEM), хмарні сервіси, платформи обміну повідомленнями, соціальні мережі. Для кожного джерела важливо зберегти цілісність і автентичність даних, документувати умови отримання, фіксувати часові параметри, описувати використані інструменти копіювання. З криміналістичної точки зору принципово важливо, щоб цифрові сліди не лише існували технічно, а й були легітимно введені у процес доказування, оскільки інакше їх аналітична цінність не трансформується у процесуальну доказовість.

Попередня обробка даних включає нормалізацію форматів і кореляцію подій. У кіберрозслідуваннях поширеною проблемою є несинхронізовані часові мітки: різні системи можуть мати різний час, різні часові пояси, або відхилення годинників. Якщо ці фактори не врахувати, аналіз послідовності подій може бути спотворений. Іншою проблемою є «шум» у даних: масові системні події, які не мають відношення до інциденту, але створюють інформаційне перевантаження. Інтелектуальний аналіз потребує коректного відсіву шуму, збереження релевантних подій і формування структурованих наборів ознак [4]. При цьому надмірне очищення даних може бути не менш небезпечним, ніж його відсутність, оскільки деякі поведінкові ознаки є слабкими і проявляються лише у сукупності малопомітних сигналів.

Ключовим етапом є виділення ознак (feature extraction), тобто перетворення первинних подій у параметри, придатні для аналізу. У поведінковому контексті ознаки можуть бути статистичними (частоти дій, розподіли часу), структурними (послідовності команд), семантичними (класи дій: розвідка, експлуатація, закріплення), контекстними (які об'єкти і у якій черговості використовувалися), лінгвістичними (n-грами, стилометричні показники), а також комбінованими. У криміналістичній інтерпретації важливо розуміти, які ознаки є стабільними, а які – ситуативними. Наприклад, вибір конкретного інструменту може змінюватися залежно від середовища, а «ритм» роботи або стиль кодування є більш стійкими. Визначення ваги ознак і їх релевантності є не лише математичною, а й криміналістичною проблемою, оскільки від цього залежить доказова значущість висновку.

Після формування набору ознак відбувається моделювання поведінки. На цьому етапі можна будувати профілі активності, здійснювати класифікацію суб'єкта за типом, порівнювати невідомий профіль з відомими, формувати ймовірнісні оцінки належності. Для слідчої практики суттєвим є питання порогу ідентифікації: коли можна вважати, що збіг ознак достатній для висновку про тотожність суб'єкта, а коли він має лише орієнтуюче значення. У традиційній криміналістичній ідентифікації існують критерії достатності та стійкості сукупності ознак; у цифровому поведінковому аналізі ці критерії потребують адаптації, оскільки ознаки часто мають ймовірнісний характер і залежать від контексту [5]. Тому в науковій площині важливим є вироблення підходів до оцінки надійності моделей, їх валідації та встановлення меж застосовності. У прикладній площині – розроблення процесуальних алгоритмів, які дозволяють коректно оформляти результати аналізу у вигляді висновку експерта або спеціаліста та інтегрувати їх із іншими доказами.

Питання допустимості та доказової сили результатів інтелектуального аналізу поведінкових слідів тісно пов'язане з принципом перевірюваності. Якщо алгоритм є «чорною скринькою», а його висновки неможливо пояснити, це створює ризик некритичного сприйняття результатів та порушення права на справедливий суд. Тому в криміналістичному й процесуальному аспектах перевагу мають такі аналітичні підходи, які забезпечують відтворюваність і прозорість: можливість повторити аналіз на тих самих даних; документування параметрів моделі; збереження проміжних результатів; пояснюваність ключових ознак, що визначили висновок. У цьому контексті особливої ваги набуває роль експерта, який здатен інтерпретувати результат, пояснити межі його надійності та співвіднести його з матеріалами провадження. Таким чином, інтелектуальний аналіз не підміняє експертне мислення, а виступає його інструментальним підсилювачем.

Значущою є також проблема помилкових спрацювань і хибних кореляцій. У великих масивах даних закономірності можуть виникати випадково, а алгоритми можуть «навчитися» на нерелевантних ознаках. У кримінальному провадженні це може призвести до необґрунтованої підозри, порушення прав людини та дискредитації технологічних підходів. Тому необхідною умовою є багаторівнева верифікація: поєднання поведінкових висновків з технічними індикаторами, з даними про пристрої, з фінансовими слідами, з показаннями, з оперативною інформацією, з матеріалами негласних заходів (у разі їх наявності та допустимості). Важливо, щоб поведінкова модель не була єдиною підставою для висновку про винуватість, але могла слугувати засобом уточнення версій і спрямування пошуку доказів.

У межах ідентифікації суб'єктів кіберзлочинів доцільно розрізняти індивідуальну та групову поведінкову атрибуцію. Індивідуальна атрибуція спрямована на встановлення, що певні дії у кіберпросторі вчинені

конкретною фізичною особою [6]. Групова атрибуція полягає у встановленні приналежності дій до певної організованої групи або спільноти (наприклад, угруповання, що спеціалізується на ransomware чи шахрайстві), навіть якщо конкретні оператори всередині групи можуть змінюватися. Для групової атрибуції важливими є «організаційні» поведінкові ознаки: типова структура кампанії, характер комунікації, стандартизовані шаблони вимог, повторювані технічні рішення, інфраструктурні звички. Для індивідуальної атрибуції більш значущими є мікро-патерни: стиль коду, дрібні звички у командному рядку, повторювані помилки, лінгвістичні особливості приватного спілкування. У реальних розслідуваннях ці рівні поєднуються: спочатку встановлюється групова приналежність, що звужує поле пошуку, а потім – індивідуальна ідентифікація через сукупність стійких персональних ознак.

Необхідно враховувати і протидію з боку кіберзлочинців, які дедалі частіше застосовують методи ускладнення атрибуції: використання «одноразових» інструментів, автоматизацію через боти, генерацію коду за допомогою різних джерел, поділ функцій між операторами, навмисне змішування стилів. Однак і ці форми протидії самі по собі можуть утворювати поведінкові сліди. Наприклад, систематичне використання конкретних сервісів анонімізації, специфічний порядок переходів між вузлами, повторювані «вікна» активності для ротації інфраструктури, характерні схеми взаємодії з криптовалютними гаманцями – усе це може бути використано для виявлення стійких закономірностей. Більше того, спроби «зробити поведінку випадковою» часто призводять до появи неприродних патернів, що фіксуються алгоритмами як аномалії, і тим самим стають додатковим джерелом ідентифікаційної інформації.

Суттєвим виміром є психологічний аспект цифрової поведінки. Попри технічну природу середовища, кіберзлочин вчиняє людина, і її рішення відображають мотивацію, установку на ризик, рівень самоконтролю, домінуючі когнітивні стратегії. Деякі суб'єкти діють імпульсивно, швидко, допускаючи помилки; інші – обережно, з резервним плануванням. Одні проявляють схильність до «надконтролю», ретельно очищаючи сліди, інші – недооцінюють можливості аналітики. Психологічні риси можуть відображатися у цифровій манері роботи: у тривалості сесій, у реакції на непередбачувані події, у виборі тактики взаємодії з жертвою [7]. Такі параметри не є прямими «психологічними тестами», але у сукупності з іншими ознаками дозволяють збагачувати профіль суб'єкта й уточнювати слідчі версії, що має особливе значення в умовах дефіциту інформації про особу правопорушника.

Окремим напрямом є стилометрія та аналіз авторства у цифровому середовищі. Кіберзлочинці залишають текстові сліди у фішингових листах, повідомленнях, інструкціях, кодових коментарях, переговорах із потерпілими, оголошеннях на форумах. Стилометричний аналіз дозволяє виявляти індивідуальні особливості письма: частотність функціональних слів, довжину речень, пунктуаційні звички, типові орфографічні помилки, характерні мовні конструкції. У поєднанні з часовими й інструментальними ознаками це підвищує точність атрибуції. Водночас слід враховувати ризики: тексти можуть бути перекладені автоматично, можуть копіюватися з шаблонів, можуть навмисно стилізуватися. Тому стилометрія має найбільшу цінність тоді, коли аналізуються великі корпуси текстів, а результати співвідносяться з іншими доказами.

Практична цінність інтелектуального аналізу поведінкових слідів проявляється також у можливості раннього виявлення злочинної активності та запобігання кіберінцидентам. У корпоративних системах безпеки поведінкова аналітика (User and Entity Behavior Analytics) використовується для виявлення відхилень у поведінці користувачів і пристроїв. З криміналістичної точки зору, результати такого моніторингу можуть стати підставою для початку досудового розслідування або для фіксації важливих доказів на ранньому етапі, коли сліди ще не знищені. Однак це ставить питання про межі допустимого спостереження, правові підстави збору даних і захист персональної інформації. В умовах демократичної правової держави застосування поведінкової аналітики має супроводжуватися чіткими регламентами доступу, зберігання, використання та передачі даних, інакше виникає ризик перетворення технологічних можливостей на інструмент надмірного контролю.

У кримінальному процесі України важливим є забезпечення того, щоб результати аналізу поведінкових цифрових слідів могли бути належним чином закріплені та перевірені. Це передбачає, що слідчий повинен уміти формулювати завдання для експерта, визначати об'єкти дослідження, забезпечувати їх цілісність та документувати процес отримання. Експерт, у свою чергу, має володіти не лише технічною компетентністю, а й методологією криміналістичної ідентифікації, розуміти процесуальні вимоги до висновку, вміти пояснити суду логіку застосованих методів. Практика переконує, що технологічна складність кіберінцидентів часто вступає у суперечність з обмеженим рівнем цифрової грамотності учасників процесу, що може призводити до непорозумінь, некоректної оцінки доказів або до спрощення складних висновків. Відтак, розвиток цього напряму неможливий без підвищення кваліфікації слідчих, прокурорів, суддів та експертів у сфері цифрових доказів і поведінкової аналітики.

Системний підхід до ідентифікації суб'єктів кіберзлочинів передбачає інтеграцію поведінкового аналізу з іншими видами цифрових слідів. Поведінкові патерни ефективно доповнюються артефактами пристроїв (наприклад, сліди інсталяції інструментів, історія підключення зовнішніх носіїв, дані про мережеві з'єднання), мережевими індикаторами (шаблони трафіку, домени командно-керуючих серверів), фінансовими слідами (криптовалютні транзакції, платіжні шлюзи), соціальними слідами (профілі у соціальних

мережах, активність на форумах), а також даними оперативного характеру. Взаємна перевірка різних джерел знижує ризик помилок і підвищує переконливість доказування. У цьому сенсі поведінкові цифрові сліди виконують роль «склеювального» елемента: вони дозволяють пов'язати різнорідні дані в єдину модель діяльності суб'єкта.

Висновки та перспективи. Підсумовуючи, слід наголосити, що ідентифікація суб'єктів кіберзлочинів шляхом інтелектуального аналізу поведінкових цифрових слідів є перспективним напрямом сучасної криміналістики, здатним суттєво підвищити ефективність розслідування у ситуаціях, де традиційні підходи виявляються обмеженими. Його цінність полягає у можливості працювати з великими даними, виявляти приховані закономірності, формувати профілі невстановлених суб'єктів, розмежовувати ролі у груповій злочинності, а також здійснювати деанонімізацію на основі стійких поведінкових ознак. Водночас застосування цього підходу потребує високого рівня методологічної дисципліни, процесуальної коректності, етичних запобіжників і науково обґрунтованих критеріїв надійності. Подальший розвиток цієї сфери має бути пов'язаний з розробленням стандартизованих методик виділення та оцінки поведінкових ознак, удосконаленням пояснюваних моделей аналізу, розширенням можливостей експертної верифікації та формуванням узгоджених підходів до використання результатів алгоритмічного аналізу в судовому доказуванні. У сучасних умовах саме такий синтез криміналістичної теорії та інтелектуальних технологій здатен забезпечити адекватну відповідь на виклики кіберзлочинності, не виходячи за межі правових гарантій і фундаментальних принципів кримінального процесу.

Список використаних джерел:

1. Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці : матеріали міжнар. «круглого столу» (Харків, 12 груд. 2019 р.) / редкол.: В. Ю. Шепітько (голов. ред.), В. А. Журавель, В. М. Шевчук, Г. К. Авдєєва. Харків : Право, 2019. 164 с.

2. Самойленко О. А. Протидія кіберзлочинам: криміналістичний аспект : навчально-методичний посібник. Одеса, 2020. 133 с.

3. Зінченко Д. А. Стратегія боротьби з кіберзлочинністю в умовах глобалізації інформаційних просторів. *Застосування інформаційних технологій у правоохоронній діяльності* : мат-ли кругл. столу. Харків, 2023. С. 105–107.

4. Кіберзлочинність та електронні докази : навчальний посібник / Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан ; за ред. О. Денькович, Г. Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с.

5. Піцик Ю. М. Аналіз особистості кіберзлочинця, який вчиняє злочини проти власності в кіберпросторі. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція*. 2017. № 26. С. 105–107.

6. Титаренко А. В. Особа кіберзлочинця як елемент криміналістичної характеристики. *Журнал східноєвропейського права.* 2019. № 62. С. 159–168.

7. Швець Д. В. Підходи до визначення психологічного портрета кіберзлочинця. *Актуальні питання протидії злочинності та торгівля людьми* : зб. матеріалів всеукр. наук-прак. конф. (Харків, 23 листопада 2018 р.). Харків : ХНУВС, 2018. С. 118–121.

Дата першого надходження статті до видання: 30.01.2026
Дата прийняття статті до друку після рецензування: 20.02.2026
Дата публікації (оприлюднення) статті: 23.03.2026