

*Дмитренко Тетяна Леонідівна,*  
завідувач відділу міжнародних фінансів  
та фінансової безпеки відділення глобальної  
економіки і міжнародних фінансів НДФІ  
ДННУ «Академія фінансового управління»,  
AML-консультант ОБСЄ та УНЗ ООН  
(м. Відень, Австрія), кандидат економічних  
наук

## **ПРОТИДІЯ ГЛОБАЛЬНИМ ВИКЛИКАМ, ПОВ'ЯЗАНИМ З ВИКОРИСТАННЯМ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ У ЗЛОЧИННИХ ЦІЛЯХ, ШЛЯХОМ ПІДВИЩЕННЯ СТАНДАРТІВ КРИМІНАЛЬНОГО АНАЛІЗУ**

Посилення процесів глобалізації, невизначеність щодо обрання вектору соціально-політичного розвитку, сповільнення темпів стійкого економічного зростання та неефективність механізму державного управління системою економічних відносин зумовлюють інтенсифікацію розвитку тіньової економічної діяльності, поширення корупції, зниження рівня економічної безпеки країни та сприяють зростанню рівня офшоризації національної економіки. Акумуляція тіньового капіталу внаслідок зростання прибутковості та мобільності операцій з фінансовими ресурсами сприяють розвитку нелегального сектора економіки, результати діяльності якого потребують легалізації та залучення в офіційну економіку. За таких умов актуалізується проблема забезпечення ефективної протидії зазначеним дестабілізуючим чинникам та розроблення дієвого механізму ідентифікації зовнішніх та внутрішніх загроз і ризиків, що чинять істотний вплив на систему протидії відмиванню коштів та фінансуванню тероризму.

Достатньо деталізоване розуміння та розмежування значення категорій «загрози», «ризиків» та «вразливості» подане у Методиці національної оцінки ризиків відмивання коштів та фінансування тероризму в Україні [8, с. 9, 20], відповідно до якої загрозами системи протидії легалізації (відмиванню) коштів та фінансуванню тероризму вважаються особи або групи осіб, об'єкти, діяльність, які в сукупності або окремо спроможні завдати шкоди державі, суспільству та економіці, а вразливостями являються фактори, що створюють умови для виникнення й реалізації загроз, та сфери, в яких загрози можуть реалізуватися.

На прикладі протидії використанню криптовалют для забезпечення розрахунків в торгівлі наркотичними речовинами покажемо зростаючу важливість використання новітніх аналітичних програм, висококваліфікованого персоналу, що забезпечує високі стандарти та ефективність проведення кримінального аналізу злочинів.

За рахунок використання нових аналітичних програм дослідження операцій з криптоактивами, такими як Chainalysis Reactor [1], Crystal [2], CipherTrace [3], Elliptic [4], DarkOwl [5] та подібного аналітичного програмного забезпечення США й Німеччина

спільними зусиллями знешкодили найбільший у світі нелегальний російськомовний ринок даркнету Hydra Market.

«Існують підозри щодо комерційної діяльності кримінальних торгових майданчиків в Інтернеті, комерційного придбання чи надання можливості для несанкціонованої купівлі або несанкціонованого продажу наркотиків, а також щодо відмивання комерційних грошей», – зазначається в прес-релізі Федерального відомства кримінальної поліції Німеччини [6]. Вони закрили сервери «Гідри» у ФРН та конфіскували біткоїни на суму \$25 мільйонів. Водночас проти нелегального ринку запровадив санкції американський уряд.

«Сьогодні OFAC (Офіс контролю за іноземними активами Міністерства фінансів США, – ред.) запровадив санкції проти найбільшого та найвідомішого у світі ринку даркнету Hydra Market у межах скоординованих міжнародних зусиль щодо припинення торгівлі зловмисними кіберпослугами, небезпечними наркотиками та іншими незаконними пропозиціями, доступними через російський сайт», – йдеться у повідомленні відомства [7].

Hydra Market – нелегальний ринок даркнету. Через мережу Tor доступ до нього можна отримати з 2015 року. Майданчик налічував близько 17 мільйонів клієнтів та понад 19 000 продавців.

Німецькі спецслужби зазначають, що Hydra Market мала найвищий обсяг продажів у світі серед усіх нелегальних торгових платформ. Лишень у 2020 році його продажі склали не менше 1,23 мільярда євро [6].

Нещодавні новини про те, що влада Німеччини видала наказ про конфіскацію біткоїнів на суму 25 мільйонів доларів США з основного російського даркнет-ринку, сколихнули криптовалютну спільноту. Німецька поліція зазначила, що змішувач конфіденційності Hydra Market доставляв їм багато проблем під час розслідування.

Федеральна кримінальна поліція Німеччини та Франкфуртське управління боротьби з кіберзлочинністю вилучили 543 BTC під час конфіскації серверів сайту. Невдовзі після того, як вибухнула новина про поглинання Hydra, з'явилося, що нове місце в даркнеті змагається за перше місце.

Огляд динаміки біткоїнів і даркнету у другому півріччі 2022 року порівняно з 2020 і 2021 роками. Показав, що даркнет маркетплейс OMG! OMG! Може стати новим Hydra Market [8].

В сучасних умовах новітніх технологій швидкий аналіз та оперативне реагування на виклики стає необхідною складовою роботи правоохоронних органів, а це можливо завдяки висококваліфікованому персоналу та забезпеченню сучасними ефективними засобами для аналізу та відслідковуванню злочинної діяльності.

Проведення аналізу операцій з крипто активами та, відповідно, фінансового моніторингу крипто активів потребує використання спеціальних баз даних, які дозволяють визначити належність певних «гаманців» в крипто валютах (так званий публічних адрес) до об'єктів

реального світу (бірж, обмінників, онлайн ринків у Даркнеті, кримінальних сервісів, тощо)

Найбільш критичним елементом є навчання фахівців. Як працівники органу нагляду, так і правоохоронних органів повинні знати, як працювати з криптовалютами. При цьому, навчання повинно базуватись на виконанні практичних вправ з реальними крипто активами та з використанням професійного програмного забезпечення.

Власне програмне забезпечення є відносно простим, для багатьох установ достатньо отримання доступу через інтернет-браузер («software as a service»). З досвіду тренінгових програм UNODC, достатньо кількох днів навчання для самостійного аналізу криптоактивів за допомогою програмного забезпечення в режимі реального часу на учбовій онлайн-платформі UNODC [9].

Представниками Департаменту кримінального аналізу Національної поліції України пройдено перший етап навчальних програм UNODC, які сприяли підвищенню кваліфікації співробітників. Необхідно зазначити, що в ході проведення тренінгів відбулось безпосередня комунікація з розробниками програмного забезпечення для проведення розслідувань діяльності на крипторинку, що збагатило досвід слухачів та сприяло встановлення інформаційного обміну як на національному, так і на міжнародному рівні в визначених законодавством межах та виконання покладених державою завдань та повноважень.

#### **Список використаних джерел**

1. 2020-Crypto-Crime-Report Chainanalysis. URL: <https://ag-pssg-sharedservices-ex.objectstore.gov.bc.ca/ag-pssg-cc-exh-prod-bkt-ex/257%20-%200001%20Appendix%20A%20-%202020-Crypto-Crime-Report%20Chainanalysis.pdf>.

2. Crystal Blockchain End of Year Report 2020. URL: <https://crystalblockchain.com/articles/crystal-blockchain-end-of-year-report-2020>.

3. Ciphertrace cryptocurrency intelligence, «Cryptocurrency Anti-Money Laundering Report, 2019 Q3», November 2019, 34. URL: <https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/>.

4. Elliptic Typologies Report Exposes Real Impact of Illicit Behavior in Crypto. URL: [https://www.elliptic.co/blog/elliptic-typologies-report-exposes-real-impact-of-illicit-behavior-in-crypto?utm\\_campaign=Typologies%20Report%202022&utm\\_content=202181793&utm\\_medium=social&utm\\_source=linkedin&hss\\_channel=lcp-5027267](https://www.elliptic.co/blog/elliptic-typologies-report-exposes-real-impact-of-illicit-behavior-in-crypto?utm_campaign=Typologies%20Report%202022&utm_content=202181793&utm_medium=social&utm_source=linkedin&hss_channel=lcp-5027267).

5. Superior Darknet Data Powering Better Decisions URL: <https://www.darkowl.com/>.

6. Illegal Darknet-Marktplatz «Hydra Market» abgeschaltet // Bundeskriminalamt. URL: [https://www.bka.de/DE/Presse/Listenseite\\_Pressemitteilungen/2022/Presse2022/220405\\_PM\\_IllegalerDarknetMarktplatz.html](https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220405_PM_IllegalerDarknetMarktplatz.html).

7. Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex // U.S. DEPARTMENT OF THE TREASURY. URL: <https://home.treasury.gov/news/press-releases/jy0701>.

8. Bitcoin & Darknet 2022: Is OMG!OMG! The New Hydra?// The Crystal analytics team. URL: [https://crystalblockchain.com/articles/darknet-interactions-2022-is-omgomg-the-new-hydra/?utm\\_source=Digest&utm\\_medium=email&utm\\_campaign=June+2022](https://crystalblockchain.com/articles/darknet-interactions-2022-is-omgomg-the-new-hydra/?utm_source=Digest&utm_medium=email&utm_campaign=June+2022).

9. Навчальний курс УНП ООН по криптовалютам. URL: <https://lms.gpml-crypto.org/login/canvas>.

*Заєць Олександр Михайлович,*  
науковий співробітник відділу  
інноваційного розвитку освіти та бізнесу  
Інституту ринку і економіко-екологічних  
досліджень Національної академії наук  
України, кандидат юридичних наук, доцент

## **НАВЧАЛЬНІ ПРАКТИКИ ВИКОРИСТАННЯ МЕТОДУ ВСТАНОВЛЕННЯ ПРИХОВАНИХ ДОХОДІВ ПІДОЗРЮВАНИХ ОСІБ (FININT)**

Гібридна форма злочинності виникла з традиційно відмінних форм організованої злочинності та тероризму, щоб створити нову загрозу для правоохоронних органів. Злочинні групи, які колись вважалися такими, що використовують злочинні доходи лише для фінансування атак, живуть переважно за рахунок доходів від наркобізнесу, тоді як злочинні групи використовують насильницькі терористичні акти, щоб погрожувати громадам, щоб вони підкорилися. У небезпечній формі адаптації до конкуренції злочинні та терористичні групи застосували тактику та методи перехресного стилю, які сприяють створенню підприємницької мережі, очевидно, здатної протистояти правоохоронним органам. У офшорних зонах стає все важче відрізнити незаконні потоки доходів, посередників і підставні компанії, які підтримують тероризм, від тих, хто підтримує злочинність. Фінансова конвергенція є настільки серйозною, що спроби розмежувати ці два напрямки перешкоджатимуть зусиллям правоохоронних органів, спрямованих на знищення та ліквідацію злочинних і терористичних груп.

Швидкий технологічний прогрес і зростання підприємництва кардинально змінили суспільний ландшафт, у якому діють ці групи. Фінансова розвідка (FININT) є цінним інструментом, який правоохоронні органи можуть використовувати, щоб йти в ногу з супротивником, що постійно розвивається, і перешкоджати спробам фінансування незаконної діяльності. Поточні ініціативи щодо використання цього цінного джерела розвідувальних даних можна посилити на державному та місцевому