УДК 343.98
DOI https://doi.org/10.32782/2307-1745.2026.79.23

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

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

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

КРИМІНАЛІСТИЧНІ АСПЕКТИ ВИЯВЛЕННЯ ТА ФІКСАЦІЇ ЦИФРОВИХ СЛІДІВ ФІНАНСОВОГО ШАХРАЙСТВА В ПЛАТІЖНИХ СИСТЕМАХ

Анотація. Статтю присвячено комплексному дослідженню криміналістичних аспектів виявлення та фіксації цифрових слідів фінансового шахрайства в сучасних платіжних системах в умовах інтенсивної цифровізації фінансових послуг. Обґрунтовано, що трансформація платіжної інфраструктури, поява дистанційних каналів обслуговування, мобільних застосунків, відкритих API та автоматизованих систем протидії шахрайству зумовлюють зміну механізму слідоутворення та структури доказової інформації у кримінальних провадженнях відповідної категорії. Показано, що цифрові сліди фінансового шахрайства мають нематеріальну природу, є фрагментарними, розпорошеними у багатосуб'єктному інформаційному середовищі та характеризуються обмеженим строком збереження, що істотно ускладнює їх своєчасне виявлення, належну фіксацію і подальше використання в доказуванні.

У статті розкрито криміналістичну сутність цифрових слідів фінансового шахрайства, їх місце в механізмі злочинної діяльності та значення для реконструкції послідовності дій правопорушників. Проаналізовано основні контури формування цифрових слідів у платіжних системах, зокрема транзакційний, ідентифікаційний та контекстний, а також окреслено типові джерела такої інформації: журнали процесингу, логи автентифікації, метадані сесій доступу, дані систем протидії шахрайству, відомості про пристрої та канали зв'язку. Особливу увагу приділено криміналістичним проблемам фіксації цифрових слідів, зокрема забезпеченню їх цілісності, автентичності та перевірюваності, дотриманню ланцюга збереження, синхронізації часових міток і збереженню доказового контексту.

Наголошено, що ефективне розслідування фінансового шахрайства неможливе без поєднання криміналістичних, технічних та процесуальних підходів, а також без налагодженої взаємодії слідчих органів із банками, платіжними організаціями та іншими володільцями інформаційних ресурсів. Обґрунтовано необхідність формування уніфікованих криміналістичних алгоритмів дій у типових слідчих ситуаціях, орієнтованих на оперативне виявлення нестійких цифрових слідів і їх належну фіксацію на ранніх етапах кримінального провадження. Зроблено висновок, що розвиток криміналістичної теорії цифрових слідів і впровадження системного підходу до їх виявлення та фіксації є ключовою умовою підвищення ефективності доказування у провадженнях про фінансове шахрайство в платіжних системах.

Ключові слова: фінансове шахрайство, платіжні системи, цифрові сліди, докази, криміналістика, фіксація доказів, транзакційні дані, метадані, антифрод-системи, розслідування, злочин.

Постановка проблеми зумовлена тим, що стрімка цифровізація фінансових послуг і масове використання дистанційних платіжних інструментів трансформували фінансове шахрайство з переважно "контактного" та документально-матеріального виду злочинності у високотехнологічну, динамічну та часто транскордонну кримінальну діяльність, у межах якої ключовим носієм криміналістично значущої інформації стають цифрові сліди. Водночас у практиці досудового розслідування зберігається дисбаланс між темпами еволюції шахрайських схем у платіжних системах і наявними криміналістичними методиками їх виявлення та фіксації: традиційні підходи до слідоутворення, доказування та документування процесуальних дій не завжди адекватно враховують нематеріальну природу цифрових артефактів, їх розпорошеність у багатосуб'єктній інфраструктурі, нестійкість у часі та залежність від технічних політик зберігання даних.

Проблемність посилюється тим, що цифрові сліди фінансового шахрайства переважно виникають і зберігаються у середовищах, які перебувають під контролем приватних суб'єктів

(банки, процесингові центри, платіжні організації, провайдери аутентифікації, оператори зв'язку, хмарні сервіси), що породжує об'єктивні труднощі доступу до первинних журналів, метаданих і технічних атрибутів транзакцій, а також ускладнює забезпечення безперервності ланцюга збереження та перевірюваності цілісності даних. Додатковим викликом є наявність "вікна збереження" цифрової інформації: автоматичне перезаписування логів, обмежені строки архівування, оновлення систем, токенізація та шифрування, що унеможливлюють відтворення істотних обставин події при несвоєчасному реагуванні. Унаслідок цього в кримінальних провадженнях нерідко фіксується лише факт списання чи переказу коштів (виписка, довідка), тоді як технічно насичений доказовий контекст – дані сесій, пристроїв, каналів доступу, механізмів підтвердження, антифрод-оцінок та кореляційних ідентифікаторів – залишається поза межами належної фіксації або втрачається ще на початковому етапі.

Постановка проблеми також пов'язана з тим, що сучасні шахрайські практики активно використовують засоби маскування та ускладнення ідентифікації (анонімізація мережевого трафіку, підставні акаунти та "дропи", соціальна інженерія, розподілені транзакційні ланцюги, інструменти швидкого "розшарування" коштів), що змінює структуру слідової картини: ключові докази стають непрямими, кореляційними й потребують синхронізації даних із різних джерел, у тому числі з різними стандартами часу, форматами журналювання та рівнями деталізації. Відсутність уніфікованих криміналістичних алгоритмів дій слідчого і спеціаліста в типових ситуаціях (заява потерпілого, спрацювання антифрод-системи, виявлення аномальних зарахувань, інцидент у мерчанта) призводить до фрагментарного збору інформації, процесуальних ризиків (сумніви щодо допустимості та автентичності цифрових доказів) і, як наслідок, зниження ефективності викриття організаторів та виконавців.

Отже, проблема полягає у необхідності науково обґрунтувати та методично конкретизувати криміналістичні підходи до виявлення і фіксації цифрових слідів фінансового шахрайства в платіжних системах як цілісного процесу, що поєднує діагностику події, визначення релевантних джерел даних, забезпечення технічної цілісності та процесуальної коректності фіксації, а також створення умов для подальшої експертної інтерпретації й доказової реконструкції механізму злочину. Саме розв'язання цієї проблеми є передумовою підвищення результативності досудового розслідування, мінімізації втрат доказової інформації та формування належної доказової бази у провадженнях про фінансове шахрайство в умовах цифрової економіки.

Метою статті є наукове обґрунтування та систематизація криміналістичних підходів до виявлення і фіксації цифрових слідів фінансового шахрайства в платіжних системах з метою забезпечення їх повноти, цілісності, процесуальної допустимості та ефективного використання для доказової реконструкції механізму злочину і встановлення причетних осіб.

Виклад основного матеріалу. Криміналістичне забезпечення протидії фінансовому шахрайству в умовах цифровізації економіки та стрімкого розвитку платіжних систем набуває особливого значення з огляду на трансформацію способів злочинної діяльності, зміну структури доказової інформації та зростання ролі нематеріальних, цифрових слідів у механізмі вчинення кримінальних правопорушень. Сучасні платіжні системи – від класичних банківських карткових процесингів і міжбанківських переказів до мобільних гаманців, інтернет-еквайрингу, P2P-переказів, сервісів "купити зараз – сплатити потім", агрегаторів платежів і платіжних ініціацій через відкриті API – формують складне інформаційне середовище, у межах якого фінансові операції здійснюються з високою швидкістю, багаторівневою аутентифікацією та залученням значної кількості технічних і програмних компонентів. У такому середовищі злочинна активність часто набуває гібридного характеру: поєднує соціальну інженерію, технічні атаки на інформаційні системи, маніпуляції з реквізитами, зловживання процедурними прогалинами бізнес-процесів, використання підставних осіб ("дропів"), транскордонну інфраструктуру та автоматизовані інструменти управління злочинними кампаніями. За цих умов фінансове шахрайство постає як складне криміналістичне явище, що характеризується специфічним механізмом утворення цифрових слідів, особливостями їх локалізації, динамічністю та високим рівнем латентності, а також високою "конкуренцією за час" між правопорушником, який прагне швидко вивести й замаскувати кошти, та слідчим, який має встигнути зберегти цифрові артефакти до їх зникнення, перезапису чи втрати доказового контексту.

Цифрові сліди фінансового шахрайства в платіжних системах є різновидом криміналістично значущої інформації, зафіксованої в електронно-цифровій формі, яка відображає підготовчі, безпосередні та посткримінальні дії суб'єктів злочинної діяльності. Принципово важливо підкреслити, що "цифровий слід" у криміналістичному розумінні не зводиться до будь-якого електронного запису: він є відображенням конкретної події або дії, має інформаційний зв'язок із механізмом вчинення правопорушення та потенційну доказову цінність. На відміну від традиційних матеріальних слідів (відбитків, мікрооб'єктів, слідів знарядь), цифрові сліди не мають сталої фізичної форми, існують у вигляді електронних даних, записів, лог-файлів, метаданих, транзакційних журналів, телеметричних параметрів та мережевих артефактів, що зумовлює специфіку їх виявлення, фіксації, збереження та інтерпретації. Вони можуть існувати одночасно в різних станах: як активні записи в оперативних базах даних платіжного процесингу, як журнали подій у системах моніторингу, як кешовані дані в мобільних застосунках, як копії в резервних сховищах, як пакети в мережевому трафіку або як "тіні" у вигляді кореляційних ознак, що виникають у результаті взаємодії різних компонентів [1]. Водночас саме цифрові сліди дозволяють реконструювати ланцюг фінансових операцій, встановити послідовність і логіку дій зловмисника, виявити використані технічні засоби та програмні інструменти, визначити мережеві маршрути й тактики маскування, а також зіставити інформацію з різних джерел для формування єдиної криміналістичної картини події.

Криміналістичний аналіз фінансового шахрайства в платіжних системах ґрунтується на розумінні опосередкованості впливу злочинця на об'єкт посягання через цифрову інфраструктуру. Ця опосередкованість породжує особливий механізм слідоутворення: по-перше, цифрові сліди виникають як прямий результат дій зловмисника (вхід у систему, ініціювання транзакції, зміна реквізитів, додавання нового платіжного інструменту, підтвердження через одноразовий код, обхід обмежень тощо); по-друге, вони утворюються як побічний продукт функціонування платіж-

ної інфраструктури (логування, аудит, антифрод-оцінювання, токенізація, авторизаційні повідомлення, клірингові й розрахункові записи, журналювання помилок); по-третє, вони можуть формуватися як результат реакції системи безпеки або персоналу (блокування, постановка в чергу на ручну перевірку, запити на додаткову аутентифікацію, створення інциденту в системі управління подіями). Саме тому навіть ретельно спланована шахрайська операція, яка на поверхні виглядає "звичайним платежем", здатна залишати множинні інформаційні відбитки в різних сегментах платіжної екосистеми.

Для криміналістики принципово важливо, що платіжна система є багаторівневою: користувацький рівень (пристрої та облікові записи клієнтів), прикладний рівень (мобільні застосунки, веб-кабінети, API-клієнти), транспортний рівень (мережеві з'єднання, TLS-сесії, маршрутизація), процесинговий рівень (авторизація, антифрод, правила ризику, токенізація), рівень платіжних повідомлень (формати та протоколи, журнали повідомлень), рівень банку-емітента та еквайра, а також рівень зовнішніх сервісів (SMS-шлюзи, push-провайдери, провайдери KYC/AML, системи верифікації, хмарні компоненти). Злочинна дія може відбутися на одному рівні, але цифрові сліди "розсипаються" по всіх інших. Тому криміналістична методика виявлення та фіксації повинна бути спрямована не на пошук "одного файлу" чи "одного запису", а на системне вилучення й синхронізацію відомостей з кількох джерел із подальшим зіставленням за часовими мітками, ідентифікаторами транзакцій, сесій, пристроїв, клієнтів і мережевих атрибутів.

Початковим етапом виявлення цифрових слідів фінансового шахрайства є встановлення події та її меж, тобто конкретизація того, що саме розглядається як потенційно злочинна транзакційна активність, які рахунки або платіжні інструменти залучені, у який часовий проміжок відбувалися ключові дії, які канали доступу використовувалися. Саме на цьому етапі виникає потреба криміналістичної діагностики: за зовнішніми проявами (скарга потерпілого, повідомлення банку, спрацювання антифроду, відмова в авторизації з подальшим успішним платежем, багаторазові спроби входу) необхідно визначити ймовірний механізм шахрайства та сформувати первинні слідчі версії. Діагностичний підхід дозволяє відразу задати "вектор пошуку" цифрових слідів: якщо маємо ознаки соціальної інженерії, то критичними будуть записи комунікації, логи зміни лімітів, додавання отримувачів, а також дані про пристрій та IP; якщо йдеться про компрометацію облікового запису через шкідливе ПЗ, то зростає значення артефактів на кінцевому пристрої, токенів сесії, відбитків браузера, аномалій поведінки в застосунку; якщо є ознаки підміни реквізитів або "перехоплення" платіжного потоку, то основними стають журнали API-викликів, дані інтеграційного шлюзу, зміни платіжних форм і адресатів.

Виявлення цифрових слідів у платіжних системах, з криміналістичної точки зору, доцільно розглядати як поєднання трьох взаємодоповнювальних рівнів: рівень транзакційних слідів, рівень ідентифікаційних слідів і рівень контекстних слідів [2]. Транзакційні сліди – це безпосередні записи про платіж: авторизаційні та фіналізаційні повідомлення, ідентифікатори транзакцій, сума, валюта, мерчант, MCC-код, реквізити отримувача, тип операції, статуси обробки, записи клірингу та розрахунку, журнали помилок і повторів, а також внутрішні службові поля процесингу (наприклад, токени, маркери ризику, коди причин відмови). Ідентифікаційні сліди пов'язані з тим, "хто" і "звідки" ініціював дію: дані автентифікації, логи входу, IP-адреси, геолокаційні параметри, відбитки пристрою (device fingerprint), ідентифікатори SIM, параметри браузера чи застосунку, токени push-повідомлень, інформація про зміну пароля, додавання нового пристрою, результати багатофакторної аутентифікації. Контекстні сліди відображають "обстановку" вчинення: правила антифрод-системи, спрацьовування тригерів, зміни лімітів, скасування або підтвердження операцій, комунікацію з підтримкою, листування, звернення потерпілого, внутрішні записи про інцидент, а також дані про пов'язані транзакції, що утворюють "серію".

Особливість цифрових слідів полягає у фрагментарності та розпорошеності: інформація про одну шахрайську операцію може одночасно зберігатися в банку-емітенті, у процесинговому центрі, у платіжного агрегатора, у мерчанта, у провайдера 3-D Secure/аутентифікації, у мобільного оператора (якщо були SMS-коди), у виробника пристрою (push-сервіси), у хмарної платформи (якщо застосунок або частина інфраструктури працює в хмарі). Це зумовлює потребу комплексного підходу та чіткої організації взаємодії слідчого з володільцями інформації. На практиці виявлення слідів неможливе без своєчасного "заморожування" даних у ключових точках: збереження логів, закріплення записів аудиту, фіксації налаштувань правил і конфігурацій, а також оперативного вилучення інформації з кінцевих пристроїв, якщо вони доступні. Нерідко саме несвоєчасність є причиною втрати критичних елементів: наприклад, дані про сесію входу можуть зберігатися обмежений час; журнали веб-шлюзу можуть бути перезаписані; у системах антифроду детальні "скорингові" параметри можуть не архівуватися довго; а в мобільному застосунку локальні журнали можуть очищатися під час оновлення.

Фіксація цифрових слідів фінансового шахрайства становить самостійний криміналістичний етап, що має на меті забезпечення збереження доказової інформації в автентичному вигляді та створення умов для її подальшого дослідження. Тут доцільно розмежувати поняття технічної фіксації та процесуальної фіксації. Технічна фіксація охоплює заходи з копіювання, експорту, створення образів носіїв, отримання дампів, збереження логів і метаданих, обчислення хеш-значень, документування параметрів середовища. Процесуальна фіксація пов'язана з оформленням відповідних дій у межах кримінального провадження, забезпеченням належного правового підґрунтя, дотриманням вимог допустимості та належності, а також фіксацією "ланцюга збереження" (chain of custody) – тобто простежуваності того, хто, коли і з яким обсягом даних працював.

Технічні вимоги до фіксації цифрових слідів зумовлені їх крихкістю та можливістю непомітної модифікації. На відміну від матеріальних об'єктів, цифрові дані можуть бути змінені без видимих ознак втручання, а їх копіювання може супроводжуватися автоматичною зміною метаданих (наприклад, час доступу). Тому криміналістична тактика передбачає використання процедур, що мінімізують ризик змін: створення форензичних копій із використанням спеціалізованих інструментів; фіксацію хеш-значень для кожного набору даних; розмежування "робочої копії" і "еталонної копії"; застосування режимів лише читання; документування всіх операцій та середовища (версії ПЗ, налаштування експорту, формат файлів) [3]. Особливо важливим є збереження первинного контексту: цифровий слід цінний не

лише як набір символів, а як дані, прив'язані до системи, часу, ідентифікаторів та взаємозв'язків. Наприклад, експорт транзакції без супровідних полів аудиту, без даних про сесію або без "пакета" суміжних логів може істотно знизити її доказову силу.

Процесуальний вимір фіксації вимагає чіткого відображення в протоколах і додатках до них таких елементів, як джерело інформації, спосіб її отримання, обсяг, формат, технічні засоби, що застосовувалися, а також заходи забезпечення цілісності. У ситуаціях, коли дані отримуються від платіжної організації або банку, додатково значення мають внутрішні регламенти ведення журналів і систем аудиту, оскільки вони дозволяють обґрунтувати достовірність походження даних. У криміналістичному сенсі важливо забезпечити, щоб цифрові сліди були відтворюваними: тобто за наданими даними можна було повторно перевірити їх структуру, хеш-значення, відповідність часових міток і логічну узгодженість між джерелами.

Окремої уваги потребує питання часових міток і синхронізації часу. Для платіжних систем характерна взаємодія багатьох серверів і сервісів, які можуть використовувати різні часові пояси, різну точність часу, а іноді й мати розбіжності через некоректну синхронізацію. У криміналістичній практиці це створює ризик помилкової реконструкції подій. Тому фіксація має включати відомості про часову зону, формат часу, джерело синхронізації (NTP), а також зіставлення подій за відносними інтервалами. Встановлення коректної хронології особливо важливе для доведення причинно-наслідкових зв'язків: наприклад, що спочатку відбулася зміна пароля, потім додано нового отримувача, потім підвищено ліміти, а після цього здійснено серію переказів. Саме така послідовність нерідко демонструє "сценарій" шахрайства й дозволяє відмежувати випадкові дії користувача від цілеспрямованого втручання.

Значну криміналістичну цінність у розслідуванні фінансового шахрайства мають метадані, що супроводжують транзакції та технічні процеси. Їх цінність полягає в тому, що вони часто є менш "очевидними" для зловмисника та складнішими для повного знищення [4]. Наприклад, злочинець може видалити листування в месенджері на пристрої потерпілого, але метадані сесії входу в банкінг або записи антифроду залишаться в системі. Метадані дають змогу відповісти на ключові криміналістичні питання: з якого пристрою здійснено доступ, чи був пристрій раніше відомим для цього акаунта, чи змінювався канал доступу, чи відрізнявся "відбиток" браузера, чи був нетиповий маршрут IP, чи збігалися параметри мережі із попередніми входами. Особливу роль відіграють кореляційні ідентифікатори: ідентифікатор сесії, токен авторизації, ідентифікатор транзакції, ідентифікатор пристрою, які дозволяють "прошити" інформацію через різні журнали й системи.

Типовою криміналістичною помилкою є фіксація лише "видимих" даних (сума, рахунок, дата платежу) без вилучення технічних атрибутів. Унаслідок цього доказова база стає слабкою: вона підтверджує факт списання коштів, але не дозволяє встановити механізм, суб'єкта та спосіб вчинення. Для розслідування фінансового шахрайства необхідно фіксувати максимально повний набір атрибутів транзакції: не лише реквізити, але й статуси авторизації, коди відповіді, використані методи аутентифікації, інформацію про підтвердження (SMS/push/біометрія), ознаки токенізації, дані про пристрій і мережу, а також антифрод-оцінку. Саме ці відомості часто стають "мостом" від події до особи.

Суттєвий криміналістичний інтерес становлять дані систем протидії шахрайству (anti-fraud). Такі системи збирають поведінкові характеристики, формують ризикові профілі, оцінюють транзакції за правилами і моделями, зберігають "причини" спрацювання та рішення (пропущено/заблоковано/на ручну перевірку). Для криміналістики це цінне джерело не лише для доведення, але й для пошуку: антифрод часто здатний виявляти серійність, пов'язаність акаунтів, повторювані патерни (одні й ті самі IP-діапазони, однакові пристрої, однакові мерчанти), що дозволяє слідчому розширювати межі епізоду та виходити на організовані групи. Фіксація даних антифроду повинна здійснюватися з урахуванням того, що моделі й правила можуть змінюватися, а тому необхідно зафіксувати стан правил на момент інциденту, інакше подальший аналіз може бути спотворений ретроспективними налаштуваннями.

У сучасних платіжних системах широко застосовується багатофакторна аутентифікація та механізми підтвердження операцій. Злочинці, однак, адаптуються: використовують SIM-swap, перехоплення SMS, переконують потерпілих повідомити коди, підмінюють push-повідомлення, використовуючи шкідливі програми або фішингові сторінки. Для криміналістики це означає необхідність виявлення та фіксації слідів не лише транзакції, а й процесу підтвердження: журналів відправлення і доставки SMS, логів push-провайдера, записів про підтвердження біометрією або PIN-кодом, даних про зміну "довіреного" пристрою. Особливо важливо встановити, чи була аутентифікація виконана штатно власником, чи це результат компрометації. Наприклад, поєднання нової IP-адреси, нового пристрою й успішного підтвердження може вказувати на соціальну інженерію, тоді як новий пристрій без типової поведінки користувача може свідчити про шкідливе ПЗ або викрадення токенів.

Виявлення цифрових слідів на кінцевих пристроях потерпілих і підозрюваних є окремим напрямом криміналістичної роботи. Саме на пристрої можуть залишатися сліди фішингових переходів, встановлення шкідливих застосунків, конфігурацій VPN, збережених паролів, кешу браузера, історії push-повідомлень, скриншотів, переписок із "операторами банку". Проте фіксація таких слідів потребує особливо обережного підходу: неправильні дії користувача або слідчого можуть призвести до очищення даних (наприклад, автоматичне оновлення застосунку). Важливо також дотримуватися криміналістичного принципу мінімального втручання: фіксація повинна бути такою, щоб не змінювати дані без необхідності, і супроводжуватися документуванням кожної дії, зокрема включення/вимкнення пристрою, підключення до мережі, розблокування, підключення носіїв [5].

Особливу складність становить фіксація цифрових слідів у випадках використання зловмисниками засобів анонімізації та розподіленої інфраструктури. Анонімізація сама по собі не знищує сліди, а змінює їхню "прочитуваність": замість прямого встановлення адреси чи місцезнаходження потрібно шукати опосередковані зв'язки. Криміналістичне значення мають повторювані патерни: однакові часові інтервали активності, схожі параметри пристроїв, повторювані "помилки" в поведінці, використання одних і тих самих платіжних маршрутів, однакові мерчанти або сервіси, до яких ведуть платежі. У випадках криптовалютного "відмивання" або швидкого "розшарування" коштів важливими стають точки входу і виходу між фіатною

та цифровою економікою, де залишаються записи KYC, дані банківських переказів на біржу, журнали поповнення, а також інформація про пристрої, що використовувалися для доступу.

Криміналістична тактика виявлення та фіксації цифрових слідів також повинна враховувати організований характер фінансового шахрайства. У реальності значна частина таких злочинів здійснюється не одиночними виконавцями, а групами з розподілом ролей: "скаути" збирають персональні дані та реквізити, "соціальні інженери" контактують із потерпілими, "технарі" забезпечують фішингову інфраструктуру, "дропи" приймають кошти, "каси" займаються конвертацією та виведенням. Цей розподіл ролей відображається в цифрових слідах: різні етапи операції можуть залишати сліди в різних інформаційних контурах, що потребує "збирання мозаїки". Зокрема, окремі IP-адреси можуть належати технічній інфраструктурі, тоді як пристрої "дропів" фігуруватимуть у частині отримання переказів, а комунікація з потерпілим відбуватиметься через інші канали.

У контексті методики розслідування доцільно детально окреслити типові криміналістичні ситуації, в яких здійснюється виявлення цифрових слідів. Перша ситуація – звернення потерпілого про несанкціоноване списання коштів. Тут пріоритетом є максимально швидке отримання від банку даних про транзакцію та сесію доступу, а від потерпілого – відомостей про останні дії (дзвінки, повідомлення, переходи за посиланнями, встановлення застосунків), а також фіксація екранних відображень (скриншоти повідомлень, історія операцій). Друга ситуація – спрацювання антифрод-системи банку чи платіжного провайдера. Тут первинними є дані ризикового скорингу, тригери, зв'язки з іншими інцидентами, а також інформація про блокування і спроби обходу. Третя ситуація – виявлення шахрайства на боці мерчанта або агрегатора (наприклад, "card-not-present" шахрайство, "friendly fraud", підміна платіжної сторінки). Тут ключовими є логи мерчанта, журнали API, дані про ініціювання платежу, а також веб-артефакти (скрипти, підміни, домени). Четверта ситуація – виявлення "дроп-мережі" через серію підозрілих зарахувань. Тут головним є аналіз транзакційних графів, часових закономірностей та ідентифікація вузлів мережі [6].

Фіксація цифрових слідів у зазначених ситуаціях повинна бути стандартизована в межах криміналістичних рекомендацій. Стандартизація не означає "шаблонності", а передбачає формування мінімально необхідного переліку даних, які слід здобути в кожному випадку. Для банківського карткового шахрайства та несанкціонованих переказів такий мінімум може включати: повний запис транзакції з усіма службовими полями; дані про канал ініціювання; логи входу/сесії за відповідний період; дані про пристрій і мережу; інформацію про аутентифікацію та підтвердження; відомості про зміни профілю (пароль, телефон, пристрої, ліміти); антифрод-оцінку і тригери; відомості про отримувача (рахунок, банк, платіжний провайдер, мерчант); інформацію про подальші переміщення коштів; пов'язані інциденти. Для шахрайства на боці мерчанта – журнали API-викликів, серверні логи, дані платіжного шлюзу, інформацію про зміни на сайті/платіжній сторінці, журнали адміністрування, відомості про домени й сертифікати.

Окремою криміналістичною проблемою є забезпечення цілісності й незмінності цифрових слідів, оскільки захист від фальсифікації та підміни має критичне значення для доказування. У цифровому середовищі можливі як прямі підробки (створення фіктивних логів, редагування журналів), так і опосередковані маніпуляції (вибіркове надання даних, "обрізання" полів, відсутність частини записів). Криміналістична тактика тут передбачає отримання даних із першоджерела, бажано в автоматизованому режимі експорту, де система формує звіт із підписом або контрольними сумами. Додатковим способом перевірки є перехресна верифікація: одна й та сама подія повинна відображатися в кількох незалежних джерелах (наприклад, транзакція – у процесингу, у банку-емітенті, у мерчанта, у системі антифроду). Якщо джерела не узгоджуються, це сигнал як для технічної перевірки, так і для криміналістичного аналізу можливого втручання.

Для належної криміналістичної оцінки цифрових слідів необхідно розуміти, що вони мають різні рівні "первинності". Первинні цифрові сліди утворюються безпосередньо в момент події в основних журналах платіжної системи. Вторинні – це похідні записи, сформовані в результаті реплікації, агрегації або звітування. Третинні – це інтерпретації, наприклад аналітичні висновки антифроду або звіти комплаєнсу. У доказуванні найвищу цінність мають первинні та належно зафіксовані вторинні, тоді як третинні можуть бути важливими для орієнтації, версій і пояснення, але потребують обов'язкової опори на первинні дані [7]. Нерідко в практиці виникає ситуація, коли банк надає "виписку" або "довідку", яка не містить технічних атрибутів; з криміналістичної точки зору це недостатньо для ідентифікації механізму. Тому методика повинна орієнтувати слідчого на запит саме первинних журналів аудиту й технічних логів у межах процесуальних можливостей.

Проблема локалізації цифрових слідів ускладнюється використанням хмарних сервісів і міжнародної інфраструктури. Дані можуть зберігатися в дата-центрах за межами юрисдикції, а доступ до них регламентується політиками провайдерів. У криміналістичному аспекті це підсилює роль раннього "інцидент-респонсу": якщо у власника платіжної системи є можливість локально зафіксувати журнали до їх переміщення або зміни, це може стати вирішальним. Крім того, у таких умовах підвищується значення співпраці з суб'єктами приватного сектору: банками, платіжними організаціями, телеком-операторами, провайдерами сервісів. Криміналістика тут виходить за межі традиційної "слідчої дії" й потребує розвинених моделей взаємодії, які забезпечують отримання технічно повних і належно оформлених даних.

Важливим елементом криміналістичної фіксації є документування "цифрової обстановки" події. Це поняття охоплює не лише факт транзакції, а й стан систем, налаштування безпеки, активні сесії, зміни конфігурацій, типові поведінкові патерни користувача. Документування обстановки дозволяє відповісти на питання, чи була подія типовою або аномальною, чи порушник діяв у межах звичайного сценарію чи використав обхідні шляхи. Наприклад, якщо для клієнта характерні входи лише з одного пристрою та одного регіону, а в момент шахрайства відбувається вхід із іншого регіону та здійснюється зміна лімітів, це формує криміналістично значущу сукупність обставин, яка підсилює висновок про несанкціонованість. Саме сукупність, а не один параметр, зазвичай має доказове значення.

Окремо слід зупинитися на специфіці фіксації "поведінкових" цифрових слідів. Сучасні системи безпеки часто використовують поведінкову біометрію: динаміку набору тексту,

характер торкань екрана, швидкість і траєкторію рухів, типові патерни навігації в застосунку. Такі дані можуть бути надзвичайно цінними, оскільки дозволяють відмежувати дії власника акаунта від стороннього виконавця навіть за умови використання правильних логін-паролів. Проте їх фіксація потребує особливого підходу: ці дані зазвичай зберігаються у вигляді скорингових оцінок або агрегованих показників, а не "сирих" сенсорних записів. Для криміналістики важливо зафіксувати принаймні факт спрацювання поведінкових правил, рівень ризику, ідентифікатор сесії та параметри, що лягли в основу рішення системи.

У межах криміналістичного забезпечення розслідування фінансового шахрайства необхідно також деталізувати типові способи протидії, які застосовують зловмисники, і відповідні слідові "контрвідбитки". Поширеною є тактика швидкого виведення коштів через ланцюг дрібних переказів, що ускладнює блокування. Цифровими слідами тут будуть серійні транзакції з мінімальними інтервалами, повторювані отримувачі, однотипні призначення платежів, одночасні входи в кілька акаунтів з одних технічних параметрів. Інша тактика – "розподіленість" операцій: частина дій виконується через один канал, частина через інший, щоб уникнути антифрод-правил. Слідова картина тут виявляється у зміні каналів доступу, нетипових переходах між пристроями, спробах обійти підтвердження. Ще одна тактика – створення інформаційного шуму: численні спроби входу, зміни пароля, хибні транзакції. Для криміналістики важливо не втратити "сигнал" у цьому шумі, а тому фіксація має охоплювати весь масив подій із подальшим аналітичним відсівом.

Для забезпечення належного обсягу й глибини криміналістичного аналізу доцільно розгорнути питання класифікації цифрових слідів фінансового шахрайства. Така класифікація може здійснюватися за кількома критеріями. За місцем локалізації: сліди на стороні клієнта (пристрій, застосунок, браузер), сліди на стороні провайдера (процесинг, шлюз, антифрод), сліди на стороні контрагентів (мерчант, агрегатор, банк-отримувач), сліди на стороні третіх сторін (оператор зв'язку, провайдер email/push). За функціональним призначенням: сліди автентифікації, сліди ініціювання транзакції, сліди підтвердження, сліди маршрутизації, сліди клірингу, сліди реакції безпеки. За стабільністю: стійкі (архівні журнали, резервні копії), середньостійкі (оперативні логи з обмеженим строком зберігання), нестійкі (кеш, тимчасові токени, оперативна пам'ять). За доступністю: доступні безпосередньо слідству (вилучені носії), доступні лише через запити (банківські системи), доступні лише через міжнародну правову допомогу (закордонні провайдери) [8]. Така класифікація не є суто теоретичною: вона задає алгоритм пошуку й визначає пріоритети фіксації, зокрема у "вікні часу".

Оскільки користувач часто є першоджерелом частини цифрових слідів, важливо розкрити криміналістичну тактику роботи з потерпілим у провадженнях про фінансове шахрайство. Йдеться не про допит як такий, а про забезпечення повноти цифрового контексту: які повідомлення отримував, чи встановлював застосунки, чи вводив коди, чи надавав доступ до пристрою, чи переходив за посиланнями, чи телефонував "працівник банку", чи були підозрілі запити на підтвердження. Водночас така взаємодія повинна бути організована так, щоб не спровокувати втрату даних: наприклад, не рекомендувати потерпілому "почистити телефон", "перевстановити застосунок", "видалити вірус" до фіксації. Належним є фіксування скриншотів і екранних відеозаписів (за умови дотримання процесуальних вимог), збереження листування, деталізації дзвінків, а також фіксація повідомлень банку про підтвердження операцій.

У подальшому дослідженні цифрові сліди фінансового шахрайства набувають форми цифрових доказів, які підлягають оцінці з погляду належності, допустимості, достовірності та достатності. Достовірність у цифровому вимірі часто залежить від технічної цілісності та відсутності модифікацій, що підтверджується контрольними сумами та простежуваністю зберігання. Належність пов'язана з установленням логічного зв'язку між даними і подією. Допустимість визначається процесуальними вимогами до отримання. Достатність формується сукупністю: один цифровий слід рідко є вирішальним, натомість комплекс слідів – транзакційні записи, логи входу, дані про пристрій, антифрод-параметри, комунікація – у сукупності створюють переконливу доказову конструкцію.

З огляду на складність цифрового середовища, важливою є роль судової експертизи та спеціаліста. Проте криміналістичний підхід вимагає, щоб слідчий уже на початкових етапах розумів, які саме дані потрібні для експертного дослідження. Неповний обсяг зібраних слідів може зробити експертизу формальною, позбавленою можливості відповісти на суттєві питання. Саме тому методика виявлення і фіксації повинна містити орієнтири щодо формулювання питань експерту: не лише "чи є ознаки втручання", а "чи відбувалася автентифікація з пристрою, який не належить користувачу", "чи є ознаки використання анонімізаторів", "чи узгоджуються часові мітки різних журналів", "чи можливо встановити послідовність дій у застосунку". У криміналістичному вимірі експертне дослідження є продовженням правильної фіксації: без належного збору артефактів експерт позбавлений матеріалу для висновку.

Слід також деталізувати питання доказової реконструкції фінансових потоків. У провадженнях про платіжне шахрайство часто необхідно встановити, куди саме були спрямовані кошти, через які рахунки вони пройшли, у який момент відбулося зняття, конвертація або перерахування. Тут цифрові сліди набувають вигляду транзакційних графів, де вузлами є рахунки, карти, мерчанти, гаманці, а ребрами – операції [9]. Криміналістична цінність графового підходу полягає в можливості виявити "центри" (рахунки-концентратори), "коридори" (сталі маршрути), "маскувальні ланцюги" (розгалуження на дрібні перекази), "повернення" (повторні перекази між пов'язаними рахунками). Фіксація повинна забезпечити дані для такого аналізу: повні реквізити операцій, часові мітки, коди банків, мерчанти, призначення платежів, а також інформацію про пов'язаність акаунтів за технічними атрибутами.

Значення має й фіксація організаційно-технічних умов функціонування платіжної системи. У криміналістичному аспекті це дозволяє встановити, чи були використані прогалини процедур, чи порушник діяв шляхом обману персоналу, чи мав місце інсайдерський компонент. Наприклад, якщо шахрайство стало можливим через некоректні налаштування лімітів або відсутність обов'язкової повторної верифікації при зміні ключових реквізитів, це може свідчити про недоліки системи контролю. Водночас, якщо в логах є ознаки доступу з внутрішніх службових акаунтів, це може вказувати на компрометацію

або інсайдера. У таких випадках цифрові сліди охоплюють журнали адміністрування, записи змін політик, дії операторів, доступи до консолей, що вимагає особливого порядку фіксації та збереження.

Не можна оминути й аспект фіксації "комунікаційних" цифрових слідів, оскільки значна частина шахрайства починається з комунікації з потерпілим. Цифрові сліди тут включають записи дзвінків (деталізація, іноді – записи кол-центрів у межах законних процедур), повідомлення в месенджерах, електронні листи, фішингові сторінки, доменні реєстрації, журнали переходів за посиланнями [10]. Важливо, що комунікаційні сліди часто є найбільш "людинозрозумілими" і дають змістовне пояснення механізму обману, але для доведення вони мають бути підкріплені технічними слідами транзакцій та доступів. Фіксація комунікації повинна забезпечити автентичність: збереження оригінальних повідомлень, заголовків email (headers), метаданих, посилань, скриншотів із відображенням часу та ідентифікаторів, а також, за можливості, отримання даних від провайдера.

Підвищеної уваги потребує питання співвідношення "шахрайських" і "помилкових" операцій. У практиці можливі ситуації, коли потерпілий заперечує здійснення операції, але вона була виконана ним самим або членами сім'ї; або коли операція стала наслідком помилки системи. Саме тому криміналістика повинна опиратися на об'єктивні цифрові сліди, які дозволяють встановити, чи була операція санкціонованою. Тут важливі ознаки: чи був введений правильний PIN або біометрія, чи застосовувався пристрій користувача, чи є типовий поведінковий патерн, чи були до операції зміни безпеки. Сукупний аналіз дозволяє зробити висновок із високим ступенем обґрунтованості й уникнути помилок кваліфікації.

У контексті вимог до фіксації цифрових слідів важливим є впровадження криміналістичних алгоритмів, які можна умовно поділити на алгоритм "першої години", "першої доби" та "першого тижня". У "першу годину" критично зафіксувати найбільш нестійкі дані: сесії входу, токени, оперативні логи, дані підтвердження, статуси блокувань, а також забезпечити тимчасове збереження даних у банку/провайдера. У "першу добу"– зібрати повні транзакційні записи, антифрод-дані, деталізації, а також зафіксувати дані з пристроїв. У "перший тиждень" – виконати системний аналіз зв'язків, отримати додаткові дані від контрагентів, призначити експертизи. Така поетапність є криміналістично виправданою саме через різну "живучість" цифрових слідів.

Висновок. Підсумовуючи розгорнуте дослідження, слід акцентувати, що цифрові сліди фінансового шахрайства в платіжних системах становлять складний багатовимірний об'єкт криміналістичного пізнання, який вимагає адаптації традиційних криміналістичних підходів до умов цифрового середовища. Виявлення та фіксація таких слідів повинні розглядатися не як суто технічна процедура, а як цілісний криміналістичний процес, спрямований на забезпечення повноти, достовірності та доказової цінності інформації. Ключовими принципами цього процесу є своєчасність (врахування "вікна" збереження даних), комплексність (охоплення кількох контурів джерел), контекстуальність (збереження зв'язків і метаданих), перевірюваність (можливість незалежної верифікації та відтворення), а також процесуальна коректність (дотримання вимог допустимості). Саме поєднання криміналістичної логіки з технічною дисципліною роботи з даними формує умови, за яких цифрові сліди перетворюються на переконливу доказову систему, здатну не лише підтвердити факт незаконного списання чи переказу, а й розкрити механізм, ідентифікувати суб'єктів та встановити структуру злочинної діяльності. Розвиток криміналістичної теорії та практики в цьому напрямі є необхідною передумовою підвищення ефективності розслідування фінансових шахрайств, удосконалення взаємодії слідчих органів із фінансовими установами та платіжними провайдерами, а також посилення загальної стійкості платіжної інфраструктури в умовах сучасних цифрових ризиків.

Література:

1. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін. Київ : Скіф, 2012. 728 с.
2. Кривенка О. І. Оперативно-розшукова протидія шахрайствам через мережу Інтернет : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.09. Харків, 2018. 20 с.
3. Афанасенко С. І. Віктимологічна профілактика шахрайства : автореф. дис. ... канд, горид. наук: 12.00.08 / Нац, акад, внутр. справ. Київ, 2013. 23 с.
4. Пчеліна О. В. Особливості предмета доказування у кримінальних справах про економічні злочини та їх вплив на методику розслідування : автореф. дис. ... канд. юрид. наук : 12.00.09 / Харк. нац. ун-т внутр. справ. Харків, 2010. 20 с.
5. Чернявський С. С. Методика розслідування злочинів у сфері банківського кредитування : автореф. дис. ... канд. юрид. наук : 12.00.09 / Національна академія внутрішніх справ України. Київ, 2002. 20 с.
6. Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах : монографія / за ред. проф. В. Ю. Шепітька. Харків : Право, 2009. 168 с.
7. Кириленко Н. Ю. Методка розслідування шахрайств у сфері побутових відносин : автореф. дис. ... канд. юрид. наук : 12.00.09 / Нац. Ун-т «Одеська юридична академія». Одеса. 2013. 20 с.
8. Заяць К. Д. Методика розслідування шахрайств : дис. ... канд. юрид. наук : 12.00.09 / Харківський національний університет внутрішніх справ. Харків, 2020. 20 с.
9. Анапольська А. І. Розслідування шахрайств і пов'язаних із ним злочинів, вчинених у сфері функціонування електронних розрахунків : автореф. дис. ... канд. юрид. наук : 12.00.09 / Харк. нац. ун-т внутр. справ. Харків, 2010. 20 с.
10. Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. ... д-ра філософії (081 – Право) / Національна академія внутрішніх справ. Київ, 2021. 20 с.

Arkusha L., Chernov O., Dykyi O. Criminal aspects of detecting and recording digital traces of financial fraud in payment systems

Summary. The article is devoted to a comprehensive study of the criminalistic aspects of detecting and recording digital traces of financial fraud in modern payment systems in the context of intensive digitalisation of financial services. It is argued that the transformation of the payment infrastructure, the emergence of remote service channels, mobile applications, open APIs, and automated anti-fraud systems are causing changes in the mechanism of trace formation and the structure of evidence in criminal proceedings of the relevant category. It is shown that digital traces of financial fraud are intangible, fragmentary, scattered in a multi-subject information environment and characterised by a limited storage period,

which significantly complicates their timely detection, proper recording and further use in evidence.

The article reveals the criminalistic essence of digital traces of financial fraud, their place in the mechanism of criminal activity and their significance for reconstructing the sequence of actions of offenders. It analyses the main contours of the formation of digital traces in payment systems, in particular transactional, identification and contextual traces, and outlines the typical sources of such information: processing logs, authentication logs, access session metadata, anti-fraud system data, device and communication channel information. Particular attention is paid to the forensic problems of recording digital traces, in particular ensuring their integrity, authenticity and verifiability, compliance with the chain of custody, synchronisation of timestamps and preservation of the evidentiary context.

It is emphasised that effective investigation of financial fraud is impossible without combining forensic, technical and procedural approaches, as well as without well-established cooperation between investigative authorities, banks, payment organisations and other information resource owners. The need to develop unified forensic algorithms for typical investigative situations, focused on the rapid detection of unstable digital traces and their proper recording at the early stages of criminal proceedings, was justified. It is concluded that the development of forensic theory of digital traces and the introduction of a systematic approach to their detection and recording is a key condition for improving the effectiveness of evidence in cases of financial fraud in payment systems.

Key words: financial fraud, payment systems, digital traces, evidence, forensics, evidence preservation, transaction data, metadata, anti-fraud systems, investigation, crime.

Дата першого надходження статті до видання: 03.01.2026
Дата прийняття статті до друку після рецензування: 29.01.2026
Дата публікації (оприлюднення) статті: 23.03.2026