МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
ФАКУЛЬТЕТ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ
КАФЕДРА КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ

ТЕМА:

Аналіз зарубіжного досвіду використання системи поліцейської інформації та розвідки

Кваліфікаційна робота
студента 2 курсу навчання
освітнього ступеню «магістр»
ННІЗДН факультету № 2
Кордонський Михайло Сергійович

Науковий керівник:
кандидат юридичних наук, доцент
Мельнікова Олена Олександрівна

Рецензент: кандидат юридичних наук, доцент Форос Ганна Володимирівна

Кваліфікаційна робота допущена до захисту
_____ 2022 р., протокол № ___
В.о. завідувача кафедри кібербезпеки та інформаційного забезпечення,
доктор юридичних наук, доцент
_____А.М. Бабенко
(підпис)

Одеса – 2022

ЗМІСТ

ВСТУП

Реформування правоохоронних органів, яке здійснюється в контексті європейської інтеграції України, обумовлює важливість питань запровадження новітніх інформаційно-комунікаційних технологій, завдяки яким можна значно підвищити продуктивність правоохоронної діяльності.

У зв'язку з цим, незважаючи на вітчизняні досягнення у справі інформаційного забезпечення службової діяльності правоохоронних органів, особливого значення набуває вивчення міжнародного та зарубіжного досвіду застосування інформаційних технологій та обліку його у вдосконаленні інформаційно-аналітичного забезпечення правоохоронної діяльності в Україні.

Сьогодні інформаційне забезпечення правоохоронних органів України потребує вдосконалення для ефективної та успішної протидії злочинам проти життя та здоров'я людини, пов'язаних із незаконним обігом наркотиків, а також в економічній, екологічній та інших сферах. Дедалі актуальнішими стають проблеми, що породжуються транснаціональною злочинністю: тероризм, торгівля людьми та сексуальна експлуатація жінок та дітей, незаконна торгівля наркотиками, незаконна торгівля зброєю, відмивання грошей, підробка платіжних засобів.

Методологія поліцейської інформації та розвідки покладена в основу низки спеціалізованих програмних рішень для правоохоронних органів (Crimeview Server, My Neighborhood Map System, CrimeReports Plus).

Питання вивчення зарубіжного досвіду застосування системи поліцейської інформації та розвідки розкрито в роботах С. Албула, О. Бочкова, Х. Брейді, М. Грибова, Дж. Грива, Р. Девіса, Т. Джона, Є. Жицького, О. Зайця, К. Ісмайлова, Д. Картера, П. Клеркса, О. Користіна, В. Коаді, В. Кребса, М. Макгуаера, А. Манжая, С. Брауна, В. Некрасова, М. Петерсона, Дж. Ретклiфа, О. Райбаха, К. Россі, Ст. Сімовиця, М. Сперoу, Н. Тіллі, В. Філіповскі, Ф. Фортіна, А. Ханькевича, Дж. Хаулетта,

В. Шендріка, Дж. Шептицького, І. Шинкаренко, С. Шнейдера та інших дослідників. Водночас слід зазначити, що в українському науковому просторі дослідження моделей системи поліцейської інформації та розвідки, застосовуваних у західних країнах, особливо відповідної методології, є вкрай бідними, що ускладнює впровадження передових методів правоохоронної діяльності в українську практику.

Останнім часом в Україні спостерігається інтенсивне впровадження сучасних інформаційних технологій практично у всі сфери життєдіяльності держави, у тому числі в діяльність Національної поліції. Створюються, впроваджуються й успішно використовуються в правоохоронній діяльності міжвідомчі банки даних та інші комп'ютеризовані системи.

Метою дипломної роботи є аналіз основних елементів системи поліцейської інформації та розвідки в країнах Євроспільноти та США.

Для досягнення поставленої мети слід виконати такі завдання:

- розглянути організаційні та тактичні аспекти поліцейської інформації та розвідки, а також пов'язані з ними термінологію та правову основу;

- провести аналіз окремих методів, що застосовуються для підготовки аналітичних висновків для використання в системі поліцейської інформації та розвідки;

- провести аналіз зарубіжного досвіду застосування інформаційних технологій у діяльності правоохоронних органів;

- проаналізувавши зміст терміна «кримінальна розвідка» та «кримінальний аналіз», розглянути поширені стратегії, в яких викладено процес створення системи поліцейської інформації та розвідки, її етапи, окремі застосовувані методи та форми подання результатів цього виду поліцейської діяльності.

РОЗДІЛ 1.
ТЕОРЕТИЧНЕ ПІДҐРУНТЯ ВИКОРИСТАННЯ ВИКОРИСТАННЯ СИСТЕМИ ПОЛІЦЕЙСЬКОЇ ІНФОРМАЦІЇ ТА РОЗВІДКИ

1.1. Сутність та зміст поліцейської інформації та розвідки

У цьому підрозділі буде розглянуто організаційні та тактичні аспекти поліцейської інформації та розвідки, а також пов'язані з ними термінологія та правова основа.

Зміст інформаційно-аналітичного забезпечення поліцейської розвідки набагато ширший, ніж формальне наведення довідок. Тому слід дещо заглибитись у теорію аналітичної роботи у сфері поліцейської діяльності.

Із позицій даної теорії аналітична робота розглядається не тільки як відповідна дослідницька діяльність спеціалізованих суб'єктів – співробітників інформаційно-аналітичних підрозділів, оперативних апаратів правоохоронних органів, але і як пізнавальний процес у цілому, окремими навичками якого повинні володіти всі без винятку суб'єкти поліцейської діяльності.

Добре відомо, що інформаційно-аналітична робота, незалежно від сфери свого застосування, є творчою діяльністю, пов'язаною з оцінкою наявної інформації та підготовкою на її основі оптимальних рішень. Дане твердження повною мірою відноситься і до аналітичної роботи у сфері поліцейської діяльності, основний зміст якої полягає у приведенні розрізнених оперативно-розшукових та інших відомостей, що становлять оперативний інтерес, у логічно стрункy та обґрунтовану систему залежностей (просторово-часових, причинно-наслідкових та ін.), дозволяють дати правильну оцінку як всієї сукупності фактів, і кожному їх окремо.

Як характерну особливість аналітичної діяльності слід виділити її непроцесуа-

льний характер, специфіку суб'єктів, що її здійснюють, інформаційну базу, цілі, завдання, об'єкти та предмет дослідження, а також форми, види, засоби, методи та способи її здійснення.

На основі підходів, зазначених у цій теорії науковцями [36] сформульовані концептуальні положення інформаційно-аналітичного забезпечення поліцейської розвідки, які мають вельми різнобічний характер і включають до свого складу елементи предмета теорій та вчень різних галузей знань. Однак основним ядром, що консолідує ці знання, безумовно, є елемент предмета теорії поліцейської діяльності, що цілком переконливо підтверджується подальшими висновками.

Науковий та прикладний напрям концептуальних основ інформаційно-аналітичного забезпечення поліцейської інформації та розвідки формує його цілі та завдання, що визначають у сукупності стратегію та тактику розвитку даної сфери діяльності.

У практичній сфері метою концептуальних основ інформаційно-аналітичного забезпечення поліцейської розвідки є загальна спрямованість досліджень, очікуваний кінцевий результат у передбачуваному реальному вираженні, дозволяє використовувати його в оперативно-розшуковому, а в необхідних випадках – і в кримінальному процесі.

Як завдання прикладного елемента концептуальних основ інформаційно-аналітичного забезпечення поліцейської розвідки у кожному даному випадку виступає сукупність цільових установок, у яких формулюються основні вимоги до аналізу та вирішення досліджуваної проблеми [26].

Як відомо, цільові установки в теорії поліцейської діяльності визначаються її організаційно-тактичними формами, до яких належать:

1) виявлення первинних оперативних даних та оперативна перевірка осіб, які мають до них відношення;

2) оперативне запобігання злочинам;

3) оперативна технологія;

4) оперативне супроводження досудового розслідування та судового розгляду [42].

Саме форми поліцейської діяльності, що поєднують у собі оперативно-тактичні та організаційно-тактичні (управлінські) заходи, визначають практично характер прикладних завдань концептуальних основ інформаційно-аналітичного забезпечення поліцейської розвідки.

Завдання прикладного елемента концептуальних основ інформаційно-аналітичного забезпечення поліцейської розвідки безпосередньо пов'язані з чітким визначенням у тій чи іншій ситуації об'єкта та предмета проведеного аналізу, вибором форм, засобів та методики здійснення останнього, а також створенням та планомірним удосконаленням його інформаційної основи.

Як основні об'єкти інформаційно-аналітичного забезпечення поліцейської розвідки розглядаються протиправні дії та пов'язані з ними кримінально активні особи, сукупність яких характеризує загалом поняття злочинності. Крім того, до них належать правопорушення, що не мають кримінального характеру, пізнання яких прямо чи опосередковано сприяє виконанню завдань, що стоять перед правоохоронними органами; факти й обставини непротиправної властивості, що вимагають відповідно до приписів чинних нормативних правових актів перевірки шляхом застосування оперативних заходів [2].

Однак для детальнішого аналізу фактографічної та криміналістичної складових оперативної інформації, що використовується в аналітичній діяльності, застосовується ширший перелік її об'єктів. До нього входять особи (фізичні та юридичні), корпоративні об'єкти (наприклад, злочинні формування), предмети, речовини, тварини, трупи, приміщення, споруди, ділянки місцевості, явища, процеси, події, навички, зовнішні дії людини.

Предметом інформаційно-аналітичного забезпечення поліцейської розвідки є найбільш суттєві властивості об'єктів дослідження, пізнання яких необхідне досягнення поставлених цілей [26]. Іншими словами, це характерні особливості або

ознаки об'єктів, зафіксовані на відповідних носіях або в пам'яті людей, а також їх відображення.

Під інформаційним забезпеченням інформаційно-аналітичного забезпечення поліцейської розвідки розуміється система заходів для застосування оперативно-розшукової інформації, яка знаходить своє реальне втілення у створенні інтегрованого банку даних оперативно-розшукового призначення підрозділів поліцейської розвідки. Його структура є єдиною корпоративною територіально розподіленою системою, що включає в себе два організаційні рівні: локальний і загальнодержавний.

Функціональним ядром інтегрованого банку даних оперативного призначення підрозділів поліцейської розвідки має стати оперативно-розшуковий облік, який формується співробітниками поліцейської розвідки. Важливим елементом цього обліку, на думку авторів [36], мають бути бази даних, які містять результати комплексної оперативно-розшукової реєстрації фізичних осіб, які обґрунтовано підозрюються у злочинній діяльності. Основним способом отримання обліково-реєстраційної інформації є негласна чи зашифрована оперативно-розшукова реєстрація.

Як основні засоби, що застосовуються в ході здійснення інформаційно-аналітичного забезпечення поліцейської розвідки, розглядаються відповідні апаратно-програмні комплекси та різні технічні пристрої, за допомогою яких здійснюється оброблення оперативних та інших відомостей фактографічного та біометричного характеру з найбільш високою якістю кінцевих результатів. До таких насамперед належать автоматизовані інформаційно-пошукові, експертні та логіко-аналітичні системи.

Окремі елементи завдань інформаційно-аналітичного забезпечення поліцейської розвідки пов'язані з поняттям методик останнього, які багато в чому визначають і його правової основи. Вони є сукупність методів, способів, прийомів, розумових операцій, здійснюваних у певній послідовності з використанням аналітичних засобів, що призводять до досягнення цілей та завдань аналітичної діяльності.

Як консолідуючу ідею пізнання сутності інформаційно-аналітичного забезпечення поліцейської розвідки в теорії поліцейської діяльності виступає думка про необхідність здійснення в інформаційному середовищі пошуково-розвідувальної діяльності з виявлення осіб та фактів кримінальної властивості. Ця ідея ще у період зародження та становлення теорії поліцейської діяльності неодноразово висловлювалася та послідовно розвивалася С.В. Албулом, О.Ф. Долженковим, К.Ю. Ісмайловим, О.Є. Користіним та іншими вітчизняними вченими. Вона покликана консолідувати всі поняття, терміни, міркування та принципи, що сприяють реалізації положень концептуальних основ інформаційно-аналітичного забезпечення поліцейської розвідки у різних умовах діяльності співробітників поліцейської розвідки на всіх рівнях управлінської вертикалі правоохоронних органів.

Іншою неодмінною умовою формування концептуальних основ є наявність у них певних теоретичних принципів - загальних та спеціальних. Як загальні принципи концептуальних основ інформаційно-аналітичного забезпечення поліцейської розвідки розглядаються керівні ідеї, пов'язані з генезою та змістом останніх, що характеризують їх як органічну частину теорії аналітичної роботи та теорії поліцейської діяльності [37 С. 175–186.]. Спеціальні принципи інформаційно-аналітичного забезпечення поліцейської розвідки аналогічні принципам будь-якої пізнавальної діяльності і пов'язані із закономірностями, що випливають із сутності самого цього процесу. До них належать безперервність нагромадження інформації, системність, узгодженість, варіантність, верифікованість, ефективність та ін. [8].

Результати інформаційно-аналітичного забезпечення поліцейської розвідки можна диференціювати за принципом їх використання у межах певних часових періодів. Наприклад, деякі фахівці поділяють методи аналітичної діяльності на ретроспективний аналіз, сучасний аналіз та прогностичний аналіз [28]. Аналіз окремих видів інформаційно-аналітичного забезпечення поліцейської розвідки дозволяє конкретизувати цю градацію з позицій застосування певних методик, і навіть спе-

цифіки результатів. Реально сформовані у вітчизняній розшуковій практиці елементи інформаційно-аналітичного забезпечення поліцейської розвідки можна диференціювати на ідентифікаційну, діагностичну та прогностичну складові. Об'єктивно існує такий комплексний вид здійснення інформаційно-аналітичного забезпечення поліцейської розвідки, як аналітичний пошук.

Оперативна ідентифікація та оперативна діагностика націлені на ретроспективний аналіз подій, але можуть здійснюватись і в реальному часі. На передбачення подій, що ще не настали, націлене оперативно-розшукове прогнозування. Аналітичний пошук, зазвичай, пов'язані з аналізом подій що триває характеру чи зачіпає всі зазначені часові періоди.

Заходи ідентифікаційного характеру полягають у проведенні таких оперативних заходів: дослідження предметів та документів (у частині проведення ідентифікаційних досліджень); ототожнення особистості; наведення довідок (в обліках).

Таким чином, правова кваліфікація ідентифікаційного елемента інформаційно-аналітичного забезпечення поліцейської розвідки, що передбачає дослідження матеріально визначених об'єктів, практично не викликає труднощів, як і у разі проведення інших розвідувальних заходів, що включають до складу зазначені оперативні методи. Цього не можна сказати про інші складові інформаційно-аналітичного забезпечення поліцейської розвідки, які нерідко ґрунтуються на аналізі неформалізованої, подійної інформації, а як об'єкти дослідження розглядаються не мають матеріального втілення події, явища та психічні акти людини. Якщо слідувати положенням теорії аналітичної роботи, їх необхідно розглядати з позицій поєднання діагностичного дослідження предметів і документів, оперативно-розшукового прогнозування та аналітичного пошуку (аналітичної розвідки).

У ситуаціях, коли доводиться мати справу з аналізом не тільки криміналістичних даних, а й фактографічних відомостей, поряд із традиційними пошуковими ознаками доцільно вести мову про систему базових категорій, властивих тим чи ін-

шим подіям, явищам, психічним актам людини. Вона містить сукупність матеріальних об'єктів, задіяних у тій чи іншій події; різноманіття ознак, властивих цим об'єктам; сукупність зв'язків, які встановлюються між різними об'єктами; тимчасові фактори; просторові фактори; умови перебігу події, явища.

У різних поєднаннях ці базові категорії сприяють формуванню найбільш наближеної до реальності картини тієї чи іншої дії, події чи явища з допомогою діагностичних методик.

Без діагностики, як і ідентифікації, немислима реалізація й усіх відомих оперативних заходів. Ще в період зародження кримінального розшуку, коли більшість його співробітників не мала ані найменшого уявлення про будь-які наукові методи розкриття злочинів, запорукою їхнього успіху були вміння спостерігати, знання людської натури та здатність до вироблення версій [53]. На цих трьох «китах» продовжує базуватися і сучасна оперативна діагностика.

Серед основних видів оперативної діагностики фігурують методи поліцейської діяльності «оперативне розпізнання»; «опитування» і «спостереження», які з використанням технічних засобів (так звана «детекція брехні»), і навіть інші нетрадиційні методи поліцейської діяльності, пов'язані з «інструментальною діагностикою емоційного стану»; оперативна дія «розроблення оперативно-розшукової версії»; діагностична складова методу «дослідження предметів та документів».

Саме оперативне розпізнання, яке здійснюється під час проведення розвідувальних заходів усіх видів, надає їм характеру пошукових. Ідеться насамперед про факти підготовки та скоєння злочинів; про інші обставини, що мають значення для боротьби зі злочинністю (зокрема, що характеризують злочини та особистість винних, а також причини та умови, що сприяють скоєнню злочинів); про сліди та знаряддя підготовки до злочину; сліди, залишені злочинцями; викрадене майно та інші предмети, що мають значення для встановлення та викриття винних осіб; про предмети та речовини, заборонені до зберігання, носіння чи користування; про осіб, які

замишляють, готують і вчинили злочин або причетні до нього; про осіб, які допускають протиправну поведінку, яка свідчить про можливість скоєння ними злочинів; про осіб, які володіють інформацію, що має значення для розкриття злочину; про здатних систематично надавати допомогу у боротьбі зі злочинністю тощо [35]. Безумовно, оперативне розпізнання широко застосовується й в інформаційно-аналітичному забезпеченні поліцейської розвідки.

Ще один напрям інформаційно-аналітичного забезпечення поліцейської розвідки пов'язаний з методом «дослідження предметів та документів», який дозволяє здійснювати аналіз оперативної обстановки та діагностику злочинних діянь. До найперспективніших методів аналізу оперативної обстановки та діагностичного аналізу злочинних діянь фахівці відносять евристичний метод, метод аналогії, метод експертних оцінок; метод зіставлення паралельних рядів, метод кореляційного аналізу, регресійний та факторний аналіз; контент-аналіз; системний аналіз; структурно-функціональний аналіз; комплексний багатовимірний аналіз даних, інформаційно-аналітичне розслідування; метод оперативно-економічного аналізу; метод імітаційного об'єктно-структурного моделювання; метод аналізу мережі зв'язків; метод аналізу потоків подій; метод аналізу телефонних білінгів та інших. Усі вони мають яскраво виражений діагностичний характер. Основною метою їх використання є пошук «вузьких місць» в організації боротьби з правопорушенням, виявлення кримінальних структур, їх керівників та окремих учасників, а також встановлення та документування конкретних вчинених ними правопорушень. Можливості даних методів примножуються за рахунок застосування новітніх інформаційних технологій, які дозволяють аналізувати фактографічну інформацію природною мовою. Крім оптимізації самих результатів аналізу, це сприяє мінімізації втрат використовуваних інформаційних ресурсів.

Поряд з оперативною ідентифікацією, оперативним розпізнаванням та діагностичним дослідженням предметів та документів у структурі інформаційно-аналіти-

чного забезпечення поліцейської розвідки досить чітко вбачається й елемент, пов'язаний з оперативним прогнозуванням, яке кваліфікується на сьогоднішній день як метод поліцейської діяльності. Практично всі види оперативного прогнозування, насамперед засновані на методах логічної екстраполяції, створення прогнозних моделей та ін., за своїм змістом та алгоритмом здійснення вельми тісно стикаються з діагностикою [6], а значить – з оперативним розпізнаванням та дослідженням предметів та документів. Разом із тим у теорії аналітичної роботи оперативне прогнозування розглядається не тільки як оперативний метод, але і як самостійна форма оперативного аналізу, а серед функцій організації поліцейської діяльності воно фігурує як один з елементів управлінської діяльності [2].

Підсумовуючи різні точки зору, можна зробити висновок, що оперативне прогнозування є науково обґрунтованим судженням про передбачувані стани об'єктів поліцейської діяльності. На його створення, безумовно, слід використовувати базові положення основ кримінологічного прогнозування і навіть теорії криміналістичного прогнозування.

Оперативне прогнозування з метою його правової легітимізації, а також оперативне розпізнання слід визнати самостійним оперативним заходом.

Як ще одну складову інформаційно-аналітичного забезпечення поліцейської розвідки слід розглядати аналітичний пошук [34;13], який на сьогодні також належить до методів поліцейської діяльності. Ще відносно недавно кримінальний аналіз розглядався як один з основних методів інформаційно-аналітичного забезпечення поліцейської розвідки, щоправда, у цій якості він більше нагадував звичайний інформаційний пошук, тобто автоматизоване наведення довідок. Класичний ж аналітичний пошук дозволяє виконувати завдання набагато складніші, ніж пошук інформаційний. Головна його відмінність від останнього полягає в тому, що, крім звичайної «розвідки» в інформаційному середовищі, він спрямований на отримання «нових знань про об'єкт, що розвідується, або явище на підставі аналітичної обробки видобутої інформації та відомостей про відомі факти».

Як відомо, відображення ознак досліджуваного об'єкта, яким би повним воно не було, відтворює не всю їхню систему, а лише деякі з них. Найважливішим завданням аналітичного пошуку є встановлення прихованих, непомітних здавалося б процесів, що пов'язані з латентною зміною тих чи інших властивостей досліджуваних об'єктів. Через певну кількість ітерацій іноді можна встановити між різними об'єктами ланцюжок опосередкованих зв'язків, причому в деяких випадках ці об'єкти (особи, кримінальні угруповання) і самі не підозрюють про їх існування.

Абсолютно мають рацію ті фахівці, які вважають, що «аналітичний пошук (аналітична розвідка) — це компонент розвідувальної діяльності, що полягає у виявленні, оцінюванні, прогнозуванні соціальних процесів, подій, заходів на основі відомостей, які переважно отримують з відкритих джерел, а також добуваються розвідкою інших. видів (агентурної, технічної та ін.)» [5]. Цілком очевидно, що аналітичний пошук поряд з оперативним розпізнаванням та оперативним прогнозуванням також має бути віднесений до переліку оперативних заходів.

Таким чином, на основі проведеного сутнісного аналізу змісту інформаційно-аналітичного забезпечення поліцейської розвідки простежується його чіткий взаємозв'язок з певними оперативними заходами (установленням особи, наведенням довідок, дослідженням предметів та документів) та деякими оперативними методами.

Одне із завдань, пов'язаних з удосконаленням правової бази, що регламентує діяльність суб'єктів поліцейської розвідки, полягає в тому, щоб віднести оперативні методи «оперативне розпізнання», «оперативно-розшукове прогнозування» та «аналітичний пошук» до категорії методів, перелік яких передбачений у відомчій нормативно-правовій базі.

Формальних перешкод для такого рішення немає, оскільки ряд оперативних заходів, уже визнаних на сьогодні такими (оперативне впровадження, контрольоване постачання, обстеження приміщенні, будівлі, споруді, ділянок місцевості та транспортних засобів та ін.), мають набагато складнішу структуру і алгоритм здійснення і більшою мірою підпадають під визначення методу поліцейської діяльності,

ніж оперативне розпізнання, оперативне прогнозування та аналітичний пошук.

З усіх існуючих методик аналізу оперативної інформації, прийнятих на озброєння правоохоронними органами більшості розвинених країн світу, найчастіше використовуються програмні продукти i2 і ANACAPA. Такі програмні рішення візуального аналізу даних і отримання нових знань призначені для оперативних підрозділів і слідчих, чия діяльність пов'язана з необхідністю аналітичної обробки інформаційних потоків і даних, представлених у різних форматах. Зокрема, програмний продукт i2 – це комп'ютерне програмне забезпечення на базі SQL-server, покликане узагальнювати, аналізувати, висувати ймовірнісні зв'язки, а також візуалізувати в реальному часі обмін інформацією. Це програмне забезпечення є набором сумісних між собою різних програм, що виконують відповідні специфічні функції на всіх етапах розкриття і розслідування злочинів [9]. Аналітична лінія продуктів i2 представлена елементами, які здатні вирішувати переважну більшість аналітичних завдань як окремо, так і в їх різній комбінації (зокрема, Analyst's Notebook, Analyst's Notebook – Esri® Edition, Analyst's Workstation, iBase, iBase IntelliShare, iXv Visualizer, iBridge, iXa, TextChart, Chart Reader, PatternTracer). У сфері кримінального аналізу i2, як правило, застосовується із програмними продуктами iBase, iBridge, iGlass, Analyst's Workstation. Серед користувачів даної операційної аналітичної системи можна виділити правоохоронні органи США та Канади (ФБР, ЦРУ, DEA, NSA, RCMP), правоохоронні органи країн Євросоюзу, Інтерпол та Європол [7].

Програмний продукт компанії «ANACAPA Sciences Inc.» є передовою методикою розслідування злочинів і аналізу оперативної інформації. ANACAPA стояла біля витоків розробки спеціальних аналітичних методик для сфери безпеки і ще в 1971 році почала проведення навчальних курсів з підготовки фахівців-аналітиків. На даний момент ANACAPA пропонує такі 4 базові курси: аналіз інформації в ході проведення розслідувань Criminal Intelligence Analysis (CIA); аналітичні методи розслідування Analytical Investigation Methods (AIM); аналіз фінансових махінацій

Financial Manipulation Analysis (FMA); поглиблений аналіз з використанням комп'ютерних технологій Computer-Aided Analysis (CAA).

Використання аналітичних програм при аналізі даних забезпечує низку переваг, які допомагають підвищити ефективність і результативність роботи суб'єктів доказування. У процесі інтеграції інформації здійснюється її каталогізація та введення в систему контролю і пошуку інформації, яка дозволяє легко знаходити необхідну інформацію та отримувати до неї доступ. Програмні продукти є досить гнучкими. Вони пристосовані для зберігання вже зібраної інформації, а також можуть бути адаптовані до інтеграції додаткової інформації, яка надійде в майбутньому. У ході розслідування злочинів й аналізу інформації в інформаційну систему можуть вводитися нові розділи та підрозділи. Дані програмні продукти здатні сприймати величезні обсяги інформації, забезпечені засобами безпеки для обмеження доступу до інформації, отриманої в процесі розслідування. Збір відомостей з декількох джерел підвищує ймовірність отримання ключової доказової інформації і забезпечує можливість підтвердження та перевірки достовірності відомостей [44, с. 25].

Визначення теоретико-прикладного змісту поліцейської інформації та розвідки можна надати з аналізу визначення науковців та нормативних актів:

- сукупність систематичних аналітичних процесів, спрямованих на отримання своєчасної та достовірної інформації щодо змін у характеристиках та тенденціях злочинності з метою допомоги оперативним та адміністративним підрозділам у розподілі сил і засобів для попередження та припинення злочинної діяльності, допомоги у процесі розслідування (С. Готліб);

- вивчення певних характеристик та тенденцій з метою розкриття злочинів або запобігання їм (Експертна група Ради Європи з питань кримінального права та кримінології);

- визначення та розуміння (осмислення) зв'язків між кримінальною інформацією (інформацією про злочин) та іншою потенційно значимою інформацією з метою поліцейської та судової практики (Інтерпол) [28];

- професійна систематична специфічна інформаційно-аналітична діяльність, яка допомагає розкривати та розслідувати злочини або приймати управлінські рішення [9];

- опрацювання інформації, яка є суттєвою для керування та становить підставу для прийняття рішень.

Залежно від одержувача дана інформація має характер бази для планування, оціночний, керівний або контрольний характер [47].

Таким чином, можемо виокремити основні риси та складові поліцейської інформації та розвідки:

- сукупність систематичних аналітичних процесів;

- вивчення певних характеристик та тенденцій;

- визначення та розуміння (осмислення) зв'язків між кримінальною інформацією (інформацією про злочин) та іншою;

- систематична специфічна інформаційно-аналітична діяльність;

- опрацювання інформації, яка є суттєвою для управління або прийняття рішення;

- здійснюється з метою запобігання, припинення, розкриття та розслідування злочинів або прийняття управлінських рішень.

Як наслідок, сьогодні деякі науковці виокремлюють два види кримінального аналізу – аналітичний пошук та аналітичне дослідження. Основним змістом аналітичного пошуку є організація інформації таким чином, щоб полегшити завдання з вилучення сенсу із зібраних даних. Аналітичне дослідження полягає у встановленні взаємозв'язків між особами, подіями та предметами [54].

Ураховуючи думку науковців про прогнозування оперативної обстановки, як складової її моніторингу, як першої стадії кримінального аналізу, та враховуючи завдання, що вирішуються під час оперативно-розшукової діяльності, можемо визначити види оперативно-розшукового прогнозування:

а) стратегічне прогнозування тенденцій та чинників розвитку середовища функціонування, кримінологічної обстановки, сил та засобів правоохоронних органів, результативності протидії злочинності, громадської думки про стан середовища функціонування, криміногенної ситуації, результативність діяльності правоохоронних органів (у межах стратегічного кримінального аналізу);

б) тактичне прогнозування ситуації на період здійснення конкретних оперативно-розшукових заходів (у межах тактичного аналізу):

- прогнозування імовірної ситуації, що може скластися в період проведення оперативно-профілактичних заходів, для визначення варіантів моделі використання оперативно-розшукових сил та засобів та вибору тактики протидії злочинності (організаційно-управлінське прогнозування);

- прогнозування імовірної поведінки об`єктів оперативно-профілактичного впливу з метою визначення тактичних прийомів здійснення оперативно-розшукових заходів щодо протидії злочинності;

- прогнозування імовірної поведінки негласних співробітників у певних умовах під час виконання завдань оперативних працівників, що необхідно для визначення моделі їх навчання та інформаційно-тактичного забезпечення їхньої діяльності.

Аналіз думок кримінологів, криміналістів, які досліджують проблеми криміналістичного, кримінологічного прогнозування, та вчених у галузі поліцейської діяльності дозволяє надати типовий формалізований алгоритм оперативного прогнозування як складової кримінального аналізу, який, на думку науковців [35], повинен складатися з таких етапів:

- формулювання мети і завдань прогнозу;

- аналіз результатів оперативного моніторингу, негативні та позитивні чинники, що впливають на стан оперативної обстановки;

- систематизація, перевірка з використанням альтернативних джерел (ЗМІ, державні та суспільні установи, опитування громадян, соціологічний моніторинг) та

аналіз зібраної інформації;

- оцінка існуючого на конкретному об`єкті оперативної уваги та в цілому в державі (залежно від ієрархічного положення оперативного підрозділу) стану оперативної обстановки щодо попередження злочинності;

- визначення чинників, що впливають на стан оперативної обстановки, їх позитивного та негативного впливу;

- побудова математичної моделі оперативної обстановки;

- отримання вихідних даних щодо прогнозу;

- розроблення альтернатив розвитку оперативної ситуації залежно від вибору варіанта моделі організації поліцейської діяльності;

- розроблення узагальнюючого прогнозу.

Аналогічно прогноз може здійснюватися відповідно до поведінки осіб зі злочинного середовища тощо. При цьому прогнозування може бути:

- для планування та проведення окремого заходу та поліцейської операції;

- короткострокове – квартал, півріччя, рік;

- середньострокове – п`ять-десять років;

- довгострокове – п`ятнадцять та більше років.

Таким чином, оперативне прогнозування повинно розглядатися як невід'ємна частина процесу оперативного моніторингу у складі кримінального аналізу та бути його результативною частиною. Логіка сьогодення вимагає, що означені види кримінального аналізу повинні бути засновані на сучасному програмному забезпеченні та відповідному рівні комп'ютерної техніки.

Водночас для управління оперативними даними і їх максимального використання необхідна відповідна структура або модель, так само як і для збору, оброблення та використання даних та інформації в суворій відповідності з національним законодавством і міжнародними стандартами в галузі прав людини [72].

1.2. Загальна характеристика методів, що використовуються в системі поліцейської інформації та розвідки

Метою та завданням цього підрозділу є аналіз окремих методів, що застосовуються для підготовки аналітичних висновків для використання в системі поліцейської інформації та розвідки.

За сучасних умов правоохоронні органи всього світу дедалі активніше застосовують новації та потужний аналітичний апарат у протидії злочинності. У багатьох країнах створені спеціалізовані підрозділи, завданням яких є оброблення інформації, що надходить, з подальшим поданням аналітичних висновків, що мають оперативний, тактичний або стратегічний характер. Найчастіше така діяльність проводиться у рамках інституту кримінальної розвідки, який вже міцно вкоренився у професійній сфері національних та міжнародних правоохоронних органів [26].

Для ефективної підготовки відповідних розвідувально-аналітичних висновків застосовуються знання з різних наукових галузей, яким надано форму конкретних методів. Аналіз цих методів є важливим завданням вивчення інституту поліцейської розвідки як цілісного механізму.

Центральним елементом поліцейської розвідки як процесу є аналіз, без проведення якого сама ця діяльність втрачає сенс, а нагромадження даних буде здебільшого марною тратою часу.

Під час аналізу можуть бути застосовані різні методи та використовуватися конкретні моделі роботи з даними.

Відповідно до британської Національної розвідувальної моделі розвідувально-аналітичні продукти формуються з використанням 9-ти основних методик: аналіз результатів, аналіз кримінальних моделей, профіль ринку, аналіз демографічних та соціальних трендів, профіль злочинної діяльності, мережевий аналіз, аналіз ризиків, аналіз цільових профілів, оцінка оперативної розвідувальної інформації [67].

Указану класифікацію не можна назвати стійкою, оскільки під час здійснення

поліцейської розвідки постійно впроваджуються нові методи аналізу.

С. Р. Шнейдер виділяє аналіз телефонних зв'язків, аналіз потоків, мережевий аналіз, фінансовий аналіз, візуальний аналіз, контент-аналіз, складання змішаних таблиць кримінального аналізу, картографування підозрюваних [77, с. 9].

Практика показує, що переважна кількість аналітичних висновків містить елементи аналізу.

Цей метод є особливо актуальним в умовах вивчення великих злочинних груп та організацій, оскільки зі збільшенням мережі, що підлягає аналізу, зростає та ймовірність виявлення в ній слабких місць, з'являється можливість простежити відповідні зв'язки. Мережевий аналіз передбачає застосування теорії графів до певних об'єктів, подій тощо.

Однією з популярних методологій, що застосовуються для проведення полыцейської розвідки та містить велику кількість елементів мережевого аналізу, є ANACAPA. М. Спероу [4], досліджуючи застосування методології ANACAPA у полыцейській розвідці, відзначає її корисність для наочного представлення аналітику зібраних даних. По-перше, аналітик репрезентує зв'язки між фігурантами і таким чином визначає злочинну роль кожного. По-друге, спроектований граф в ідеалі повинен мати структуру, коли його ребра нічого очікувати перетинатися (планарність графа). Аналітик намагається досягти цієї мети. По-третє, у центрі графа поміщаються фігури, які відіграють ключові ролі.

Методи ANACAPA мають дещо спрощений характер із погляду мережевого аналізу. М. Спероу називає у зв'язку із цим кілька проблемних моментів: двомірність моделей, складність досягнення ефекту планарності графа в реальних умовах, визначення центральних фігур за обмеженими даними [80].

Остання проблема полягає в тому, що можна помилково визначити як ключові фігури осіб, які мають найбільшу кількість зв'язків, проте насправді вони не будуть такими. Це може статися або через обмеженість відомих даних, або з інших причин.

Так, наприклад, під час дослідження зв'язків в італійській мафії виявили, що

лідери злочинних угруповань виходять на зв'язок з іншими членами групи через обмежену кількість контактів [58]. Цей факт може сприяти тому, що під час автоматизованого аналізу телефонних зв'язків членів організованого злочинного угруповання дійсні лідери опиняться на периферії збудованого графа.

Узагалі, аналізуючи кримінальні мережі, для кожного з її учасників доцільно вираховувати крім соціального також так званий «кримінальний капітал» (корисні кримінальні знання та навички, доступ до знарядь та засобів скоєння злочинів, зв'язки з іншими особами з кримінальною репутацією). У сукупності вони визначатимуть вагу особи у кримінальному середовищі. В рамках аналізу зв'язків у соціальних кримінальних структурах для визначення механізмів їх розкладання та дезінтеграції необхідно залучати методологічний апарат теорії аналізу соціальних мереж (SNA), у тому числі визначити для кожного об'єкта відповідні метрики: ступінь центральності, силу зв'язку, еквівалентність тощо [73].

Звичайно, під час побудови відповідних графів та обчислення закономірностей слід пам'ятати про важливість визначення характеру зв'язків між об'єктами дослідження.

Створення окремих графів із подібними зв'язками дає можливість також зробити їх візуально прийнятними для сприйняття людським оком в силу їх меншого розміру. Також для наочнішого представлення даних окремі дослідники пропонують застосовувати техніки збільшення окремих ділянок графа (fisheye), фокусування, геопозиціонування даних графа, а також комбінування зазначених технік [66].

Мережевий аналіз може застосовуватися як визначення ролей та активності злочинного елемента, але й пошуку осіб, є потенційними конфідентами. Використання мережного аналізу з цією метою розглядають, наприклад, нідерландські дослідники П. Дуайн та П. Клеркс. Зокрема, вони пропонують це робити у сфері протидії кіберзлочинності та торгівлі людьми [65].

Як показує практика, істотну частину функцій кримінального аналізу можна

формалізувати, отже, і запрограмувати. Це серед іншого досягається використанням моделей (шаблонів), які враховують як просторові, і тимчасові параметри скоєння тих чи інших правопорушень. Деякі автори також пропонують враховувати кількісні параметри та безпосередньо зв'язки для візуалізації опрацьованих відомостей. Сама ж візуалізована модель повинна відображати інформацію про події, місця, об'єкти, зв'язки, профілі та ресурси.

Пошук асоціативних зв'язків у межах мережного аналізу є досить нетривіальним завданням. І тому можуть застосовуватися різні математичні алгоритми (див., наприклад, роботу Дж. Ксю і Х. Чена [85]).

Разом з тим для пошуку пропущених зв'язків між об'єктами, які не були підтверджені фактичними відомостями, також можуть застосовуватися досить прості математичні рішення, як той самий підрахунок кількості загальних зв'язків для кожного вузла мережі з подальшим їх порівнянням.

Ще одним ефективним методом, який застосовується під час здійснення поліцейської розвідки, є картографування злочинних проявів. Однією з цілей, що досягають із використанням цього методу, є побудова так званих географічних профілів.

Зазначені профілі дозволяють окреслити просторові рамки, у яких правопорушник може жити чи вести якусь діяльність. Використання описаних профілів разом із психологічними дозволяють цілісніше підійти до розслідування кримінальних правопорушень.

В основі побудови географічних профілів лежить теорія, згідно з якою як жертви, так і правопорушники мають певні стійкі маршрути руху, в рамках яких вони власне здійснюють свою повсякденну діяльність.

Як зазначає Дж. Реткліф, правопорушники зазвичай не вирушають далеко від свого постійного місцезнаходження для скоєння злочину, оскільки це вимагає від них додаткових зусиль та підвищує ризик бути спійманими. Разом із знаннями типової злочинної поведінки географічне профілювання дає можливість правоохоронним органам визначити точку ймовірного перебування правопорушника на певній

місцевості [76].

Ефективне картографічне профільування за сучасних умов практично неможливо здійснювати без застосування спеціалізованого програмного забезпечення. Як приклад останнього можна назвати продукти Rigel компанії ECRI (ecricanada.com), Crimestat (www.nij.gov/topics/technology/maps/crimestat.aspx), вітчизняний комплекс RICAS (police.Nh.ua). Паралельно зі створенням географічних профілів, як правило, відбувається побудова так званих «теплових карт», які мають візуалізувати на карті найбільш криміногенні ділянки. Ці ділянки відображаються більш насиченим кольором, як правило, із червоним відтінком.

Як зазначає А.Н. Ханькевич, техніка географічного профілювання дозволяє спростити оброблення інформаційного потоку, з яким стикаються поліцейські підрозділи під час розслідування серійних злочинів, а також оптимізувати оперативно-розшукову тактику пошуку злочинця: звузити коло підозрюваних за рахунок зіставлення переліку підозрюваних та осіб, які перебувають у високому рівні; силами поліції організувати у цій зоні інтенсивне патрулювання за години найбільш ймовірного скоєння злочину; активізувати на зазначеній території систему громадського інформування тощо [55].

Загальний алгоритм побудови географічного профілю досить докладно описав Р.М. Коксис [68]. Відповідний порядок дій правоохоронця можна подати в такий спосіб.

1. Необхідно уважно вивчити особливості та принципи географічного профілювання. Слід пам'ятати, що цей метод не застосовується до всіх видів серійних злочинів. Найкориснішим географічне профільування стає під час розслідування насильницьких злочинів проти особи (серійні/сексуальні вбивства, зґвалтування, підпали тощо), натомість вона мало підходить для розслідування корисливих злочинів, як ті ж квартирні крадіжки тощо.

Географічний профіль орієнтований на осіб, які мають постійне місце перебу-

вання. Якщо ж особа веде бродячий спосіб життя або постійно змінює місцезнаходження, цей спосіб ідентифікації є малопридатним. Ще однією особливістю цього методу є те, що для його ефективного застосування потрібно мати інформацію про місця вчинення кількох (принаймні двох, а краще не менше чотирьох) правопорушень, до яких ймовірно причетна одна особа.

2. Географічний профіль має базуватися на якомога більшій кількості точних перевірених даних. Має бути враховано як місце безпосереднього скоєння злочину, а й інші локації, наприклад, місця, де злочинець зустрів жертву, де приховав сліди скоєння злочину, де зняв готівку з викраденої кредитної картки чи реалізував викрадені речі тощо.

3. Позначення ключових точок на карті. Ці точки зазвичай відображаються різними кольорами і повинні містити відповідну хронологічну інформацію, а також закодовану інформацію про обставини події.

4. Визначення базового кола. Із цією метою незалежно від хронології подій на карті вибирають дві найвіддаленіші ключові точки, які були визначені раніше. Пряма – відстань між ними виступатиме діаметром відповідного кола. Зазначене коло можна розглядати як орієнтовну локацію, в межах якої діє злочинець. Саме на території в межах окресленого кола варто сконцентрувати основні зусилля щодо розслідування.

5. Застосування домоцентричного підходу. Для цього вибирають перші за часом чотири інциденти, позначені на карті, і аналогічно попередньому пункту вибудовують нове коло, яке зазвичай буде менше попереднього. Цей підхід базується на тому, що існує висока ймовірність (~66%) поведінки злочинця, яке характеризується скоєнням спочатку злочину подалі від місця проживання, з поступовим обранням найближчих до його розміщення місць для протиправної активності.

6. Для більш точного фокусування на території розслідування необхідно провести так звану кластеризацію (виділення груп за певними ознаками). Наприклад, визначити локацію, де є найбільша кількість злочинів, або з урахуванням хронології

подій визначити просторовий вектор їх розвитку. Це дозволяє ще більше звузити територію пошуку, створити передумови для раціональнішого розміщення сил і засобів. При цьому слід ураховувати, що спадаючий тренд злочинів на відстані може свідчити про готовність злочинця «мандрувати» для вчинення протиправних дій.

7. Під час побудови географічного профілю варто враховувати характер території пошуку. Слід розглянути питання про виключення за межі зони розслідування поверхонь водойм та інших ділянок місцевості, де місце перебування злочинця є малоймовірним.

8. Потрібно постійно коригувати профіль з урахуванням інформації, що надходить. Цей процес повинен враховувати динаміку розслідування.

9. У результаті відбувається інтерпретація одержаних результатів.

Результати, отримані внаслідок географічного профілювання, можуть бути використані як у проактивній, так і реактивній поліцейській діяльності. У першому випадку йдеться, наприклад, про посилення патрулювання конкретної місцевості, орієнтування громадськості на повідомлення про підозрілу активність у межах певної зони тощо. Якщо йдеться про реактивну діяльність, то під час розслідування можна зіставляти географічний профіль з місцями проживання підозрюваних, пріоритетно відбирати біологічні зразки у тих осіб, які живуть або працюють у межах окресленої зони тощо.

За даними Д. Узлова, та В. Струкова інструментарій системи кримінального аналізу ґрунтується на математичних моделях і методах інтелектуального семантичного аналізу, візуального темпорального аналізу, аналізу поведінкового профілю, аналізу прихованих закономірностей.

Візуальний темпоральний аналіз базується на відтворенні та візуалізуванні хронології подій, які відбулися і тимчасове розмежування, що дає змогу оперативно виявляти приховані просторово-тимчасові закономірності між різними подіями.

Аналіз поведінкового профілю. Найпостійнішим і найточнішим з погляду психології злочинця є його поведінковий профіль. Він відображає багато параметрів

діяльності злочинця – звичний спосіб вчинення злочину, місця скоєння та інші залежності, які сукупно відповідають одному профілю. Наявність різних поведінкових ознак з певною часткою ймовірності може свідчити про те, що цей суб'єкт може бути причетний до події. З цього принципу формується так званий груповий поведінковий аналіз. Безумовно, поведінковий профіль злочинця ніяк не може існувати без впливу на інших суб'єктів. Аналіз групового поведінкового профілю дає змогу визначати спільників без явних зв'язків між собою.

Аналіз прихованих закономірностей. Між особами, довільним чином причетними до правопорушення, об'єктивно існують зв'язки (родинні, за родом професійної діяльності, географічні – стосовно до місця проживання, місця відбування покарання тощо). Подібні зв'язки існують також між особами і подіями, а також між різними подіями. Такі зв'язки можуть бути явними, опосередкованими і прихованими. Крім того, група злочинів, скоєних однією і тією ж особою, обов'язково має певні характерні загальні риси, які явно не зафіксовані. Виявлення таких прихованих закономірностей з високою часткою вірогідності може встановити ідентифікаційні зв'язки між злочинцем і всіма скоєними ним злочинами.

У практиці кримінального аналізу розрізняють такі типи аналітичних продуктів:

1. Аналітичний звіт: сепарована інформація з внутрішніх і зовнішніх джерел; висновки; рекомендації, прогнози, настанови; додаткові матеріали (графіки, схеми, дані геолокації).

2. Профіль (досьє) особи, об'єкта організованої злочинної групи: максимальний обсяг інформації на об'єкт аналізу відповідно до запиту ініціатора.

3. Інформаційне зведення: оброблені табличні дані шляхом вибірки з баз даних за критеріями ініціатора.

4. Витяг інформації: вибірка інформації з баз даних за критеріями ініціатора.

За результатами проведеного аналізу змісту сиситеми поліцейської інформації

та розвідки, зокрема кримінальної розвідки та кримінального аналізу, доходимо висновку, що діяльність, яка проводиться у рамках обох інститутів поліцейської діяльності, є подібною. Ураховуючи це, уявляється корисним імплементація рішень в означених сферах, які показали позитивний ефект, до національних законодавств. Серед іншого варто розширити функції аналітичних підрозділів у рамках здійснення поліцейської діяльності в пострадянських країнах, а також розробити стратегію оперативного обслуговування.

Дослідники поліцейської діяльності виділяють п’ять моделей: традиційна поліцейська діяльність (Traditional policing), соціально орієнтована поліцейська діяльність (community policing or Community-oriented policing), проблемно орієнтована поліцейська діяльність (problem-oriented policing), комп’ютерна статистична поліцейська діяльність (Computer statistics model (CompStat)), поліцейська діяльність, керована аналітикою (intelligence-led policing (ILP)) [21, с. 17].

Поліцейська діяльність, керована розвідувальною аналітикою (ILP), – організаційна модель і філософія управління, згідно з якою кримінальна аналітика та розвідувальна робота є ключовими інструментами в досягненні мети шляхом імплементації об’єктивного й дієвого механізму прийняття рішень щодо протидії й запобігання злочинам із використанням стратегічного менеджменту та ефективних правоохоронних методик, спрямованих на нейтралізацію особливо небезпечних для суспільства злочинців [21, с. 36].

У країнах Європейського Союзу, США та інших розвинених країнах світу використання можливостей кримінального аналізу є обов’язковим для всіх правоохоронних органів. Його зміст, правила та процедури чітко визначено й урегульовано в нормативно-правових актах. Це, зокрема, стосується ведення оперативно-розшукової діяльності, досудового розслідування та розгляду кримінальних проваджень у суді. Консультативна місія Європейського Союзу в Україні (КМЄС) підтримує впровадження в Національній поліції України моделі поліцейської діяльності, керованої аналітикою (Intelligence-Led Policing/ILP) [40].

ILP є моделлю поліцейської діяльності, згідно з якою оперативно-аналітична інформація (intelligence) слугує підставою для проведення операцій/ розслідувань, а не навпаки. Ця модель дозволяє зменшити матеріальні витрати, знизити рівень злочинності, забезпечити більш високий рівень безпеки особового складу [60].

Зокрема, проблеми впровадження моделі поліцейської діяльності, керованої аналітикою (Intelligence-Led Policing/ILP) досліджено у праці Дж. Картера, С. Філіпса та М. Гайадина «Впровадження слідчого поліцейського: застосування теорії вільного поєднання» [60]. Окремі аспекти виявлення прихованих закономірностей щодо зв'язків між злочинцем і вчиненими ним злочинами відтворив К. Вестфал у роботі «Отримання даних для розвідки, шахрайства та кримінального виявлення. Розширені технології аналітичного та інформаційного обміну» [84].

ILP є моделлю поліцейської діяльності, згідно з якою оперативно-аналітична інформація/intelligence слугує підставою для проведення операцій/розслідувань, а не навпаки. Ця модель дає змогу зменшити матеріальні витрати, знизити рівень злочинності, забезпечити більш високий рівень безпеки особового складу [60].

Кримінальний аналіз – це дії, спрямовані на ідентифікацію і точне визначення взаємозв'язків між відомостями, які стосуються подій злочинного характеру, осіб, пов'язаних із ними, та даними, що походять із різних джерел, і їх використання правоохоронними органами і судами.

До головних завдань кримінального аналізу слід віднести:

1) якісне планування окремої слідчої (розшукової) дії, допомога у прийнятті управлінського рішення (ILP);

2) аналітичне супроводження ОРД і досудового розслідування;

3) аналіз стану та ефективності досудового розслідування, оперативно-розшукової та превентивної діяльності (тактичний аналіз);

4) оброблення великого обсягу інформації (bigDATA) з метою досягнення можливості відстеження та пов'язування фактів (застосування спеціальних аналітичних методів);

5) аналіз складної і розгалуженої структури зв'язків між об'єктами оперативно-розшукової справи або матеріалами кримінального провадження;

6) виявлення ризиків, тенденцій майбутнього розвитку злочинності та її запобігання з урахуванням аналітичних рекомендацій;

7) вирішення масштабних, довгострокових проблем і постановка цілей, для виявлення тенденцій у злочинному світі;

8) напрацювання нових напрямів у досудовому розслідуванні, а також отримання повноцінного аналітичного продукту щодо об'єктів кримінального аналізу;

9) прогнозування розвитку видів злочинної діяльності і встановлення пріоритетів діяльності Національної полівції України та інших суб'єктів правоохоронної діяльності;

10) аналіз інформації, з метою виявлення тенденцій, закономірностей, а також прогнозування розвитку ситуації на тривалий період часу (стратегічний аналіз).

Систему кримінального аналізу в правоохоронних органах можна розділити на два основні напрями:

– аналіз злочинності, її причин і умов, особистості тих, хто скоює злочини, а також методів контролю за злочинністю та протидії їй;

– аналіз злочинів, механізм їх відображення в джерелах інформації, діяльність із розкриття, розслідування та попередження всіх видів злочинів і розроблення на цій основі найбільш ефективних методів і засобів розкриття злочинів.

Слід зазначити, що Міжнародна асоціація працівників кримінального аналізу розмежовує аналіз злочинів і кримінальний аналіз. «Якщо ми аналізуємо злочинця, це звужує коло діяльності», – підкреслює старший радник з питань загальної правоохоронної діяльності представництва КМЄС в Україні Георгіос Покас.

Під час кримінального аналізу забезпечується цілеспрямований пошук, виявлення, фіксація, вилучення, упорядкування, аналіз та оцінка кримінальної інформації, її представлення (візуалізація), передача та реалізація. Зокрема, в аналітичній роботі використовується:

- оперативний аналіз (аналіз даних телефонних дзвінків, аналіз злочинних угруповань, аналіз справ, порівняльний аналіз);

- тактичний аналіз (кримінальний аналіз, аналіз кримінальних тенденцій, геопросторовий аналіз, аналіз місць концентрації злочинності, часовий аналіз, МО-аналіз, кримінальні моделі, профілі підозрюваних/жертв);

- стратегічний аналіз (SWOT-аналіз, PEST-аналіз, аналіз моделей/форм злочинності та профілювання, аналіз тенденцій, аналіз із використанням географічного профілювання).

За джерелами даних аналіз розподіляється на:

– аналіз даних із відкритих джерел (OSINT);

– аналіз даних із агентурних джерел (HUMINT);

– аналіз даних радіотехнічної розвідки (SIGINT);

– аналіз даних із багатьох джерел (*Multi-Source Analysis*) тощо.

Система кримінального аналізу в правоохоронних органах вирізняє кілька рівнів, для кожного з яких характерна мета, відповідні види і обсяги вихідної інформації, що підлягають збору, вивченню та оцінці, зокрема: 1) національний (загальнодержавний); 2) регіональний (районний); 3) місцевий.

Кримінальний аналіз на національному рівні передбачає спостереження і прогнозування на тривалі терміни еволюції кримінальної ситуації на державному рівні (географічні зони, види і типи дій) і розроблення на цій основі перспективних заходів щодо їх можливої нейтралізації, зміцнення правопорядку та вдосконалення діяльності правоохоронних органів на тривалий термін. Період, що аналізується на національному рівні, становить не менше одного року, а рекомендації аналітиків розраховані на строк до 3–5 років. Кримінальний аналіз на регіональному рівні є комплексним аналізом оперативної обстановки за короткі, середні і тривалі строки (квартал, півріччя, дев’ять місяців, рік) у певних географічних районах.

Метою аналізу інформації на оперативному рівні є виявлення змін у стані правопорядку і спрямування діяльності керівництва за всіма рівнями ухвалення рішень

(місцевий, регіональний і національний) щодо ефективного розподілу організаційних ресурсів, розстановки сил і засобів, розробки комплексних заходів і прийняття рішення щодо посилення боротьби з найбільш поширеними і небезпечними правопорушеннями.

Зазвичай час для аналізу на регіональному рівні визначається на основі оцінки добової, декадної і місячної інформації, не перевищуючи одного року. На місцевому рівні кримінальний аналіз здійснюється відразу після отримання даних/інформації про настання події або про ті події, які можуть відбутися найближчим часом, і у складних кримінальних провадженнях.

Роль такого аналізу полягає в направленні і підтриманні інформаційних знань із метою виявлення кримінальних об'єктів (осіб, груп, організацій), відносин між ними, злочинних діянь, тактики дій, а також їх становища. Результати аналізу на тактичному рівні (залежно від їх масштабу і можливості реалізації) використовуються в прийнятті оперативних рішень, розстановці сил і засобів, за проведення різних комплексних, типових і разових операцій. В. Мельник і В. Некрасов уважають, що для сфери кримінального аналізу економічної злочинності більш притаманним є аналіз джерел інформації, що містяться у великих масивах даних, зокрема:

– у зазначених масивах здійснюється пошук певних незначних відхилень у господарському процесі, а також закономірностей, притаманних злочинним схемам і технологіям;

– інформація, що характеризує процеси в легальному секторі економіки, розпорошена різними масивами інформації, сформована на різних платформах та має різну інституційну належність;

– фінансові та господарські операції, що відображені в облікових і звітних документах, містять сліди інтелектуальних підробок. Саме тому необхідно проводити дослідження відповідності відомостей, що містяться у звітних документах із фактичною діяльністю;

– правоохоронні органи сьогодні не володіють методологією кримінального

аналізу та аналізу ризиків щодо підозрілих фінансових і господарських операцій [29].

Слід зазначити, що, надаючи аналітикам змогу опрацьовувати дані про злочини, оперативні працівники та слідчі отримують можливість використовувати готовий оперативно-аналітичний продукт, а не первинну інформацію. У цьому вони отримують такі переваги:

по-перше, окреслюються конкретно тенденції злочинності не лише за географічною ознакою, а й у часових рамках;

по-друге, продукт надає можливість мати більше інформації щодо місць ймовірного вчинення злочинів. Це допомагає покращити попередження правопорушень;

по-третє, працівники поліції мають більше можливостей у разі потреби надати допомогу колегам у розкритті та розслідуванні злочинів.

Водночас підхід до поліцейської діяльності, керованої аналітикою, наражається на низку проблем на різних рівнях аналізу, зокрема:

– для оперативного аналізу дані часто недоступні ззовні підрозділу або робочої групи і прив’язані до оперативного працівника;

– для тактичного аналізу наявні інструменти дають широкі можливості для візуалізації, але інколи відчувається слабкість математичного апарату;

– для стратегічного аналізу дані часто відсутні через те, що їх ніхто не узагальнює для аналізу або аналіз проводиться лише з точки зору покращення звітності правоохоронного органу, при тому, що, скажімо, PEST-аналіз і SWOT-аналіз можна застосовувати для передбачення очікуваних змін у діяльності злочинних угруповань [70].

З урахуванням проведеного аналізу можна констатувати, що під час проведення кримінальної розвідки на етапі аналізу використовується ціла низка методів, що поєднують у собі різні наукові знання. Це робить роботу аналітика однією з найбільш кваліфікованих і, як наслідок, потребує суттєвої підготовки. Не дивно, що у

багатьох провідних державах світу штат аналітиків правоохоронних органів значно перевищує кількість польових співробітників.

В українських правоохоронних органах, зокрема в поліції, кількість аналітиків поки що невелика, проте розвиток цього напряму перебуває під постійним контролем керівництва Національної поліції. Підготовку відповідних фахівців можуть здійснювати закладти вищої освіти Міністерства внутрішніх справ, у яких є досвід викладу відповідних курсів, а також існує напрям технічних та психологічних досліджень для виконання завдань правоохоронної діяльності [30].

РОЗДІЛ 2.
ОСОБЛИВОСТІ ВИКОРИСТАННЯ СИСТЕМИ ПОЛІЦЕЙСЬКОЇ ІНФОРМАЦІЇ ТА РОЗВІДКИ В ДІЯЛЬНОСТІ ПОЛІЦІЇ ЗАРУБІЖНИХ КРАЇН

2.1. Застосування інформаційних технологій у діяльності поліції зарубіжних країн

У цьому підрозділі буде проведено аналіз зарубіжного досвіду застосування інформаційних технологій у діяльності правоохоронних органів.

Науковці вважають цілком справедливою думку про те, що міжнародне поліцейське співробітництво слід розглядати сьогодні як один із компонентів взаємодії держав у сфері боротьби зі злочинністю, що саме по собі є важливою частиною міжнародних відносин [18]. Це викликає необхідність інтеграції вітчизняних інформаційно-аналітичних систем у міжнародні, що зумовлює необхідність удосконалення цих систем відповідно до технологічного рівня вимог розвинутих країн і насамперед країн Європейського Союзу.

Незважаючи на численні роботи, присвячені вивченню проблем інформаційного забезпечення діяльності правоохоронних органів, проблематика вивчення міжнародного та зарубіжного досвіду застосування інформаційних технологій у діяльності правоохоронних органів залишається ще недостатньо вивченою.

За сучасних динамічних умов міжнародного життя ефективність заходів, спрямованих на протидію транснаціональної злочинності, безпосередньо залежить від здатності Міжнародної організації кримінальної поліції розвивати свою інституційну систему, пристосовувати її до потреб міжнародного поліцейського співробітництва [45].

Тому насамперед розглянемо обліки Інтерполу – *International Criminal Police Organization*. Вони охоплюють, як правило, злочини, що становлять суспільну небезпеку, такі як тероризм, незаконний обіг наркотиків, розкрадання культурних цінностей та інші. На облік ставиться інформація, що зачіпає інтереси двох і більше країн: про осіб, які вчинили небезпечні злочини за кордоном; про посягання, пов'язані з міжнародними злочинними організаціями; про осіб, які зникли за кордоном після скоєння злочину тощо.

Інформаційна база даних «ASF» (Автоматична пошукова система), яка перебуває в Генеральному Секретаріаті Інтерполу, складається з таких підсистем:

– розшук злочинців за їхніми зображеннями, зв'язками тощо;

– викрадені документи – щодо викрадених або втрачених паспортів, дорожніх документів, інформації про бланки викрадених або підроблених документів;

– викрадений автотранспорт – щодо інформації про викрадені автомобілі та їхні номерні запчастини;

– викрадені твори мистецтва – щодо предметів, що мають історичну чи культурну цінність з докладним описом та фотографіями;

– дактилоскопічна база відбитків пальців злочинців та осіб, що розшукуються;

– розшук терористів (інформація надається лише працівникам Національного центрального бюро Інтерполу, які мають персональний ідентифікаційний номер);

– інформація про сексуальне насильство над дітьми;

– профілі ДНК злочинців, обвинувачених, розшукуваних та потерпілих [37].

4 грудня 2009 року у Києві підписано Угоду між Україною та Європейським поліцейським офісом про стратегічну співпрацю, яка була ратифікована 5 жовтня 2010 року. Метою цієї угоди є посилення співпраці держав-членів Європейського Союзу, що діють через Європол, з Україною у запобіганні міжнародній злочинності, їх виявленні, припиненні та розслідуванні таких злочинів у рамках мандату Європолу, зокрема, шляхом обміну стратегічною та технічною інформацією. Так, стратегічна інформація включає заходи правоохоронного характеру, які можуть

бути корисними для запобігання злочинам; нові засоби скоєння злочинів; спостереження та дані, отримані в результаті успішного застосування нових правоохоронних методів та засобів; маршрути, які використовуються контрабандистами або особами, причетними до злочинів, пов'язаних із торгівлею людьми та змінами цих маршрутів тощо. Однак ця угода не дає повноважень на передачу даних, що належать до встановлення осіб, які вчинили злочин [52].

Як визначено положеннями Лісабонського договору, завдання Європолу полягає в тому, щоб підтримувати та зміцнювати діяльність поліції та інших правоохоронних органів держав-членів, їх взаємну співпрацю щодо запобігання злочинності, що впливають на дві або більше держави-члени, тероризм та види злочинів, що впливають на інтереси, охоплені політикою Європейського Союзу [20].

До завдань Європолу, зокрема, входить збирання, зберігання, оброблення та аналіз інформації, у тому числі тієї, яку надають органи держав-членів або треті держави або органи, та обмін такою інформацією [64].

Державами, що входять до Європейського Союзу, у рамках Європолу організовано єдину автоматизовану систему обліку кримінальних відомостей, що діє з 2002 року. До складових комплексної інформаційно-аналітичної системи TECS (*The Europol Computer System*), крім власне AIC, також належать аналітичний центр та індексна підсистема. Комп'ютерна система TECS дозволяє одночасно обробити та проаналізувати майже мільйон записів. Вся інформація до системи надається безпосередньо державами-членами ЄС. Кожна країна має власну організацію-представника в Гаазі, так звану ELOS. Тільки ці організації мають доступ до національних баз даних. Формування AIC TECS здійснюється централізовано під контролем керівництва Європолу.

Банки даних AIC TECS призначені для зберігання інформації окремо за злочинами та особами. Занесенню до обліку Європолу підлягають такі категорії: підозрювані, засуджені, свідки, потерпілі та потенційні жертви тощо. Відомості в систему надходять із національних відділів зв'язків з Європолом, а також заносяться

самим Європолом на основі даних зі своїх джерел, у тому числі отримані від третіх країн.

Зазначена система складається з трьох елементів:

1) власне інформаційної системи, куди заносяться відомості щодо осіб, засуджених чи підозрюваних у скоєнні злочинів, що перебувають у компетенції Європолу;

2) інформаційної системи щодо осіб, щодо яких є «вагомі підстави» припускати, що вони планують вчинити такі злочини у майбутньому;

3) аналітичної системи, куди заносяться звані робочі досьє з метою аналізу. Робочі досьє є інструментом для оброблення та систематизації даних, які необхідні для розкриття конкретних злочинів, що перебувають у компетенції Європолу [64].

У зв'язку з тим, що ці досьє включають дані про приватне життя громадян, установлено досить жорсткі правила для їх створення та використання. Держави ЄС вживають необхідних заходів для обробки персональних даних для забезпечення стандарту захисту даних відповідно до Конвенції Ради Європи про захист осіб у зв'язку з автоматизованим обробленням персональних даних 1981 року [19].

Бази даних аналітичного центру містять відомості про особисті дані; фізичного опису, у тому числі шрамів, татуювань тощо; про засоби ідентифікації, а саме: документів, відбитків пальців, ДНК тощо; заняттях та навичках (освіті, кваліфікації, знанні іноземних мов тощо); економічної та фінансової інформації, до якої відносяться дані про банківські рахунки, власність та активи тощо; характеристики особистості динаміці, тобто спосіб життя, поведінка, місця частого відвідування, наявність зброї, зловживання наркотиками тощо; дані про засоби комунікації, а саме: телефон, факс, Інтернет-зв'язок тощо; про засоби пересування; посилання на інші бази даних, де є інформація про особу (поліція, митні органи, міжнародні організації тощо).

До зазначених баз даних включається інформація як щодо підозрюваних, засу-

джених, так і щодо осіб, які виявилися залученими до злочинів, а саме: свідки, потерпілі та інші [62].

Інформація баз даних аналітичного центру застосовується при розкритті конкретних злочинів, що належать до компетенції Європолу. З огляду на особливу важливість інформації, що надходить до аналітичного центру, забезпечено достатньо надійний захист баз даних від несанкціонованого доступу через зовнішні комп'ютерні мережі. Так, щоб унеможливити доступ операторів, які не мають спеціального дозволу, до робочих файлів аналітичних груп, існує правило, згідно з яким для поширення інформації з файлів аналітичного центру потрібне узгодження з усіма керівниками дослідницьких програм. Прямого зв'язку в режимі online між цим центром та національними АІС у поліцейських відомствах країн-членів Європолу на користь інформаційної безпеки також не передбачено [4].

Індексна підсистема є елементом, що доповнює систему робочих карток аналітичного центру, і є тематичний рубрикатор. Так, за допомогою зазначеної підсистеми офіцери зв'язку мають можливість здійснювати швидкий пошук інформації про злочини, що стосуються їхніх держав-членів [11].

Якщо розглядати інформаційні системи країн Європейського Союзу в цілому, то можна бачити, що вони утворені на загальнонаціональному рівні та забезпечують стратегічний аналіз даних щодо функціонування злочинних угруповань.

На центральному рівні ведуться узагальнені обліки осіб, які вчинили злочини та їх дій, готуються пропозиції щодо вдосконалення нормативного регулювання роботи кримінальної поліції, підтримуються контакти з Інтерполом. І це цілком обґрунтовано, оскільки дозволяє краще спрямовувати та координувати зусилля, враховуючи розширення міжрегіональних та міжнародних контактів, а також міграцію організованих злочинців, забезпечує більший рівень конспірації за значного впливу криміналітету на політичні, економічні, а нерідко й правоохоронні структури на місцях, особливо в невеликих містах [18].

Зупинимося на інформаційному забезпеченні деяких країн – членів Європейського Союзу. У розробленні та впровадженні корпоративної об'єднаної інформаційної моделі даних для потреб поліції, на нашу думку, на особливу увагу заслуговує досвід Сполученого Королівства Великої Британії. Як слушно зауважив В.О. Заросило, реалізація цих відносин під час попередження правопорушень та їхнього швидкого розкриття у Великій Британії забезпечується запровадженням новітніх комп'ютерних відеоспостережень, створених завдяки фінансуванню міських адміністрацій та приватних підприємств [17]. Так з 2013 року до *National Crime Agency* (NCA) (Національне кримінальне агентство) передано інформаційну систему *The National Policing Improvement Agency* (NPIA). Доступ до неї мають усі територіальні поліцейські сили Великобританії, поліція Північної Ірландії (PSNI), Британська транспортна поліція (BTP), поліцейська служба Шотландії, Національна служба ідентифікації (NIS), Національна агенція зі злочинності (NCA), Служба безпеки (MI-5) та Секретна розвідувальна служба (MI-6), Асоціація начальників поліції (ACPO) та інші.

Зазначена інформаційна система складається з декількох баз даних:

– «Імена», яка містить великий обсяг інформації щодо осіб, засуджених, попереджених або нещодавно заарештованих. Включає дані відбитків пальців та ДНК; фізичні описи; відомості про попередні арешти та вироки, винесені за кожне правопорушення; всіх попередніх адрес та інше;

– «Автомобіль», яка містить докладну інформацію про зареєстровані автомашини, у тому числі номери шасі, двигуна тощо, дані про статус транспортного засобу (викрадено, страховий стан тощо), їх власників тощо;

– «Нерухомість», яка містить відомості про сільськогосподарську та будівельну техніку, зареєстровані тварини, морські судна та інше;

– «Водій», яка містить інформацію про близько 50 000 000 осіб, які або мають посвідчення водія або дискваліфіковані. Відомості містять інформацію про проходження тесту, підтвердження та ліцензії. Ця база даних оновлюється щоранку [37].

Національна база даних ДНК кримінальної розвідки Великої Британії *National Criminal Intelligence DNA Database* (NDNAD) створена у 1995 році. У березні 2012 року база даних містила відомості близько 6000 000 осіб. Щомісяця вона зростає на 30 000 зразків, що надходять з місць скоєння злочинів, взяті поліцейськими у підозрюваних, арештованих та осіб, які утримувалися під вартою у поліцейській дільниці. Вона знаходиться у віданні Міністерства внутрішніх справ Великої Британії. Дані, що містяться в NDNAD, належать поліцейському органу, який надав зразок для аналізу. Зразки постійно зберігаються компаніями, які аналізують їх за щорічну плату.

NDNAD Великої Британії у своєму роді є головною і найбільшою у світі базою даних судових ДНК та містить дані щодо приблизно 10% населення, порівняно з 0,5% у США. Дані, що містяться в Національній базі даних ДНК, складаються з даних приватних осіб, відібраних на підставі Закону про поліцію та докази у кримінальних справах, та вилучених у нерозкритих злочинах у вигляді плям (наприклад, від крові, сперми, слини, волосся тощо), тих, хто залишився на місці злочину). Щоразу, коли надходить новий профіль, відбувається автоматичний пошук на збіг серед записів NDNAD між даними фізичних осіб та даними нерозкритих злочинів.

Серед інформаційно-аналітичних систем правоохоронних органів Франції насамперед хотілося б зупинитись на програмному комплексі ANACRIM, який використовується багатьма спецслужбами як цієї країни, так і інших країн Європейського Союзу. Національна жандармерія ANACRIM використовується для аналізу стану злочинності. До бази даних внесено дані щодо осіб, місць, подій та інші пов'язані з ними відомості, наприклад, телефонні номери, автомобілі тощо.

Зазначене програмне забезпечення дозволяє встановити зв'язок між усіма записами базі даних, а висновок надається у вигляді графічної презентації. Це дозволяє аналітикам сформулювати відповідні гіпотези або скласти запит, щоб заповнити прогалини або перевірити деякі інтелектуальні припущення. Так, аналіз, проведе-

ний за допомогою ANACRIM, дозволяє допомогти встановити місця, які часто відвідує особа, що перевіряється, її репутацію або ставлення до алкоголю і так далі.

Законодавство Франції дозволяє вносити різноманітну інформацію до бази даних зазначеної інформаційно-аналітичної системи навіть без доказів, на розсуд слідчого. Дані щодо суддів, адвокатів, експертів, свідків та потерпілих, які беруть участь у розслідуванні, також можуть бути збережені. Водночас слід зазначити, що для внесення даних до ANACRIM повинно мати місце не лише скоєння чи підозра у скоєнні особливо тяжкого злочину, а й вагомі та послідовні докази щодо особи.

До автоматизованих інформаційно-пошукових систем, що використовуються у правоохоронній діяльності, також належать JUDEX – це система для реєстрації кримінальних правопорушників та потерпілих, що містить близько 3 млн записів; *Fichier National Automatisé des Empreintes Génétiques* (FNAEG) – автоматизований національний банк даних генетичних відбитків ДНК, створений у 1998 році, який спочатку використовувався для реєстрації сексуальних злочинців, але надалі став містити дані про інші злочини, у тому числі й про осіб, які беруть участь у протестних рухах громадянської непокори З 2807 профілів у 2003 році FNAEG зросла до 330 000 у 2006 році, і 127 0000 у 2009 році.

Автоматизована база даних сексуальних злочинців, що перебуває у віданні Міністерства юстиції, була створена в 2004 році. До неї вносяться ім'я, стать, дата та місце народження, національність, псевдонім, адреса, характер правопорушення, дата та місце скоєння правопорушення, характер та дата рішення та санкції або вжиті заходи. Станом на жовтень 2008 року база даних містила записи щодо 43 408 осіб [50].

L'application de gestion des dossiers des ressortissants étrangers en France (AGDREF AGEDREF) – база даних іноземців у Франції, заснована в березні 1993 року, знаходиться у віданні Міністерства внутрішніх справ і об'єднує відомчі бази даних, що знаходяться у віданні префектур громадян Міністерства внутрішніх справ України.

Автоматична інформаційно-пошукова система «Кассіопея» містить інформацію про скарги, зареєстровані суддею в ході судового розгляду, про обвинувачених, свідків, потерпілих та цивільних позивачів тощо.

Автоматизована система ідентифікації відбитків пальців осіб, які вчинили злочини або правопорушення – *Système d'identification automatique par empreintes digitales* (AFIS), створена 1987 року, знаходиться під управлінням Головного управління судової поліції Міністерства внутрішніх справ та під контролем Генерального прокурора та Апеляційного суду Парижа.

Державний автоматизований банк даних судимостей перебуває у віданні міністра юстиції (Департамент у кримінальних справах та помилування). У березні 2011 року французький парламент ухвалив закон, спрямований на забезпечення внутрішньої безпеки «Loppsi II», який став основою модернізації нормативно-правових актів, що стосуються інформаційно-телекомунікаційного забезпечення. Так, запроваджено кримінальну відповідальність за крадіжку особистих даних під час розслідування злочинів, пов'язаних із дитячою порнографією, поліції надано право підключення до Інтернету та телефонних ліній, а також звернення до провайдерів для фільтрації Інтернет-з'єднання тощо. Також ухваленим законодавчим актом дозволено створення інформаційної платформи, що поєднує численні державні бази даних.

У Федеративній Республіці Німеччина функція центрального органу щодо забезпечення інформацією та встановлення контактів між усіма поліцейськими органами та службами країни у сфері боротьби зі злочинністю покладена на Федеральну кримінальну поліцію – *Bundeskriminalamt* (BKA), яка фактично є центром збору та електронної обробки необхідних поліції даних (кримінальні обліку , матеріали дактилоскопічної реєстрації).

Як у розглянутих вище країнах, правоохоронні органи Федеративної Республіки Німеччина активно використовують телекомунікаційні засоби та вводять інно-

ваційні комп'ютерні технології для ефективного та якісного інформаційного забезпечення своєї службової діяльності. Так, наприклад, інформаційно-пошукова система Федеральної кримінальної поліції – *Informationssystem der Polizei* (INPOL) – включає базу даних усіх осіб, оголошених у розшук, відомості про викрадені автомобілі, документи тощо. Дані щодо осіб, розшукуваних німецькою поліцією чи судовими органами, вже за кілька секунд після внесення до бази стають доступні всім користувачів зазначеної системи, а це все відділення поліції та митні органів ФРН.

У базі даних *Inpol-Personenfahndungsdatei* станом на 1 лютого 2014 року було зареєстровано близько 382 597 запитів на арешт та 181 794 на встановлення місцезнаходження осіб; в базі даних *Sachfahndungsdatei* перебували станом на цю ж дату відомості щодо близько 10 600 000 об'єктів, що перебувають у розшуку, у тому числі 138 568 автомобілів, 739 426 велосипедів, 5 597 512 документів, що посвідчують 3 особи.

Як і Велика Британія та Франція, Федеративна Республіка Німеччина має потужну централізовану базу даних зразків ДНК – *Die DNA-Analysedatei*, яка функціонує з квітня 1998 року та перебуває під управлінням Федеральної кримінальної поліції. Джерелом даних служать генетичні зразки конкретних осіб, звані персональні записи, і зразки невстановлених осіб, вилучені з місць скоєння злочину. У всіх затриманих або заарештованих осіб вилучається один генетичний зразок: або шляхом використання ватного тампона, або аналізу крові, якщо людина відмовляється проникати в її порожнину. Отриманий зразок заноситься до бази даних ДНК і автоматично звіряється із зразками невстановлених осіб, вилучених під час огляду місця злочину.

За даними Федеральної кримінальної поліції протягом п'яти років з 2008 по 2013 кількість даних у базі даних ДНК зросла з 756 990 до 1 048 771. Щомісяця додається близько 7 000 нових записів, з яких понад 1400 – це генетичні зразки осіб, які затримувалися підозрою у скоєнні правопорушення. В даний час ДНК-докази

вважаються в Німеччині найуспішнішим кримінальним інструментом для встановлення злочинця.

У Центральному регістрі іноземців – *Das Ausländerzentralregister* (AZR) – зберігається близько 20 000 000 персональних записів. Серед них дані 4470 тисяч громадян Європейського Союзу (станом на лютий 2009 року). Тут знаходяться особисті дані, а також інформація про статус особи (депортація, відмова, обмеження тощо). Реєстрація ведеться у Федеральному відомстві з питань міграції та біженців. AZR є одним із найповніших автоматизованих реєстрів державного управління в Німеччині. Доступ до цієї бази даних мають 6500 органів-партнерів, у тому числі всі імміграційні установи, поліція, митні органи. При цьому поліцейські та митні органи мають доступ через вищеописану інформаційно-пошукову систему Inpol.

Велике зацікавлення також викликає база даних OneDOJ, яка знаходиться на озброєнні всіх ланок правоохоронної системи Сполучених Штатів Америки, вітчизняних аналогів якої не існує. Електронний доступ до всіх кримінальних справ країни викликає великий інтерес для розслідування будь-яких серійних злочинів, встановлення спільників або місця знаходження особи, оголошеної в розшук тощо.

Безумовно, вимагають вивчення та поступового впровадження програмних комплексів, що дозволяють перевести паперове діловодство у всіх сферах правоохоронної діяльності у цифровий режим відповідно до сучасних вимог. Тим більше, що без їх застосування не може йтися про створення та впровадження баз даних, аналогічних OneDOJ.

Проведеним аналізом установлено, що інформаційне забезпечення правоохоронних органів розвинених країн умовно можна поділити кілька груп. Водночас слід зазначити, що деякі з них не мають аналогів у нашій країні.

По-перше, це інформаційно-пошукові бази даних, що містять відомості щодо осіб або майна, пов'язаних з тим чи іншим злочином, а саме: підозрювані та засуджені, особи, оголошені у розшук, особи, схильні до сексуальних чи насильницьких злочинів, які зникли без вести, а також викрадене майно, транспорт, документи

тощо.

До другої групи належать бази даних відбитків пальців, ДНК та інших біометричних властивостей; будь-яких оболонок боєприпасів тощо, призначені для проведення автоматичного порівняльного аналізу.

До третьої групи належать інформаційно-аналітичні програмні комплекси, такі як TECS або ANACRIM, що дозволяють встановлювати зв'язки між будь-якою інформацією щодо особи, яка підлягає перевірці з метою побудови версій, прогнозів щодо поведінки та інше. Правоохоронні органи України нині, незважаючи на численні спроби розробити подібні комплекси, на жаль, подібні програми відсутні взагалі.

До четвертої групи доцільно віднести системи відстеження дорожнього руху чи телекомунікаційних зв'язків.

Зрештою, п'яту групу складають статистичні програмні комплекси. Зважаючи на те, що такий програмний комплекс, як CompStat має вітчизняні аналоги (наприклад, автоматизована система Міністерства внутрішніх справ України «Статистика 2012»), було б доцільним використати досвід департаменту поліції Нью-Йорку для вдосконалення вітчизняної статистичної системи правоохоронних органів для загального застосування. Таким чином, сьогодні, враховуючи необхідність створення умов для інтеграції вітчизняних програмних комплексів у такі системи Європейського Союзу, як SIS та TECS, є доцільним налагодити співпрацю з правоохоронними відомствами Європейського Союзу та США з метою удосконалення існуючих вітчизняних аналогів та розробки нових, що відповідають світовим стандартам. Крім того, необхідно створити умови для підвищення матеріально-технічної складової інформаційного забезпечення всіх ланок правоохоронної системи України та їх ефективного використання з метою створення програмних комплексів із використанням інноваційних технологій.

2.2. Кримінальна розвідка та кримінальний аналіз у системі поліцейської інформації та розвідки

Завдання цього підрозділу полягає в тому, щоб, проаналізувавши зміст терміна «кримінальна розвідка» та «кримінальни аналіз», розглянути поширені стратегії, в яких викладено процес створення системи поліцейської інформації та розвідки, її етапи, окремі застосовувані методи та форми подання результатів цього виду поліцейської діяльності.

Сучасні тенденції правоохоронної діяльності у 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.

Указані 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» є одною з таких дефініцій, які потребують наукового осмислення та порівняння.

На теперішній час в усьому світі набуває популярності провадження правоохоронними органами кримінальної (поліцейської) розвідки (criminal intelligence process) з метою запобігання та прогнозування злочинності. Завдяки такій діяльності нагромаджується 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 [15].

На сайті Вікіпедії можна віднайти базове визначення оперативної 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 [63]. Як можна побачити з даного визначення, за своєю суттю воно є дуже подібним до застосовуваного на теренах пострадянських країн терміну «оперативно-розшукова інформація».

Сенс системи поліцейської інформації та розвідки полягає в нагромадженні розвідувальної інформації (criminal intelligence), яка відповідним чином аналізується. У результаті формуються висновки, які містять пропозиції щодо подальшого руху кримінального розслідування. Поліцейську інформацію прийнято поділяти на два види:

- стратегічну (стосується довготермінових цілей правоохоронних органів. Вона зазвичай відображає поточні та перспективні тенденції у злочинному середовищі, загрози громадській безпеці та порядку тощо);

- оперативну (забезпечує групу, яка бере участь у розслідуванні, версіями та висновками стосовно будь-яких протизаконних дій. Вона включає в себе припущення та висновки щодо організованих злочинних угруповань, груп або окремих осіб, втягнених у злочинну діяльність, їх методів, можливостей, вразливих місць тощо, які можуть бути використані в діяльності правоохоронних органів) [63].

Загальновідомими стратегіями кримінальної розвідки є:

- «Національна розвідувальна модель» (National Intelligence Model), застосовувана у Великої Британії [67];

- «Національний план розподілу розвідувальної інформації» (National Criminal

Intelligence Sharing Plan), розроблений у США [81].

З указаними стратегіями тісно пов'язана інша дефініція – «організація діяльності поліції на основі розвідувальних даних» або «модель поліцейської діяльності» (Intelligence-Led Policing (ILP)) [26, с. 101]. Останній термін, як зазначають Дж. Картер, С. Філіпс та М. Гайадин, співвідноситься із описаними стратегіями таким чином, що стратегії визначають структуру, у рамках якої ILP може бути застосована в правоохоронних органах [60, с. 435].

Поліцейська розвідка містить декілька основних етапів, які об'єднано в циклічне коло. У різних стратегіях ці етапи незначно різняться між собою, проте сенс залишається приблизно однаковим:

- збирання даних;
- оцінка даних;
- обробка даних;
- аналіз даних;
- поширення інформації;
- повторна оцінка інформації [44, с. 2].

На кожному етапі використовуються різні методології аналітичної роботи. Однією з таких методологій є розроблена на початку 1970-х років ANACAPA, яка застосовується з-поміж іншого у ФБР та Скотланд-Ярді.

Розглянемо зазначені етапи та методологію більш докладно. Так, збирання даних передбачає їх одержання з різних джерел: відкритих, службових, секретних. При цьому говорять про різні види розвідок: з відкритих джерел (OSINT), агентурну (HUMINT), радіотехнічну (SIGINT) тощо.

Після того, як дані було належним чином зібрано, відбувається їх оцінка, покликана визначити надійність набутої інформації. Найбільш часто застосовуваними системами оцінки є: 4x4, 5x5, 6x6. Система 4x4, наприклад, використовується Європолом.

В інших правоохоронних органах західних країн використовуються подібні системи. Наприклад, у Великій Британії значного поширення набула система оцінки 5x5. За потреби інформація може бути з легкістю конвертована з однієї системи в іншу. Загальний процес оцінки можна представити дослідженням ступенів надійності джерела та актуальності інформації. Наприклад, у системі оцінки 4x4 використовуються чотири ступені оцінки джерела інформації та чотири ступені оцінки самої інформації, у системах 5x5 та 6x6 таких критеріїв відповідно п’ять та шість. В окремих випадках у бланки оцінки потрібно вносити інформацію про ступінь поширення відповідної інформації, так звані «коди обробки».

Слід зауважити, що чим простішою є система оцінки, тим меншою є її суб’єктивність. На етапі обробки даних відбувається їх структуризація (приведення до певного формату) та інтеграція (об’єднання інформації з різних джерел). Інтегровані дані мають бути належним чином проаналізовані та інтерпретовані. Для цього серед іншого будують діаграми, які допомагають наочно побачити картину в цілому. При цьому слід пам’ятати, що діаграми не є кінцевим продуктом аналізу, а є лише додатком до висновків.

Існує достатньо багато видів таких діаграм, серед яких найбільш популярними є дерево зв’язків (link charting) та дерево подій (event charting). Перед тим як побудувати означені діаграми, потрібно визначити їх фокус (об’єкт, який цікавить правоохоронні органи) та скласти матрицю асоціацій (для визначення зв’язків між об’єктами). Назви об’єктів (фізичних осіб) у матриці розташовуються в алфавітному порядку зверху до низу. Після фізичних осіб у такому ж порядку розташовуються назви інших об’єктів, наприклад, юридичних осіб. Після створення матриці асоціацій відбувається її заповнення відповідними кодами зв’язку. Після заповнення матриці підраховується кількість відповідних зв’язків. Для кожного об’єкта враховується сума зв’язків по вертикалі та по горизонталі

З використанням заповненої матриці асоціацій здійснюється побудова попередньої діаграми. При цьому фізичні особи відображаються у вигляді кіл, юридичні –

прямокутниками, підтверджені зв’язки – суцільною лінією, можливі – пунктиром. Членство у юридичній особі позначається розміщенням відповідного кола в середині прямокутника. Підтверджені або можливі права володіння відповідно позначаються суцільною та пунктирною лініями.

Якщо в попередній діаграмі присутні лінії, що перетинаються, або недостатньо проглядається фокус діаграми тощо, то вона переробляється з урахуванням виявлених недоліків аби бути більш доступною для сприйняття. Розміщення блоків при цьому здійснюється на власний розгляд аналітика. У результаті одержується кінцева діаграма зв’язків. Для відображення хронології подій за аналогією з деревом зв’язків можна побудувати дерево подій.

Для створення таких діаграм дуже корисно використовувати спеціалізоване програмне забезпечення, як от, наприклад, IBM i2.

Слід наголосити, що від виду вихідних даних може залежати методика побудови та вигляд відповідної діаграми. Наприклад, це можна спостерігати на прикладі аналізу телефонних з’єднань. Для побудови відповідної діаграми телефонних з’єднань за наявними даними використовується заповнена трикутна матриця.

Під час побудови матриці номери телефонів потрібно розміщувати у порядку зростання, щоб було легко відшукати потрібний номер у матриці. Усі наявні номери вносяться в заголовки матриці таким чином, щоб номери, розміщені у n-му стовпчику та n-му рядку заголовку матриці були однаковими, а на перетині ставляться відповідні позначки, які вказують на кількість з’єднань. Підсумкова кількість з’єднань відображатиметься на діаграмі. Для побудови відповідної діаграми можна використати кола, лінії зі стрілками, що вказуватимуть напрям з’єднання та позначку, що відображатиме кількість таких з’єднань

Варто зазначити, що окрім телефонних номерів у вузлах графу може бути розташовано логічні адреси відповідних терміналів, наприклад, комп’ютерів тощо. Велику допомогу в побудові графів з’єднань надає спеціалізоване програмне забезпе-

чення. У цьому сенсі варто згадати програму «Мобильный криминалист: Детектив», у якій присутня функція побудови графу зв'язків як у середині одного пристрою, так і об'єднаного в рамках однієї справи графу контактів декількох пристроїв.

Більшими колами позначено контакти, з якими найчастіше відбувався зв'язок з використанням досліджуваних мобільних пристроїв. Після побудови діаграм за визначеними методами внаслідок інтерпретації даних формується аналітичний продукт – висновки, яких виділяють чотири види: гіпотеза, прогноз, розрахунок, умовивід. Висновки мають містити інформацію про ключову особу чи осіб (WHO?); кримінальне діяння (WHAT?); методику дій (HOW?); місцезнаходження (WHERE?); мотив (WHY?); період часу (WHEN?). Така система запитань одержала назву 5W+H (Who, What, When, Where, Why and How).

Гіпотеза чи будь-який висновок повинні містити відповіді на такі ключові запитання:

- Хто? Ключові особи;

- Що? Злочинна діяльність;

- Як? Методи, що використовуються;

- Де? Географічна інформація та сфера охоплення;

-Чому? Мотив;

- Коли? Терміни.

Саме ця модель нерідко застосовується під час навчання поліцейських кадрів у країнах Європи та США. У різних моделях поліцейської розвідки форми висновків можуть різнитись. Наприклад, у Британській моделі кінцевий продукт аналізу може подаватися у вигляді:

- 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 короткострокових планів діяльності поліції згідно із загальною стратегією, а також може використовуватися для доповнення існуючих вимог до поліцейської розвідки;

- цільового профілю стосовно конкретної особи (підозрюваного чи жертви) або групи осіб відповідно до стратегічних пріоритетів;

- проблемного профілю, у якому проаналізовано конкретний злочин або серію подій тощо [67, с. 67].

Приклад висновку: Джон Сільвер (WHO?) є головою злочинного угруповання, задіяного у вчиненні насильницьких злочинів (WHAT?). Він здійснює свою діяльність, нападаючи на неозброєні торгівельні судна та грабуючи їх (піратство) (HOW?) з метою наживи (WHY?). Група промишляє у Карибському морі (WHERE?) останні 12 років (WHEN?).

Висновки підлягають поширенню у формі звітів, презентацій, тижневих оглядів, цільових інструктажів тощо. Після завершення циклічного кола кримінальної розвідки відбувається повторна оцінка, спрямована на вдосконалення аналітичного продукту.

На теперішній час найбільш поширеними стратегіями, в яких викладено процес кримінальної розвідки, є британська «Національна розвідувальна модель» (National Intelligence Model) [67] та американський «Національний план розподілу розвідувальної інформації» (National Criminal Intelligence Sharing Plan) [81].

З указаними стратегіями тісно пов’язана організація поліцейська діяльність на основі оперативних даних та інформації або модель поліцейської діяльності Intelligence-Led Policing (ILP). Останній термін, як відмічають Дж. Картер, С. Філіпс та М. Гайадин, співвідноситься з описаними стратегіями таким чином, що стратегії визначають структуру, у рамках якої ILP може бути застосована у правоохоронних органах [60, с. 435].

Потрібно зауважити, що прийняття стратегій поліцейської розвідки у названих

країнах не означає, що раніше поліцейська (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 саме в означений період, що підтверджується даними науковців цієї країни [79, с. 181].

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

– оперативні 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 [44].

Кримінальна розвідка складається із шести головних етапів, об’єднаних у циклічне коло: планування та визначення напрямів (цілей); збирання інформації; обро-

блення інформації; аналіз інформації; поширення інформації; повторна оцінка інформації [81, 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 нагромадження 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.

Потрібно зауважити, 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 таких форм:

– стратегічного аналізу, за допомогою якого виробляються довгострокові 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 відповідно до стратегічних пріоритетів;

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

У 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 [71]). Також останніми роками набув популярності метод збирання розвідувальної інформації з комп'ютерних соціальних мереж, як різновид розвідки з відкритих джерел.

Моніторинг у режимі реального часу оновлень у Facebook, Twitter та інших соціальних медіа дозволяє правоохоронним 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 [74, с. 102].

Варто зауважити, 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» [3 с. 281], у 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 в 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 вищого «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.

Цікаву новацію у розстановці конфідентів, яку, на нашу думку, корисно використовувати правоохоронним органам, було запропоновано австралійськими науковцями. У рамках проєкту 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 [75].

У рамках виконання завдань поліцейської діяльності основні зусилля поліції провідних західних країн повинні скеровуватися на виявлення та запобігання злочинам, ураховуючи те, що на запобігання правопорушенням витрачається набагато менше ресурсів, аніж на подолання наслідків їх учинення. Це ж саме стосується і встановлення пріоритетних напрямів у роботі конфідентів. Із цього приводу варто навести твердження Карла Круза [64], 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 запобігання злочинам.

Суттєву роль у здійсненні кримінальної розвідки за кордоном відіграє її інформаційне забезпечення. На теперішній час створено та інтегровано потужні інформаційні масиви за різними напрямами 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 [46].

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. Із цією метою застосовується матричний або графовий підхід, який було детально описано в попередньому підрозділі.

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 [57] на теперішній час лише розробляється система нагромадження оперативної 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 [61, с. 55].

Крім того, зарубіжні фахівці наголошують, на потребі застосування так званого «екологічного» підходу під час збирання поліцейської інформації [59, с. 193], який полягає у тому, що будь-яка система як її екологічний аналог еволюціонує та змінюється, що потребує постійного збирання та оновлення інформації про злочинну діяльність.

Указані пропозиції цілком збігаються із викладеною моделлю поліцейської (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 [43]. Дане визначення, на нашу думку, є одним із найбільш комплексних та прийнятних для застосування у сучасних умовах.

За результатами аналізу терміна «оперативне обслуговування», нами було виділено його головні ознаки: поєднання активних і пасивних заходів оперативного 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, за-

побігання злочинам, а також сприяння розслідуванню і відшкодуванню матеріальних збитків; взаємодія суб'єктів-учасників оперативного обслуговування; особливості щодо конкретних напрямів правоохоронної діяльності.

Ураховуючи викладене, можна побачити, що діяльність із поліцейської (кримінальної) розвідки, яка здійснюється на заході, цілком узгоджується із вітчизняним інститутом оперативного обслуговування. На цій підставі виправданим є застосування 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) [82], який 22 квітня 2015 року був погоджений Палатою представників США. Зміст нововведень, запропонованих у законопроєкті, полягає в 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 [83], та федеральними правоохоронним органами. Очевидно, що у разі прийняття даного законопроєкту 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.

Указана законодавча ініціатива щодо вдосконалення оперативного обслуговування високотехнологічних об'єктів стала реакцією на часті атаки на великі компанії з боку хакерів. Одні з останніх таких атак, які сколихнули громадськість, були компрометація 40 млн. платіжних карт клієнтів у великій мережі роздрібної торгівлі Target [78], а також викрадення 53 млн. адрес електронної пошти та 56 млн. платіжних даних клієнтів компанії з продажу будматеріалів і ремонтних пристосувань

Home Depot [69].

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 [31].

В умовах сплеску високотехнологічної злочинності новації даного законопроєкту, на думку науковців [35], 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.

Також, на думку науковців, корисним було б переглянути сучасну систему оперативного обслуговування у бік надання більш ширших повноважень інформаційно-аналітичним підрозділам щодо нагромадження та оброблення оперативної 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.

Сучасні системи кримінального аналізу та реалізація моделі поліцейської діяльності керованої аналітикою «Intelligence Led Policing».

За даними [14] інформаційно-аналітичну діяльність ототожнюють із поняттям аналізу, визначаючи його як дослідницьку функцію в управлінні підрозділами, без якої науково організувати їхню діяльність неможливо. Проте це твердження є не зовсім правильним.

Аналітична робота є діяльністю з дослідження інформації, у той час як аналізом є метод теорії пізнання, коли шляхом розумової діяльності ціле ділиться на частини. Відтак аналіз є одним з методів аналітичної роботи, тобто способом дослідження інформації, зокрема, у сфері організаційно-аналітичної роботи у підрозділах поліції. Аналітик, спираючись на інформаційні моделі (відбитки в інформаційному просторі подій, фактів, дій, ідей, думок, почуттів людей, природних, політичних, соціальних, соціоінженерних, фінансових, економічних процесів тощо), виявляє об'єктивні закономірності і тенденції, визначає рушійні механізми та, що найголовніше, причинно-наслідкові зв'язки. У цьому змісті аналітик створює нове знання про той фрагмент реальності, який стосується його професійного інтересу, будучи дослідником своєї предметної області.

Управління кримінального аналізу в підрозділах поліції, власне, створюються з метою консолідації усіх розрізнених джерел оперативної інформації з подальшим глибоким аналізом для прийняття обґрунтованих, оптимальних стосовно критичних ситуацій управлінських рішень на усіх керівних рівнях, що повинно активувати оперативно-розшукову діяльність.

Отже, за визначенням керівника Управління кримінального аналізу Національної поліції України, кримінальний аналіз – це мисленнєво-аналітична діяльність працівників правоохоронних органів, що полягає у перевірці та оцінці інформації, її інтерпретації, встановленні зв'язків між даними, що отримуються у процесі розслідування та мають значення для кримінального провадження, з метою їх використання правоохоронними органами та судом, подальшого проведення оперативного і стратегічного аналізу.

Науковці подають таке розуміння терміна «кримінальний аналіз» [24]. Кримінальний аналіз є специфічним видом інформаційно-аналітичної діяльності, яка полягає в ідентифікуванні та точному визначенні внутрішніх зв'язків між інформаціями (відомостями, даними), що стосуються злочину, і довільними іншими даними,

отриманими з різних джерел, їх використанням в інтересах ведення оперативно-розшукової та слідчої діяльності, прийняття адекватних управлінських рішень на основі їх аналітичної підтримки.

З огляду на викладене виникла нагальна необхідність у реорганізації та вдосконаленні методів протидії кіберзлочинності. Одним із засадничих підходів стосовно застосування сучасних технологій у сфері протидії кіберзлочинності на якісно новому рівні та водночас прийняття оптимальних рішень є кримінальний аналіз. Отже, від того, якою мірою підрозділи кримінального аналізу поліції спроможні якісно аналізувати наявну інформацію і як результат надавати аналітичні продукти, які є підтримкою для прийняття адекватних кіберзагрозам управлінських рішень, залежить успіх виконання поставлених завдань.

Технології кримінального аналізу передбачають впровадження моделі поліцейської діяльності, керованої аналітикою «Intelligence Led Policing» (ILP) [24], як моделі, яка спрямована на підтримку, супровід інституційного управління та рішень посадових осіб на основі процесу аналізу інформації і даних.

Основні складові розвитку моделі ILP є такими: нормативно-правова база для врегулювання; інформаційні ресурси; система наповнення інформаційних ресурсів; система оцінювання джерел та достовірності інформації; спеціальне програмне забезпечення; інтегрування спеціалізованого програмного забезпечення з інформаційними ресурсами МВС та інших джерел інформації; тренінги для аналітиків практичних підрозділів Національної поліції України; стандартизовані форми аналітичних продуктів.

Поліцейська діяльність на основі оперативних даних та інформації спрямована на ідентифікування і точне визначення взаємозв’язків між відомостями, які стосуються злочинів, осіб, пов’язаних з ними, та даними, що походять з різних джерел і їх використання кримінальними підрозділами Національної поліції України

Основними елементами та засобами реалізації інформаційно-аналітичної дія-

льності є система поліцейської інформації та рохвідки – системи зв’язку та трансмісії даних, інформаційно-телекомунікаційна інфраструктура, бази даних правової інформації, технічні, програмні, лінгвістичні, правові, організаційні засоби. Згадані аспекти відтворені у статтях 25, 26, 27 Закону України «Про Національну поліцію». Своєю чергою, технологічна платформа системи поліцейської інформації та розвідки дає змогу здійснювати інтегрування та координування дій між різними підрозділами Національної поліції України.

ВИСНОВКИ

Проведеним аналізом установлено, що інформаційне забезпечення правоохоронних органів розвинених країн умовно можна поділити кілька груп. Водночас слід зазначити, що деякі з них не мають аналогів у нашій країні.

По-перше, це інформаційно-пошукові бази даних, що містять відомості щодо осіб або майна, пов'язаних з тим чи іншим злочином, а саме: підозрювані та засуджені, особи, оголошені у розшук, особи, схильні до сексуальних чи насильницьких злочинів, які зникли без вести, а також викрадене майно, транспорт, документи тощо.

До другої групи належать бази даних відбитків пальців, ДНК та інших біометричних властивостей; будь-яких оболонок боєприпасів тощо, призначені для проведення автоматичного порівняльного аналізу.

До третьої групи належать інформаційно-аналітичні програмні комплекси, такі як TECS або ANACRIM, що дозволяють встановлювати зв'язки між будь-якою інформацією щодо особи, яка підлягає перевірці з метою побудови версій, прогнозів щодо поведінки та інше. Правоохоронні органи України нині, незважаючи на численні спроби розробити подібні комплекси, на жаль, подібні програми відсутні взагалі.

До четвертої групи доцільно віднести системи відстеження дорожнього руху чи телекомунікаційних зв'язків.

П'яту групу складають статистичні програмні комплекси. Зважаючи на те, що такий програмний комплекс, як CompStat має вітчизняні аналоги (наприклад, автоматизована система Міністерства внутрішніх справ України «Статистика 2012»), було б доцільним використати досвід департаменту поліції Нью-Йорку для вдосконалення вітчизняної статистичної системи правоохоронних органів для загального застосування. Таким чином, сьогодні, враховуючи необхідність створення умов для

інтеграції вітчизняних програмних комплексів у такі системи Європейського Союзу, як SIS та TECS, є доцільним налагодити співпрацю з правоохоронними відомствами Європейського Союзу та США з метою удосконалення існуючих вітчизняних аналогів та розробки нових, що відповідають світовим стандартам. Крім того, необхідно створити умови для підвищення матеріально-технічної складової інформаційного забезпечення всіх ланок правоохоронної системи України та їх ефективного використання з метою створення програмних комплексів із використанням інноваційних технологій.

Поліцейська (кримінальна) розвідка – це колективний процес, а тому одній людині практично нереально домогтися успіху в розслідуванні більш-менш серйозного злочину в прийнятні строки. Для цього повинен працювати злагоджений колектив. Удосконалення знань, наполеглива праця та постійне навчання колективу дозволять значно покращити його оперативно-службову діяльність, зокрема у сфері протидії злочинності.

З урахуванням проведеного аналізу можна констатувати, що під час проведення кримінальної розвідки на етапі аналізу використовується ціла низка методів, що поєднують у собі різні наукові знання. Це робить роботу аналітика однією з найбільш кваліфікованих і, як наслідок, потребує суттєвої підготовки. Не дивно, що у багатьох провідних державах світу штат аналітиків правоохоронних органів значно перевищує кількість польових співробітників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ананьєва Є. А. Фінансування поліції у Великобританії. Сучасна європейська поліцеїстика та можливості її використання в діяльності Національної поліції України : зб. тез доп. учасників Міжнар. наук.-практ. конф. (Харків, 11 квіт. 2019 р.). Харків : ХНУВС, 2019.С. 46–47.
2. Бакутін Є.І. Аналіз європейського та вітчизняного досвіду щодо здійснення правозастосовної діяльності поліції. Часопис Київського університету права. № 1. 2020. С. 328-332.
3. Бандурка О. М. Оперативно-розшукова компаративістика: [монографія] / О. М. Бандурка, М. М. Перепелиця, О. В. Манжай. – Харків: ХНУВС, 2013. – 352 с.
4. Беляков К.І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення. Монографія. – К. : КВІЦ, 2008 – 576 с.
5. Безпалова О.І. Адміністративно-правовий механізм реалізації правоохоронної функції держави : монографія. Харків : НікаНова, 2014. 544 с.
6. Братель С.Г. Громадський контроль за діяльністю міліції : автореф. дис. … канд. юрид. наук; Київський нац. ун-т внут. справ України. К., 2007. 22 с.
7. Возможности использования аналитических программ в борьбе с организованной преступностью. URL: https://articlekz.com/article/11838
8. Гуменюк Б. І., Задорожній О. В. Інтерпол. Українська дипломатична енциклопедія : у 2 т. / [редкол.: Л. В. Губерський (голова) та ін.]. Київ, 2004 Т. 1. С. 451.
9. Гринчак Я. В. Деякі аспекти використання кримінального аналізу в діяльності правоохоронних органів країн Європи та США. Центральноукраїнський правничий часопис Кіровоград. юрид. ін.-ту ХНУВС. 2010. Спец. вип. С. 268–273.
10. Губин А.В., Хлуднев П.Н., Яковец Е.Н. Современные подходы к информационно-аналитическому обеспечению оперативно-розыскной деятельности органов внутренних дел // Информатизация и информационная безопасность правоохранительных органов: сб. трудов XII Межд. науч. конф. (20-21 мая 2003 г.). М., 2003
11. Деревягін О. О. Перспективи розвитку міжнародного поліцейського співробітництва через сучасні механізми Інтерполу та Європолу. Сучасна європейська поліцеїстика та можливості її використання в діяльності Національної поліції України : зб. тез доп. учасників міжнар. наук.-практ. конф.(Харків, 11 квіт. 2019 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2019. С. 97-98.
12. Директива Європейського Парламенту і Ради (ЄС) 2016/2019 про правову допомогу підозрюваним та обвинуваченим у кримінальних провадженнях та розшукуваним особам у провадженнях за європейським ордером на арешт : прийнята 26 жовт. 2016 р. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/984_020-16#Text.
13. Дирекция по международному полицейскому сотрудничеству. Посольство Франции : [сайт]. URL: https://ru.ambafrance.org/Direkciya-pomezhdunarodnomu-

policejskomu-sotrudnichestvu-DMS.
14. Єрофєєв В. Кримінальний аналіз – це ефективна робота поліції та безпека громадян. URL: http://mvs.gov.ua/ua/news/10309_Kriminalniy_analiz_ce_efektivna_robota_policii_ta_bezpeka_gromadyan_FOTO.htm.
15. Єсімов С. С. Юридична природа інформаційно-аналітичної діяльності Національної поліції. URL: http://aphd.ua/publication-151/.
16. Жицький Є. О. Роль ДСБЕЗ у оперативному обслуговуванні об'єктів, які надають інформаційні послуги з використанням Інтернет. Сучасні проблеми правового, економічного та соціального розвитку держави: матеріали міжнародної науково-практичної конф. (м. Харків, 12 грудня 2014 р.) МВС України; Харків. нац. ун-т внутр. справ. Харків: ХНУВС, 2014. С. 343-345.
17. Заєць О. М. Інститут аналітичного супроводження досудового розслідування кримінального провадження в Україні. Сучасний стан і перспективи розвитку. Вісник кримінального судочинства. 2016. № 4. С. 17–25.
18. Заросило В.О. Порівняльний аналіз адміністративної діяльності міліції України та поліції зарубіжних країн (Великобританії, США, Канади та Франції) : дис. … канд. юрид. наук : спец. 12.00.07. К., 2002. 250 с.
19. Калаянов Д.П. Поліція країн ЄС та використання її досвіду в адміністративній діяльності органів внутрішніх справ України: теорія і практика : дис. ... докт. юрид. наук : спец. 12.00.07. О., 2010. 468 с.
20. 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. … канд. юрид. наук: спец. 12.00.09. М., 2006. 190 с.
21. Князєв С. У навчанні майбутніх поліцейських ми повинні рухатися до нової моделі підготовки. URL: https://www.npu.gov.ua/uk/ publish/article/2168283
22. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Закон України від 6 липня 2010 року № 2438-VI. Офіційний вісник України. 2011. № 1. Ст. 85.
23. Конституційні акти Європейського Союзу (в редакції Лісабонського договору) / за заг. ред. Г. Друзенка. К. : К.І.С., 2010. 536 с.
24. Конституція України від 28.06.1996 р. №254к/96-ВР.
25. Користін О. Є., Пефтієв Д. О., Некрасов В. А. Довідник керівника поліції – поліцейська діяльність, керована розвідувальною аналітикою/ILP : навчальний посібник / за заг. ред. М.Г. Вербенського. К., 2019. 120 с.
26. Користін О.Є. Сучасні моделі правоохоронної діяльності. Юридична наука: сучасний стан та перспективи розвитку : збірники наукових праць, матеріали конференцій (семінарів, круглих столів). 2017. URL: http://elar.naiau.kiev.ua/bitstream/123456789/4117/1/-%20%d0%d0%97%20%20%d0%be%d1%81%d1%82._p075-076.pdf.

27. Криміналістика: підручник / за ред. В.Ю. Шепітька. 5-те вид. переробл. та доповн. Київ : Ін-Юре, 2016. 640 с.
28. Кримінальний аналіз у діяльності Національної поліції України. Концепція впровадження в Національній поліції України моделі поліцейської діяльності, керованої аналітикою «Intelligence Led Policing». URL: http://www.slideshare.net/NationalPolice/ss-75925350.
29. Манжай О. В., Манжай І. А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків : Промарт, 2020. 162 с.
30. Манжай О.В., Жицький Є. О. Кримінальна розвідка та її співвідношення з оперативним обслуговуванням. Jurnalul Juridic National: Teorie si Practică. 2015. № 3(13). С. 100-105.
31. Матюхіна Н.П. Сучасний погляд на управління правоохоронними органами Сполучених Штатів Америки. Право і безпека. 2005. Т.4. №5. С. 7-9.
32. Махнюк А. В. Теоретичні основи провадження кримінального аналізу у сфері правоохоронної діяльності. Науковий вісник Державної прикордонної служби. 2011. № 94. С. 3–7.
33. Мельник В., Некрасов В. Як подолати ворога, багатшого за транснаціональні корпорації? URL: http://n-v.com.ua/yak-podolaty-vorogabagatshogo-za-korporatsyi/
34. Мельникова О.О., Форос Г.В. Особливості використання інформаційно-аналітичного забезпечення оперативного пошуку ознак злочинів, пов'язаних з торгівлею людьми. *Правова держава*. 2021. № 42. С. 189-196.
35. Носов В.В., Манжай О. В. Організація та забезпечення інформаційної безпеки: навчальний посібник. Х. : Вид-во Харк. нац. ун-ту внутр. справ, 2007. 216 с.
36. Носов В. В. Система протидії кіберзлочинності FBI U. S. 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.
37. О компании Anacapa Sciences Inc. URL: http://www.spi2.ru/about/partners/anacapa/
38. Овчинский А.С. Информация и оперативно-розыскная деятельность: монография / под ред. В.И. Попова. М., 2002.
39. Овчинский А.С. Оперативно-разыскная аналитика (Ответ современным угрозам): монография. М., 2015.
40. Оніщенко Н. М. Правове регулювання та правовий вплив: поняття, взаємообумовленість та відмінність. Держава і право : зб. наук. праць. Юридичні і політичні науки. Київ, 2004. Вип. 25. С. 3–8.
41. Операции по пресечению торговли людьми. Интерпол : [сайт]. URL: https://www.interpol.int/Crimes/Human-trafficking/Operations-to-curb-humantrafficking.
42. Основи кримінального аналізу: посіб. з елементами тренінгу / О. Є. Користін, С. В. Албул, А. В. Холостенко та ін. Одеса: ОДУВС, 2016. 112 с.

43. Основи адміністративного судочинства та адміністративного права : навч. посіб / за заг. ред. Н. В. Александрової, Р. О. Куйбіди. Київ : Конус-Ю, 2006. 256 с.
44. Офіційний вебсайт National Crime Agency. – Режим доступу: http://www. nationalcrimeagency.gov.uk.
45. Офіційний вебсайт Інтерпола. Режим доступу: http://www.interpol.int.
46. Петровський О. Проблемні питання формування єдиного інформаційного простору правоохоронних органів. Підприємництво, господарство і право. 2017. (8). С. 145–148.
47. Правоохоронна діяльність, керована аналітикою: передова методика сучасної правоохоронної діяльності. URL: http://euam.php7.postbox.kiev.ua/ua/news/opinion/ intelligence-led-policing-the-cuttingedge-of-modern-law-enforcement/
48. Преследование киберпреступников по всем направлениям. Europol. European Cybercrime Centre : сайт. URL: https://www.europol.europa.eu/crimeareas-and-trends/crime-areas/cybercrime.
49. Про затвердження Положення про Департамент кримінального аналізу Національної поліції України: наказ Національної поліції України від 29.12.2019 № 1354.
50. Протидія злочинам у сфері земельних відносин: навч. посібник / С. В. Андрусенко, О. М. Бандурка, М. С. Рябченко та ін.; за заг. наук. ред. С. М. Гусарова. Харків: ХНУВС, 2013. 170 с.
51. 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. URL: https://www.unodc.org/ pdf/criminal_justice/10-52547_1_Policing_4_ebook. pdf.
52. Смелік В.Б. Міжнародно-правові засади інституційної системи Інтерполу : дис. ... канд.юрид. наук : спец. 12.00.11. Ірпінь, 2005. 225 с.
53. Соколенко О. Зарубіжний досвід захисту прав громадян у діяльності поліції. Вісник Київського національного університету імені Тараса Шевченка. 2013. № 95. С. 28–30.
54. Стратегічний кримінальний аналіз: презентація. Варшава : Прикордонна Варта Республіки Польща, 2008. 35 с.
55. Стратегія розвитку органів системи Міністерства внутрішніх справ на період до 2020 року: розпорядження Кабінету Міністрів України від 15 листопада 2017 року № 1023-р.
56. Танкушина Т.Ю. Автоматизовані інформаційні системи в структурі реєстраційної діяльності міліції: становлення, розвиток, сучасність [Електронний ресурс/ Вісник Запорізького національного університету. Юридичні науки. 2011. № 2. (ч. 1). – Режим доступу: http://www.stattionline.org.ua/filologiya/79/13452-avtomatizovani-informacijnisistemi-v-strukturi-reyestracijnoї-diyalnosti-milicії-stanovlennya-rozvitoksuchasnist.html..

57. Теорія управління в органах внутрішніх справ : [навч. посіб.] / за ред. В.А. Ліпкана. К. : КНТ, 2007. 884 с.
58. Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво : підписана 12 лип. 2017 р. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/984_001-16#Text..
59. Угода між Україною та Європейським поліцейським офісом про стратегічне співробітництво : Закон України від 5 жовтня 2010 року № 2576-VI. Офіційний вісник України. 2010. № 96/№ 84. Ст. 2934/3432.
60. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, ратифікована із заявою Законом України від 16.09.2014 № 1678-VII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/984_011.
61. Узлов Д. Ю. Применение интеллектуальной системы криминального анализа в реальном времени (RICAS) для аналитического сопровождения оперативно-розыскной деятельности и досудебного расследования / Д. Ю. Узлов, В. М. Струков [та ін.]. Право і безпека: Юриспруденція. Юридична психологія (психологічні науки). 2015. № 2. С. 132–139.
62. Ханькевич А. М. Географічне профілювання як інноваційний метод встановлення місцезнаходження осіб, які вчиняють серійні злочини // Сучасні проблеми правового, економічного та соціального розвитку держави : тези доп. VI Міжнар. наук.-практ. конф. (м. Харків, 1 груд. 2017 р.) / МВС України, Харків. нац. ун-т внутр. справ. Х., 2017. С. 338-340.
63. Шинкаренко І.Р. Моніторинг оперативної обстановки: теоретичні підвалини. Вісник Луганського держ. ун-ту внутр. справ імені Е.О. Дідоренка. Спецвип. № 4. 2010. С. 175–186..
64. Яковец Е.Н. Основы информационно-аналитического обеспечения оперативно-розыскной деятельности: учеб. пособ. М., 2009
65. Яніцкі М. Оперативний кримінальний аналіз. Міжнародна організація з міграції. К., 2009. 86 с.
66. About the company Anacapa Sciences Inc. URL: http://www.spi2.ru/about/partners/anacapa/
67. Agreste S., Catanese S., De Meo P., Ferrara E., Fiumara G. NetworN Structure and Resilience of Mafia Syndicates. Information Sciences. 2016. Vol. 351. pp. 30-47.
68. Albrech C. C. Fraud and Forensic Accounting In a Digital Environment: White Paper for The Institute for Fraud Prevention. URL: http://www.theifp.org/research-grants/IFP-Whitepaper-4.pdf
69. Ayling J. Criminal Organizations and Resilience. International Journal of Law, Crime and Justice. 2009. № 37. P. 182-196.
70. Berlusconi G., Calderoni F., Parolini N., Verani M, Piccardi C. LinN Prediction in Criminal NetworNs: A Tool for Criminal Intelligence Analysis. PloS one. 2016. № 11(4). :e0154244 (DOI:10.1371/journal.pone.0154244).
71. Carter J. G., Phillips S. W., Gayadeen S. M. Implementing Intelligence-Led Policing:

An Application of Loose-Coupling Theory. Journal of Criminal Justice. 2014. № 42. P. 433-442.
72. 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. P. 50-56.
73. Council act of 3 November 1998 adopting rules applicable to Europol analysis files. Official Journal of the European Communities. Brussels, 1999. № C26/01. P. 1–9.
74. Criminal Intelligence. Manual for Analysts [Електронний ресурс]. – United Nations, 2011. – 96 с. – Режим доступу: https://www.unodc.org/documents/organizedcrime/Law-Enforcement/Criminal _Intelligence_for_Analysts.pdf.
75. Crous C. Human Intelligence Sources: Challenges in Policy Development / C. Crous // Security Challenges. 2009. № 3 (5). P. 117-127.
76. Daniel J. Koenig. International Police Cooperation. A world perspective / Daniel J. Koenig, Dilip K. Das. Oxford. 2001. P. 57–59.
77. Duijn P., KlerNs P. Social NetworN Analysis Applied to Criminal NetworNs: Recent Developments in Dutch Law Enforcement, NetworNs and NetworN Analysis for Defence and Security, Lecture Notes in Social NetworNs. 2014. pp. 121-159 (DOI: 10.1007/978-3319-04147-6_1).
78. Ferrara E., De Meo P., Catanese S., Fiumara G. Visualizing criminal networNs reconstructed from mobile phone records // In: Hypertext 2014 Extended Proceedings: Late-breaNing Results, Doctoral Consortium and WorNshop Proceedings of the 25th ACM Hypertext and Social Media Conference (Hypertext 2014), Santiago, Chile, September 1-4, 2014. URL: https://arxiv.org/abs/1407.2837.
79. 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 p.
80. i2 TextChart. URL: http://www-01.ibm.com/support/docview.wss? uid=swg27027043.
81. Intelligence-Led Policing: the cutting edge of modern law enforcement. URL: http://euam.php7.postbox.kiev.ua/ua/news/ opinion/intelligenceled-policing-the-cutting-edge-of-modern-law-enforcement.
82. Kocsis R. N. Criminal Profiling: Principles and Practice. Humana Press Inc., 2006. 273 p.
83. Kumar D. K. Home Depot says about 53 million email addresses stolen in breach [Електронний ресурс]. – Режим доступу: http://www.reuters. com/article/2014/11/07/us-home-depot-dataprotection-idUSK BN0IQ2L120141107?feedType=RSS&feedName=technology News.
84. Manzhai O. V. Procedure Analysis of the Special Investigative Actions Through Cyberspace in Countries of Common and Continental Law. Internal Security. 2012. No 1(4). pp. 141-152.
85. Movchan A. V. and V. Yu. Taranukha. Constructing an Automation System to Implement Intelligence-Led Policing Into the National Police of Ukraine. Cybernetics

and Systems Analysis, Vol. 54, No. 4, July, 2018. P. 643-649.
86. 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.
87. Open-source intelligence [Електронний ресурс]. – Режим доступу: http://en.wikipedia.org/wiki/Open-source_ intelligence#Law_enforcement.
88. OSCE Guidebook Intelligence-Led Policing, TNTD/SPMU Publication Series Vol. 13. Дата оновлення: 03.07.2017. URL: https://www.osce.org/files/f/documents/d/3/327476.pdf.
89. Perez Ch., German R. Graph Creation and Analysis for LinNing Actors: Application to Social Data // Automating Open Source Intelligence: Algorithms for OSINT / Edited By Robert Layton, Paul A. Watters. Elsevier, 2016. pp. 103-129.
90. 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.
91. 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.
92. Ratclife J. H. Crime Mapping and the Training Needs of Law Enforcement. European Journal on Criminal Policy and Research. 2004. Vol. 10. Iss. 1. pp. 65-83.
93. Ribaux O., Margot P. Case based reasoning in criminal intelligence using forensic case data. Science & Justice. 2003. № 3. pp. 135-143.
94. Rossy Q, Ribaux O. A collaborative approach for incorporating forensic case data into crime investigation using criminal intelligence analysis and visualization. Science & Justice. 2014. № 54. pp. 146-153.
95. Schneider S. R. The Criminal Intelligence Function: Toward a Comprehensive and Normative Model. Law Enforcement Intelligence Analyst Digest. 1995. Vol. 9. No. 2. pp. 1-26.
96. Sidel R. Target Hit by Credit-Card Breach [Електронний ресурс] / Robin Sidel, Danny Yadron, Sara Germano. http://www.wsj.com/news/articles/SB10424052702304773104579266743230242538.
97. Šimovic V. Research of Classical and Intelligent Information System Solutions for Criminal Intelligence Analysis. National Security and the Future. 2001. № 3-4 (2). P. 181-200.
98. Sparrow M. K. The application of networN analysis to criminal intelligence: An assessment of the prospects. Social NetworNs. 1991. № 13. pp. 251-274.
99. The National Criminal Intelligence Sharing Plan. Department of Justice. 2003. 54 p. [Електронний ресурс]. – Режим доступу: https://it.ojp.gov/documents/ncisp/National_ Criminal_Intelligence_Sharing_Plan.pdf.
100. The Protecting Cyber Networks Act [Електронний ресурс]. – Режим доступу: http://intelligence.house.gov/ ProtectingCyberNetworksAct.

101. U. S. House Passes Cybersecurity Information sharing Legislation: special report (27 April 2015) [Електронний ресурс]. – Режим доступу: http://www.isaca.org/cyber/Documents/CSXSpecial-Report-0427_misc_Eng_0415.pdf.
102. Westphal C. Data Mining for Intelligence, Fraud and Criminal Detection. Advanced Analytic & Information Sharing Technologie. New York: CRC Press Taylor & Francis Group, 2009. 440 p.
103. Xu J. J., Chen H. Fighting organized crimes: using shortest-path algorithms to identify associations in criminal networNs. Decision Support Systems. 2004. № 38(3). pp. 473-487 (DOI:10.1016/S0167-9236(03)00117-9).