4. Калугін В. Ю., Сіфоров О. І. Використання OSINT у встановленні фактів воєнних злочинів та особи воєнних злочинців. Воєнний стан: теоретико-праксеологічні проблеми юриспруденції : колективна монографія. Львів ; Торунь : Liha-Pres, 2025. С. 202–225. URL: https://doi.org/10.36059/978-966-397-421-7-10.

5. Книженко С. О. Стратегія розслідування воєнних злочинів. Аналітично-порівняльне правознавство. 2026. Т. 3. 476 с. URL: https://doi.org/10.24144/2788-6018.2026.01.3.11.

Деревягін Олексій Олександрович,
професор кафедри оперативно-розшукової діяльності та розкриття злочинів ННІ № 2 Харківського національного університету внутрішніх справ, кандидат юридичних наук, старший науковий співробітник

ЦИФРОВА КРИМІНАЛІСТИЧНА РОЗВІДКА В СИСТЕМІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ

Трансформація сучасної кримінальної протиправності детермінувала фундаментальну зміну об’єктів криміналістичного дослідження та оперативно-розшукової діяльності. В умовах тотальної цифровізації традиційні матеріальні сліди-відображення стрімко втрачають своє пріоритетне значення, що нівелює ефективність виключно ретроспективного підходу та класичних слідчих (розшукових) дій [1, с. 37]. З огляду на дистанційний характер вчинення злочинів та використання зловмисниками засобів анонімізації, правоохоронна система змушена переходити до проактивних моделей інформаційно-аналітичного забезпечення.

У цій новій архітектурі протидії кримінальній протиправності ключову роль відіграє цифрова криміналістична розвідка. З позицій сучасної правової науки, інтеграція криміналістичного компонента у концепцію «цифрової розвідки» (Digital Intelligence) відображає об’єктивну еволюцію вчення про сліди. Оскільки неструктурований цифровий слід вимагає застосування проактивних пошукових алгоритмів, розвідка кіберпростору

переростає статус допоміжного оперативного інструменту і стає фундаментальним елементом криміналістичної тактики.

Водночас генезис та функціонал цього явища нерозривно пов'язані саме з оперативно-розшуковою діяльністю. Традиційна криміналістика працює з переважно локалізованими об'єктами, тоді як кіберпростір вимагає проактивного пошуку в умовах абсолютної інформаційної невизначеності. Головним суб'єктом такої розвідки об'єктивно виступає оперативний працівник або кримінальний аналітик. Їхнє завдання полягає не лише у фіксації електронних слідів, а в інтелектуальному моделюванні поведінки зловмисника, превентивній деанонімізації та виявленні латентних кримінальних мереж. Синтез оперативної форми пошуку та криміналістичної мети доказування дозволяє правоохоронцям трансформувати абстрактну оперативну гіпотезу (яка генерується на основі розрізнених цифрових артефактів) у чітко структуровану слідчу версію.

Отже, розвідка не просто обслуговує досудове розслідування, вона його спрямовує. Її цільове призначення полягає в генерації тактичної переваги для слідчого: від формування версій до картування локацій та трасування прихованих мережевих зв'язків. Водночас для ефективного правозастосування цей інструментарій необхідно суворо розмежовувати із цифровою криміналістикою у її вузькому, судово-експертному розумінні. Якщо остання фокусується на процесуально регламентованому дослідженні вилучених цифрових артефактів для формування прямої доказової бази, то цифрова криміналістична розвідка оперує великими даними (Big Data) на початкових етапах оперативно-розшукової діяльності. Отже, вона не підміняє традиційну комп'ютерно-технічну експертизу, а забезпечує орган досудового розслідування матрицею первинної орієнтуючої інформації для визначення точного алгоритму, об'єкта та віртуальної географії подальшої процесуальної легалізації електронних доказів.

Об'єктивною основою для реалізації розвідувальних алгоритмів виступає парадигма цифрового сліду, який акумулює інформацію про діяльність суб'єкта в мережі Інтернет. З позицій кримінального аналізу такі сліди доцільно диференціювати на активні (свідомо згенерований контент) та пасивні (апаратно-програмні відомості, лог-файли, телекомунікаційні метадані). Водночас інформаційно-аналітичним «мостом» між віртуальним

простором і матеріальним світом виступає цифровий ідентифікатор – стійкий набір мережевих, апаратних чи персональних ознак (IP/MAC-адреси, IMEI, рекламні ідентифікатори) [2, с. 145]. Встановлення взаємозв'язку між цифровим ідентифікатором та цифровим слідом дозволяє оперативним підрозділам не лише деанонімізувати користувача, а й реконструювати хронологію та географію його протиправної діяльності.

Для ефективної інтеграції цього інструментарію в практичну діяльність необхідно концептуально розмежовувати цифрову криміналістичну розвідку та цифрову криміналістику. Прикметник «криміналістична» у цьому контексті вказує на її цільове призначення – забезпечення потреб досудового розслідування. Якщо остання фокусується на процесуально регламентованому експертному дослідженні вилучених цифрових артефактів для формування прямої доказової бази, то цифрова криміналістична розвідка оперує неструктурованими масивами даних на етапі оперативно-розшукової діяльності. Її первинна мета – генерація тактичної переваги: виявлення прихованих мережевих зв'язків, трасування віртуальних активів та просторово-часова реконструкція подій. Отже, цифрова криміналістична розвідка не підміняє судово-експертну криміналістику, а забезпечує оперативного працівника масивом первинної орієнтуючої інформації для формування тактики її подальшої процесуальної легалізації.

Архітектура цифрової криміналістичної розвідки ґрунтується на суворій класифікації об'єктів дослідження за правовим режимом доступу до них. Дистанційний моніторинг відкритих інформаційних ресурсів методами OSINT, SOCMINT чи GEOINT здійснюється без застосування заходів процесуального примусу. Натомість інформаційне проникнення у закриті телекомунікаційні спільноти (у тому числі в тіньовому сегменті Darknet), що супроводжується активною комунікацією під легендою або застосуванням цифрових пасток, виходить за межі відкритих методів криміналістичної розвідки. Залежно від інтенсивності втручання та характеру взаємодії, такі заходи потребують санкціонування в межах негласних слідчих (розшукових) дій, зокрема зняття інформації з електронних інформаційних систем (ст. 268 КПК України), виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації (ст. 272 КПК

України) або контролю за вчиненням злочину (ст. 271 КПК України). Ігнорування цієї процесуальної межі між пасивним моніторингом (OSINT) та активним оперативним проникненням неминуче призводить до визнання здобутих фактичних даних недопустимими в суді.

Технологічний інструментарій цифрової криміналістичної розвідки еволюціонував від фрагментарного ручного пошуку до застосування комплексних інформаційно-аналітичних платформ [4, с. 206]. У межах її спеціалізованих напрямів, зокрема розвідки в соціальних медіа (SOCMINT) та Telegram OSINT, оперативні підрозділи залучають засоби автоматизованого парсингу й платформи для генерації аналітичних графів зв'язків (Maltego, вітчизняний комплекс IRBIS). Видова розвідка (IMINT) спирається на технології біометричної ідентифікації облич на базі нейромереж (PimEyes, Clearview AI). Проте застосування таких систем в оперативній практиці стикається з викликами у сфері захисту персональних даних та верифікації алгоритмів. З огляду на це, результати автоматизованого розпізнавання облич мають розглядатися виключно як орієнтуюча інформація (ймовірнісний збіг), що генерує оперативно-розшукову версію, але для процесуального доведення вимагає обов'язкового проведення традиційних слідчих (розшукових) дій (пред'явлення для впізнання) або судово-портретної експертизи. Водночас фінансова розвідка (FININT) та аналіз віртуальних активів (CRYPTOINT) використовують потужності спеціалізованих блокчейн-платформ (Chainalysis, Crystal Intelligence) для кластеризації транзакцій, деанонімізації криптогаманців і встановлення кінцевих точок виведення тіньових активів у фіатну валюту.

Застосування активних методів збору даних та специфічних сервісів криміналістичної розвідки об'єктивно корелює з високими тактичними ризиками компрометації оперативно-розшукових заходів. Наприклад, використання комерційних агрегаторів контактів або сканування мережевої інфраструктури (CYBINT) вимагає від правоохоронців беззаперечного дотримання жорстких правил операційної безпеки (OPSEC) [5, с. 42]. З позицій оперативно-розшукової тактики, обов'язкова апаратна та програмна ізоляція робочого середовища (розгортання віртуальних машин, застосування ОС Tails, маршрутизація трафіку через мережі анонімізації)

необхідна не лише для убезпечення правоохоронця. Вона гарантує технологічну чистоту процесу збору даних, унеможливлюючи контамінацію (змішування) цифрових слідів правопорушника зі слідами оперативного працівника, що є критичною умовою для їх подальшого визнання належними та допустимими доказами.

Критичним і фінальним етапом циклу цифрової криміналістичної розвідки є процесуальна легалізація здобутих даних. Аналіз актуальної практики Касаційного кримінального суду (зокрема, постанови у справі № 947/22776/22) підтверджує безальтернативність технологічної верифікації [6]. В умовах волатильності цифрового середовища легалізація результатів відкритої розвідки вимагає суворого дотримання вимог статті 99 КПК України щодо роботи з електронними документами. Фіксація вебсторінок чи цифрових комунікацій повинна здійснюватися із застосуванням спеціалізованого апаратно-програмного інструментарію (зокрема для збереження вихідного коду або створення криміналістичних веб-архівів) з обов'язковим обчисленням криптографічних хеш-сум (наприклад, сімейства SHA-256) згенерованих файлів. Механізм побітового копіювання в алгоритмах OSINT не застосовується, оскільки об'єктом фіксації є динамічні мережеві дані, а не локальні фізичні носії інформації. Отже, інтеграція криміналістичного підходу до розвідувальної діяльності в кіберпросторі є не термінологічною гіпотезою, а об'єктивною вимогою: вона підпорядковує пошукові алгоритми кінцевій меті кримінального судочинства – конвертації орієнтуючої інформації у верифіковану процесуальну форму. Проте результативність цієї системи повністю залежить від здатності всіх уповноважених суб'єктів (оперативних працівників, кримінальних аналітиків, слідчих та спеціалістів) неухильно дотримуватися стандартів забезпечення цілісності цифрових слідів.

Список використаних джерел

1. Степанюк Р. Л. Цифрова криміналістична розвідка: поняття та перспективи розвитку. *Право і безпека*. 2026. № 1 (100). С. 36–47.

2. Теоретико-прикладні засади протидії кіберзлочинності : монографія / В. Б. Коба, В. Г. Дрозд, О. В. Манжай, К. О. Чаплинський та ін. ; МВС України, Нац. поліція України. Вінниця : ТВОРИ, 2026. 300 с.

3. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17.

4. OSINT у правоохоронній діяльності: міжнародний досвід та українські перспективи / К. Є. Борисова, К. Р. Жмуровська, Є. Є. Кришталь, О. О. Деревягін. *Universum*. 2025. № 25. С. 205–210.

5. Використання кримінальної розвідки, OSINT, SOCINT та інших механізмів для збору доказів торгівлі людьми і організації нелегальної міграції : наук.-метод. рек. / розроб. О. В. Манжай. Харків : ХНУВС, 2025. 109 с.

6. Постанова Касаційного кримінального суду від 27 січ. 2025 р. : справа № 947/22776/22. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/124866093.

Дідух Надія Тарасівна,
курсант Львівського державного університету безпеки життєдіяльності
Науковий керівник:
старший викладач кафедри права та менеджменту у сфері цивільного захисту Львівського державного університету безпеки життєдіяльності, кандидат юридичних наук
Сеник Петро Романович

ПРАВА Й ОБОВ'ЯЗКИ ГРОМАДЯН У СФЕРІ ДЕРЖАВНОГО УПРАВЛІННЯ

Сучасний етап розвитку України як демократичної, соціальної та правової держави передбачає активну участь громадян у процесах державного управління. Саме людина, її права і свободи визнаються найвищою соціальною цінністю, що закріплено в Конституції України. У цьому контексті особливого значення набуває питання реалізації прав і виконання обов'язків громадян, адже вони є основою взаємодії особи і держави. Права громадян у сфері державного управління становлять систему юридично закріплених можливостей, які забезпечують участь особи у формуванні та реалізації державної політики. Одним із