З одного боку, необхідно зберегти налагоджену за десятки років взаємодію слідчих і оперативних підрозділів при розслідуванні кримінальних правопорушень, з іншого, – подолати відомчу залежність слідчих від керівників територіальних правоохоронних органів, що жодним чином не суперечитиме законодавству України (насамперед, Закону України «Про центральні органи виконавчої влади»), яке повною мірою поширюватиметься й на діяльність відповідного слідчого апарату.

Таким чином, завдяки трансформації органів досудового розслідування України в ДСДР повною мірою буде забезпечено ідеї щодо «вертикального» підпорядкування слідчих підрозділів. При цьому статус особи, яка безпосередньо реалізує функцію керівництва досудовим слідством – керівника органу досудового розслідування, буде виведено на один рівень з керівниками територіальних правоохоронних органів, що знову ж таки є необхідною умовою ефективного керівництва досудовим розслідуванням. Така реорганізація системи органів досудового розслідування (з чітким підпорядкуванням і структурою) на сьогодні вкрай необхідна, що зумовлено необхідністю функціонального відмежування їх від діяльності територіальних правоохоронних органів. В кінцевому результаті це дасть змогу суттєво підвищити якість та ефективність самого досудового розслідування.

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

МІЖНАРОДНИЙ ДОСВІД ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ У ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

У нинішніх умовах важливого значення у протидії організованій транснаціональній злочинності набуває використання сучасних технологій і проєктів. Зокрема, файл аналізу проєкту Інтерполу Millennium надає країнам-учасницям дані про високопоставлених членів російськомовних ОЗГ, а саме: персональні та біометричні дані, відомих учасників ОЗГ, посилання на ОГ та ЗО, місця злочинної діяльності та впливу, особисті ідентифікаційні ознаки (татуювання, фізичні атрибути тощо). Найчастіше українські правоохоронці використовують відомості з бази даних проєкту «Millennium» для проведення оперативно-розшукових або контррозвідувальних заходів, у ході яких можуть обмінюватись оперативною інформацією з правоохоронними органами інших країн. Наслідком таких заходів може стати заборона іноземцю в'їзду в Україну або ж, навпаки, заборона громадянину України в'їзду на територію інших країн [1].

У червні 2021 року Європол повідомив про успішне проведення масштабної операції «Троянський щит», спрямованої проти організованої злочинності у 16 країнах, у ході якої було затримано понад 800 підозрюваних, проведено понад 700 обшуків в Європі, Новій Зеландії, Австралії та США, конфісковано понад 30 тонн наркотиків, зброю та готівку. За інформацією ФБР, слідчим вдалося отримати доступ до зашифрованої платформи ANOM, що використовується бандами, і увійти в їх чати. Зокрема більш ніж у 100 країнах були розповсюджені захищені від прослуховування телефони серед 300 угруповань, з допомогою яких прослуховувалися телефонні розмови та відстежувалися інші види комунікації, було перевірено понад 27 млн електронних повідомлень. Це дало можливість розкрити плани членів мафіозних угруповань, злочинних кланів та азіатських злочинних синдикатів у сферах наркоторгівлі та відмивання грошей, а також вбивства, що планувалися, більш ніж у 100 країнах [2].

Натомість у жовтні 2021 року Європол провів операцію Dark Huntor проти організованої злочинності в даркнеті, у ході якої було затримано 150 підозрюваних у нелегальній торгівлі та придбанні протизаконних товарів у тіньовому секторі інтернету. Зокрема, у Німеччині було затримано 47 осіб, у США – 65, у Великій Британії – 24, а також по чотири – в Італії та Нідерландах. Загалом поліція конфіскувала 26,7 млн євро, 45 одиниць зброї, 152 кг амфетаміну та метамфетаміну, 22 кг кокаїну та 27 кг опіоїдів [3].

Крім того, 29 жовтня 2021 р. у ході міжнародної поліцейської операції під егідою Європолу було затримано 12 підозрюваних у кібервимаганні в Україні та Швейцарії, при обшуках у них конфісковано близько 52 тис. доларів та п’ять автомобілів класу люкс. В операції брали участь представники поліції Великобританії, Німеччини, Нідерландів, Норвегії, США, Швейцарії та України. Жертвами злочинців стали близько 1800 компаній у 71 країні. Члени ОЗУ отримували доступ до ІТ-систем фірм за допомогою так званих фішингових електронних листів та іншими способами. Потім за допомогою вірусів-вимагачів (ransomware) блокували фірмам доступ до документації, шифруючи його, і вимагали викуп за надання ключа для розшифрування [4].

У листопаді 2021 року в ході операції Trivium правоохоронні органи 17 європейських країн за підтримки Європолу здійснювали перевірки людей і транспортних засобів на дорогах Євросоюзу та обшуки приміщень, під час яких було заарештовано 174 підозрюваних, вилучено 27 автомобілів, понад 200 інших товарів, у тому числі зброя та наркотики, перевірено майже 25 тис. осіб, понад 16 тис. транспортних засобів, близько 800 місць. Досягненню позитивного результату сприяло застосування поліцією таких методів, як автоматичне розпізнавання номерних знаків (ANPR) та моніторинг водіїв на предмет підозрілої поведінки в рамках операції Trivium XV [5].

У резолюції Глобальної контртерористичної стратегії, ухваленій Генеральною Асамблеєю ООН 30 червня 2021 р., висловлюється глибока стурбованість використанням інтернету, інших інформаційних і

комунікаційних технологій, соціальних мереж у терористичних цілях, зокрема поширенням терористичного контенту, та заохочуються держави-члени ООН працювати разом із відповідними зацікавленими сторонами, щоб гарантувати, що терористи не знайдуть місця в інтернеті, одночасно підтримуючи відкритий, спільний, надійний та безпечний інтернет. Зокрема проєкт CT-Tech, що фінансується ЄС і реалізується в рамках Глобальної антитерористичної програми UNCCT/UNOC з кібербезпеки та нових технологій, спрямований на зміцнення спроможності правоохоронних органів і органів кримінального правосуддя протидіяти використанню нових технологій у терористичних цілях, а також підтримувати використання новітніх технологій у боротьбі з тероризмом [6].

Відтак, для виявлення моделей злочинності та встановлення зв'язків між злочинцями і 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 [7].

Своєю чергою, аналітичні проєкти (AP), що входять до системи аналізу Європолу, зосереджуються на певних сферах злочинності, наприклад, торгівлі наркотиками, ісламістському тероризму, італійській організованій злочинності тощо. Як приклад, 76 країн-членів Інтерполу взяли участь в операції під кодовою назвою «First Light 2022» (березень-травень 2022 р.), направленій проти ОЗУ, що стоять за електронними комунікаціями та шахрайством із соціальною інженерією і маніпуляціями або обманом змушують людей надати конфіденційну або особисту інформацію, яка потім може бути використана для отримання фінансової вигоди. У ході операції поліція проводила рейди в національних кол-центрах, які підозрювались в комунікаційному шахрайстві або шахрайстві із соціальною інженерією, усього перевірено 1770 об'єктів, заморожено близько 4 тис. банківських рахунків, перехоплено незаконних коштів на суму майже 50 млн доларів США [8].

Натомість проєкт Інтерполу HOTSPOT використовує біометричні дані для виявлення іноземних бойовиків-терористів і злочинців, які намагаються незаконно перетнути кордон за допомогою нелегальних міграційних потоків, а також припинення роботи мереж, які сприяють таким подорожам. Проєкт HOTSPOT має на меті збільшити кількість перевірок, які країни-члени Інтерполу здійснюють за базами даних Інтерполу щодо відбитків пальців і зображень обличчя. У рамках операції Інтерпол навчає національних офіцерів використанню портативних пристроїв для збору біометричних даних; 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

Автоматизованою системою ідентифікації відбитків пальців Інтерполу (AFIS) за допомогою захищеної глобальної поліцейської системи зв'язку I-24/7 [9].

Список використаних джерел

1. Project Millennium helps countries identify the people and companies behind transnational Eurasian organized crime URL: https://www.interpol.int/Crimes/Organized-crime/Project-Millennium
2. У рамках операції Європолу затримано понад 800 осіб URL: https://www.dw.com/ru/evropol-i-fbr-soobshhili-ob-uspeshnom-provedenii-krupnomasshtabnoj-operacii-v-bolee-chem-100-stranah/a-57813672
3. Європол затримав 150 ймовірних злочинців із даркнету URL: https://www.dw.com/ru/evropol-zaderzhal-po-vsemu-miru-150-podozrevaemyh-v-prestuplenijah-v-darknete/a-59633465
4. Європол розкрив мережу кіберздирників URL: https://www.dw.com/ru/evropol-raskryl-set-kibervymogatelej/a-59669666
5. Over 150 arrests made in 3-day operation against organised property crime URL: https://www.europol.europa.eu/media-press/newsroom/news/over-150-arrests-made-in-3-day-operation-against-organised-property-crime
6. Project CT-Tech URL: https://www.interpol.int/Crimes/Terrorism/ Counter-terrorism-projects/Project-CT-Tech
7. Criminal intelligence analysis URL: https://www.interpol.int/How-we-work/Criminal-intelligence-analysis
8. 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
9. Using biometric data to strengthen border security URL: https://www.interpol.int/Crimes/Terrorism/Counter-terrorism-projects/HOTSPOT

Оперук Віталій Ігорович,
професор кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ, кандидат юридичних наук, доцент

МОЖЛИВОСТІ ВИКОРИСТАННЯ КЛАСИЧНОГО ТА НОВІТНЬОГО ПОЛІГРАФА «EYEDETECT» З МЕТОЮ ВИКРИТТЯ ВІЙСЬКОВИХ ЗЛОЧИНЦІВ ТА КОЛОБАРАНТІВ

Колабораціонізм, або військова й політична співпраця з окупаційним режимом, є частиною російсько-українського протистояння ще з 2014 року. Росія вкладає дуже багато ресурсів у «м'яку силу» і створення мережі агентів впливу, тому хтось, на жаль, ще до приїзду російських танків був готовий зустріти загарбників «з