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.

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

рівнях через впровадження навчальних практик у освітньої професійні програми за відповідними напрямами.

FININT вимагається законом і суворо регулюється низкою заходів протидії відмиванню грошей і фінансуванню тероризму. FININT, заповнений у вищезазначених формах, є, зрештою, записом фінансової операції або серії операцій, які брали участь у одній або кількох фінансових установах і були ідентифіковані шляхом спостереження, слідчих (розшукових) дій будь-якою з фінансових установ. FININT у багатьох формах може містити особисту ідентифікаційну інформацію, дані облікового запису, дати, час, суми та історію транзакцій.

Звіти про підозрілу діяльність (SAR), за задумом, були винайдені, щоб служити фінансовим співтовариством методом конфіденційного звітування для правоохоронних органів [1]. Фінансові установи зобов'язані подавати їх, якщо фінансові операції чи предметна діяльність відповідають певним пороговим значенням або іншим чином визначаються як «підозрілі». Однак через вимоги до фінансових установ є певний простір для розсуду, коли справа доходить до подання звіту.

Звіт про підозрілу діяльність зазвичай займає кілька сторінок, перші кілька сторінок містять поля для ідентифікаційної інформації, реквізитів рахунку, дат і сум. Зміст звіту про підозрілу діяльність вимагають значної аналітичної майстерності, щоб створювати їх і часто слугують джерелом підозрюваної злочинної діяльності. Звіт відображає точне звітування про фінансові операції та підозрілу діяльність, будь-які деталі, необхідні для підтримки подання, аналітичну здатність тріангуляції джерел, а також дослідницьку та розслідувальну майстерність для виявлення, пошуку та фіксації слідів злочину.

FININT є цінним, оскільки він дає уявлення про доходи, витрати, активи, ділову діяльність, соціальні та ділові мережі, партнерів, подорожі та іншу діяльність окремих осіб і компаній. Наявність звіту про підозрілу діяльність щодо фізичної особи чи підприємства не завжди є явним свідченням злочинної діяльності. Проте, синхронізуючи з іншими формами розвідки, FININT може надати правоохоронним органам достатні докази для активного початку або продовження розслідування кримінальних правопорушень, які включають організовану злочинність, бандитизм, торгівлю наркотиками, тероризм, торгівля краденими або підробленими товарами, порушення авторських та суміжних прав, дитяча порнографія, торгівля людьми, контрабанда зброї та товарів.

Кожне розслідування та аналіз правоохоронних органів має містити фінансову складову. Незалежно від того, деталізовано транзакції в FININT або вказано в квитанції про оренду автомобіля, конкретна фінансова інформація повинна бути задокументована детективами та аналітиками, зафіксована в розвідувальних звітах для подальшого використання. Крім того, детективи повинні завжди допитувати підозрюваних про характер їхньої фінансової діяльності, у

деяких випадках підозрювані можуть охочіше говорити про гроші, ніж про ймовірну злочинну діяльність. Аналітики розвідки повинні також включати FININT і фінансову інформацію як одне з багатьох джерел розвідки. FININT може бути корисним для виявлення прихованих або офшорних рахунків і активів, моделей подорожей, додаткового майна, джерел доходу, партнерів, звичок і витрат. Якщо аналітик розвідки зіставляє дані про доходи об'єкта та порівнює їх із відомими витратами, він може виявити розбіжності, які вказують на додаткову злочинну діяльність, таку як відмивання грошей, ухилення від сплати податків або шахрайство з фінансовими ресурсами.

Дані FININT мають величезну цінність для розслідування правоохоронними органами кримінальних правопорушень. Мережа боротьби з фінансовими злочинами володіє понад 180 мільйонами записів фінансових операцій та інших звітів, які можна використовувати проактивно, ретроактивно або реактивно та стратегічно [2]. FININT попередніх фінансових операцій допомагає правоохоронним органам виявити мотиви, асоціації та зв'язки з людьми, місцями та основною злочинною діяльністю. Традиційне проактивне використання FININT включає запити даних для виявлення аномалій, підозрілих моделей і тенденцій, які можна використовувати для запобігання злочинній діяльності [3]. FININT також можна використовувати стратегічно для виявлення більших моделей у більш широкому масштабі.

Можливості для подальшої освіти та навчання є одним із найважливіших способів, за допомогою яких правоохоронні органи можуть залишатися актуальними, оскільки злочинці та терористи продовжують використовувати технологічні досягнення та займатися підприємництвом. Ряд дослідників показали, що злочинці та терористи об'єдналися й тепер використовують багато однакових тактик, методів і процедур [4, с. 129–145; 180–198]. Навчання правоохоронних органів щодо ролі FININT у процесі фінансування кримінальних правопорушень має вирішальне значення для їхнього успіху в підриві та ліквідації незаконної фінансової діяльності.

Тому викладачі повинні пропонувати курси, які передбачають використання сценаріїв, настільних і червоних (оборонно-наступальних) командних вправ, які зосереджуються на стратегії розслідування, а також на тому, як виглядатимуть злочини, скоєні в майбутньому. Тренінги та семінари також повинні включати компонент «засвоєних уроків», протягом якого правоохоронні органи та інструктори можуть переглядати тематичні дослідження та обговорювати методи розслідування, тобто те, що працює, що не спрацювало і що може спрацювати.

Наприклад:

Ситуаційні вправи. Навчання FININT, яке включає в себе ситуаційні вправи, де правоохоронні органи та аналітики працюють над вигаданими «сценаріями», дозволяє викладачам посилити

навчальні моменти, дозволяючи учасникам опрацьовувати набори проблем. У таких випадках правоохоронні органи та аналітики повинні працювати в невеликих групах і заохочуватися до творчої роботи та співпраці один з одним. В ідеалі кожна група повинна мати рівну кількість аналітиків і правоохоронних органів, які працюватимуть разом над одним довгостроковим сценарієм, який включає як слідчі, так і аналітичні методи. Коротші сценарії, які не передбачають групової роботи та виконуються всім класом одночасно, можна використовувати, але навряд чи вони сприятимуть міжвідомчій груповій участі, яка може мати місце під час довшої вправи. Сценарії можуть базуватися на попередніх подіях або бути повністю вигаданими [5, с. 204–257].

Настільні вправи також включають сценарії, однак у настільних вправах кожному учаснику призначається роль, вони одночасно «грають» і зосереджуються на процедурах і методології замість вирішення справи. Настільні вправи часто використовуються для тестування внутрішнього протоколу, міжвідомчої координації та операційної безпеки, і їх можна застосувати до сценарію розслідування, що передбачає використання FININT. Наприклад, слідчі та аналітики можуть опрацьовувати кейс із заявленою метою перегляду кожного етапу розслідування, аналітичного підходу, ведення справи та техніки звітування. Учасники обговорюють свою методологію та прийняття рішень замість фактів. Настільна вправа допоможе правоохоронним органам і аналітикам визначити припущення та упередження, зрозуміти стратегії розслідування, удосконалити методи та покращити робочі стосунки.

Червоні (оборонно-наступальні) командні вправи – це практика розгляду проблеми з точки зору суперництва або протилежності [6]. У навчальній вправі червона команда повинна грати або моделювати нападника, супротивника чи просто злодія, тоді як синя команда повинна грати за законом виконання – захисника. Червона команда, наприклад, може перевіряти безпеку системи (Bug Bounty), або, у випадку FININT, червона команда може працювати над створенням незаконного підприємства та відмиванням грошей. Суть вправи полягає в тому, щоб поставити під сумнів припущення та визначити ситуації, в яких менталітет є фіксованим, це можливість побувати в місцях, за межами найсміливішої уяви. Тактика і техніка, які використовують супротивники, не обмежені кордонами, інституційними упередженнями та структурними перешкодами. Червоні (оборонно-наступальні) командні вправи можуть допомогти звільнити правоохоронні органи та аналітиків від їх власної добре розвиненої ментальної моделі – власного почуття раціональності, культурних норм і особистих цінностей [7; 8].

Стрімкий розвиток технологій надали злочинним і терористичним мережам можливість розширювати свої операції та зв’язки далеко за межі їхніх зон конфлікту. У відповідь на зусилля

правоохоронних органів транснаціональні злочинні організації почали використовувати гібридну форму підприємництва. Оновлена оцінка та аналіз встановлення прихованих доходів підозрюваних осіб можуть надати правоохоронним органам можливість краще зрозуміти, як працюють незаконні мережі, приймаються рішення, розподіляють діяльність і функціонують злочинні середовища. Збільшення ресурсів і навчання на додаток до впровадження інноваційних стратегій навчання, таких як червоні (оборонно-наступальні) командні вправи нададуть правоохоронним органам України можливість сприяти знищенню та ліквідації гібридних злочинних груп та інших форм злочинних угруповань.

Список використаних джерел

1. Steve Gurdak, «The Trouble with SARs», ACAMs Today (March–May 2010). URL: http://files.acams.org/ACAMS_Today/Mar10-May10/trouble_w_sars.pdf.
2. Calvery, Jennifer Shasky. «Remarks of Jennifer Shasky Calvery». National Cyber-Forensics Training Alliance Cyfin 2013 Conference. Financial Crimes Enforcement Network. Pennsylvania, Pittsburgh. 16 Apr 2013. URL: http://www.fincen.gov/news_room/speech/html/20130416.html.
3. Cassara, John and Avi Jorisch, On the Trail of Terror Finance: What Law Enforcement and Intelligence Officers Need to Know (Arlington, VA: Red Cell Intelligence Group, 2010).
4. Tamara Makarenko, «The Crime-Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism», Global Crime 6:1 (2004): 129–145; John T. Picarelli, «Osama bin Corleone? Vito the Jackal? Framing Threat Convergence Through an Examination of Transnational Organized Crime and International Terrorism», Terrorism and Political Violence 24:2 (2012): 180–198.
5. Основи кримінального аналізу: підручник / Бабенко А.М., Заєць О.М., Некрасов В.А., Ісмайлов К.Ю., Пефтієв Д.О. та ін.; за заг. ред. Користіна О.Є., 2020. 296 с.
6. Mark Mateski, «Red Teaming: A Balance View», Red Team Journal (Bebruary 14, 2013). URL: http://redteamjournal.com/2013/02/red-teaming-a-balanced-view/.
7. Heuer, R. J., and R. H. Pherson. Structured Analytic Techniques for Intelligence Analysis. Washington D.C.: CQ Press, 2012.
8. Walton, Anne. «Financial Intelligence: Uses and Teaching Methods (Innovative Approaches from Subject Matter Experts)». Journal of Strategic Security 6, no. 3 Suppl. (2013) P. 393–400.
9. Peters, Grechen. «The Intersection of Crime and Conflict». Trans. Array The «New» Face of Transnational Crime Organizations (TCOs): A Geopolitical Perspective and Implications to U.S. National Security (Washington, D.C.: Kiernan Group Holdings, 2013): 81–85. URL: https://www.hsdl.org/?view&did=733208.