Проблеми виявлення та розслідування злочинів, що вчиняються в офшорних зонах

Загальна кількість офшорних зон у світі визначається дуже умовно. Процес їх виникнення та зникнення є відносно динамічним. Фахівці сьогодні називають понад 60 стійких комплексних офшорних центрів, де традиційно функціонують офшорні компанії.

З європейських офшорних центрів найбільш відомі Гібралтар, Ліхтенштейн, Андорра, Монако, острови Джерсі, Гернсі, Сарк, Кіпр, Мальта, Мен; у Центральній Америці – Панама, Коста-Ріка, Бермудські, Віргінські, Багамські Острови, Кайман, Барбадос, Антигуа і Барабуда, а також острови Теркс і Кайокс, Аруба, Кюрасао.

На Африканському континенті найбільшими офшорними зонами є Ліберія та Маврикій. Тихоокеанський регіон представлений Науру, Фіджі, Західним Самоа; Південно-Східна Азія – Гонконгом та малайзійським островом Лабуан. У зоні Перської затоки найбільший офшорний центр знаходиться у Державі Бахрейн.

У кругообігу грошових коштів офшорна зона є головним фільтром, де “відмиваються брудні” гроші, що отримано від торгівлі людьми, наркотиками, , контрабандною зброєю. Процес легалізації коштів, отриманих злочинним шляхом, має таку схему. Спочатку “брудні” кошти “підмішуються” до “чистих” через сфери з послабленим податковим контролем – казино, шоу-бізнес, нічні клуби, реклама. Після цього готівкою або з цінними паперами кошти доставляються в офшорні зони (частіше на більш-менш законних підставах). Пізніше через офшорні банки за допомогою платіжних електронних систем грошові кошти переказуються до країни з підвищеною банківською конфіденційністю – до Гонконгу, Швейцарії, Сінгапуру. І тільки після зазначених операцій “очищені” чи “відмиті” кошти потрапляють до міжнародного фінансового обігу. Офшорні юрисдикції “зацікавлені” не тільки у грошових коштах, але й у нелегальному товарі – не даремно більшість офшорних зон розташовано на островах, а острови – на перехресті шляхів торгівлі наркотиками (Карибський басейн), або контрабанди зброєю (Середземне море). Кораблі, що заходять в офшорні порти, звільнено від митного контролю, плата за постій є суто символічною.

Ідея “офшору” нічого кримінального та незаконного в собі не містить. Більш того, подібні схеми дійсно допомагають у послабленні тягаря податків, але абсолютно уникнути їх не дозволяють.

Саме поняття “offshore” означає “поза берегом”. Офшорні зони з’явилися на економічній карті Світу приблизно у 60-ті роки, коли виникла концепція вільних економічних зон. Необхідно зазначити, що офшори мають велику кількість переваг, які вигідно відрізняють їх від інших (неофшорних) зон. Всіх їх можна об’єднати поняттям “валютно-фінансовий режим найбільшого сприяння”. Це і пільгове оподатковування, і вільний вивіз прибутку, і м’який валютний регламент, і “митний рай” для іноземних інвесторів. Не останню роль відіграє для потенційного клієнта зони низький поріг статутного капіталу. Найчастіше він тільки декларується, але реально не сплачується. Податок з прибутку в деяких офшорних зонах складає зазвичай 1 – 2 % або заміщається невеликим (до 1000 дол. США) внеском, що не залежить від розміру прибутків.

Бізнесменів та фінансових “ділків” офшор приваблює своєю стабільністю. Зазвичай, у подібних фінансових анклавах цикл стабільності розтягнуто на 10 – 25 років. Тобто, бізнесмен може бути упевнений, що протягом зазначеного періоду в обраній зоні не відбудеться непередбачених несприятливих змін у політичному ладі, законодавстві та макроекономічних тенденціях.

Ще одним плюсом офшорної зони є конфіденційність інвестицій. Особистості власників фірм не розголошуються. Процедуру їх реєстрації спрощено до максимуму. Але слід зауважити, що згідно із законодавством, чинним в офшорній зоні, розкривати анонімність інвестицій можна лише у разі кримінального переслідування інвестора. Але у деяких офшорних зонах акції випускають “на пред’явника”, тому власники компаній залишаються, як правило, у “тіні”.

Іноді ліберальність законодавства деяких офшорних зон не наближається до анархії. У деяких країнах кваліфікується за злочин порушення митного, валютного та податкового законодавства. Переважно від фірм не вимагаються податкові декларації, зовнішній аудит, звіт стосовно рахунків. Рахунки ж фірми можуть бути перевіреними лише за рішенням власників. Єдиною формою звітності для багатьох компаній є щорічний фінансовий звіт.

Останнім часом в офшорному бізнесі намітився  ряд “неприємних моментів”, що відштовхує значну кількість ділових структур. Наприклад, органи фінансового контролю Сполучених Штатів Америки та Європи уважно відстежують всі угоди за участю офшорного капіталу. Крім того, в деяких країнах набуває чинності спеціальне законодавство щодо зниження податкових втрат від подібних фірм. До офшорних компаній з крайньою недовірою ставляться також державні та банківські структури, що спричиняє труднощі з кредитуванням.

Проте, у 90-ті роки кількість офшорних компаній у світі становило вже кілька сот тисяч із сукупним обігом понад трлн дол. США [1].

Виникає природне питання, яку роль виконують у цьому процесі контролюючі органи? На жаль, самостійно працювати їм важко, якщо взагалі це можливо, тим більше боротися з відтоком фінансових ресурсів та матеріальних цінностей за кордон. Слід зауважити, що різноманітне розкрадання є масштабними. Розкривати злочини такого виду складно. Як правило, діяльність злочинців, які здобули свої капітали злочинним шляхом та переправили їх за межі України, потрапляє в поле зору правоохоронних органів лише через деякий час після вчинення злочину. Злочинець встигає виїхати за кордон. Саме з цієї причини при величезних відтоках коштів з України вдається повернути лише мінімум.

Вважаємо, що одними законодавчими актами у цьому разі не обійтися. Необхідні кардинальні рішення: по-перше, держава має максимально запобігти незаконному збагаченню та вивозу коштів з України; по-друге, має діяти експертиза договорів; по-третє, необхідним є чіткий перелік випадків, коли кожна особа зобов’язана подавати декларацію щодо прибутків, контроль за ними, врешті-решт, необхідно передбачити кримінальну відповідальність за легалізацію “тіньових” прибутків. В іншому разі всі вжиті заходи виявляються неефективними.

Практика офшорного бізнесу виділила три основні напрями у формуванні компаній. До першого – відносяться компанії холдінгового типу (оперативно-холдінгові, інвестиційні, судновласницькі, промислові та компанії, що працюють із нерухомістю). Другий напрям – це фінансові компанії, до яких відносяться і банки, і посередницькі структури, і страхові фірми. Третій тип “офшору” – торговельно-посередницький бізнес. Фахівці у межах цих трьох генеральних напрямів виділяють і більш вузькі спеціалізації.

Найбільшу зацікавленість правоохоронних органів викликає реєстрація подібних структур, яку на комерційній основі здійснюють спеціалізовані “секретарські” компанії, що забезпечені необхідними технологіями, освоїли необхідні юридичні процедури та мають кваліфікований персонал.

В офшорних зонах вельми популярними є фінансові операції. Адже банк, що зареєстровано в одній із зон, сплачує клієнтам відсотки поза податкових схем та може вільно “грати” своїм капіталом, ввозячи або вивозячи його.

Останнім часом деякі великі міжнародні банки заснували в офшорних зонах власні дочірні банківські організації. Як вважають російські експерти у сфері оподаткування, найбільш перспективним регіоном для банківського “офшору” стає Бахрейн. Через фінансову інфраструктуру зазначеної держави проходить чималий потік регіональних нафтодоларів, перетворюючи його для арабського Сходу на своєрідний банківський сейф.

На підтвердження цього може бути політична стабільність навколо Бахрейну. Військові конфлікти та валютні коливання, що роздирають регіон Перської затоки, дивно обминають цю країну.

Серед напрямів інформаційно-технічної протидії сучасній злочинності, що здійснює свою діяльність безпосередньо за допомогою офшорних зон, необхідно виділити комплекс заходів (аналітична та комп’ютерна розвідка).

Сутність аналітичної розвідки можна визначити за “розвідку в інформаційному середовищі”, за “отримання нових знань про розвідувальний об’єкт або явище на підставі аналітичного опрацювання наявної розвідувальної інформації і зведень про відомі факти”.

Аналітична розвідка передбачає вивчення матеріалів прихованого спостереження, оперативних установок, повідомлень негласних співробітників, даних перехоплення з різних каналів зв’язку, а також аналіз повідомлень, публікацій і виступів у засобах масової інформації, статистичних даних, зведень, що містяться в державних і недержавних автоматизованих банках даних і інформаційних системах.

Інформаційна революція, що триває, стрімко змінює ситуацію у сфері накопичення та опрацювання інформації, що представляє оперативний інтерес. Можна навести дві обставини, що виводять інформаційно-аналітичну діяльність (аналітичну розвідку) за межі традиційних рамок оперативно-розшукової діяльності (далі – ОРД) і відкривають якісно нові можливості для вирішення оперативних задач по боротьбі з організованою злочинністю.

Перша обставина, що наповнює аналітичну розвідку новим змістом, полягає в тому, що на сьогодні уже створено і створюються сотні електронних банків даних, що містять найрізноманітніші відомості. Маються на увазі банки даних як державних органів, так і приватних підприємств. У першу чергу, – це банки даних різних служб правоохоронних органів, податкових і митних служб, реєстраційних органів, фондів медичного і соціального страхування, медичних закладів, банків і фінансових компаній, транспортних підприємств, авіа- і залізничних кас, банки даних з електронними версіями періодичних видань і банки даних приватних підприємств, що надають інформаційні послуги охоронних структур, служб безпеки і т. ін.

Друга обставина, що виділяє аналітичну розвідку в самостійний вид діяльності, полягає в тому, що сьогодні уже створені, застосовуються і удосконалюються вельми ефективні методи опрацювання різноманітної інформації. Ряд таких методів, що дозволяють виявити латентні зв’язки між об’єктами і за виявленими зв’язками оцінювати роль і статус будь-якого члена злочинного співтовариства, уже перебувають на озброєнні інформаційно-аналітичних підрозділів правоохоронних органів. Аналітична розвідка, побудована на застосуванні останніх досягнень у розвитку інформаційних технологій, є одним з центральних напрямів діяльності Інтерполу по боротьбі з транснаціональною організованою злочинністю.

У цілому аналітична розвідка, а більш конкретно, застосування інформаційних технологій в аналітичній розвідці, забезпечуючи ОРД, одночасно виходить за рамки ОРД, є паростком нового перспективного напряму в діяльності правоохоронних органів.

Сьогодні існують окремі приклади створення об’єднаних інформаційно-аналітичних центрів в системі органів внутрішніх справ, відчутних результатів аналітичної розвідки, забезпечення спеціалізованих підрозділів кримінальної міліції стратегічною і тактичною інформацією про стан організованої злочинності.

У свою чергу, комп’ютерна розвідка полягає в пошуку й отриманні інформації з комп’ютерних систем і мереж. Здійснюється комп’ютерна розвідка за допомогою апаратно-програмних комп’ютерних засобів, шляхом застосування логічних операцій і прийомів. Необхідність комп’ютерної розвідки у правоохоронних органах обумовлена багатьма чинниками. Відзначимо тільки деякі з них:

по-перше, всі великі обсяги інформації, що може мати оперативний інтерес, переводиться на машинні носії. Практично вся інформація про фінансову діяльність підприємств і фірм уже міститься в електронному вигляді в комп’ютерних системах;

по-друге, комп’ютерні телекомунікації все частіше виявляються засобами зв’язку для злочинних формувань. Вони стають засобом неконтрольованого кримінального перекидання фінансових коштів, зокрема у закордонні банки й офшорні зони;

по-третє, глобальна комп’ютерна мережа Інтернет, що відбиває не тільки досягнення, але й практично всі відомі недоліки людського суспільства, стає носієм кримінальної інформації і загрозою її поширення.

Сьогодні одним із завдань правоохоронних органів стає відстежування кримінальних явищ у мережі Інтернет. Така робота ведеться за кордоном, зокрема у США (ФБР) і у Німеччині (ВКА), де створено спеціальні підрозділи комп’ютерної розвідки в мережі Інтернет.

Нарешті, комп’ютерна розвідка є одним із найбільше ефективних засобів профілактики, протидії і боротьби з найрізноманітнішими комп’ютерними злочинами, оскільки до завдань комп’ютерної розвідки входить і пошук зловмисників у комп’ютерних мережах.

Перспективність цього напряму діяльності правоохоронних органів обговорювалася на Міжнародній нараді експертів у Японії у вересні 1998 р., на якій розглядалося питання щодо правових основ і методики організації обшуку комп’ютерних систем без вилучення комп’ютерів за допомогою віддаленого доступу, тобто із застосуванням методів і засобів мережної комп’ютерної розвідки.

У правовому відношенні комп’ютерну розвідку можна розглядати як різновид таких оперативно-пошукових заходів, як зняття інформації з технічних каналів зв’язку, спостереження, дослідження предметів і документів, оперативний огляд.

Якщо йдеться про телекомунікаційний зв’язок між комп’ютерними системами, то це переривання зв’язку може означати активний вплив на комп’ютерну систему, зокрема, з метою виведення її з ладу. Це також входить до функцій комп’ютерної розвідки, що у разі потреби стає засобом інформаційного нападу.

Говорячи про надзвичайну необхідність організації комп’ютерної розвідки в мережі Інтернет, необхідно мати на увазі те, що інформація, розташована і циркулює в цій мережі, не потрапляє до зони правового регулювання. Практично не передбачено відповідальності за введення і поширення інформації. Інтернет абсолютно не підлягає цензурі. Більш того, розміщена інформація легко знеособлюється. Зокрема, інформація кримінального характеру може бути розташована на сайтах, що належать як юридичним, так і фізичним особам. Саме поняття приналежності сайта є розмитим. Інформаційний сайт може бути фізично розміщеним на комп’ютері, що знаходиться на іншому континенті, але при цьому забезпечено його доступ по всій території країни.

Інформація, отримана в результаті комп’ютерної розвідки, у деяких випадках потребує аналітичного опрацювання, тобто застосування апарата аналітичної розвідки. У той самий час застосування методів комп’ютерної розвідки істотно підвищує ефективність розвідки аналітичної, тому що відкриває можливість “добувати” інформацію з банків даних і комп’ютерних систем, що мають, зокрема, вихід в Інтернет. Зауважимо, що в мережі Інтернет на сьогодні можна знайти електронні версії практично всіх періодичних видань, що забезпечує більш легкий доступ і наступне автоматизоване опрацювання відкритої інформації, що отримується в електронному вигляді.

Ці обставини природно виділяють комп’ютерну розвідку у самостійний напрям діяльності правоохоронних органів, а у поєднанні із аналітичною розвідкою дозволяють вести розмову про комплекс розвідувальних заходів, заснованих на сучасних інформаційних технологіях [2; 3].

І, врешті-решт, можна додати до всього зазначеного, що найбільша результативність досягається в розслідуванні злочинів, якщо сам слідчий достатньо володіє необхідними спеціальними знаннями, досвідом та навичками. Це стосується особливо правопорушень у сфері інформаційних технологій, які останнім часом бурхливо розвиваються, що пояснюється тим, що сьогодні засоби обчислювальної техніки, телекомунікаційні пристрої, програмне забезпечення є складною системою, яка динамічно розвивається і потребує глибоких спеціальних знань [4].

1. Матасова С. Г., Михеева Э. А., Трофименко А. Г. Банкиры умирают первыми: Документальный детектив. – Нижний Новгород: Юпитер, 1996. – 630 с.

2. Овчинський С. С. Оперативно-розшукова інформація / Під ред. А.С. Овчинського і В. С. Овчинського. – М.: ИНФРА – М., 2000. – 367 с.

3. Ронин Р. Своя розвідка: способи вербування агентури, методи проникнення в психіку, форсований вплив на особистість, технічні засоби схованого спостереження і знімання інформації: Практ. посіб. – М.: Харвест, 2000. – 368 с.

4. Романюк Б. Залучення спеціалістів до розслідування злочинів у сфері інформаційних технологій // Міліція України. – 2002.  – № 1. – С. 22–23.