ukraini-zaversheno-masshtabnyi-tsykl-treninhiv-socta-nats politsiia-vprovadzhuie-ievropeisku-model-protydii-orhanizovanii-zlochynnosti

4. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «SOCTA» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : Наказ Міністерства внутрішніх справ України від 08.11.2023 № 902. Зареєстровано в Міністерстві юстиції України 27 листопада 2023 р. за № 2041/41097. URL: https://zakon.rada.gov.ua/laws/show/z2041-23

5. Рішення BriefCam для швидкого аналізу та відеоаналітики. URL: https://ukrinformsystems.com.ua/uk/technologii/videoanalityka/briefcam.

6. Загальний регламент про захист даних (GDPR). URL: https://gdpr-text.com/uk/

Василинчук Віктор Іванович,
професор кафедри оперативно-розшукової діяльності та національної безпеки Національної академії внутрішніх справ, доктор юридичних наук, професор;
Дремблюга Марина Тарасівна,
здобувач ступеня вищої освіти магістра Національної академії внутрішніх справ

МІЖНАРОДНА ВЗАЄМОДІЯ ПІД ЧАС ПРОВЕДЕННЯ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ У DARKNET

Darknet – анонімна частина глобальної мережі, що функціонує з використанням спеціалізованих протоколів шифрування та маршрутизації (Tor Browser, I2P). Він перетворився на основний майданчик для вчинення кіберзлочинів, обігу наркотичних засобів, зброї та інших товарів забороненого цивільного обігу. Складність ідентифікації суб'єктів у цьому середовищі унеможливлює ефективне розслідування зусиллями правоохоронних органів лише однієї держави [1, с. 33].

Правова природа міжнародної взаємодії у сфері негласних слідчих (розшукових) дій ґрунтується на загальному принципі співробітництва держав, закладеному в нормах Статуту ООН (ст. 1, 11, 13, 55, 56) та Віденській конвенції про право

міжнародних договорів. Водночас спеціалізоване регулювання, що охоплює аспекти негласного збору інформації, переважно фрагментоване. Воно базується на низці конвенцій ООН у сферах протидії міжнародному тероризму (Конвенції 1963, 1970, 1971, 1979 років), незаконному обігу наркотичних засобів (Конвенції 1961, 1971, 1988 років) та інших транскордонних злочинах [2, с. 9].

Слід зауважити, що негласний характер діяльності вимагає специфічних механізмів довіри. У державах із різними правовими системами дії негласного характеру мають відмінні поняття: «кримінальна розвідка», «негласні розслідування» тощо [1, с. 34]. У випадках відсутності спільних положень, міжнародні угоди обмежуються лише загальними формулюваннями, що залишає правове регулювання застосування спеціальних методів у «сірій зоні».

Однією з головних проблем залишається територіальність юрисдикції. Правоохоронні органи держави мають повноваження лише в межах власної території, тоді як цифрові активи в Даркнеті можуть бути розподілені між серверами в різних юрисдикціях одночасно. Жорсткі вимоги законодавства про державну таємницю стають проблемою, що змушує правоохоронців вдаватися до неофіційних форм комунікації, таких як: електронною поштою, через особисті контакти тощо.

Також існує проблема встановлення реальної особи користувача та фізичного розташування серверів. Використання криптовалют у зашифрованих каналах комунікації робить фінансові транзакції наркокартелів і хакерських угруповань практично недоступними для моніторингу. За даними УНЗ ООН, злочинні організації активно використовують ці ресурси для продажу наркотичних засобів, зброї, контрафактних товарів, а також торгівлі персональними даними [1, с. 42].

Показовим прикладом успішної міжнародної взаємодії стала операція RapTOR, проведена за підтримки Європолу та за участю команди JCODE. У межах цієї операції правоохоронні органи США, країн Європи, Азії та Південної Америки здійснили перевірку Darknet, зокрема сайтів Nemesis, Tor2Door, Bohemia та Kingdom Markets. Результатом стало вилучення понад 200 мільйонів доларів США у валютних та цифрових активах, конфіскація понад 2 тонн наркотичних засобів (зокрема

фентаніл) та понад 180 одиниць вогнепальної зброї. Понад 270 підозрюваних були затримані в різних юрисдикціях [3].

Аналогічно важливим є кейс операцій щодо торговельних майданчиків AlphaBay та Hansa. Успіх операції був зумовлений використанням методу «міграції» злочинців. Після закриття доступу до AlphaBay під керівництвом США, користувачі були вимушені перейти на ресурс Hansa, який вже перебував під контролем нідерландської поліції [4, с. 96].

На сьогодні найбільш прогресивною моделлю міжнародної співпраці у кримінальних провадженнях є досвід Європейського Союзу. Правове регулювання в межах ЄС базується на механізмах взаємної правової допомоги. Вагомим є впровадження Європейського ордера на розслідування, закріпленого Директивою 2014/41/ЄС. Він дозволяє компетентним органам однієї держави-члена здійснювати процесуальні дії від отримання доказів до допитів на території іншої держави без проходження багатоетапних процедур [5]. Цифровізація кримінального процесу в ЄС досягла свого апогею з ухваленням Регламенту 2023/1543 щодо електронних доказів. Він передбачає можливість прямого звернення правоохоронних органів до провайдерів електронних послуг у межах ЄС, фактично виключаючи необхідність залучення центральних органів влади до кожного запиту на отримання даних [6].

Для України, яка прагне інтеграції в європейський правовий простір, цей досвід є важливим. Чинне законодавство України значною мірою зосереджене на внутрішніх процедурах, що об'єктивно обмежує можливості оперативних підрозділів у міжнародному вимірі. Зокрема, існуюча процедура отримання доказів від інших держав через механізми міжнародної правової допомоги часто не відповідає вимогам оперативності.

Попри значні успіхи в уніфікації правил у межах ЄС, Б. М. Висоцький слушно зауважує, що навіть за умови активного використання цифрових інструментів, залишаються суттєві відмінності у процесуальних стандартах держав щодо судового контролю. Часто виконання запитів про доступ до електронних даних вступає у колізію з вимогами захисту персональних даних та принципом пропорційності. Тому для України важливо не лише копіювати європейські стандарти, а й забезпечити належний баланс між ефективністю розслідувань і дотриманням прав людини [7, с. 228].

Отже, міжнародне співробітництво є безальтернативним інструментом протидії злочинності в мережі Darknet. З огляду на анонімний характер цього сегменту мережі та швидкість транскордонних операцій, класичні механізми міжнародної правової допомоги потребують реформування. Ефективність боротьби з кіберорганізованою злочинністю безпосередньо залежить від участі держави у спільних слідчих групах. Також правоохоронна діяльність у сфері Darknet неможлива без використання спеціалізованого програмного забезпечення для аналізу криптовалютних транзакцій та відстеження анонімних комунікацій.

Подальший розвиток системи міжнародного співробітництва під час проведенні негласних слідчих (розшукових) дій у Даркнеті має відбуватися шляхом об'єднання теорії та практики.

Список використаних джерел

1. Кружкова Є. Міжнародна співпраця у боротьбі з наркоторгівлею у державах Південно-Східної Азії : бакалаврська кваліфікаційна робота / Нац. ун-т «Львівська політехніка». Львів, 2025. 63 с.

2. Князєв С. М., Чернявський С. С., Грібов М. Л. Міжнародне співробітництво у сфері негласних розслідувань. *Науковий вісник Національної академії внутрішніх справ*. 2020. № 4 (117). С. 7–19. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/fa85f01b-ffb4-4706-b25d-6503f376a319/content

3. ICE, Europol, law enforcement partners, dismantle major illicit drug networks in global Darknet crackdown : U.S. Immigration and Customs Enforcement official website. *U.S. Immigration and Customs Enforcement*. 2025. May 22. URL: https://www.ice.gov/news/releases/ice-europol-law-enforcement-partners-dismantle-major-illicit-drug-networks-global

4. Гуцалюк М. В. Загрозливі тенденції організованої кіберзлочинності. *Інформація і право*. 2020. № 1 (32). С. 88–98.

5. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. URL: https://eur-lex.europa.eu/eli/dir/2014/41/oj/eng

6. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal

proceedings and for the execution of custodial sentences following criminal proceedings. URL: https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng

7. Висоцький Б. М. Зарубіжний досвід регулювання процесуальних дій у кримінальних провадженнях під час міжнародного співробітництва. *Київський часопис права*. 2026. № 2. С. 226–231. URL: https://kyivchasprava.kneu.in.ua/index.php/kyivchasprava/article/view/836/791

Власова Олена Вікторівна,
начальник відділу Департаменту кримінального аналізу Національної поліції України

ВІД НАЦІОНАЛЬНОГО ДО РЕГІОНАЛЬНОГО ОЦІНЮВАННЯ ЗАГРОЗ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ: ІНСТИТУЦІОНАЛІЗАЦІЯ SOCTA УКРАЇНА В СИСТЕМІ КРИМІНАЛЬНОГО АНАЛІЗУ

Трансформація правоохоронної системи України в умовах повномасштабної збройної агресії та євроінтеграційних процесів потребує переходу до проактивної моделі поліцейської діяльності, керованої аналітикою (Intelligence-Led Policing) [1, с. 66]. Фундаментальним інструментом цієї моделі є система оцінювання загроз серйозної та організованої злочинності (SOCTA Україна), яка дає змогу ідентифікувати кримінальні ризики та формувати пріоритети державної політики на основі об’єктивних даних. Процес інституціоналізації SOCTA в Україні пройшов шлях від схвалення Стратегії боротьби з організованою злочинністю у 2020 році до практичного впровадження регіонального оцінювання у 2026 році.

Нормативно-правовий фундамент системи було закладено розпорядженням Кабінету Міністрів України від 16.09.2020 № 1126-р, яке визначило трирівневу модель формування державної політики: проведення оцінювання загроз, визначення стратегічних цілей та виконання комплексних планів заходів [2]. На виконання цієї Стратегії постановою Кабінету Міністрів України від 26.01.2022 № 59 офіційно запроваджено систему оцінки SOCTA Україна, затверджено порядок збирання інформації та утворено відповідну міжвідомчу робочу групу [3].