Сюсюкало Вероніка Юріївна,
студентка навчально-наукового інституту права та інноваційної освіти Дніпровського державного університету внутрішніх справ
Науковий керівник:
Волобуєв Анатолій Федорович,
професор кафедри кримінально-правових дисциплін Дніпровського державного університету внутрішніх справ, доктор юридичних наук, професор

ВИЯВЛЕННЯ ТА ДОСЛІДЖЕННЯ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ ЦИФРОВИХ СЛІДІВ ФІНАНСОВИХ ПРАВОПОРУШЕНЬ

У сучасних умовах цифровізації економічних відносин фінансові правопорушення дедалі частіше переміщуються у сферу електронних комунікацій та інформаційних систем. Це зумовлює зміну не лише способів їх вчинення, а й характеру слідів, які вони залишають: замість традиційних матеріальних об'єктів все більшого значення набувають цифрові дані, що фіксуються в інформаційних системах, мережах та електронних пристроях. Такі сліди мають специфічну природу, є динамічними, можуть швидко змінюватися або зникати, що ускладнює їх своєчасне виявлення та належне процесуальне закріплення. У зв'язку з цим питання виявлення і дослідження цифрових слідів фінансових правопорушень набуває особливої актуальності для кримінального провадження.

У науковій літературі питання властивостей цифрових слідів розглядається у працях багатьох дослідників. Зокрема, К. В. Караман дає таке визначення цифровим слідам: «це будь-який фрагмент цифрової інформації, що може бути зафіксований, верифікований та використаний для встановлення обставин події, ідентифікації особи або об'єкта» [1, с. 277]. Є. Є. Демидова виділяє основні властивості цифрових слідів, до яких належать: а) цифрова форма існування, що передбачає відсутність традиційної матеріальної форми; б) утворення внаслідок взаємодії певного об'єкта з цифровими пристроями, технологіями та інформаційними мережами; в) перебування у цифровому середовищі (сервері, комп'ютері, смартфоні тощо); г) можливість їх виявлення та дослідження за допомогою спеціального технічного обладнання та спеціалізованого програмного забезпечення; ґ) можливість копіювання (створення дублікатів) без втрати якості, у

тому числі дистанційно; д) можливість їх дистанційної зміни або знищення [2, с. 75].

Для ефективного розслідування кримінальних правопорушень у сфері економіки необхідно підвищувати кваліфікацію судових експертів, криміналістів і слідчих, а також розробляти інноваційні методики аналізу цифрових слідів. Ключовим моментом є виявлення та дослідження різних типів цифрових слідів, які можуть розкрити інформацію про вчинені у сфері економіки кримінальні правопорушення, а також розуміння їх особливостей і специфіки. Для ефективного виявлення цифрових слідів ключовим етапом є відшукання та подальше вилучення носіїв даних, на яких зосереджені електронні бухгалтерські записи, інформація про фінансові та операційні дії, облікові дані для доступу до вебсайтів і застосунків, а також скриншоти з криміналістично значущими даними.

На практиці такі сліди не «знаходяться самі по собі» – їх необхідно цілеспрямовано шукати у конкретних носіях інформації та інформаційних системах, де вони об'єктивно фіксуються в процесі фінансових операцій. Насамперед виявлення цифрових слідів відбувається під час проведення огляду або обшуку. Йдеться як про огляд місця події, так і про огляд технічних пристроїв – комп'ютерної техніки, мобільних телефонів, серверного обладнання, зовнішніх носіїв інформації. У ході такого огляду фіксуються дані, що можуть свідчити про здійснення фінансових операцій: історія транзакцій у банківських застосунках, листування в месенджерах щодо переказів коштів, файли з обліковими записами або чорновою фінансовою документацією, доступ до електронних гаманців тощо. Важливо, що вже на цьому етапі має забезпечуватися належна фіксація цифрового середовища – із врахуванням ризику втрати або зміни даних. К. В. Караман робить акцент на тому, що «Особливо складними є випадки, коли цифрові дані містяться на пошкоджених жорстких дисках, мобільних пристроях із розбитими екранами, заблокованих телефонах, носіях із порушеною файловою системою чи пошкодженими секторами пам'яті. За таких умов будь-які необережні дії можуть остаточно знищити інформацію або зробити її недоступною для подальшого дослідження» [3, с. 21].

Під час проведення обшуку слід мати на увазі, що сучасні носії інформації можуть бути інтегровані у різні предмети (флеш-накопичувачі, наручні годинники, кулони, телевізори OLED тощо). Тому обшук доцільно проводити із застосуванням відповідних технічних засобів (приладів нелінійної локації), що дозволяють виявити мобільні пристрої та електронні носії у приміщеннях, транспортних засобах, у тому числі під час огляду осіб або проведення особистого обшуку. Якщо під час обшуку були здійснені спроби знищити або приховати мобільні пристрої (знищити інформацію, що зберігається на

їхніх носіях пам'яті), про це у протоколі обшуку робиться відповідний запис із зазначенням вжитих заходів.

При виявленні цифрових слідів їх може бути вилучено. Тимчасовий доступ до речей і документів (ст. 159–164 КПК України [4]) дає змогу отримати інформацію, що перебуває у володінні третіх осіб і фактично недоступна без відповідного процесуального рішення, – насамперед у банківських установах, платіжних системах, фінансових компаніях та операторів телекомунікацій. Саме через цей інструмент слідство отримує доступ до даних про рух коштів по рахунках, IP-адреси входів до систем онлайн-банкінгу, історію авторизацій, прив'язані пристрої, а також інформацію про фінансові операції, які не зберігаються безпосередньо у підозрюваного. Такі відомості є ключовими для встановлення маршруту переміщення коштів і зв'язків між учасниками правопорушення.

Підрозділи Національної поліції України застосовують спеціалізовані апаратно-програмні комплекси цифрової криміналістики, зокрема «Cellebrite UFED Touch 2 Ultimate» та «Cellebrite UFED 4PC Physical Analyzer». Використання таких систем дозволяє здійснювати вилучення, копіювання та подальший аналіз інформації з мобільних терміналів, включаючи дані про телефонні з'єднання, текстові повідомлення, електронну переписку, файли, геолокацію та інші цифрові сліди, що можуть мати доказове значення у кримінальних провадженнях щодо фінансових правопорушень посадових осіб [5, с. 71].

Окрему роль у дослідженні цифрових слідів відіграє розвідка на основі відкритих джерел (OSINT). Застосування цього підходу дозволяє поєднати інформацію, отриману під час досудового розслідування, із даними з відкритих реєстрів, соціальних мереж та інших публічних джерел. Наприклад, аналіз фотографій у соціальних мережах може допомогти встановити фактичне місцезнаходження нерухомості або транспортних засобів, що не були зазначені у деклараціях посадових осіб, а метадані таких зображень можуть містити інформацію про точні координати їх створення [6].

Подальше дослідження вилучених або отриманих даних здійснюється в межах судової експертизи. Йдеться насамперед про комп'ютерно-технічну експертизу, яка дозволяє відновити видалені файли, проаналізувати структуру даних, встановити факти використання конкретних програм або сервісів, а також визначити, які саме дії виконувалися на пристрої. У разі необхідності можуть призначатися й інші види експертиз, наприклад, економічна – для оцінки характеру фінансових операцій, або телекомунікаційна – для аналізу мережевої активності.

Показовим прикладом є кримінальне провадження щодо фінансових правопорушень під час ремонту доріг у Харківській області. За даними правоохоронних органів, злочинна схема була організована посадовцем органу місцевого самоврядування за участю представників підрядних компаній та працівників сільської ради. У межах реалізації схеми укладалися договори з попередньо визначеними підприємствами, після чого до офіційної документації вносилися недостовірні відомості про обсяги виконаних робіт і вартість матеріалів. У результаті таких дій територіальній громаді було завдано збитків на суму майже 20 млн грн [7].

Отже, під час здійснення фінансових правопорушень посадові особи залишають різноманітні цифрові сліди в електронному середовищі. Використання сучасних методів цифрової криміналістики та спеціалізованого програмного забезпечення дозволяє правоохоронним органам виявляти такі сліди, встановлювати обставини правопорушення та осіб, причетних до незаконних фінансових операцій.

Список використаних джерел

1. Караман К. В. Сучасна парадигма криміналістичного значення цифрових слідів у кримінальному провадженні. *Вісник Кримінологічної асоціації України*. Т. 35. № 2. 2025. С. 224–233. URL: https://visnyk.univd.edu.ua/index.php/VNUAF/article/view/936 (дата звернення: 26.03.2026).

2. Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського національного університету.* Серія «Право». Т. 4. № 85. 2024. С. 71–75. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/315983 (дата звернення: 26.03.2026).

3. Караман К. В. Проблемні аспекти фіксації цифрових слідів під час проведення слідчих (розшукових) дій і процесуальних заходів. *Вісник Кримінологічної асоціації України.* Т. 38. № 1 (Part II). 2026. С. 16–24. URL: https://vca.univd.edu.ua/index.php/vca/article/download/729/796

4. Кримінальний процесуальний кодекс України : Кодекс України від 13 квіт. 2012 р. № 4651-VI : станом на 1 квіт. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 26.03.2026).

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

6. Степуренко Д. О., Шарий А. І., Клімушин П. С. OSINT-методи в розслідуваннях відмивання коштів через крипто активи. *Національна економіка в умовах війни: безпека та розвиток :* збірник тез Всеукраїнської науково-практичної конференції. 2025 С. 421. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/9218/1/14_11_2025.pdf#page=422 (дата звернення: 26.03.2026).

7. Артемчук О. Поліція виявила фінансові правопорушення посадовців на 20 мільйонів при ремонті доріг. *Економічна правда*. 30.01.2025. URL: https://epravda.com.ua/power/policiya-viyavila-finansovi-mahinaciji-posadovciv-na-20-milyoniv-pri-remonti-dorig-802638/ (дата звернення: 26.03.2026).