УДК 343.1:65.012.8 + 004

КРИМІНАЛЬНА РОЗВІДКА ТА ЇЇ СПІВВІДНОШЕННЯ З ОПЕРАТИВНИМ ОБСЛУГОВУВАННЯМ

Олександр МАНЖАЙ,
кандидат юридичних наук, доцент, доцент кафедри захисту інформації
Харківського національного університету внутрішніх справ
Євген ЖИЦЬКИЙ,
здобувач
Харківського національного університету внутрішніх справ

SUMMARY

In the article content of term „criminal intelligence process" is analyzed and compared it with definition „operative service". Attention is devoted to the activity aspect of these institutes in different countries. Widespread strategies of the criminal intelligence process are explored; its stages, separate applied methods and forms of results presentation are expounded. Assets which are used in criminal intelligence process are separately considered, and informational support of this process is explored. Underline a role of work with human sources of information in criminal intelligence process. A definition of operative service is given and its content is analyzed. Modern tendencies are considered in operative service of hi-tech objects. On the basis of the conducted analysis suggestions are expounded in relation to the improvement of domestic institute of operative service.

Key words: intelligence process, criminal intelligence, operative service, law enforcement authorities.

АНОТАЦІЯ

У статті проаналізовано зміст терміну «кримінальна розвідка» та порівняно її з дефініцією «оперативне обслуговування». Сконцентровано увагу на діяльнісному аспекті цих інститутів в різних країнах. Розглянуто поширені стратегії, в яких викладено процес кримінальної розвідки, її етапи, окремі застосовувані методи та форми подання результатів. Окремо розглянуто засоби, які використовуються у кримінальній розвідці, та її інформаційне забезпечення. Підкреслено роль роботи з конфідентами під час провадження кримінальної розвідки. Надано визначення та проаналізовано зміст оперативного обслуговування. Розглянуто сучасні тенденції в оперативному обслуговуванні високотехнологічних об'єктів. На підставі проведеного аналізу викладено пропозиції щодо удосконалення вітчизняного інституту оперативного обслуговування.

Ключові слова: кримінальна розвідка, оперативно-розшукова інформація, оперативне обслуговування, правоохоронні органи.

Постановка проблеми. Сучасні тенденції правоохоронної діяльності в світі свідчать про те, що головні пріоритети роботи поліцейських структур поступово зміщуються від послідуючого до превентивного реагування на злочинні прояви. Превентивна діяльність на теперішній час не лише обговорюється в наукових колах, але й реалізуються через впровадження змін та доповнень до чинного законодавства. В Україні, наприклад, у зв'язку з прийняттям Кримінального процесуального кодексу у 2012 році головними завданнями оперативно-розшукової діяльності стали саме виявлення та попередження злочинів, а не їх розкриття. При цьому варто наголосити, що у різних країнах застосовуються різні концепції та інститути діяльності поліції у попереджувальній роботі. Вказані обставини потребують узгодження відповідних термінів для того, аби можна було імплементувати корисний досвід один одного до національного законодавства, а також покращити відповідну міжнародну взаємодію. «Кримінальна розвідка» та «оперативне обслуговування» є одними з таких дефініцій, які потребують наукового осмислення та порівняння.

Аналіз останніх досліджень і публікацій. Вивченням питань оперативного обслуговування на теренах СРСР та України займалися К. В. Антонов, О. М. Бандурка, Б. Є. Богданов, Р. А. Зінтарс, А. Г. Лєкарь, В. А. Лукашов, В. Л. Ортинський, М. М. Перепелиця, М. А. Погорецький, В. Д. Пчолкін, Г. К. Синілов, Є. В. Токарєв, І. А. Федчак та багато інших авторів. Питання кримінальної розвідки вивчали Х. Брейді, Дж. Грів, Д. Картер, М. Петерсон, Дж. Ретклiф, К. Россі, В. Симовиць, М. Сперoу, Ф. Фортін та інші. Разом з тим порівняння діяльнісного аспекту цих інститутів в різних країнах не проводилось.

Мета статті полягає в тому, щоб проаналізувати зміст терміну «кримінальна розвідка» та порівняти її з дефініцією «оперативне обслуговування».

Виклад основного матеріалу. На теперішній час в усьому світі набуває популярності провадження правоохоронними органами кримінальної (поліцейської) розвідки (criminal intelligence process) з метою попередження та прогнозування злочинності. Завдяки такій діяльності накопичується розвідувальна інформація (criminal intelligence) та вживаються дії превентивного характеру. Дослідженню вказаної сфери на теперішній час приділяють досить велику увагу за кордоном, розробляючи на її основі відповідні стратегії правоохоронних органів [1, с. 345].

На сайті Вікіпедії можна віднайти базове визначення розвідувальної інформації. Згідно з цим ресурсом – це оброблена, проаналізована та/або поширена інформація, яка використовується з метою прогнозування, попередження або спостереження за кримінальною активністю. Вона збирається за допомогою конфідентів, спостереження, опитування або особистого пошуку окремих офіцерів поліції [2]. Як можна побачити з даного визначення, за своєю суттю воно є дуже подібним до застосовуваного на теренах пострадянських країн терміну «оперативно-розшукова інформація».

На теперішній час найбільш поширеними стратегіями, в яких викладено процес кримінальної розвідки, є британська «Національна розвідувальна модель» (National Intelligence Model) [3] та американський «Національний план розподілу розвідувальної інформації» (National Criminal Intelligence Sharing Plan) [4]. Із вказаними стратегіями тісно пов'язана інша дефініція – «організація діяльності поліції на основі розвідувальних даних» або «модель поліцейської діяльності» (Intelligence-Led Policing (ILP)). Останній термін, як відмічають Дж. Картер, С. Філіпс та М. Гайадин, співвідноситься із описаними стратегіями таким чином, що стратегії визначають структуру, у рамках якої ILP може бути застосована у правоохоронних органах [5, с. 435].

Потрібно відмітити, що прийняття стратегій кримінальної розвідки у названих країнах не означає, що раніше кримінальна розвідка не застосовувалась. Натомість цими документами її було включено до стратегічних планів роботи правоохоронних органів. Цю тенденцію можна прослідкувати у багатьох розвинутих країнах, починаючи з 90-х років минулого сторіччя. Це ж стосується і країн, які нещодавно стали членами Європейського союзу. Наприклад, у Хорватії подібну практику почали впроваджувати як раз в означений період, що підтверджується даними науковців цієї країни [6, с. 181].

На теперішній час правоохоронними органами багатьох країн світу визнаються наступні принципи стосовно кримінальної (поліцейської) розвідки:

– дані поліцейської розвідки, які є своєчасними, дають підстави для вживання заходів, необхідних для результативного попередження, скорочення і розслідування серйозних злочинів і дій організованої злочинності, особливо, якщо вони мають транснаціональний характер (визначення «своєчасні» означає, що відомості надаються в належний час, а визначення «дають підстави для вживання заходів» припускає, що відомості є достатньо докладними і достовірними для проведення відповідних заходів);

– поліцейська розвідка може грати важливу роль у справі сприяння розподілу ресурсів і встановленню відповідних пріоритетів під час попередження, скорочення і розслідування всіх форм злочинної діяльності на основі виявлення і аналізу тенденцій, способів вчинення злочинів, «гарячих точок» і злочинців як на національному, так і на транснаціональному рівнях;

– розвідка служить наріжним каменем ефективної моделі поліцейської діяльності ILP, відповідно до якої розвідка необхідна для забезпечення стратегічного управління і грає ключову роль у справі розподілу кадрів для всіх форм тактичної поліцейської діяльності, включаючи роботу з громадами і звичайне патрулювання [7, с. 2].

У рамках навчання кримінальній розвідці використовуються різні моделі. Однією з таких моделей, спрямованих на досягнення мети розслідування, є так звана «5W+H» (Who, What, When, Where, Why and How) [8, с. 149]. Саме ця модель нерідко застосовується під час навчання поліцейських кадрів у країнах Європи та США.

Кримінальна розвідка складається із шести головних етапів, об'єднаних у циклічне коло:

– планування та визначення напрямів (цілей);
– збирання інформації;
– обробка інформації;
– аналіз інформації;
– поширення інформації;
– повторна оцінка інформації [4, с. 16].

У британській версії моделі зміст кримінальної розвідки описано більш докладно аніж в американській, тому вважаємо виправданим навести окремі елементи кримінальної розвідки, які корелюються з оперативним обслуговуванням саме з цього документу.

Британська «Національна розвідувальна модель» базується на узагальненні бізнес-стратегій для потреб правоохоронних органів. Стрижнем цієї моделі є засоби, за допомогою яких проводиться накопичення та вироблення відповідної розвідувальної інформації. Засоби поділяються на:

– *знання*, що охоплюють професійні знання, нормативні документи, правила, бази даних, які є в наявності у правоохоронних органах та партнерських організаціях;

– *системні засоби* – продукти, що використовуються для безпечного збирання, приймання, зберігання, компонування, аналізу та використання інформації. Вони складаються із засобів фізичної безпеки, управління доступом, правил безпеки, протоколів обміну інформацією тощо;

– *джерела*, за допомогою яких одержується різна інформація, яка належить до правоохоронної сфери, на національному та міжнародному рівнях. Вони включають жертв та свідків, громадські об'єднання та представників громадськості, фахівців з протидії злочинності, засуджених, криміналістичну інформацію, результати негласної роботи, результати спостереження, конфідентів;

– *сили*, які застосовуються для підтримки функціонування Національної розвідувальної моделі [9, с. 7].

Потрібно відмітити, що на відміну від української моделі оперативно-розшукової діяльності, де її сили і засоби є окремими категоріями, у британській правоохоронній практиці сили є складовою частиною засобів.

У результаті опрацювання даних, одержаних з використанням окреслених вище засобів, формується кінцевий розвідувальний продукт, у вигляді однієї з наступних форм:

– стратегічного аналізу, за допомогою якого виробляються довготермінові плани діяльності правоохоронних органів, розробляється стратегія та вимоги до кримінальної розвідки;

– тактичного аналізу, на підставі якого здійснюється розробка короткотермінових планів діяльності поліції згідно із загальною стратегією, а також може використовуватися для доповнення існуючих вимог до кримінальної розвідки;

– цільового профілю стосовно конкретної особи (підозрюваного чи жертви) або групи осіб у відповідності до стратегічних пріоритетів;

– проблемного профілю, в якому проаналізовано конкретний злочин або серію подій тощо [3, с. 67].

На підставі одержаних даних розробляються конкретні заходи та елементи взаємодії поліцейських підрозділів.

Одним з інструментів збирання оперативної інформації під час кримінальної розвідки є використання розвідки з відкритих джерел (open-source intelligence (OSINT)). В деяких правоохоронних органах західних держав навіть існують спеціальні підрозділи, що здійснюють таку діяльність (Scotland Yard OSINT, Royal Canadian Mounted Police OSINT, OSINT unit of New York Police Department, OSINT unit of the Los Angeles County Sheriff's Department [10]).

Також останніми роками набув популярності метод збирання розвідувальної інформації з комп'ютерних соціальних мереж, як різновид розвідки з відкритих джерел. Моніторинг в режимі реального часу оновлень у Facebook, Twitter та інших соціальних медіа дозволяє пра-

воохоронним органам одержати потрібну інформацію про вчинені або заплановані злочини. У даному випадку мова йде як про ювенальну злочинність, так і про особливо тяжкі злочини, відомості про які залишають окремі правопорушники в мережі. Володіння цією інформацією дозволяє правоохоронцям встановити злочинців та, за можливістю, припинити їх протиправну діяльність [11, с. 102].

Варто відзначити, що США стали однією з перших країн, в якій було нормативно урегульовано питання одержання інформації з інформаційно-телекомунікаційних систем правоохоронними органами. Маються на увазі «Правила онлайнових розслідувань для правоохоронних органів» 1999 р. Задля розуміння змісту цього документу, відмічають автори монографії «Оперативно-розшукова компаративістика» [12, с. 281], в ньому наведено багато аналогій між кіберпростором (cyberspace) та реальним середовищем (physical world).

Кримінальна розвідка у провідних західних країнах супроводжується обов'язковою оцінкою ризиків. Така практика серед іншого є характерною для країн західної Європи, Канади, США, Австралії, Нової Зеландії. Означена діяльність є актуальною для застосовуваного у рамках вітчизняної оперативно-розшукової практики поділу об'єктів за режимом обслуговування. Оцінка ризиків застосовується за кордоном також під час розстановки сил і засобів, зокрема у рамках прийняття рішення про використання конфідентів.

Досліджуючи агентурну роботу правоохоронних органів ФРН, О. В. Кльопов зауважує, що аналіз та оцінка ризиків та складання планів управління ризиками є інтегральною складовою частиною професійної роботи з негласним апаратом. Сенс аналізу ризиків полягає в тому, що безпосередній керівник оперативного підрозділу постійно інформує вищестоящого «реєструючого» керівника про свій план управління ризиками. Цей керівник, у свою чергу, має санкціонувати реєстрацію та використання агентів тільки в тому випадку, якщо буде доведено, що ризики та способи їх нейтралізації глибоко продумані та відображені у плані дій [13, с. 50].

Цікаву новацію у розстановці конфідентів, яку, на нашу думку, корисно використовувати правоохоронним органам, було запропоновано австралійськими науковцями. У рамках проекту з покращення управління агентурою у західних районах Австралії ними встановлено, що результативність використання агентури значно підвищується, якщо застосовувати для її розстановки комп'ютерні системи. Адже використання відповідних систем може допомогти акумулювати важливі деталі, що характеризують роботу конфідента, які у майбутньому сприятимуть його ефективному використанню. Наприклад, якщо встановлено певні події, які відбулися за участю особи А, яка становить оперативний інтерес, у певному місці Б, то дані А і Б вносяться до системи, яка перевіряє асоціації з цими параметрами наявних конфідентів. Надалі приймається рішення про можливість використання відповідних конфідентів для збирання оперативної інформації. Чим більше деталей про роботу конфідентів буде зберігатися у системі, тим якісніше можна бути прийняти рішення про їх використання [14, с. 21-22].

У рамках вирішення завдань правоохоронної діяльності основні зусилля поліції провідних західних країн повинні скеровуватися на виявлення та запобігання злочинам, враховуючи те, що на попередження правопорушень витрачається набагато менше ресурсів, аніж на подолання наслідків їх вчинення. Це ж саме стосується і встановлення пріоритетних напрямів у роботі конфідентів. З цього приводу варто навести твердження Карла Круза [15, с. 121, 127], який наголошує на необхідності зміни стратегії використання конфідентів. Для цього їх потрібно не тільки залучати для послідуючого реагування на вже вчинені злочини, але змінити пріоритет на попередження злочинів.

Суттєву роль у здійсненні кримінальної розвідки за кордоном відіграє її інформаційне забезпечення. На теперішній час створено та інтегровано потужні інформаційні масиви за різними напрямками діяльності, що дозволяє ефективно здійснювати правоохоронну діяльність.

Як правило, ці тенденції стосуються лише провідних країн світу. Наприклад, у Німеччині основними інформаційними базами, які можуть бути застосовані у негласній роботі, є:

– INPOL (Informationssystem der Polizei) – інформаційна система поліцій федерації і земель ФРН в цілях розшуку людей/предметів в інтересах кримінального переслідування і запобігання небезпеки;

– SIS (Schengener Informationssystem) – Шенгенська інформаційна система – поліцейська комп'ютерна система розшуку, що забезпечує працівникам європейських поліцій держав-учасниць Шенгенського договору прямий доступ до баз даних по розшуку осіб і предметів;

– VERMI/UTOT – поліцейська база даних безвісти зниклих/невпізнаних трупів;

– AFIS – поліцейська автоматизована система ідентифікації відбитків пальців;

– DAD – поліцейська база даних ДНК;

– SPUDOK – поліцейська база даних документації слідів злочинів;

– INTRANET/EXTRANET – закриті поліцейські розшукові бази даних;

– AZR – центральний реєстр іноземців;

– ZEVIS – Центральна інформаційна транспортна система федерального автотранспортного відомства ФРН тощо [16, с. 118].

У правоохоронних органах США та низки країн Європи значна увага приділяється візуалізації, під час провадження кримінальної розвідки, зокрема під час розбудови зв'язків між особами, які становлять оперативний інтерес. З цією метою застосовується матричний або графовий підхід (рис. 1.1). Як показує практика, візуалізована інформація набагато краще сприймається правоохоронцями, а це у свою чергу підвищує ефективність їхньої діяльності.

Попри наведені досягнення слід наголосити, що в окремих країнах, які розвиваються, спостерігається відставання у сфері інформаційного забезпечення. Наприклад, у Нігерії [19] на теперішній час лише розробляється система накопичення оперативно-розшукової інформації, подібна до європейських.

Важливе значення у рамках кримінальної розвідки має портретування особи потенційних злочинців для своєчасного їх виявлення на об'єктах оперативної уваги. Якщо мова йде про високотехнологічні злочини, то під час проведення кримінального аналізу для встановлення особи кіберзлочинців деякі дослідники пропонують застосовувати асоціативні та кластерні методи [20, с. 55]. Крім того, зарубіжні фахівці наголошують, на потребі застосування так званого «екологічного» підходу під час збирання оперативно-розшукової інформації [21, с. 193], який полягає у тому, що будь-яка система як її екологічний аналог еволюціонує та змінюється, що потребує

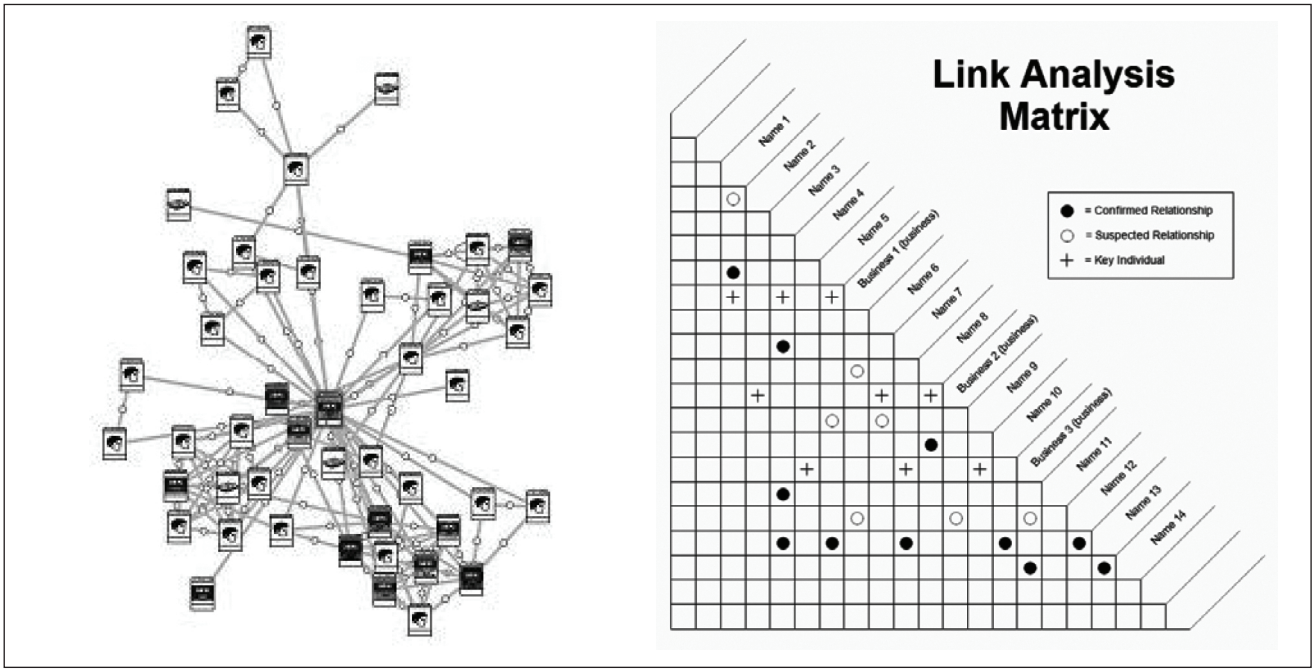

Рис. 1.1. Форми візуалізації аналізу зв'язків осіб, які становлять оперативний інтерес [17], [18]

постійного збирання та оновлення інформації про злочинну діяльність. Вказані пропозиції цілком збігаються із викладеною моделлю кримінальної розвідки у вигляді циклічного кола.

На теренах пострадянських країн за своїм змістом кримінальна розвідка найбільш асоціюється із оперативним обслуговуванням та аналітичною розвідкою. Остання є невід'ємним елементом оперативного обслуговування. Саме у рамках цієї діяльності аналітична розвідка є чи не найбільш важливим інструментом правоохоронних органів.

Одне з останніх визначень поняття «оперативне обслуговування» можна знайти у навчальному посібнику «Протидія злочинам у сфері земельних відносин», автори якого дають сучасну інтерпретацію цієї дефініції, розуміючи під нею систему реалізації запланованих заходів стратегічного, тактичного та організаційного характеру, що здійснюються з метою забезпечення безперервного процесу отримання первинної інформації про стан оперативної обстановки на лінії, території чи об`єктах обслуговування, її аналізу, систематизації та подальшого використання в кримінальному провадженні, а також задля своєчасного та ефективного виявлення, попередження та розслідування злочинів [22, с. 83]. Дане визначення, на нашу думку, є одним із найбільш комплексних та прийнятних для застосування у сучасних умовах.

За результатами аналізу терміну «оперативне обслуговування», нами було виділено його головні ознаки:

– поєднання активних і пасивних заходів оперативно-розшукового характеру;

– системність;

– безперервність;

– циклічність;

– визначене коло об'єктів оперативної уваги;

– пошуковий характер;

– чітко визначена мета (стратегічна, тактична та оперативна), яка у загальному вигляді може бути представлена як виявлення, попередження злочинів, а також сприяння розслідуванню і відшкодуванню матеріальних збитків;

– взаємодія суб'єктів-учасників оперативного обслуговування;

– особливості щодо конкретних напрямів правоохоронної діяльності.

Враховуючи викладене, можна побачити, що діяльність із кримінальної розвідки, яка здійснюється на заході, цілком узгоджується із вітчизняним інститутом оперативного обслуговування. На цій підставі вважаємо виправданим застосовувати новації у сфері кримінальної розвідки, які показали позитивний ефект за кордоном, у правоохоронній практиці країн пострадянського простору.

У цьому сенсі варто звернути увагу на сучасні тенденції в оперативному обслуговуванні об'єктів інформаційної діяльності у США, а саме: на законопроект «Про кібербезпеку» (Protecting Cyber Networks Act) [23], який 22 квітня 2015 року був погоджений Палатою представників США. Зміст нововведень, запропонованих у законопроекті, полягає у забезпеченні інформування правоохоронних органів компаніями про виявлені ними кібератаки. Обмін інформацією планується здійснювати в режимі онлайн через спеціальні кіберпортали під керівництвом Міністерства внутрішньої безпеки США. Вказані зміни до законодавства активно обговорюються провідними організаціями з безпеки, зокрема ISACA [24], та федеральними правоохоронним органами. Очевидно, що у разі прийняття даного законопроекту суттєво підвищиться рівень оперативного обслуговування об'єктів інформаційної діяльності, оскільки інформація регулярно надходитиме від самих об'єктів, які потребують перекриття, а відтак значно зменшиться час потрібний для вивчення оперативної обстановки у відповідному сегменті.

Вказана законодавча ініціатива щодо удосконалення оперативного обслуговування високотехнологічних об'єктів стала реакцією на часті атаки на великі компанії з боку хакерів. Одні з останніх таких атак, які сколихну-

ли громадськість, були компрометація 40 млн. платіжних карт клієнтів у великій мережі роздрібної торгівлі Target [25], а також викрадення 53 млн. адрес електронної пошти та 56 млн. платіжних даних клієнтів компанії з продажу будматеріалів і ремонтних пристосувань Home Depot [26].

Реалізація ідеї, закладеної у законопроекті є продовженням більш вузького проекту створення системи національного кіберінформування (National Cyber Awareness System, NCAS), яка забезпечується командою реагування на комп'ютерні надзвичайні події (US-CERT) Міністерства внутрішньої безпеки США шляхом представлення можливості підписатися на розсилку електронних листів щодо: виявлених надзвичайно небезпечних для загалу інцидентів з інформаційної безпеки; своєчасного інформування з питань інформаційної безпеки, виявлених вразливостей і експлойтів; щотижневого огляду вразливостей і можливих шляхів їх усунення; порад по загальних питаннях з безпеки [27, с. 191-192].

В умовах сплеску високотехнологічної злочинності новації даного законопроекту, на нашу думку, було б корисним імплементувати до українського законодавства. Це є особливо актуальним в умовах розбудови сучасної стратегії інформаційної безпеки України та такої її складової як кібербезпека, про що наголошує і керівництво держави [28]. Також, на нашу думку, корисним було б переглянути сучасну систему оперативного обслуговування у бік надання більш ширших повноважень інформаційно-аналітичним підрозділам щодо накопичення та обробки оперативно-розшукової інформації. Ця пропозиція цілком узгоджується із практикою провідних країн світу. По об'єктах, які надають послуги з використанням Інтернет, реалізувати вказану ідею більш легко, оскільки збирати великий обсяг необхідної інформації можливо опосередковано, за допомогою комп'ютерних мереж.

Висновки. За результатами проведеного аналізу змісту кримінальної розвідки та оперативного обслуговування доходимо висновку, що діяльність, яка проводиться у рамках обох інститутів правоохоронної діяльності, є подібною. Враховуючи це, представляється корисним імплементація рішень в означених сферах, які показали позитивний ефект, до національних законодавств. Серед іншого варто розширити функції аналітичних підрозділів у рамках здійснення оперативно-розшукової діяльності в постадянських країнах, а також розробити стратегію оперативного обслуговування.

Список використаної літератури

1. Жицький Є. О. Роль ДСБЕЗ у оперативному обслуговуванні об'єктів, які надають інформаційні послуги з використанням Інтернет / Є. О. Жицький // Сучасні проблеми правового, економічного та соціального розвитку держави: матеріали міжнародної науково-практичної конференції (м. Харків, 12 грудня 2014року) МВС України; Харків. нац. ун-т внутр. справ. – Харків: ХНУВС, 2014. – С. 343-345.

2. Criminal intelligence [Електронний ресурс]. – Режим доступу: http://en.wikipedia.org/wiki/Criminal_intelligence.

3. Guidance on the National Intelligence Model / Produced on behalf of the Association of Chief Police Officers by the National Centre for Policing Excellence. – 2005. – 213 с. [Електронний ресурс]. – Режим доступу: https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf.

4. The National Criminal Intelligence Sharing Plan / Department of Justice. – 2003. – 54 с. [Електронний ресурс]. – Режим доступу: https://it.ojp.gov/documents/ncisp/National_Criminal_Intelligence_Sharing_Plan.pdf.

5. Carter J. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory / J. G. Carter, S. W. Phillips, S. M. Gayadeen // Journal of Criminal Justice. – 2014. – № 42. – P. 433-442.

6. Šimovic V. Research of Classical and Intelligent Information System Solutions for Criminal Intelligence Analysis / Vladimir Šimovic // National Security and the Future. – 2001. – № 3-4 (2). – P. 181-200.

7. Работа полиции. Системы полицейской информации и разведки: пособие по оценке систем уголовного правосудия. – Нью-Йорк: Управление Организации Объединенных Наций по наркотикам и преступности, 2010. – 36 с.

8. Rossy Q. A Collaborative Approach for Incorporating Forensic Case Data into Crime Investigation Using Criminal Intelligence Analysis and Visualisation / Quentin Rossy, Olivier Ribaux // Science & Justice. – 2014. – № 54 (2). – P. 146-153.

9. National Intelligence Model: Code of Practice. – CENTREX, 2005. – 14 с. [Електронний ресурс]. – Режим доступу: http://library.college.police.uk/docs/npia/NIM-Code-of-Practice.pdf.

10. Open-source intelligence [Електронний ресурс]. – Режим доступу: http://en.wikipedia.org/wiki/Open-source_intelligence#Law_enforcement.

11. Perry W. L. The Role of Crime Forecasting in Law Enforcement Operations / W. L. Perry, B. McInnis, C. C. Price, S. C. Smith, J. S. Hollywood. – RAND Corporation, 2013. – 155 p.

12. Бандурка О. М. Оперативно-розшукова компаративістика: [монографія] / О. М. Бандурка, М. М. Перепелиця, О. В. Манжай. – Харків: ХНУВС, 2013. – 352 с.

13. Клёпов А. В. Правовые и организационные основы оперативно-розыскной деятельности таможенной службы Германии и их учет в обеспечении правоохранительного сотрудничества таможенных служб России и Германии: дисс. на соиск. уч. степени канд. юрид. наук: спец. 12.00.09 – «Уголовный процесс, криминалистика и судебная экспертиза; оперативно-розыскная деятельность» / А. В. Клёпов. – М., 2006. – 190 с.

14. Rajakaruna N. Community Intelligence: Exploring Human Source as a New Frontier / N. Rajakaruna, P. Henry, Ch. Crous, A. Fordham // Australasian Policing: A Journal of Professional Practice and Research. – 2013. – № 5 (1). – P. 19-22.

15. Crous C. Human Intelligence Sources: Challenges in Policy Development / C. Crous // Security Challenges. – 2009. – № 3 (5). – P. 117-127.

16. Сокол В. Ю. Полицейский розыск в Германии / В. Ю. Сокол // Вестник Краснодарского университета МВД России. – 2009. – № 1. – С. 116-123.

17. Chen H. Visualization in Law Enforcement / H. Chen, H. Atabakhsh, Ch. Tseng, B. Mars // Extended Abstracts Proceedings of the 2005 Conference on Human Factors in Computing Systems (Portland, Oregon, USA, April 2-7), 2005. – P. 34-37.

18. Link Analysis Matrix [Електронний ресурс]. – Режим доступу: http://www.rff.com/matrix_sample.htm.

19. Adeola S. O. National Crime Intelligence System / S. O. Adeola, B. K. Alese, S. O. Falaki // Information Technology Journal. – 2007. – № 6 (5). – P. 633-647.

20. Chen H. Crime Data Mining: a General Framework and Some Examples / Hsinchun Chen, Wingyan Chung, Jennifer Jie Xu, Gang Wang Yi Qin, Michael Chau // Computer. – 2004. – № 37. – С. 50-56.

21. Ayling J. Criminal Organizations and Resilience / J. Ayling // International Journal of Law, Crime and Justice. – 2009. – № 37. – P. 182-196.

22. Протидія злочинам у сфері земельних відносин: навч. посібник / С. В. Андрусенко, О. М. Бандурка, М. С. Рябчен-

ко та ін.; за заг. наук. ред. С. М. Гусарова. – Харків: ХНУВС, 2013. – 170 с.

23. The Protecting Cyber Networks Act [Електронний ресурс]. – Режим доступу: http://intelligence.house.gov/ProtectingCyberNetworksAct.

24. U. S. House Passes Cybersecurity Information sharing Legislation: special report (27 April 2015) [Електронний ресурс]. – Режим доступу: http://www.isaca.org/cyber/Documents/CSX-Special-Report-0427_misc_Eng_0415.pdf.

25. Sidel R. Target Hit by Credit-Card Breach [Електронний ресурс] / Robin Sidel, Danny Yadron, Sara Germano. – Режим доступу: http://www.wsj.com/news/articles/SB10001424052702304773104579266743230242538.

26. Kumar D. K. Home Depot says about 53 million email addresses stolen in breach / Devika Krishna Kumar [Електронний ресурс]. – Режим доступу: http://www.reuters.com/article/2014/11/07/us-home-depot-dataprotection-idUSKBN0IQ2L120141107?feedType=RSS&feedName=technologyNews.

27. Носов В. В. Система протидії кіберзлочинності FBI U. S. / В. В. Носов // Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності: матеріали міжнарод. наук.-практ. конф. (Харків, 12 листопада 2014 р.) МВС України; Харк. нац. ун-т внутр. справ. – Х. : Права людини, 2014. – 200 с. – С. 143-145.