Побудовану матрицю можна використовувати для планування роботи правоохоронного органу щодо протидії, як окремим організованим злочинним угрупованням, так і організованій злочинності в цілому.

Список використаних джерел

1. Tusikov N., Fahlman R. C. Threat and risk assessments // Ratcliffe J.H. (Ed.), Strategic Thinking in Criminal Intelligence / 2nd ed. Federation Press, Sydney, 2009. pp. 147–164.

2. Bureau C. et al. Strategic Early Warning for Criminal Intelligence Theoretical Framework and Sentinel Methodology. 2007. 24 p. URL: pdfs.semanticscholar.org/8107/ce7733c54223f058c1c594de3ff583b70dfc.pdf.

Мовчан Анатолій Васильович,
професор кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ,
доктор юридичних наук, професор

ВИКОРИСТАННЯ АНАЛІТИЧНИХ ІНСТРУМЕНТІВ І ПРОЄКТІВ ІНТЕРПОЛУ ТА ЄВРОПОЛУ В ПРОТИДІЇ ТРАНСНАЦІОНАЛЬНІЙ ЗЛОЧИННОСТІ

У нинішніх умовах транснаціональна організована злочинність підриває економіку, суспільство та інститути держави. І це проблема переважної більшості країн світу. За результатами проведеного Європолом опитування SOCTA 2021, мільярди євро незаконних прибутків, отриманих організованою злочинністю в Європейському Союзі, було інвестовано в легальну економіку, що спотворює конкуренцію та перешкоджає економічному розвитку країн-членів Євросоюзу [1].

В останній оглядовій резолюції Глобальної контртерористичної стратегії, ухваленій Генеральною Асамблеєю 30 червня 2021 року, висловлюється глибока стурбованість використанням Інтернету, інших інформаційних і комунікаційних технологій, соціальних мереж у терористичних цілях, зокрема поширенням терористичного контенту та заохочує держави-члени працювати разом із відповідними зацікавленими сторонами, включаючи наукові кола, приватний сектор і громадянське суспільство, щоб гарантувати, що терористи не знайдуть місця в Інтернеті, одночасно підтримуючи відкритий, спільний, надійний та безпечний Інтернет, що сприяє ефективності, інноваціям, комунікації та економічному процвітанню, поважаючи при цьому міжнародне право, права людини, включаючи право на свободу висловлювання поглядів.

Проєкт CT TECH – це спільна ініціатива UNOCT/UNCCT та Інтерполу, яка фінансується ЄС і реалізується в рамках Глобальної антитерористичної програми UNCCT/UNOC з кібербезпеки та нових технологій. Він спрямований на зміцнення спроможності правоохоронних

органів і органів кримінального правосуддя протидіяти використанню нових технологій у терористичних цілях, а також підтримувати використання нових технологій у боротьбі з тероризмом.

Зокрема, CT TECH сприятиме державам-членам у розробці ефективних антитерористичних заходів у відповідь на виклики та можливості нових технологій у боротьбі з тероризмом, при повній повазі до прав людини та верховенства права, шляхом підвищення оперативної спроможності та політики правоохоронних органів і кримінального правосуддя, пов'язаних з протидією використання нових технологій у терористичних цілях.

Заходи в рамках проєкту CT-Tech включають:

– проведення оцінки потреб щодо поточних загроз та їх зв'язку з новими технологіями;

– розширення міжнародного співробітництва для розслідування боротьби з тероризмом у відповідних сферах;

– підготовка посібників для висвітлення належної практики конфіскацій та співпраці з ІКТ;

– розробка вебінарів, модулів електронного навчання та прикладних навчальних сесій з розпізнавання обличчя, розвідки з відкритих джерел (OSINT) і Dark net/віртуальних активів;

– проведення навчальних курсів та зустрічей регіональних робочих груп щодо використання біометричних можливостей Інтерполу;

– проведення навчання зі збору, збереження та використання цифрових доказів у судовому переслідуванні [2].

Розуміння тенденцій злочинності та злочинної поведінки є критично важливим для роботи поліції сьогодні. Своєчасний і точний аналіз розвідданих є ключовим для розуміння внутрішньої роботи та рушійних факторів злочинних явищ і злочинних організацій. Аналітики Інтерполу постійно вивчають низку даних, таких як соціально-демографічна інформація про злочинців, а також час і місце злочинної діяльності. Ця інформація може надходити з країн-членів або зовнішніх джерел, таких як дослідницькі інститути та аналітичні центри, і може стосуватися будь-якого типу злочину чи явища.

Інтерпол створює розвідувальні звіти для кримінальних підрозділів і для країн-членів. Це допомагає національним правоохоронним органам і особам, які приймають рішення, ефективніше справлятися з невизначеністю в поліцейському середовищі, готуватися до нових викликів безпеці та визначати пріоритети. Використовуються два види звіту: оперативний і стратегічний.

Для виявлення моделей злочинності та встановлення зв'язків між злочинцями та розслідуваннями Інтерпол використовує передові інструменти для обробки та аналізу цих даних, зокрема Criminal Analysis Files, які є базами даних, що зберігають і структурують інформацію та дозволяють створювати аналітичні звіти. Наприклад, є спеціальні файли щодо торгівлі наркотиками, незаконних ринків (товарів, фармацевтичних препаратів і продуктів дикої природи),

євразійської організованої злочинності, іноземних бойовиків-терористів, виготовлення бомб і саморобних вибухових пристроїв [3].

Аналітичні проєкти (АР), що входять до системи аналізу Європолу – системи обробки інформації, зосереджуються на певних сферах злочинності, наприклад, торгівля наркотиками, ісламістський тероризм, італійська організована злочинність тощо.

Співпрацюючи з цими аналітичними проєктами, спеціалісти Європолу можуть визначати пріоритети ресурсів, забезпечувати обмеження цілей і підтримувати правоохоронні органи ЄС та інші партнерські організації в боротьбі з організованою злочинністю та тероризмом за допомогою:

– аналізу відповідної інформації та розвідданих, щоб отримати якомога більше структурованої та конкретної інформації для правоохоронних органів;

– сприяння оперативним зустрічам між партнерами, які беруть участь у розслідуваннях;

– проведення експертизи та навчання працівників правоохоронних органів для підтримки розслідувань та обміну знаннями;

– розгортання мобільних офісів Європолу на місцях для проведення операцій, надання прямого доступу до захищеної мережі обміну інформацією та баз даних Європолу;

– надання підтримки судовому розгляду та боротьбі з іншою пов'язаною злочинною діяльністю, виявленою в ході розслідувань, зокрема з відмиванням грошей [4].

76 країн-членів Інтерполу взяли участь в операції під кодовою назвою «First Light 2022» (8 березня – 8 травня 2022 року) у міжнародній боротьбі з ОЗУ, які стоять за електронними комунікаціями та шахрайством із соціальною інженерією. Шахрайство з використанням соціальної інженерії стосується шахрайства, яке маніпулює або обманом змушує людей надати конфіденційну або особисту інформацію, яка потім може бути використана для отримання фінансової вигоди.

Поліція в країнах-учасницях проводила рейди в національних кол-центрах, які підозрювались в телекомунікаційному шахрайстві або шахрайстві із соціальною інженерією, зокрема телефонному обмані, романтичному шахрайстві, обмані електронної пошти та пов'язаних з цим фінансових злочинах.

У ході операції «First Light 2022» перевірено 1770 об'єктів, встановлено близько 3 тис. підозрюваних, заарештовано майже 2 тис. операторів, шахраїв і відмивачів грошей, близько 4 тис. банківських рахунків заморожено, перехоплено незаконних коштів на суму майже 50 млн доларів США [5].

Проєкт Інтерполу HOTSPOT використовує біометричні дані, щоб допомогти виявити іноземних бойовиків-терористів і злочинців, які намагаються незаконно перетнути кордон, а також порушує роботу

мереж, які сприяють таким подорожам. Проєкт HOTSPOT має на меті збільшити кількість перевірок, які країни-члени Інтерполу здійснюють у базах даних Інтерполу щодо відбитків пальців і зображень обличчя. У довгостроковій перспективі це допоможе виявляти іноземних бойовиків-терористів і злочинців, які намагаються перетнути кордони за допомогою нелегальних міграційних потоків. Крім того, HOTSPOT Operations об'єднує кількох ключових зацікавлених сторін, таких як НЦБ Інтерполу, розвідку, прикордонну поліцію та міграційні служби протягом трьох-чотирьох днів.

У рамках операцій Інтерпол навчає національних офіцерів використанню портативних пристроїв збору біометричних даних; сприяє співробітництву шляхом встановлення контактів з підрозділами та органами поліції; забезпечує поєднання технічної інфраструктури, мобільних технологій і навчання для створення стійкого і інтегрованого механізму зміцнення безпеки кордонів.

Там, де є надійне підключення до Інтернету, перевірки здійснюються безпосередньо за Автоматичною системою ідентифікації відбитків пальців Інтерполу (AFIS) за допомогою захищеної глобальної поліцейської системи зв'язку I-24/7. Якщо немає покриття Інтернету, перехресна перевірка біометричних даних запускається під час наступного підключення до Інтернету. Таким чином, біометричні перевірки можна проводити у віддалених місцях або там, де технічна інфраструктура недостатня [6].

Глобальна торгівля нелегальними фармацевтичними препаратами є великою та прибутковою сферою злочинності, вартість якої оцінюється в 4,4 млрд доларів США і в яку залучені організовані злочинні групи по всьому світу.

23–30 червня 2022 року 94 країни-члени Інтерполу, які представляють усі континенти, розпочали скоординовану операцію проти незаконних онлайн-аптек у рамках операції «Pangea XV». У ході операції правоохоронні органи конфіскували понад 7,8 тис. заборонених ліків і товарів із неправильним брендом, загальною кількістю понад 3 млн одиниць, досліджено понад 4 тис. веб-посилань, переважно з платформ соціальних мереж і додатків для обміну повідомленнями, закрито або видалено понад 4 тис. веб-посилань, що містять рекламу заборонених товарів, перевірено майже 3 тис. пакунків і 280 поштових вузлів в аеропортах, на кордонах і центрах розподілу пошти або вантажних поштових відправлень, відкрито понад 600 нових розслідувань і видано понад 200 ордерів на обшуки, правоохоронні дії вже порушили діяльність принаймні 36 організованих злочинних груп [7].

Список використаних джерел

1. European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021. URL: https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021.

2. Project CT-Tech. URL: https://www.interpol.int/Crimes/Terrorism/Counter-terrorism-projects/Project-CT-Tech.
3. Criminal intelligence analysis. URL: https://www.interpol.int/How-we-work/Criminal-intelligence-analysis.
4. Europol Analysis Projects. URL: https://www.europol.europa.eu/operations-services-and-innovation/europol-analysis-projects.
5. Hundreds arrested and millions seized in global INTERPOL operation against social engineering scams. URL: https://www.interpol.int/News-and-Events/News/2022/Hundreds-arrested-and-millions-seized-in-global-INTERPOL-operation-against-social-engineering-scams.
6. Using biometric data to strengthen border security. URL: https://www.interpol.int/Crimes/Terrorism/Counter-terrorism-projects/HOTSPOT.
7. USD 11 million in illicit medicines seized in global INTERPOL operation. URL: https://www.interpol.int/News-and-Events/News/2022/USD-11-million-in-illicit-medicines-seized-in-global-INTERPOL-operation.

Невмержицький Сергій Миколайович,
старший викладач спеціальної кафедри № 6 Навчально-наукового інституту державної безпеки Національної академії Служби безпеки України;
Волков Михайло Сергійович,
старший викладач спеціальної кафедри № 6 Навчально-наукового інституту державної безпеки Національної академії Служби безпеки України

ОПЕРАТИВНИЙ, ТАКТИЧНИЙ І СТРАТЕГІЧНИЙ АНАЛІЗ ЯК ГОЛОВНИЙ СЕГМЕНТ ПІД ЧАС ПЛАНУВАННЯ ТА ПРОВЕДЕННЯ СПЕЦІАЛЬНИХ ОПЕРАЦІЙ У КОНТРРОЗВІДУВАЛЬНІЙ ТА ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Сьогодення вимагає від Служби безпеки України та інших правоохоронних органів України активного вдосконалення нових форм проведення спеціальних операцій в контррозвідувальній та оперативно-розшуковій діяльності з використанням форм та методів кримінального аналізу, який буде діяти на упередження та нівелювання існуючих актуальних загроз національній безпеці і обороні України.

Любому контррозвідувальному чи оперативно-розшуковому заходу передує аналіз, який може мати як оперативний, тактичний чи стратегічний характер, що включають в себе мету, завдання та ціль.

Реалізація завдань, перетворення цілей на результати в ОРД здійснюються через оперативно-розшукові заходи, в КРД через