ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УДК 343.974(007)

Інтелектуальні інформаційні технології в боротьбі з організованою злочинністю

Гавловський Владислав Данилович –
начальник відділу Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України

Розглянуто можливості використання правоохоронного моніторингу кіберпростору в поєднанні з інтелектуальними інформаційними технологіями як засобу боротьби з організованою злочинністю.

Ключові слова: організована злочинність, правоохоронний моніторинг, аналітична розвідка, соціально-мережевий аналіз.

Постановка проблеми. Однією із найбільш виразних ознак сучасності є зміщення загроз національній та міжнародній безпеці у "тіньовий" сектор. Основними факторами цього процесу, як повністю справедливо зазначається науковцями, є різного роду транснаціональні злочинні утворення, потужності яких часом перевищують наявні можливості протидії їм у більшості держав світу [1]. Сьогодні все більше західноєвропейських експертів на підставі аналізу активності транснаціональних організованих злочинних угруповань (далі – ТОЗУ) доходять висновку, що їх діяльність стає на рівень головних загроз XXI століття. Така загроза визнається ними значно більшою, ніж терористична, оскільки терористичні організації, що діють самостійно, як правило, не мають необхідних сил і засобів для створення реальної небезпеки існуванню держави. Дійсно, на відміну від терористичних груп та організацій, які намагаються публічно заявити про себе і про свої цілі, ТОЗУ діють з дотриманням найсуворішого рівня конспірації. Організована злочинність за останні роки значно зміцнилася, безпосередньо загрожуючи життю демократичних держав, прагнучи підпорядкувати собі національні економіки [2].

За даними Європолу, в ЄС діє 3600 злочинних угруповань; обіг коштів серед корупціонерів Євросоюзу оцінюється у 120 млрд євро на рік, що становить 1 % від загально-європейського валового внутрішнього продукту; наркотрафік оцінюється в 12 млрд євро на рік; щорічно казні наноситься збиток у 10 млрд євро через контрабанду сигарет; у 2011 році було конфісковано підробленої продукції на 1,1 млрд євро; 1,5 млрд на рік становить збиток за рахунок махінацій з кредитними картами [3].

За таких умов протидія організованій злочинності набуває особливого значення як ключова складова політики безпеки усіх держав і міжнародного співтовариства загалом. Однак, незважаючи на те, що протидія організованій злочинності вже тривалий час перебуває на порядку денному діяльності світової спільноти, розроблення та впровадження ефективних засобів боротьби з нею не задовольняє сучасних потреб. Крім того, що ТОЗУ саморозвивається і самодетермінується, організована злочинність на будь-яке законодавче нововведення реагує досить швидко, блискавично адаптуючись до нього. До того ж вона нерідко випереджає вжиті правоохоронними органами заходи. Тому традиційні методи боротьби зі злочинністю при протидії ТОЗУ не дають очікуваних результатів. Таким чином, природно, що одним із напрямів вдосконалення боротьби з цим явищем є використання сучасних інтелектуальних інноваційних інформаційних технологій [4]. Отже, тематика, обрана автором представленого дослідження, є важливою та **відповідає критерію актуальності**.

Мета представленої праці полягає в тому, щоб на підставі проведеного аналізу висвітлити можливості використання правоохорон-

ного моніторингу кіберпростору в сукупності з інтелектуальними інформаційними технологіями, як важливого засобу протидії транснаціональній організованій злочинності.

Аналіз останніх досліджень та публікацій. Окремі загальні та спеціальні аспекти протидії організованій злочинності з використанням кіберпростору на сучасному етапі досліджували такі вчені, як І. О. Воронов, В. О. Голубєв, М. Л. Грібов, О. Ф. Долженков, В. П. Захаров, С. А. Кузьмін, О. В. Манжай, Ю. Ю. Орлов, М. М. Перепелиця, М. А. Погорецький, В. П. Шеломенцев, В. В. Шендрик, І. Ф. Хараберюш, В. Г. Хахановський, О. М. Юрченко, Є. М. Яковець та інші, певний внесок у цьому напряму наукових досліджень було зроблено і автором представленої праці. Водночас інтенсивний, стрімкий розвиток сучасних інформаційних і телекомунікаційних технологій, їх активне використання у діяльності ТОЗУ, якісна трансформація організованої злочинності зумовлюють необхідність подальших досліджень окресленої проблеми, що і зумовлює **відповідність даної праці критерію наукової новизни.**

Виклад основних положень. Досягнення науки і техніки, створені на благо людства, часто використовують у деструктивних цілях. Це повною мірою стосується й протиправного використання представниками злочинного світу кібернетичного простору. Сьогодні для реалізації своїх злочинних намірів його все частіше застосовують учасники ТОЗУ, які проводять незаконні господарські оборудки, вчиняють шахрайства з фінансовими ресурсами, відмивають кошти, отримані злочинним шляхом, збирають інформацію, необхідну для підготовки вчинення злочинів, збувають предмети та речовини, заборонені для вільного обігу, здійснюють зв'язок між собою, підбирають пособників і виконавців конкретних кримінальних діянь тощо.

Тому одним із важливих джерел отримання інформації про організовану злочинну діяльність, її структуру, конкретних учасників, їх взаємозв'язки, плани щодо підготовки та вчинення злочинів, конкретні факти протиправної діяльності є відстеження використання ними кіберпростору.

Сьогодні представники організованої злочинності активно використовують так звані соціальні мережі, складову мережі Інтернет. Тому нами було запропоновано створення в Україні цілісної продуманої системи відстеження використання соціальних мереж у деструктивних цілях, яку ми означили як правоохоронний моніторинг соціальних мереж, тобто діяльність уповноважених державних органів з відстеження використання соціальних мереж у деструктивних цілях з метою запобігання суспільно небезпечним діянням, їх виявлення та припинення. До завдань правоохоронного моніторингу соціальних мереж ми зарахували пошук і фіксацію фактичних даних щодо використання таких мереж у деструктивних цілях, встановлення та викриття суб'єктів цих дій для подальшого притягнення до юридичної відповідальності або блокування їх деструктивної діяльності [5].

Сучасні прояви організованої злочинності свідчать, що відстежувати її ознаки потрібно, не лише у певних комп'ютерних соціальних мережах, а в усьому кіберпросторі, що зробить боротьбу з нею значно ефективнішою. М. А. Погорецький і В. П. Шеломенцев розглядають кіберпростір як певне середовище, організоване за допомогою принципів, методів і засобів кібернетики; утворене в результаті функціонування кібернетичних комп'ютерних систем управління та оброблення інформації [6, с. 78]. Реалізовується кіберпростір (у його найбільш повному розумінні) регіональними і глобальними комп'ютерними мережами, насамперед мережею Інтернет. На рівні локальних інформаційних мереж можна говорити лише про окремі сегменти кіберпростору, а в автономному комп'ютері такої ознаки кіберпростору, як інформаційна взаємодія між користувачами в режимі реального часу, загалом немає [6, с. 80].

Взаємодія, що відбувається у кіберпросторі, частково відбиває реальну соціальну взаємодію, у тому числі ту, що пов'язана з організованою злочинною діяльністю. Тому результати правоохоронного моніторингу кіберпростору доцільно піддавати аналізу, застосовуючи різні методи (наприклад SNA), використовуючи різні інструменти, які дозволять з окремих слідів, що залишають ТОЗУ в цьому просторі, збудувати цілісну модель їх злочинної діяльності у реальному світі, зараховуючи її конкретних суб'єктів, їх взаємодію, плани, використовувані засоби тощо.

SNA (Social network analysis – соціальномережевий аналіз, аналіз соціальних мереж (зв'язків, взаємовідносин, взаємодій) – напрям сучасної комп'ютерної соціології, який передбачає опис та аналіз зв'язків, що виникають у ході соціальної взаємодії і комунікації мереж різної щільності та інтенсивності. Цей метод отримав поширення при вивченні процесів комунікації, які відбуваються в різних соціальних групах, у процесі формування і розвитку соціології міжособистісних відносин, політичних і міжнародних процесів, використовується для боротьби зі злочинністю. Тобто, даний метод дослідження є універсальним.

Мережа соціальних взаємодій складається з певних об'єктів: людей, юридичних осіб, соціальних груп, організацій, міст, країн і наборів взаємозв'язків між ними. Причому до поняття зв'язків входять не тільки комунікаційні взаємодії між об'єктами, але й обмін різними ресурсами, контакти, пов'язані зі спільною діяльністю, включаючи конфліктні відносини. При використанні методу SNA ключовим є опис характеристик, що відображають щільність, інтенсивність і просторову координацію соціальних зв'язків.

Отримана мережа взаємодій може бути проаналізована різними методами теорії графів, теорії інформації, математичної статистики, матричної алгебри. На відміну від класичних методів аналізу, які досліджують індивідуальні влас-

тивості об'єктів, основна мета соціально-мережевого аналізу – це дослідження взаємодії між соціальними об'єктами і виявлення причин та умов виникнення цієї взаємодії.

Окремим напрямком соціально-мережевого аналізу є візуалізація, тобто графічне відтворення соціальної мережі взаємозв'язків. Цінність аналітичних інструментів, що дозволяють візуалізувати відносини між людьми, організаціями та транзакціями, очевидна, оскільки сама можливість наочно побачити мережу дозволяє зробити важливі висновки про характер взаємодії між ними, не вдаючись до інших методів аналізу графа.

Практика переконливо свідчить, що за допомогою методів SNA, проаналізувавши діяльність злочинних угруповань у конкретному регіоні, можна візуалізувати вузлові точки, що зв'язують різну кримінальну діяльність, і нанести удар по ключових фігурах. Для цього лише потрібно адаптувати поліцейські бази даних у формат, який розуміє комп'ютерна програма.

Інструменти соціально-мережевого аналізу постійно розвиваються. В першому поколінні побудова матриць і діаграм зв'язків виконувалась вручну, а аналіз отриманих структур здійснювався без використання допоміжних технічних засобів. Ще за часів Радянського Союзу в кожній оперативно-розшуковій справі мало бути креслення схеми зв'язків розроблюваної особи, що унормовувалося відомчими інструкціями МВС та КДБ СРСР. Засновник orgnet.com, спеціаліст з соціальних мереж Валдіс Кребс, на підставі інформації, опублікованої в декількох великих виданнях, вручну побудував карту терористичної мережі, відповідальної за події 11 вересня 2001 року). Тобто була побудована мережа, в якій в якості об'єктів (вершин) виступали конкретні особи (пілоти), а в якості ліній зв'язку (ребер) – факти попарних зв'язків (переговорів). Те, що терористи готували теракт (мали надлишкові на загальному тлі комунікації), наочно видно по згущенню щільності ліній зв'язку навколо терористів [4].

Сьогодні аналіз соціальних зв'язків ефективно використовується для боротьби з відмиванням доходів, отриманих злочинним шляхом, крадіжками особистості, мережевими шахрайствами, кібератаками тощо. Зокрема, методи SNA використовувалися при розслідуванні незаконних операцій з цінними паперами, що проводилося Австралійською комісією з цінних паперів та інвестицій (Australian Securities and Investment Commission).

У монографії "Strategic Intelligence" (стратегічна розвідка), присвяченій способам аналізу інформації, Джей Лібовіц описує використання SNA-методики під час проведення резонансних розслідувань серійних зґвалтувань, підробок рецептів на наркомісні лікарські препарати, забезпечення безпеки на Чемпіонаті Європи з футболу. Так, правоохоронні органи всіх країн-учасниць цих змагань використовували методи SNA для того, щоб проаналізувати наявну у них інформацію про так званих футбольних фанів – людей, які могли б влаштовувати безлади під час матчів. Кожна країна мала свою базу даних таких правопорушників, і ця інформація була піддана перехресному аналізу за допомогою програми I2, яка є одним із інструментів SNA.

Особливо ефективно цей метод сьогодні застосовується для виявлення складних організованих схем вчинення шахрайств. Зокрема, один із найбільших проектів SNA був реалізований в Міністерстві фінансів Бельгії при розкритті схеми незаконного повернення експортного податку на додану вартість, відомої як "карусель ПДВ", втрати бюджету від якої оцінювалися в 1,1 млрд євро. В результаті застосування методу SNA була викрита ціла мережа фіктивних компаній у декількох юрисдикціях (Бельгії та Франції), які займалися послідовним перепродажем одних і тих же товарів один одному.

Саме за допомогою аналітичних інструментів SNA було виявлено окремі приховані спільноти компаній, які здійснювали всередині себе циклічні операції експорту-імпорту, а вже серед них відібрано спільноти з ознаками шахрайських операцій та проведено детальне розслідування їх діяльності. В результаті вже за перший рік використання SNA втрати Бельгії від даного виду шахрайства скоротилися на 80 % і склали 232 млн євро, а до 2012 року – на 98 %, тобто до 18,5 млн євро.

Свою високу ефективність SNA-метод показав у боротьбі з різними видами шахрайств у сфері страхування. Прикладом виявленого експертами за допомогою методу SNA шахрайства, вчиненого організованою групою в автострахуванні, є випадок, коли один маловідомий пункт автосервісу активно проводив калькуляцію вартості ремонту автомобілів тих випадків ДТП, де були присутні ознаки фальсифікації. Крім того, в окремих клієнтів автосервісу збігалися адреси і телефони, що дозволило страховій компанії виявити організовану групу, яка займалася шахрайством у сегменті автострахування. На підставі бази даних страхової компанії за допомогою методики SNA можна виявити (з глибиною в декілька років) вписаних в один і той же поліс ОСАЦВ (обов'язкове страхування цивільної відповідальності) осіб, які, на момент подачі вимоги, можуть здатися "випадковими" учасниками ДТП, а на справді є шахраями [7].

Окреслена методика за своїм змістом досить близька до сутності діяльності, яку в нашій державі вже традиційно називають аналітичною розвідкою. Визначення аналітичної розвідки, яке пропонують науковці, містять розбіжності, проте всі вони вбачають її завдання в отриманні нової інформації про злочинну діяльність на ґрунті аналізу наявної інформації та відомостей, одержаних під час проведення ОРЗ (у тому числі із застосуванням інформаційних технологій), які є складовою аналітичної розвідки.

Так, І. В. Проценко визначає аналітичну розвідку як пошук, систематизацію та аналіз розрізнених даних з метою отримання оперативно значущої інформації [8, с. 169]. О. Ф. Должен-

ков – як розвідку в інформаційному просторі, що розвідує явища та об'єкти на підставі аналітичного опрацювання відомостей і фактів [9, с. 26]. В. Г. Хахановський – як спеціальний захід, призначений для вирішення оперативно-тактичних завдань з метою отримання нових чи додаткових знань про осіб, які становлять оперативний інтерес [10, с. 192]. О. Ю. Бусол – як напрям ОРД, що полягає у збиранні, добуванні та комплексному аналізі оперативно-розшукової інформації, у тому числі із застосуванням інформаційних технологій, з метою отримання нових відомостей про злочинну діяльність осіб та груп [11].

Одна з відмінностей проектів SNA та аналітичної розвідки полягає в тому, що остання використовує для аналізу не лише доступні дані з кіберпростору, публікації у ЗМІ, різноманітні банки даних, наявну оперативно-розшукову та криміналістичну інформацію, а й може зараховувати безпосереднє проведення оперативно-розшукових заходів. Досить показовим є приклад використання аналітичної розвідки при проведенні профілактично-пошукових заходів з метою забезпечення правопорядку під час матчу Ліги Чемпіонів УЄФА між командами "Шахтар" (Донецьк) та "Зеніт" (Санкт-Петербург), який відбувся у м. Донецьку 19 жовтня 2011 р. Ще задовго до матчу із використанням ЗМІ та мережі Інтернет були вивчені особи, соціальні зв'язки, особливості поведінки вболівальників команди "Зеніт", яка відрізняється високим ступенем агресивності, схильна до насильницьких дій та заподіяння матеріальної шкоди. Отримані дані було використано для підготовки та проведення комплексу оперативно-розшукових заходів (візуальне спостереження, оперативні опитування, короткочасне оперативне впровадження). Отриману інформацію було вдало використано для організаційних, профілактичних та адміністративних заходів у результаті яких заплановану злочинну діяльність (групові порушення громадського порядку, погроми, навмисне пошкодження приватного та комунального майна) було повністю блоковано, а діяльність групи взято під повний контроль [12, с. 353–354]. Роботу донецької міліції високо оцінили на міжнародному рівні, після чого представники правоохоронних органів Російської Федерації приїжджали для вивчення досвіду.

Правоохоронний моніторинг кіберпростору, поряд із комп'ютерним спостереженням; організацією та використанням громадської допомоги, як і аналітична розвідка, може зараховувати окремі оперативно-розшукові заходи (оперативно-пошукові заходи із забезпечення оперативної закупівлі та контрольованого постачання товарів, заборонених для відкритого обігу; оперативне впровадження у віртуальні соціальні групи, що мають деструктивні цілі, окремі оперативно-аналітичні та оперативно-технічні заходи). Враховуючи те, що правоохоронний моніторинг включає низку оперативно-розшукових заходів, його потрібно зарахувати до компетенції лише тих правоохоронних органів, підрозділи яких уповноважені провадити оперативно-розшукову діяльність і негласні слідчі (розшукові) дії.

Отже, SNA методи сьогодні у примітивному вигляді (аналіз інформації проводить одна особа або група) вже використовуються у нашій країні при проведенні аналітичної розвідки та повинні бути використані у своїх найбільш досконалих формах (із застосуванням сучасних комп'ютерних технологій та програмного забезпечення) при запровадженні загальнодержавної системи правоохоронного моніторингу кіберпростору. Слід зазначити, що в деяких підрозділах правоохоронних органів України проходить пілотне використання певних інструментаріїв цього методу.

При використанні правоохоронного моніторингу кіберпростору для протидії організованій злочинності потрібно враховувати, що вона є проявом злочинності як соціального явища, яке полягає у вчиненні злочинних діянь окремими особами або їх об'єднаннями, які знаходяться між собою у стані соціальної взаємодії з приводу вчинення зазначених діянь та отримання від них матеріального або іншого зиску. Такого роду злочинність можна охарактеризувати як "системну", оскільки вона має виражений системний характер. При цьому системоутворюючим чинником є отримання певного зиску, як правило, матеріального надприбутку. Ступінь організованості таких систем може бути різним і залежить від кількості елементів, тривалості їх функціонування, тобто усталеності та здатності забезпечувати власну життєдіяльність, та ефективності, що виражається у здатності отримувати надприбутки. У широкому розумінні така система може складатися лише із двох елементів (так само, як і у легальному бізнесі суб'єкти господарювання можуть суттєво відрізнятися як за розмірами, так і за масштабами діяльності) – у той же час, з точки зору організації протидії найбільшу загрозу становлять кримінальні системи високого рівня організації і, відповідно, для забезпечення протидії їм потрібним є застосування іншого правоохоронного інструментарію. Причиною існування організованої злочинності є те, що вона задовольняє певні суспільні потреби, які не задовольняє легальна економіка, такі як наркотики, або надає послуги, які не може надати держава, наприклад, захист від рекету. Злочинність є відображенням суспільних практик, що реалізуються незаконним шляхом. Чим більш організованим стає сучасне суспільство, тим більш організованою стає і злочинна діяльність [1].

Головні висновки роботи. Правоохоронний моніторинг кіберпростору має стати одним із потужних засобів попередження, блокування та викриття діяльності організованих злочинних формувань, їх виявлення, дезорганізації та ліквідації. Такий моніторинг потрібно визначити як діяльність уповноважених державних органів з відстеження використання кібернетичних комп'ютерних систем управління та оброблення інформації у деструктивних цілях з метою запобігання суспільно небезпечним діянням, їх вияв-

лення та припинення. Його потрібно проводити у соціальних та інших комп'ютерних мережах регіонального та глобального рівня.

Для забезпечення виконання завдань протидії організованій злочинності правоохоронний моніторинг кіберпростору має ґрунтуватися на вивченні реальних соціальних мереж (зв'язків, взаємовідносин, взаємодій) через аналіз їх кібернетичних відбитків із подальшим використанням методів SNA, а також застосовувати методи і джерела інформації, що є традиційними у практиці вітчизняної аналітичної розвідки.

Перспективи подальшого використання. На переконання автора, застосування в Україні у процесі здійснення правозастосовної практики правоохоронного моніторингу кіберпростору та методів SNA має сприяти як протидії організованій злочинності взагалі, так і діяльності такої найбільш небезпечної його частини, як ТОЗУ зокрема.

Список використаних джерел

1. Міняйло Н. Є. Організована злочинність: природа та шляхи протидії (системно-функціональний підхід) / Н. Є. Міняйло // Наук. вісник Чернівец. ун-ту. – 2013. – Вип. 644. Правознавство. – С. 120–126.

2. Организованная преступность – главная угроза XXI века / [Электронный ресурс]. – Режим доступа : http://cont.ws/post/.

3. О проекте европейского закона по борьбе с мафией / [Электронный ресурс]. – Режим доступа : http://www.crime.vl.ru.

4. Прохоров А. Компьютерная визуализация социальных сетей [Электронный ресурс] / А. Прохоров, Н. Ларичев. – Режим доступа : //http://compress.ru/article.aspx?id=16593.

5. Гавловський В. Д. Правоохоронний моніторинг соціальних мереж / В. Д. Гавловський // Правова інформатика. – 2014. – № 3(43).– С. 19–25.

6. Погорецький М. А. Поняття кіберпростору як середовища вчинення злочину / М. А. Погорецький, В. П. Шеломенцев // Інформаційна безпека людини, суспільства, держави. – К., 2009. – № 2. – С. 77–81.

7. Угольков В. Как ловят мошенников в социальных сетях [Электронный ресурс] // В. Угольков. – Режим доступа : http://forbes.ua/opinions/1369438-kak-lovyat-moshennikov-v-socialnyh-setyah.

8. Проценко І. В. Розвідувальна діяльність як елемент забезпечення економічної безпеки України: поняття, види / І. В. Проценко // Наук. вісник Нац. акад. внутр. справ України. – 2003. – № 4. – Ч. 2. – С. 162–173.

9. Долженков О. Ф. Інновації – чинник оптимізації оперативно-розшукової діяльності / О. Ф. Долженков // Актуальні проблеми оперативно-розшукової діяльності : Вісник Луган. акад. внутр. справ МВС ім. 10-річчя незалежності України. – 2003. – Спецвип. № 2. – С. 23–34.

10. Хахановський В. Г. Інформаційно-аналітичне забезпечення ОРД: основні поняття та нормативно-правова база. Шляхи вдосконалення оперативно-розшукової діяльності ОВС / В. Г. Хахановський // Вісник Львів. ін-ту внутр. справ. – 2002. – № 2 (1). – С. 191–195.

11. Бусол О. Ю. Аналітична розвідка у спеціальних підрозділах по боротьбі з організованою злочинністю: сутність, проблеми / О. Ю. Бусол // Наук. вісник Київ. нац. ун-ту внутр. справ. – 2005. – № 2. – Ч. 2. – С. 94–103.

12. Грібов М. Л. Діяльність підрозділів оперативної служби МВС України: теорія та практика : [монографія] / М. Л. Грібов. – К. : Розвиток, 2013. – 532 с.

Рассмотрены возможности использования правоохранительного мониторинга киберпространства в сочетании с интеллектуальными информационными технологиями как средства борьбы с организованной преступностью.

The article deals with the use of law enforcement monitoring of cyberspace in combination with intelligent information technologies as a means of combating organized crime.

Стаття надійшла до редакції журналу 30 жовтня 2014 року.