УДК 343.1:343.98(477)
DOI https://doi.org/10.32850/sulj.2025.3.28

OSINT І ON-CHAIN-АНАЛІЗ У ПРОТИДІЇ ОНЛАЙН-ЗБУТУ НАРКОТИКІВ: ПРОЦЕСУАЛІЗАЦІЯ ЕЛЕКТРОННИХ ДОКАЗІВ ТА ЗМІНИ ДО КПК ЩОДО ВЕБ-АРХІВАЦІЇ І *CHAIN OF CUSTODY*

Дарій С. В., Матвєєвський О. В., Федоров І. В.

У статті проаналізовано, як цифровізація (даркнет-майданчики, соціальні мережі, зашифровані месенджери) змінює наркозлочинність, та які процесуальні й експертні підходи потрібні для роботи з електронними доказами у кримінальних провадженнях Показано, що міграція торгівлі наркотиками до даркнет-майданчиків, відкритих соцмереж і зашифрованих месенджерів поєднується з використанням криптовалют, сервісів анонімізації та розподілених хостинг-рішень. Це ускладнює ідентифікацію учасників, фіксацію слідів і відстеження фінансових потоків, підвищує транскордонність і «ефемерність» доказів. Для України, особливо в умовах воєнного стану та активної цифровізації комунікацій, така динаміка створює виклики для досудового розслідування й судового розгляду: короткий життєвий цикл даних, різнорідність форматів, потреба в чітких процесуальних алгоритмах залучення електронних відомостей і взаємодії з іноземними провайдерами.

Мета дослідження — виробити узгоджені з КПК підходи до збирання, фіксації, дослідження та оцінювання електронних даних у провадженнях про незаконний обіг наркотиків, інтегрувавши цифрову криміналістику, OSINT і лабораторне (фізико-хімічне) профілювання речовин. Методологію побудовано на поєднанні доктринального аналізу, кейс-методу та форензичної верифікації цифрових артефактів.

Запропоновано матрицю «сегмент цифрової екосистеми → артефакт → процесуальна дія», що задає маршрути виявлення і фіксації (від веб-архівування і скриншотингу з хеш-верифікацією до аналізу on/off-ramp вузлів), визначає належних суб'єктів (слідчий, прокурор, слідчий суддя, спеціаліст, експерт) і відсилає до релевантних норм КПК (зокрема ст. 84, 86-87, 94, 98-99, 104-107, 159-166, 170-173, 234-237, 242). Окреслено пакет точкових змін до КПК щодо легалізації технік веб-фіксації, процедур клонування носіїв і хеш-ідентифікації, процесуалізації OSINT-джерел та уточнення критеріїв допустимості електронних відомостей.

Ключові слова: *протидія наркозлочинності, легалізація доходів, отриманних злочинним шляхом; електронні докази; OSINT; chain of custody; досудове розслідування, судова експертиза.*

Darii S. V., Matvieievskyi O. V., Fedorov I. V. OSINT and On-Chain Analysis in Countering Online Drug Trafficking: Proceduralization of Electronic Evidence and Amendments to the CPC Regarding Web Archiving and Chain of Custody

The article offers a comprehensive analysis of the transformation of drug-related crime in the digital environment and its procedural-forensic dimension. It shows that the shift of drug trafficking to darknet marketplaces, open social networks, and encrypted messengers is accompanied by the use of cryptocurrencies, anonymization services, and distributed hosting solutions. This complicates the identification of participants, the preservation and recording of traces, and the tracking of financial flows, while increasing the cross-border nature and "ephemerality" of evidence. For Ukraine—especially under martial law and amid the accelerated digitalization of communications—this dynamic generates challenges for pre-trial investigation and court proceedings: the short life cycle of data, heterogeneity of formats, and the need for clear procedural algorithms for obtaining electronic information and for cooperation with foreign service providers.

The aim of the study is to develop approaches—aligned with the Criminal Procedure Code (CPC) of Ukraine—to the collection, preservation/recording, examination, and evaluation of electronic data in proceedings concerning illicit trafficking in narcotic drugs, by integrating digital forensics, OSINT, and laboratory (physico-chemical) profiling of substances. The methodology combines doctrinal legal analysis, the case method, and forensic verification of digital artefacts.

The paper proposes a matrix ("segment of the digital ecosystem → artefact → procedural action") that maps routes for detection and preservation (from web archiving

and screenshotting with hash verification to the analysis of on/off-ramp nodes), identifies the relevant actors (investigator, prosecutor, investigating judge, specialist, expert), and cross-refers to the pertinent provisions of the CPC (inter alia Arts. 84, 86-87, 94, 98-99, 104-107, 159-166, 170-173, 234-237, 242). It also outlines a package of targeted amendments to the CPC to legally recognize web-capture/preservation techniques, procedures for media cloning and hash identification, the procedural incorporation of OSINT sources, and clarification of admissibility criteria for electronic information.

Key words: *countering drug-related crime; laundering of proceeds of crime; electronic evidence; OSINT (open-source intelligence); chain of custody; pre-trial investigation; forensic examination.*

Постановка проблеми та її актуальність. Незаконний обіг наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів (НЗПРАП) упродовж десятиліть залишається однією з найсерйозніших загроз для національної та міжнародної безпеки, громадського здоров'я та економічного розвитку. В умовах XXI століття ця проблема набула нових масштабів у зв'язку зі стрімким розвитком інформаційно-комунікаційних технологій та їх активним використанням злочинними угрупованнями. Цифрові платформи, включаючи даркнет-ринки, соціальні мережі, форуми та зашифровані месенджери, перетворилися на потужні інструменти організації наркобізнесу, забезпечуючи злочинцям високий рівень анонімності, глобальне охоплення та можливість здійснювати транзакції з використанням криптовалют [1]. Згідно зі звітом Europol за 2025 рік, майже всі форми серйозної та організованої злочинності мають цифровий слід, а даркнет-ринкі щоденно генерують мільйони доларів прибутку [11]. Це створює безпрецедентні виклики для правоохоронних органів та судово-експертних установ у сфері виявлення, розслідування й припинення такої діяльності, а також дослідження вилучених наркотичних засобів.

Цифровізація наркоторгівлі не лише змінює канали збуту, а й трансформує саму структуру злочинних організацій. Традиційні ієрархічні моделі поступаються місцем децентралізованим, більш гнучким та стійким до класичних методів протидії мережевим структурам. Цифрові платформи, зокрема даркнет та зашифровані месенджери, дають змогу встановлювати прямий контакт між різними ланками злочинного ланцюга, інколи навіть між виробниками чи великими дилерами та кінцевими споживачами, минаючи традиційні ієрархічні щаблі [2]. Використання криптовалют значно ускладнює відстеження фінансових потоків, які є ключовим елементом у викритті великих злочинних мереж та конфіскації активів, здобутих злочинним шляхом [2]. Анонімність, яку забезпечують ці платформи, знижує ризики для окремих учасників і водночас сприяє залученню ширшого кола осіб до незаконної діяльності [1].

У результаті формуються складні мережеві структури, у межах яких окремі «вузли» здатні функціонувати автономно. Це робить традиційні методи «обезголовлення» злочинних організацій шляхом арешту їхніх лідерів менш ефективними, оскільки мережа швидко адаптується й відновлює втрачені елементи. Таким чином, актуальність проблеми зумовлюється тим, що боротьба з цифровою наркозлочинністю вимагає нових наукових підходів, комплексних правових рішень та застосування інноваційних криміналістичних методів, які б відповідали масштабам і динаміці сучасного цифрового середовища з урахуванням національного законодавства.

Аналіз останніх досліджень і публікацій. Наукова спільнота активно досліджує феномен використання цифрових платформ у наркоторгівлі. Значна кількість публікацій присвячена аналізу структури, функціонування та стійкості даркнет-ринків. Ці роботи часто використовують методи веб-скрейпінгу та аналізу великих даних для оцінки обсягів торгівлі, асортименту товарів, географії користувачів та динаміки цін. Зазначається, що незважаючи на періодичні успішні операції правоохоронних органів із закриття великих майданчиків, загальна екосистема даркнет-торгівлі демонструє високу адаптивність та здатність до швидкого відновлення [2].

Останніми роками зростає увага дослідників до використання загальнодоступних соціальних мереж (Facebook, Instagram, TikTok тощо) та зашифрованих месенджерів (Telegram, WhatsApp, Signal) для реклами, продажу та координації доставки наркотиків. [3] Дослідження вказують на використання специфічних кодів, емодзі, сленгу та тимчасових публікацій (наприклад, "сторіз") для уникнення автоматизованої модерації та виявлення правоохоронними органами. [5] Особливе місце серед месенджерів посідає Telegram, який завдяки своїм функціям анонімності (можливість реєстрації без SIM-карти, створення секретних чатів з автовидаленням повідомлень) та можливістю створення великих публічних і приватних каналів та груп, став надзвичайно популярним інструментом для наркодилерів. Фінансові аспекти онлайн-наркоторгівлі також є предметом пильної

уваги. Використання криптовалют, таких як Bitcoin, Monero та інших, є невід'ємною частиною функціонування цих ринків, забезпечуючи певний рівень псевдоанонімності транзакцій. Науковці аналізують методи відмивання криптовалют, що використовуються злочинцями (наприклад, через міксери, обмінники, онлайн-казино), та розробляють підходи до їх відстеження та деанонімізації учасників транзакцій [2].

Серед українських науковців цю проблематику активно опрацьовують, зокрема, О. П. Метелєв, який систематизує види цифрових доказів і пропонує чітке терміно-понятійне розмежування у КПК; А.-М. Ю. Ангеленюк, яка, спираючись на судову практику, пропонує класифікацію джерел отримання електронних доказів і окреслює проблемні питання їх використання; В. М. Фігурський, що обґрунтовує коректність поняття «докази в електронній формі» та визначає їх місце серед процесуальних джерел; О. В. Бабаєва разом із Д. В. Авербахом, які аналізують можливості використання доказів із відкритих джерел (OSINT) у світлі міжнародних рекомендацій, зокрема Протоколу Берклі, з акцентом на належність і допустимість; Ю. Ю. Орлов і С. С. Чернявський, які вводять і розкривають концепт «електронного відображення» як самостійного джерела доказів; а також О. В. Сіренко, що розробляє теоретичні засади інституту електронних доказів і обґрунтовує потребу їх чіткого законодавчого врегулювання.

Сукупно ці підходи конвергують вимогу оновлення процесуальної термінології, стандартизації процедур роботи з цифровими даними та інтеграції інструментів цифрової криміналістики й OSINT у практику досудового розслідування.

Метою цієї статті є наукове обґрунтування інтегрованої моделі протидії онлайн-наркоторгівлі, що поєднує криміналістичний аналіз цифрового середовища з процесуальними стандартами обігу електронних доказів. Передбачено систематизацію типів платформ (даркнет-ринків, соціальних мереж, зашифрованих месенджерів), технологій анонімізації та платіжних інструментів, а також опис «екосистеми» збуту з її вузлами, каналами трансакцій і типовими цифровими артефактами (метадані, логи, блокчейн-трейси). На цій основі пропонується методологія Digital Forensic Drug Intelligence (DFDI), що інтегрує цифрову криміналістику, OSINT і фізико-хімічне профілювання для ідентифікації ланцюгів постачання та доказування змови. Додатково конкретизуються процесуальні критерії належності, допустимості й достовірності електронних доказів (фіксація, хешування, chain of custody, участь спеціаліста), їх узгодження з судовою практикою та європейськими підходами, а також пропонуються прикладні рекомендації для слідчих, прокурорів і експертів щодо проактивного моніторингу, документування й збереження цифрових слідів у кримінальних провадженнях та транскордонного характеру злочинів.

Виклад основного матеріалу. Онлайн-ринок збуту наркотичних засобів функціонує як взаємопов'язана екосистема: платформи взаємодіють із засобами анонімізації та фінансовою інфраструктурою, кожен компонент якої генерує цифрові артефакти (лог-записи, метадані, блокчейн-події). Звідси — потреба в інтегрованій рамці Digital Forensic Drug Intelligence (DFDI), що поєднує цифрову криміналістику, OSINT і лабораторне профілювання для побудови єдиного ланцюга доказів [1; 2].

Перехід від опису явищ до моделювання причинно-наслідкових зв'язків створює методологічну основу для процесуальної придатності електронних доказів [1]. Тому є необхідність опису екосистеми онлайн-збуту як сукупність сегментів (даркнет-майданчики, відкриті платформи, зашифровані месенджери), кожен з яких продукує специфічні цифрові артефакти. Ця типологія слугуватиме дорожньою картою пошуку й фіксації слідів та визначатиме релевантні процесуальні дії у кожному випадку.

Для кращого розуміння логіки розвитку та взаємозв'язку сегментів цифрової наркоторгівлі на нашу думку доцільно представити її у вигляді «воронки». Вона демонструє послідовність переходу від початкових точок контакту до закріплених каналів збуту й фінансового забезпечення.

1. **Верхній рівень — відкриті соціальні платформи.** Соцмережі, форуми та дошки оголошень виконують роль «вітрини» або первинного контакту. Тут злочинці використовують кодові позначення, сленг, емодзі чи тимчасові акаунти для залучення потенційних клієнтів. Важливими слідами стають метадані публікацій, коментарі, посилання, що піддаються форензійній вебархівації.

2. **Середній рівень — даркнет-майданчики.** На цьому етапі відбувається основний збут наркотиків. Даркнет-ринки забезпечують відносну анонімність завдяки репутаційним системам, PGP-верифікації та використанню криптовалют. Вони генерують цифрові артефакти: лістинги товарів, журнали активності, ключі, адреси криптогаманців, які можна залучати як електронні докази.

3. **Логістичний рівень — зашифровані месенджери.** З E2EE-месенджерів (Telegram, Signal, WhatsApp) здійснюється координація доставки («закладки»), обмін інвайт-посиланнями та приватними повідомленнями. Тут ключовими слідами є часові патерни, метадані акаунтів, відбитки клієнтів та мережеві з'єднання. Доступ до кінцевих пристроїв і міжнародна правова допомога посилюють доказову базу.

4. **Фінансовий рівень — криптовалюти та платіжна інфраструктура.** Завершальний етап «воронки» — обіг коштів. Використовуються криптовалюти (Bitcoin, Monero), міксери, coinjoin-сервіси, а також біржі та кастодіальні провайдери з KYC/AML-вимогами. Саме тут часто з'являються найбільш стійкі точки атрибуції завдяки поєднанню блокчейн-аналізу й позаланцюгових даних.

Представлена «воронка» окреслює послідовність цифрової наркоторгівлі: від публічного залучення у відкритих платформах до укриття комунікацій у месенджерах і завершення у фінансовому контурі. Далі кожен рівень доцільно розглядати окремо, з фокусом на типових цифрових слідах, вразливостях для атрибуції та релевантних процесуальних діях (збирання, фіксація, допустимість).

1. Відкриті соціальні платформи — верхній рівень воронки

Відкриті платформи (соцмережі, форуми, дошки оголошень) виконують роль «воронки» первинного контакту та публічної вітрини збуту. Тут злочинці використовують кодові позначення, емодзі, тимчасові акаунти й редиректи у приватні канали, щоб обійти автоматизовану модерацію.

Типові цифрові сліди: пости/сторіз із геомітками, коментарі, публічні й приховані переходи («link in bio», шифровані інвайт-посилання). Навіть за суворої модерації платформи генерують достатньо метаданих (URL, час, автор, пристрій) для форензійної вебархівації та подальшої атрибуції [5].

Практичний приклад: 22.07.2024 Нацполіція України, за процесуального керівництва ОГП, ліквідувала мережу, що збувала наркотики через десятки Telegram-каналів; 14 затриманих, понад 20 кг вилучених речовин; документообіг здійснювався через месенджери та «закладки». Проблемою стало забезпечення доказового моста між публічною активністю та приватними каналами/чатами. Рішенням була вебархівація публічних матеріалів, фіксація інвайтів/URL, протоколи обшуків і вилучень пристроїв, кореляція часових патернів повідомлень із логістикою «закладок». У сукупності метадані й протоколи за ст.ст. 104–107, 234–237 КПК забезпечили допустимість електронних відомостей[9].

2. Даркнет-майданчики — середній рівень воронки

Даркнет ринки — це приховані торговельні платформи з системою репутації, ескорту та PGP-верифікації. Вони продукують специфічні цифрові артефакти: лістинги, ключі, журнали активності, адреси криптогаманців, «дзеркала» доменів. Вразливості виникають на стику онлайнових слідів і KYC-режимів обміну, а також через повторне використання ідентифікаторів [2].

Для даркнет-сегмента оптимальним є поєднання OSINT-збирання, блокчейн-кластеризації й процесуальної фіксації доступу до ресурсів із дотриманням chain of custody [1; 2].

Практичний приклад: Міжнародна операція «RapTor» (2025). 22 травня 2025 р. оголошено про затримання 270 осіб у ЄС, США та країнах Азії й Південної Америки, вилучення наркотиків, готівки та криптоактивів. Проблемою стало доведення зв'язку між лістингами, криптоплатежами та реальними особами. Вирішенням стала комбінація OSINT-моніторингу ринків під прикриттям, ончейн-аналізу транзакцій і запитів до KYC-бірж (on/off ramp), а також протоколи доступу/обшуків за національним законодавством [6].

3. Зашифровані месенджери — логістичний рівень воронки

E2EE-месенджери (Telegram, Signal, WhatsApp) забезпечують наскрізне шифрування і знижують оглядовість контенту. Водночас вони залишають спостережними часові й мережеві патерни, аватар-метадані, відбитки клієнтів, події приєднання до груп/каналів. Це дозволяє корелювати поведінкові дані з позамесенджерними артефактами (пости, платежі, геосліди) [2; 5].

Доступ до кінцевих пристроїв і міжнародні правові запити до сервісів критично посилюють доказову базу [1; 2; 5]. Приватність комунікацій також спирається на технології анонімізації (Tor/VPN, PGP, «bulletproof»-інфраструктури), що залишають характерні сліди.

Приклад: операція «Venetic» (UK, 2020–2025). Під час міжнародної співпраці (FR/NL/UK) отримано доступ до зашифрованих пристроїв; на підставі переписок і метаданих поліція довела участь у збуті наркотиків; у 2025 р. тривають вироки. Проблемою стала допустимість E2EE-даних і кореляція трафіку з контентом. Рішенням була валідація джерела, прив'язка до подій (час, місце), огляди пристроїв та допити.

Таким чином, суд приймає E2EE-докази за умови прозорої процедури їх одержання, відтворюваності та підтвердження іншими доказами.

4. Фінансовий контур — завершальний рівень воронки

Фінансовий контур формує окремий шар цифрових слідів: ончейн-транзакції, події on/off ramp, записи KYC/AML. Він часто надає найбільш стійкі точки атрибуції завдяки поєднанню блокчейн-евристик і позаланцюгових даних сервісів [2].

Bitcoin забезпечує псевдоанонімність, яка дозволяє кластеризувати адреси й відстежувати патерни витрат. Використання Monero/Zcash і міксерів/coinjoin створює «розриви» у ланцюгу. Критичними вузлами є біржі та кастодіальні сервіси з KYC/AML-вимогами. Паралельно застосовуються традиційні миттєві платежі, що полегшують кореляцію з реальними особами [5; 2].

Приклад: справа «Bitcoin Fog» (US, 2024). Громадянин Росії Роман Стерлігов, який керував криптовалютним міксером, отримав 5,5 років ув'язнення. Суд визнав доведеним, що ончейн-аналіз і дані бірж підтверджують походження коштів від даркнет-ринків [10].

Необхідно зазначити що навіть найкраща аналітика втрачає доказову силу без процесуально коректної фіксації джерел та способів доступу. Тому наступним кроком є визначення вимог КПК до виявлення, копіювання, зберігання й верифікації електронних даних та документування chain of custody. Це забезпечує перетворення цифрових артефактів і фінансових трас на допустимі докази.

Процесуальна придатність електронних доказів (т.з. КПК-рамка). Належність і допустимість електронних доказів визначаються за загальними правилами доказування: відомості мають бути отримані «у порядку, встановленому цим Кодексом» (ст. 84, 86 КПК України)[4], а порушення прав людини тягне їх недопустимість (ст. 87 КПК). Документальні джерела (у т.ч. комп'ютерні дані та їх копії) визнаються документами-доказами відповідно до ст. 99 КПК, тоді як носії інформації та техніка можуть набувати статусу речових доказів за ст. 98 КПК — за умови їхньої зв'язності з подією кримінального правопорушення [1;2;5]. Отримання електронних відомостей повинно відповідати процесуальним формам. Найпоширеніший інструмент — тимчасовий доступ до речей і документів (ст. 159–166 КПК), що дає можливість правомірно отримати лог-записи, дані облікових записів, інформацію провайдерів тощо. Якщо доступ не забезпечено добровільно, слідчий суддя може надати дозвіл на обшук (ст. 234–236 КПК) для відшукання й вилучення пристроїв або носіїв. Огляд місця події, приміщення чи комп'ютерної системи (ст. 237 КПК) застосовується для первинної фіксації слідів і збереження їхньої цілісності — у т.ч. шляхом створення точних копій даних (форензійних образів) з використанням хеш-ідентифікаторів [1; 2]. Про результати доступу/копіювання складається протокол (ст. 104 КПК) з описом дій, використаних інструментів та отриманих файлів; до протоколу долучаються матеріальні носії й електронні додатки (ст. 105 КПК). За можливості застосовується технічна фіксація (аудіо-, відеозапис) відповідно до ст. 107 КПК. Особливою гарантією належності є участь спеціаліста (ст. 71 КПК) під час ідентифікації, копіювання та верифікації даних; він забезпечує повторюваність процедури, документує контрольні хеш-суми та описує ланцюг зберігання (chain of custody). У разі потреби в спеціальних знаннях призначається експертиза (ст. 242 КПК), зокрема комп'ютерно-технічна чи телекомунікаційна, з постановкою питань щодо автентичності, цілісності та походження даних [1; 2; 5]. Для запобігання зміні або знищенню інформації доцільне накладення арешту на майно (ст. 170–173 КПК), у т.ч. на електронні пристрої й акаунти, якщо вони є знаряддям або містять сліди правопорушення. Доступ до відомостей, що знаходяться за кордоном, реалізується через міжнародну правову допомогу за правилами КПК та міжнародних договорів; при цьому запити про збереження даних (preservation) та їх надання мають бути оформлені з дотриманням вимог про компетенцію органу, межі запиту та допустимі формати надання [1; 2; 5]. У суді електронні відомості проходять подвійний тест: по-перше, на допустимість (ст. 86–87 КПК), по-друге — на достовірність і достатність у сукупності з іншими доказами (ст. 94 КПК). Типові підстави для відсікання: відсутність або дефект протоколу; недоведена автентичність файлів і метаданих; порушення порядку доступу (перевищення меж ухвали, збір без належної процесуальної підстави); відсутність безперервності ланцюга зберігання. Щоб уникнути таких ризиків, доцільно: (1) одразу фіксувати джерело даних, URL/ідентифікатори, час і умови доступу; (2) забезпечувати контрольні хеш-значення й їх відтворюваність; (3) описувати роль спеціаліста; (4) чітко прив'язувати електронні артефакти до інших джерел (допити, огляди, фінансові трейси) [1; 2]. Нарешті, варто розрізняти збирання доказів сторонами (ст. 93 КПК) та негласні слідчі (розшукові) дії, що допускаються лише за ухвалою слідчого судді і в суворих межах

розділу КПК про НСРД. Будь-які відомості, одержані поза процесуально визначеним порядком або з істотним порушенням прав, визнаються недопустимими (ст. 87 КПК) й не можуть бути покладені в основу вироку. Дотримання ст. 71, 84, 86–87, 93–99, 103–107, 159–166, 170–173, 234–237, 242, 94 КПК України забезпечує процесуальну придатність електронних відомостей; це мінімізує ризик їх відсікання судом [1; 2].

Висновки. Дослідження підтвердило, що в умовах воєнного стану та транскордонності цифрових слідів (ст. 84, 86 КПК України) цифрові платформи (даркнет-майданчики, відкриті соцмережі, E2EE-месенджери) і криптофінансова інфраструктура формують єдину екосистему онлайн-збуту наркотичних засобів. Вона генерує короткоживучі електронні артефакти та вимагає від кримінального процесу чітких, відтворюваних процедур виявлення, фіксації, збереження й оцінки таких відомостей.

У статті систематизовано «вузькі місця» судової оцінки електронних відомостей: дефект протоколу доступу/копіювання; відсутність контрольних хеш-сум і безперервного chain of custody; вихід за межі ухвали при тимчасовому доступі чи обшуку; недоведена належність акаунта/електронної адреси особі; неналежна трансформація контенту (скріншоти без верифікації метаданих/джерела). Запропонована матриця «сегмент → артефакт → процесуальна дія» орієнтує слідчого/прокурора, які саме статті КПК застосовувати для забезпечення належності й допустимості та як документувати участь спеціаліста.

На підставі викладеного пропонуємо внесення наступних змін до чинного Кримінального процесуального кодексу України:

1. **Нова ст. 99-1 КПК** про особливості вилучення, копіювання та зберігання електронних даних: обов'язкове побітове клонування, фіксація хеш-ідентифікаторів, протоколювання ПЗ/версій/методу доступу, технічна аудіо-/відеофіксація.

2. **Стандарти й підзаконні акти:** імплементація керівних принципів на кшталт ISO/IEC 27037 у відомчих інструкціях; типові форми протоколів огляду/копіювання й чек-лист chain of custody.

3. **OSINT/E2EE:** процесуальні вимоги до форензійної веб-архівації (URL, часові позначки, відтворюваність) та використання спостережних слідів із зашифрованих месенджерів (події, метадані, клієнтські відбитки) з обов'язковим підтвердженням даними кінцевих точок.

4. **Криптофінансовий контур:** закріпити порядок запитів до провайдерів on/off-ramp, вимоги до збереження журналів і форматів надання даних; узгодити на національному рівні процедури термінових preservation-запитів до закордонних суб'єктів.

5. **Міжнародна взаємодія:** уніфікувати шаблони MLAT/JIT для цифрових доказів; визначити центральний орган координації запитів і нагляду за строками/якістю відповіді.

На нашу думку доцільно створити спеціалізовані міжвідомчі групи (слідчі, прокурори, цифрові форензики, хіміки-аналітики) з єдиними наборами інструментів: форензійне клонування, блокчейн-аналітика, веб-архівація з доказовою силою, інструменти роботи з метаданими месенджерів, портативні аналізатори для експрес-діагностики. Розгорнути цільові програми підвищення кваліфікації (короткі модулі 40–80 год) з DFDI для підрозділів, що працюють із наркозлочинами й кіберзлочинністю.

Протидія цифровій наркозлочинності вимагає не «більше тих самих» заходів, а зміни парадигми: перехід від епізодичного реагування до проактивної розвідки-доказування, де цифрова криміналістика, OSINT, фінансова аналітика і лабораторні методи працюють як єдиний процесуально бездоганний механізм. Запропонована модель і пакет змін здатні зменшити поле анонімності для збувальників, підвищити стійкість доказування в суді та пришвидшити руйнування мереж збуту.

Література

1. Federal Bureau of Investigation. Global Operation Targets Darknet Drug. Federal Bureau of Investigation. 22.05.2025. URL: https://www.fbi.gov/news/stories/global-operation-targets-darknet-drug-trafficking (дата звернення: 19.08.2025).

2. Marchini C. S. The digital drug revolution: How online markets are reshaping global illicit trade. Global Initiative Against Transnational Organized Crime. 27.05.2025. URL: https://globalinitiative.net/ analysis/digital-drug-revolution-online-markets-global-illicit-trade-ocindex/ (дата звернення: 19.08.2025).

3. Dewey M., Buzzetti A. Easier, faster and safer: The social organization of drug dealing through encrypted messaging apps. *Sociology Compass*. 2024. Vol. 18, No. 2. e13175. DOI: 10.1111/soc4.13175 (дата звернення: 19.08.2025).

4. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. База даних «Законодавство України». *Верховна Рада України*. URL: https://zakon.rada.gov.ua/go/4651-17 (дата звернення: 19.08.2025).

5. Drug Enforcement Administration. Social Media Drug Trafficking Threat. U.S. Drug Enforcement Administration. 08.02.2022. URL: https://www.dea.gov/

sites/default/files/2022-03/20220208-DEA_ Social%20Media%20Drug%20Trafficking%20Threat%20Overview.pdf (дата звернення: 19.08.2025).

6. Міжнародна операція RapTor завдала нищівного удару по злочинних мережах даркнету. CyberSecureFox. 30.05.2025. URL: https://cybersecurefox.com/uk/operatsiya-raptor-mizhnarodnyy-udar-po-darknet-torhivli/ (дата звернення: 19.08.2025).

7. Міністерство внутрішніх справ України. Нацполіція ліквідувала наймасштабнішу мережу наркоділерів. Міністерство внутрішніх справ України. 22.07.2024. URL: https://mvs.gov.ua/news/ nacpolicia-likviduvala-naimasstabnisu-merezu-narkodileriv (дата звернення: 19.08.2025).

8. United Nations Office on Drugs and Crime. World Drug Report 2024. United Nations Office on Drugs and Crime. 2024. URL: https://www.unodc.org/unodc/en/data-and-analysis/world-drug-report-2024. html (дата звернення: 19.08.2025).

9. Understanding Europe's drug situation in 2024 — key findings. Santé.lu. 2024. — URL: https://santesecu.public.lu/dam-assets/fr/publications/r/rapport-europen-sur-les-drogues-2024/rapport-drogues-eu-2024.pdf (дата звернення: 19.08.2025).

10. U.S. Department of Justice, U.S. Attorney's Office for the District of Columbia. Operator of 'Bitcoin Fog' Sentenced to More Than 5 Years in Prison for Running Notorious Darknet Cryptocurrency Mixer. United States Department of Justice. 08.11.2024. URL: https://www.justice.gov/usao-dc/pr/operator-bitcoin-fog-sentenced-more-5-years-prison-running-notorious-darknet (дата звернення: 19.08.2025).

11. Europol. EU Serious and Organised Crime Threat Assessment 2025: The changing DNA of serious and organised crime. Europol. The Hague, 2025. URL: https://www.europol.europa.eu/cms/sites/default/files/ documents/EU-SOCTA-2025.pdf (дата звернення: 19.08.2025).

Дарій С. В.,
викладач кафедри оперативно-розшукової діяльності навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Національної поліції України Одеського державного університету внутрішніх справ

Матвєєвський О. В.,
старший викладач кафедри кримінально-правових дисциплін Інституту права та безпеки Одеського державного університету внутрішніх справ

Федоров І. В.,
кандидат юридичних наук, старший викладач кафедри кримінально-правових дисциплін Інституту права та безпеки Одеського державного університету внутрішніх справ

Дата надходження статті до редакції: 29.08.2025
Дата затвердження статті до друку: 15.09.2025
Дата публікації статті: 14.11.2025