Львівський державний університет
внутрішніх справ

Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції

Навчальний посібник

Львів
2017

УДК 351.745.7
М74

Рекомендовано до друку Вченою радою
Львівського державного університету внутрішніх справ
(протокол від 29 березня 2017 року № 9)

Р е ц е н з е н т и:

В. І. Василинчук, доктор юридичних наук, професор,
заслужений юрист України;

В. П. Захаров, доктор юридичних наук, професор;

В. Л. Ортинський, доктор юридичних наук, професор,
академік Академії наук вищої освіти України,
заслужений юрист України;

С. Д. Редька, заслужений юрист України

Мовчан А. В.

М74 Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник / А. В. Мовчан. – Львів: ЛьвДУВС, 2017. – 244 с.

ISBN 978-617-511-240-3

Відповідно до позиції системного підходу викладено історію розвитку та теоретико-прикладні основи інформаційно-аналітичної роботи, визначено її роль та місце в ОРД. Розглянуто форми інформаційно-аналітичної роботи, питання нормативно-правового регулювання інформаційно-аналітичної роботи в ОРД, застосування сучасних інформаційно-аналітичних технологій в ОРД, організацію інформаційно-аналітичної роботи в оперативних підрозділах Національної поліції, підготовку фахівців у сфері застосування інформаційних технологій.

Для працівників правоохоронних органів, зокрема оперативних підрозділів, викладачів та наукових працівників, курсантів, слухачів, а також тих, хто досліджує проблеми оперативно-розшукової діяльності.

УДК 351.745.7

ISBN 978-617-511-240-3

Зміст

Перелік умовних позначень

АІПС	Автоматизована інформаційно-пошукова система
АІС	Автоматизована інформаційна система
ГПУ	Генеральна прокуратура України
ГУНП	Головне управління Національної поліції
ДБЗПТЛ	Департамент боротьби зі злочинами, пов'язаними з торгівлею людьми
ДВБ	Департамент внутрішньої безпеки
ДЗЕ	Департамент захисту економіки
ДІПКП «102»	Департамент інформаційної підтримки та координації поліції «102»
ДІТ	Департамент інформаційних технологій
ДКП	Департамент кіберполіції
ДКР	Департамент карного розшуку
ДОТЗ	Департамент оперативно-технічних заходів
ДОС	Департамент оперативної служби
Закон про ОРД	Закон України «Про оперативно-розшукову діяльність»
ЗМІ	Засоби масової інформації
ІІПС	Інтегрована інформаційно-пошукова система
ІП	Інформаційна підсистема
ІС	Інформаційна система
КПК	Кримінальний процесуальний кодекс
МВС	Міністерство внутрішніх справ
НАБУ	Національне антикорупційне бюро України
НАІС	Національна автоматизована інформаційна система
НПУ	Національна поліція України
НСРД	Негласні слідчі (розшукові) дії
ОГ і ЗО	Організовані групи і злочинні організації
ОРД	Оперативно-розшукова діяльність
ОРЗ	Оперативно-розшуковий захід
ОРС	Оперативно-розшукова справа
ОТЗ	Оперативно-технічний захід
СБУ	Служба безпеки України
СТЗ	Спеціальні технічні засоби
ТЗІ	Технічний захист інформації
УРТЗІ	Управління режиму та технічного захисту інформації
ЄДР	Єдиний державний реєстр
ЄРДР	Єдиний реєстр досудових розслідувань

Вступ

Нині своєчасна та ефективна протидія виявам злочинності в Україні неможлива без проведення кропіткої інформаційно-аналітичної роботи, що за сучасних умов набуває в ОРД вагомого значення. Застосування новітніх інформаційних і телекомунікаційних технологій в ОРД дає змогу інтегрувати й опрацьовувати величезну кількість даних, що містяться у відкритих джерелах інформації та спеціалізованих АІС, отримуючи до того ж нові знання кримінологічного та оперативно-розшукового характеру.

Водночас стрімкий розвиток засобів інформатизації і телекомунікації вимагає нових підходів до організації інформаційно-аналітичної роботи, використання її можливостей в ОРД.

Проблеми інформаційно-аналітичної роботи в ОРД набувають особливої актуальності через низку чинників.

По-перше, це чинники соціально-правового характеру. Йдеться про демократизацію соціальних процесів в Україні, запровадження законодавчого регулювання ОРД, набрання чинності новим КПК України, реформування Національної поліції України, необхідність дотримання прав людини під час здійснення ОРД, захист персональних даних. Відтак виникає необхідність регламентації отримання оперативно-розшукової інформації та її використання у кримінальному судочинстві, створення нового формату правовідносин між органами досудового розслідування та оперативними підрозділами.

По-друге, це чинники технічного характеру, а саме: інтенсивний розвиток комп'ютерної техніки, інформаційних і телекомунікаційних технологій, які використовуються для отримання, обробки та використання оперативно-розшукової інформації.

По-третє, це чинники криміногенного характеру, зумовлені розвитком організованих форм злочинності в Україні, розбудовою її інфраструктури, наявністю корумпованих зв'язків в органах державної влади. Значного поширення набула зло-

чинність з міжрегіональними та міжнародними зв'язками, що потребує систематизації великих масивів інформації, здобутої з різноманітних джерел.

Злочинці стають дедалі освіченішими, використовують для вчинення злочинів новітні інформаційні технології та телекомунікаційні засоби. Крім того, сучасна злочинність швидко пристосовується до методів боротьби з нею, зокрема, шляхом активної протидії оперативно-розшуковим заходам.

Водночас інформаційно-аналітична робота в ОРД потребує правового врегулювання на законодавчому та відомчому рівнях.

Р о з д і л 1

ХАРАКТЕРИСТИКА ОСНОВНИХ ФОРМ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ РОБОТИ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ

1.1. Історичні аспекти становлення та розвитку інформаційно-аналітичної роботи в оперативно-розшуковій діяльності

Початок пізнавальної діяльності людини варто шукати у давнині, коли первісні люди для забезпечення власного виживання навчилися отримувати та аналізувати необхідну їм інформацію з навколишнього середовища. Серед перших засвоєних людьми технологій були добування вогню, вичинка шкір, виготовлення зброї тощо. Як свідчать стародавні джерела, розшук осіб, які порушили норми суспільної моралі, викрадених тварин та речей здійснювався ще за часів общинно-родового ладу.

Для отримання найбільш достовірної інформації про явища, що становили інтерес, який сьогодні б назвали оперативним, наші предки користувалися не лише безпосереднім спостереженням, а й методом таємного опитування.

Історію розвитку інформаційно-аналітичної роботи у правоохоронних органах умовно можна поділити на п'ять основних етапів: початок XVIII ст. – жовтень 1917 р.; жовтень 1917 р. – середина 50 рр. XX ст.; середина 50 рр. XX ст. – початок 90 рр. XX ст.; початок 90 рр. XX ст. – 19 листопада 2012 р.; 20 листопада 2012 р. – сьогодення.

Перший етап розвитку інформаційно-аналітичної роботи (початок XVIII ст. – жовтень 1917 р.). Витоки інформаційно-аналітичної роботи сходять до появи перших систематизованих знань про боротьбу зі злочинністю. До них насамперед належать знання в галузі криміналістики, що є базовою наукою і для кримінального процесу, і для ОРД. З цими знаннями пов'язана поява перших систем кримінальної реєстрації, а також розроблення теоретичних засад проведення окремих слідчих дій та проведення експертиз.

Починаючи з XVII ст. у роботах з кримінального судочинства з'являються рекомендації осіб, обізнаних у звірянні почерків, у розпізнанні отрут, які об'єднувалися у своєрідні корпорації «майстрів-письмоводів». У Франції та Італії друкуються перші праці Ф. Демеля, К. Бальді, Є. Равено, присвячені дослідженням почерку. М. Мальпігі (1687 р.), Б. Альбінус (1764 р.), Й. Майер (1788 р.) і Я. Пуркіньє (1823 р.) проводять наукові дослідження в галузі вивчення папілярних узорів. Детально описує період зародження криміналістичних знань на Заході Юрген Торвальд у своїй книзі «Вік криміналістики».

У працях учених-криміналістів (Н. Орлова, Я. Баршева, В. Спасовіча, А. Квачевського, П. Макалінського, Е. Бурінського, Л. Владімірова та інших), крім методичних рекомендацій з тактики ведення слідства, розглядалися питання, пов'язані з ідентифікацією особи на основі вивчення різних слідів, предметів, документів та інших доказів.

Для аналізу злочинності широко застосовувалися статистичні методи. Уперше державний облік злочинності в 1802 році було доручено вести відділенню «экспедиции спокойствия и благочиния» МВС Російської імперії. 1811 року створено Міністерство поліції, у складі якого 1-ше відділення здійснювало збирання інформації про злочини й правопорушення. У 1826 році був підписаний указ про створення III відділення на основі Особливої канцелярії МВС, якому доручалося збирати: відомості про виявлення фальшивих асигнацій, монет, штемпелів, документів; про осіб, які перебували під наглядом поліції; про всі події; статистичні відомості, що стосуються поліції.

Пізніше, до середини XIX ст. статистичні відомості про події, злочини, осіб, обвинувачених фіксувалися становими приставами у звітах і надсилалися повітовому справнику, який на підставі цих даних готував звіт губернатору, і в губернський статистичний комітет.

Кримінальний сиск Російської імперії з початку свого розвитку (першу сискну частину створено 1866 року у Санкт-Петербурзі) почав цікавитись аналітичними дослідженнями у галузі криміналістики, судової медицини та інших наук, пов'язаних з розкриттям злочинів.

Загальне керівництво органами кримінального сиску у складі Департаменту поліції здійснював спеціально створений підрозділ – 8-ме діловодство, до основних завдань якого належало: упорядкування документів з організації діяльності сискної поліції; створення центрального реєстраційного бюро; отримання звітів сискних відділень про виконану роботу; зв'язок з поліціями західноєвропейських країн щодо взаємодії, а також із фірмами, що постачали технічні засоби для органів кримінального сиску.

Знаменитий сищик А. Кошко, який перебував на посаді начальника кримінального сиску Москви (а згодом усієї Російської імперії), у своїх спогадах, які стосуються початку XX ст., зазначав, що йому регулярно доповідали відомості, які характеризували оперативну обстановку в різних частинах міста. На основі цих відомостей спеціальний чиновник-кресляр викреслював графіки за видами злочинів та місцем їх учинення і складав загальну картограму. Тобто у начальника кримінального сиску з'являлася можливість постійно стежити за оперативною обстановкою в місті та вживати відповідних запобіжних заходів.

Широкого розповсюдження у практиці боротьби зі злочинністю набув розроблений А. Бертильоном 1882 року антропологічний метод реєстрації злочинців, який полягав в обмірюванні їх зросту, розмірів голови, довжини рук, пальців, ступнів тощо. Крім того, Бертильон запровадив обов'язкову фотозйомку кожного затриманого злочинця в анфас і профіль, а також складання «словесного портрета», що заносили до облікової картки. Видимі характерні ознаки кожної особи описували за допомогою спеціальних формул, які надалі використовували під час проведення «парадів арештантів» для розпізнавання затриманих. «Словесний портрет» Бертильона був удосконалений 1905 року швейцарським професором Р. Рейссом, який застосував цифровий код для передачі даних телеграфоном, що значно прискорювало розшук злочинців.

1887 року В. Гершель і Г. Фолдс запропонували відбирати відбитки пальців рук в усіх злочинців з метою ідентифікації особи. У 1891 році Гальтон довів, що згідно з теорією ймовірності, збігання відбитків пальців рук двох людей практично неможливе.

Важливу роль у практиці боротьби зі злочинністю виконували картотеки злочинців, які були створені у 80-х роках XIX ст. і є актуальними досі. Зокрема наприкінці 1896 року Е. Генрі знайшов спосіб упорядкувати в картотеках мільйони карток з відбитками пальців. З 1901 року у Скотланд-Ярді функціонувала перша в Європі дактилоскопічна картотека, яка стала основою побудови відповідних обліків криміналістичного та оперативного призначення. Пізніше з'явилися картотеки, складені за іншими принципами ідентифікації особи (за почерком, ознаками зовнішності, татуюванням, фотопортретом тощо).

Як джерела інформації для аналітичних досліджень кримінальної поліції В. Єлінський називає дані, які надходили у процесі огляду особи потерпілого (включаючи кримінальні трупи) і речових доказів; вивчення публікацій періодичної преси; розшуку і переслідування злочинців «по гарячих слідах»; опитування; негласного спостереження. Крім того, сискні підрозділи користувалися такими джерелами інформації, як доноси, чутки, відомості, які надходили від осіб різних професій, результати обходів нічліжок і притонів, а також дані криміналістичних обліків.

Місцеві обліки злочинців, солдатів-дезертирів, осіб, які вели підозрілий спосіб життя, облік гральних закладів та інших «злачних» місць, прибулих до міста і вибулих з нього осіб, що використовували для аналізу криміногенної обстановки та розкриття неочевидних злочинів, з'явилися в поліцейських установах Росії у XVIII ст. Для виявлення осіб, які підлягали постановці на облік, проводили спеціальні облави.

Можливості фотографії в поліцейській реєстрації почали використовувати в 60-х роках XIX ст. У 1862 році при санктпетербурзькій поліції організовано фотографічне бюро для зйомки портретів обвинувачених з метою встановлення їх особи. В Україні перше поліцейське фотоательє з'явилося 1864 року у м. Бобринці Одеської губернії (нині Кіровоградської обл.), через три роки таке ж ательє створили при московській поліцейській друкарні. 1890 року при петербурзькій сискній поліції вперше з'явилися спеціальні підрозділи, які здійснювали дактилоскопіювання, фотографування злочинців і систематизацію інших даних про них. У цей же період організовано реєстрацію осіб, які володіють холодною зброєю.

1902 року при сискній поліції почав створюватися облік швейцарів, двірників, працівників питних закладів і візників. Тоді ж Г. Рудий заснував антропометричний кабінет при сискній частині київської міської поліції.

Важливе місце у практиці поліції на той час займав метод кримінальної реєстрації за способом учинення злочинів (Modus operandi). Він був доволі ефективним у частині реєстрації злочинців-професіоналів, особливо «гастролерів».

Відомий криміналіст М. Гернет зазначав, що професійна злочинність передбачає чітко виражений поділ злочинної діяльності та чисельні категорії «спеціалістів». Вона знає своїх «робітників» і своїх «підприємців», має свою «професійну» честь і «солідарність». Найбільш наочно цей поділ простежувався у професійних злодіїв. Кримінальний сиск Москви, зокрема, обліковував цю категорію злочинців за 19 основними «спеціальностями», утім фактично їх було набагато більше. До жовтневої революції 1917 року «злочинний світ» налічував понад 50 злодійських «професій».

На початку XX ст. при Департаменті МВС Росії створено Центральне реєстраційне бюро. 12 серпня 1902 р. затверджено «Положення про начальників розшукових відділень», яким пропонувалося вести за встановленими зразками: реєстрацію даних спостереження (агентурні записки, щоденники спостереження з відповідними зведеннями); листовий алфавіт осіб, відомості про яких є у відділенні.

В особливому відділі й охоронних відділеннях існували секретні канцелярії та секретні архіви, які здійснювали систематизацію та аналіз здобутої інформації. Доступ до інформації з грифом «ОО» («Особый отдел») та «СС» («Святая святых») мали тільки кадрові оперативні працівники і тільки в межах своєї компетенції. В архівах велись алфавітні картотеки, до яких заносили установчі дані на конкретну особу, його псевдоніми й прізвиська для зовнішнього спостереження, а також відмітки, в яких справах зберігаються агентурні повідомлення про «клієнта».

Згідно з «Інструкцією чинам Київської сискної поліції» (затвердженої в січні 1905 р.) до складу поліції входило розшукове відділення, спеціальним завданням якого було: реєстрація

всіх злочинців і підозрюваних осіб, ототожнення особи злочинця за допомогою антропологічного дослідження, а також реєстрація візників, швейцарів, двірників і сторожів.

1907 року прийнято низку нормативних актів, які сприяли вдосконаленню інформаційно-аналітичної роботи поліції, зокрема: Положення про охоронні відділення, Інструкція з організації і ведення внутрішнього (агентурного) спостереження.

На той час з'явилися перші теоретичні роботи, присвячені криміналістичному обліку й реєстрації. Зокрема відомий австрійський юрист і кримінолог Г. Гросс у своєму посібнику «Руководство для судебных следователей как система криминалистики» розглянув основи обліку злочинців із використанням антропометричної та дактилоскопічної інформації.

Відомий криміналіст В. Лебєдєв видав книгу «Искусство раскрытия преступлений», яка містила докладні наукові відомості про дактилоскопію, антропометрію, судово-поліцейську фотографію. У 1914 році Департаментом поліції був виданий «Розыскной альбом», який містив систематизовані відомості про злочинців-професіоналів. Першоосновою цього альбому послугував «Справочный указатель для чинов полиции» В. Лебєдєва (виданий у 1903 році), що включав фотографії та описи особливих прикмет одинадцяти категорій професійних злочинців.

1915 року С. Трєгубов опублікував практичний посібник для судових слідчих «Основы уголовной техники. Научно-технические приемы расследования преступлений», який містив широкі відомості, що стосувалися кримінальної реєстрації.

До характерних особливостей першого етапу становлення та розвитку інформаційно-аналітичної роботи у правоохоронних органах потрібно віднести: запровадження дактилоскопії в практику роботи поліцейських служб, що знаменувало істотні зміни в змісті інформаційно-аналітичної роботи; централізацію обліків і створення реєстраційної мережі, що склали методологічну основу побудови сучасних форм інформаційно-аналітичної роботи.

Другий етап розвитку інформаційно-аналітичної роботи (жовтень 1917 р. – середина 50 рр. XX ст.). Цей етап характеризується подальшим розвитком криміналістичних та інших

наукових знань, що використовувалися в інформаційно-аналітичній роботі карним розшуком, в основі діяльності якого були ті ж основні методи, які використовував колишній кримінальний сиск Російської імперії. Разом з агентурними методом, зовнішнім спостереженням, іншими методами оперативної роботи, широко практикувалася й інформаційно-аналітична робота.

Серед учених, які зробили значний внесок у розвиток криміналістики на цьому етапі, можна виокремити В. Громова, Г. Маннса, С. Потапова, П. Семеновського, І. Якімова та інших.

Варто зазначити, що в 1917 році було знищено більшу частину обліків охоронних і сискних відділень, що значно погіршило результати боротьби зі злочинністю. Причому вершилось це і представниками старої влади, і звільненими за амністією кримінальними злочинцями. Різке зростання рівня злочинності призвело до того, що, наприклад, у Москві кількість убивств перевищила довоєнний рівень у 10–15 разів.

28 жовтня 1917 р. (за старим стилем) постановою НКВС «О рабочей милиции» була створена міліція. Прийняття Колегією НКВС 5 жовтня 1918 р. Положення про організацію в органах внутрішніх справ РРФСР кримінально-пошукових установ започаткувало створення в підрозділах міліції обліково-реєстраційної служби. Дактилоскопічна й алфавітна реєстрація злочинців розглядалися як найважливіші засоби боротьби зі злочинністю. У 1919 році створено Центральне реєстраційне бюро і реєстраційні бюро в республіканських і губернських відділах та відділеннях карного розшуку.

Постановою Наркомату юстиції України від 11 травня 1919 р. введено в дію Положення про органи карного розшуку й судово-карної міліції, згідно з яким до складу Центральної секції судово-кримінального розшуку ввійшло реєстраційне бюро, яке здійснювало облік реєстраційних і розшукових карток, дактилоскопічних листків злочинців і відповідало на запити місцевих секцій карного розшуку щодо встановлення судимості затриманих злочинців.

В Україні налічувалося 40 реєстраційно-дактилоскопічних бюро, у великих містах – Харкові, Києві, Одесі, Дніпропетровську реєстраційний апарат був переданий до міських управлінь міліції та розшуку. За загальним правилом, реєстрацій-

ні бюро обслуговували всю територію округу, проводячи реєстрацію злочинного елементу та письмовий розшук.

На той час підрозділи карного розшуку активно практикували фотографування і дактилоскопіювання злочинців. У 1920 році був створений централізований облік злочинців, які перебували в розшуку, і осіб, які зникли безвісти, розроблено детальну класифікацію злочинців, практична цінність і пізнавальне значення якої актуальні і нині.

У Науково-технічному підвідділі Центророзшуку створено статистичне бюро, яке вивчало і аналізувало стан злочинності та результати розкриття злочинів. Зокрема на початку 20-х рр. підготовлено та передано в регіони такі аналітичні розробки, як «Руководство по дактилоскопии», «Руководство по судебной медицине», словник злодійської мови «Блатная музыка».

На початку 30-х років з апаратів карного розшуку були виділені науково-технічні підрозділи, які далі, у 1948 році, перетворені в самостійні структурні підрозділи міліції.

1935 року після об'єднання органів ОДПУ та міліції криміналістичні обліки були переведені з карного розшуку до Особливого бюро НКВС СРСР. Унаслідок цього інформаційно-аналітична робота втратила головні свої складові – наукову, методичну та організаційну, що зумовило тривалу втрату системного підходу до цього важливого напряму ОРД.

На той час з'являються перші криміналістичні музеї, які систематизували колекції знарядь злочину, слідів, залишених на місці події, підроблених документів тощо. У музеях накопичувалися відомості, які характеризували прийоми та способи вчинення різних злочинів, прикмети і фотографії злочинців, інші відомості, що сприяли їх встановленню, розшуку та затриманню. Першу таку установу створено ще 1919 року.

Головним суб'єктом інформаційно-аналітичної роботи був карний розшук, на базі якого 14 березня 1937 р. створено службу по боротьбі з розкраданнями соціалістичної власності, покликану виконати важливу роль у становленні інформаційно-аналітичної роботи на наступному етапі її розвитку.

1938 року був утворений Перший спецвідділ НКВС СРСР, центральний інформаційний підрозділ для ОВС. У лютому 1941 р. відбувся поділ НКВС колишнього СРСР на два

самостійних наркомати: НКВС і НКДБ. Перший спецвідділ увійшов у структуру Наркомату внутрішніх справ, до його складу були передані централізована оперативно-довідкова картотека та архів, з Головного управління міліції – алфавітна та дактилоскопічна картотеки централізованого обліку злочинців, з ГУЛАГу – картотеки централізованого обліку ув'язнених. Обліково-реєстраційні відділення й бюро, що перебували з 1918 року у складі підрозділів карного розшуку управлінь міліції областей і країв, були переведені в систему перших спецвідділів наркомату.

У воєнні та повоєнні роки перед органами внутрішніх справ постали нові завдання, пов'язані з боротьбою з бандитизмом. З метою впорядкування цього напряму оперативної роботи МВС УРСР видано директиву від 15 липня 1946 р. № 101 «Про впорядкування оперативного обліку по бандитизму в органах МВС УРСР».

1952 року відбулося організаційне розмежування у Всесоюзній науковій спілці судових медиків і криміналістів, що призвело до певної дезінтеграції наукових знань у зазначених сферах, причому не тільки в кримінально-процесуальній сфері, а й в аналітичній діяльності.

Внаслідок цих змін основну ставку зроблено на розвиток власних теоретичних і прикладних аспектів інформаційно-аналітичної роботи, пов'язаних з положеннями теорії ОРД, що зароджувалася, та відтворенням традиційних форм аналізу, розроблених засновниками вітчизняного карного розшуку.

Третій етап розвитку інформаційно-аналітичної роботи (середина 50-х рр. – початок 90-х рр.). Початок третього етапу розвитку інформаційно-аналітичної роботи пов'язаний з появою і розвитком перших систематизованих знань у сфері теорії ОРД, становлення якої розпочалося зі створення 23 жовтня 1956 р. у Вищій школі МВС СРСР самостійної кафедри оперативної роботи.

Важливими нормативно-правовими актами, спрямованими на вдосконалення інформаційно-аналітичної роботи в ОРД, стали накази МВС СРСР: від 26 березня 1958 р. «С объявлением Инструкции по организации и ведению оперативных учетов в органах милиции» та МВС УРСР від 2 серпня 1962 р.

«О состоянии и мерах по улучшению организации и ведения оперативных учетов в органах милиции».

Подальше дослідження проблем інформаційно-аналітичної роботи в ОРД знаходимо в наукових працях А. Вандишева, В. Шарова, А. Гінзбурга, Д. Гребельского, Б. Нагіленка, С. Овчинського та інших учених.

Прогрес, досягнутий у 50–70-х роках минулого століття, в теорії інформації, створенні та освоєнні технічних засобів її обробки дійшов і до органів внутрішніх справ. В окремих ГУВС, УВС (зокрема: Ленінград, Свердловськ, Рига, Вільнюс, Таллінн, Новосибірськ, Ворошиловград тощо) започатковано використання ЕОМ для обробки оперативно-розшукової інформації.

Значний внесок у створення перших інформаційно-пошукових систем, які були взяті на озброєння органів внутрішніх справ ще до оснащення їх електронно-обчислювальною технікою, зробив відомий вчений С. Овчинський. Результати його досліджень відображені у книгах, присвячених удосконаленню оперативно-розшукового обліку на основі застосування перфокарт (1967 р.) та оперативно-розшуковій інформаційно-пошуковій системі із застосуванням перфораційно-обчислювальних машин (1970 р.).

Водночас основна проблема полягала в тому, що оперативні працівники виявилися не підготовленими до використання можливостей технічних засобів обробки інформації. Своєю чергою, інженерно-технічний склад, що розробляв програми для ЕОМ, не мав необхідних знань щодо шляхів використання інформації в ОРД.

На початку 70-х років минулого століття в органах внутрішніх справ було створено близько 70-ти видів алфавітних картотек на різні категорії осіб. З метою централізації оперативно-розшукової інформації утворено систему інформаційних центрів, що зосередили більше 30-ти картотек ручного пошуку (за прізвиськами, п'яниць, небезпечних рецидивістів, власників нелегальних квартир тощо).

Упровадження ЕОМ призвело до створення перших АІПС оперативно-розшукового призначення, зокрема, «Облік», «Розшук», «Сигнал», «Фільтр», «Мережа». Ці інформаційні системи замінили існуючі картотеки та облікові справи, увели єдину

термінологію для опису оперативно-тактичних, криміногічних та криміналістичних понять і явищ, детально програмували збирання інформації та індивідуально-профілактичну роботу з особами, поставленими на облік.

Значний внесок у розроблення наукових методик, пов'язаних з аналізом оперативної обстановки та діагностичним аналізом злочину – основними видами діагностичної складової дослідження предметів і документів, був зроблений у 70–80-ті рр. минулого століття основоположниками теорії ОРД Д. Гребельским, В. Лукашовим, С. Овчинським, К. Синіловим та іншими вченими.

На початку 80-х рр. розроблено методику комплексного економіко-правового аналізу господарської діяльності об'єктів, об'єднань, галузей народного господарства, що передбачала вивчення проблем забезпечення збереження соціалістичної власності та розроблення заходів щодо попередження безгосподарності, розкрадань, посадових і господарських злочинів.

Прогностичному напряму інформаційно-аналітичної роботи присвячені роботи Л. Горшеніна, В. Кувалдіна, А. Мініна, С. Овчинського, Г. Синілова, Є. Яковця та інших учених.

На той час прийнято низку важливих відомчих нормативних актів, спрямованих на подальший розвиток інформаційної служби в системі ОВС. Зокрема наказом МВС колишнього СРСР 9 листопада 1970 р. створено Головний інформаційний центр (ГІЦ), а наказом МВС СРСР від 17 травня 1971 р. оголошено типову структуру інформаційних центрів. У 1971 році, за узгодженням з оперативними службами, були впроваджені в експлуатацію за допомогою ЕОМ інформаційні системи «Бродяги» і «Розшук».

10 листопада 1971 р. ГІЦ при МВС СРСР перетворено у Головний науково-дослідний центр управління та інформації. У регіонах почали успішно функціонувати інформаційні системи оперативно-розшукового призначення «Єрмак», «Квадрат» та ін.

Водночас ставлення до АІС оперативно-розшукового призначення в державі було неоднозначним. Зокрема у 70-ті роки створено доволі ефективну інформаційно-аналітичну систему

«Паспорт», яка давала змогу фіксувати й накопичувати інформацію про всі переміщення громадян через кордони СРСР. За допомогою цієї системи розкрито резонансні злочини щодо незаконного вивозу антикваріату та ювелірних виробів із країни, а також контрабанди у великих розмірах, проте досить швидко систему ліквідували за вказівкою вищого керівництва держави як таку, що «порушує права людини».

З метою регламентації інформаційно-аналітичного забезпечення ОРД наказом МВС СРСР від 29 грудня 1984 р. затверджено Інструкцію про порядок реєстрації, ведення справ оперативного обліку та ведення оперативно-довідкової роботи за ними. Наказом МВС СРСР від 7 липня 1989 р. визначено поняття оперативного обліку та підстав для заведення справ оперативного обліку й карток-накопичувачів, призначених для забезпечення ОРД.

Основи інформаційного забезпечення ОВС України започатковано в 70-х роках минулого століття Республіканським науково-дослідним інформаційним центром МВС УРСР, до основних напрямів діяльності якого належали: надання оперативно-довідкової, розшукової, статистичної та іншої інформації; збирання, обробка, зберігання, аналіз інформації про злочини та осіб, які їх учинили; розгляд матеріалів про оголошення та припинення розшуку осіб, які зникли безвісти, невпізнаних трупів, а також розшуку втрачених та виявлених номерних речей, зброї тощо. Першими автоматизованими інформаційними системами були «Профілактика-Розшук», «Розшук», «Статистика» та інші. У 90-ті роки на озброєння правоохоронних органів України були взяті такі комп'ютерні мережні системи, як «Бінар», «Кронус», «Єрмак», «Кондор», «Аскрін», «Легенда» та інші, що мали значно вищі пошуково-аналітичні можливості.

Ухвалення рішень правоохоронними органами на національному рівні вимагало опрацювання значних масивів інформації. Тому для обробки, зберігання та використання оперативної інформації стали застосовувати потужні АІС. Особливо це виявилося в діяльності правоохоронних органів, пов'язаній з протидією організованій злочинності, що набуло

значної актуальності наприкінці 80-х – початку 90-х років минулого століття. Цей період характеризувався бурхливими подіями в суспільно-політичному та економічному житті на теренах колишнього СРСР, зокрема й в Україні. Ці події супроводжувалися стрімким зростанням злочинності, особливо її організованих форм. Для боротьби з цими явищами 1988 року при управліннях карного розшуку були створені відділи по боротьбі з груповими злочинами – так звані «шості відділи». Наказом МВС України від 6 травня 1991 р. утворено підрозділи по боротьбі з організованою злочинністю в Україні. З метою вдосконалення інформаційно-аналітичного забезпечення ОРД спецпідрозділів БОЗ в їхньому складі були створені оперативно-інформаційні відділи «Скорпіон».

Характерною особливістю третього етапу була комп'ютеризація інформаційно-аналітичної роботи, що знаменувало революцію в технологіях отримання, обробки, систематизації, аналізу та використання оперативно-розшукової інформації.

Четвертий етап розвитку інформаційно-аналітичної роботи (початок 90-х рр. – 19 листопада 2012 р.). Початок четвертого етапу розвитку інформаційно-аналітичної роботи в ОРД пов'язаний з проголошенням незалежності України, прийняттям Закону про ОРД, структурною перебудовою органів внутрішніх справ України та системи їх інформаційно-аналітичного забезпечення.

Після проголошення незалежності України інформаційні центри були реформовані в управління (відділи) оперативної інформації, а в подальшому на їх базі створено підрозділи інформаційних технологій.

Успіх боротьби з організованою та транснаціональною злочинністю багато в чому залежить від ефективної координації та комплексного підходу до взаємодії правоохоронних органів. Ідеться про узгодження сфер компетенції та координації дій проти злочинних угруповань з боку органів різного територіального й відомчого підпорядкування, між центральними й периферійними структурами, організації їх інформаційної взаємодії. Форми та методи цієї координації в різних державах мають і певну схожість, і особливості. Важливу роль у координації діяльності правоохоронних органів різних країн

виконує Інтерпол, історія якого розпочалась з першого з'їзду кримінальної поліції 14–18 квітня 1914 р. у Монако, коли юристи та працівники поліції 14-ти держав досягли домовленості про створення центрального міжнародного банку даних і визначили процедуру передання злочинців іноземній державі. Основу діяльності Інтерполу становлять потужні обчислювальні центри, які постійно накопичують й опрацьовують величезні масиви інформації.

У червні 1998 р. уряди держав-членів Європейського Союзу ратифікували Конвенцію про заснування Європейської поліцейської установи (Європол). З метою запобігання та протидії злочинності в Європолі створено комп'ютеризовану інформаційну систему, в якій зберігаються неособисті та особисті дані.

1992 року в м. Чолпон-Ате (Киргизстан) міністрами внутрішніх справ підписано Угоду про взаємини між МВС держав-учасниць СНД у сфері обміну інформацією. Серед ухвалених рішень було створення й розвиток Міждержавного інформаційного банку (МІБ).

Подальше дослідження проблем інформаційно-аналітичної роботи в ОРД знаходимо в наукових працях В. Атмажитова, Б. Бараненка, Є. Бєлоглазова, К. Бєлякова, В. Бірюкова, І. Воронова, К. Горяїнова, Є. Демянчук, О. Джужи, О. Долженкова, В. Захарова, І. Козаченка, Я. Кондратьєва, Є. Лук'янчикова, Б. Нагіленка, Д. Никифорчука, А. Овчинського, В. Овчинського, Ю. Орлова, В. Ортинського, О. Осипенка, К. Синілова, В. Хахановського, М. Швеця, А. Шумілова, М. Яблокова, Є. Яковця та інших вчених.

Цей етап характеризується створенням обліків міжвідомчого характеру, розвитком міждержавних обліків, використанням інтегрованих банків Інтерполу; розвитком технологій аналітичної та комп'ютерної розвідки; упровадженням в оперативну практику мультимедійних технологій; розробленням технологій здійснення інформаційно-аналітичної роботи в транспортних телекомунікаційних мережах та електронних інформаційних системах (мережах).

П'ятий етап розвитку інформаційно-аналітичної роботи (20 листопада 2012 р. – сьогодення). Початок п'ятого етапу

розвитку інформаційно-аналітичної роботи в ОРД пов'язаний з набранням чинності новим КПК, запровадженням НСРД, що спричинило суттєві зміни в організації інформаційно-аналітичної роботи в ОРД. Подальший розвиток та вдосконалення інформаційно-аналітичної роботи в ОРД здійснюється під час створення та реформування Національної поліції України.

Проблеми інформаційно-аналітичної роботи в ОРД в сучасних умовах досліджували С. Албул, А. Баб'як, О. Бочковий, О. Бусол, В. Бутузов, В. Василинчук, В. Захаров, І. Катеринчук, О. Користін, Є. Лук'янчиков, О. Манжай, В. Межевой, В. Некрасов, Д. Никифорчук, Ю. Орлов, В. Ортинський, М. Перепелиця, М. Погорецький, Е. Рижков, Р. Тарасенко, В. Черков, І. Харабе-рюш, В. Хахановський, В. Шендрик та інші вчені.

Підсумовуючи історію виникнення, формування та розвитку інформаційно-аналітичної роботи в ОРД, можна виокремити кілька поворотних віх у її розвитку:

1) запровадження дактилоскопії у практику роботи поліцейських служб, що знаменувало істотні зміни в змісті інформаційно-аналітичної роботи;

2) централізація обліків і створення реєстраційної мережі, що стало методологічною основою створення сучасних форм інформаційно-аналітичної роботи;

3) комп'ютеризація інформаційно-аналітичної роботи, що знаменує революцію в технологіях отримання, обробки, систематизації, аналізу та використання оперативно-розшукової інформації;

4) створення обліків міжвідомчого характеру, розвиток міждержавних обліків, використання інтегрованих банків Інтерполу;

5) розвиток технологій аналітичної розвідки, що дає змогу здобувати нові знання шляхом систематизації та аналізу розрізнених фактів;

6) розвиток технологій комп'ютерної розвідки, що дозволяє негласно аналізувати величезні масиви даних і відомостей;

7) упровадження в оперативну практику мультимедійних технологій, що дає можливість отримувати оперативно значу-

щу інформацію з аудіо- та відеозаписів, вирішувати ідентифікаційні та діагностичні задачі, здобувати криміногенно значущу інформацію, яка може стати основою для формування доказів у кримінальних провадженнях;

8) розробка технологій здійснення інформаційно-аналітичної роботи в електронних інформаційних системах (мережах), що дозволяє розкривати кіберзлочини;

9) розробка технологій здійснення інформаційно-аналітичної роботи в транспортних телекомунікаційних мережах, що дає змогу планувати проведення ОРЗ;

10) запровадження НСРД згідно з новим КПК, що спричинило суттєві зміни в організації інформаційно-аналітичної роботи в ОРД;

11) створення та реформування Національної поліції України.

1.2. Поняття та сутність інформаційно-аналітичної роботи в оперативно-розшуковій діяльності Національної поліції

Результативність діяльності правоохоронних органів у боротьбі зі злочинністю безпосередньо залежить від якісного, своєчасного і достатнього інформаційно-аналітичного забезпечення цієї діяльності.

У нормативно-правових актах та науковій літературі з терміном «інформаційно-аналітичне забезпечення» доволі часто вживаються терміни «інформаційне забезпечення», «інформаційно-аналітична діяльність», «інформаційно-аналітична робота», «аналітична робота».

Термін «інформація» (від лат. *informatio* – роз'яснення, виклад) інтерпретується у двох значеннях: у повсякденному – як відомості (повідомлення, звістки), що передаються людьми усним, письмовим або іншим способом (за допомогою умовних сигналів тощо) і повідомляють про що-небудь; і в науковому – як обмін цими відомостями між людьми, людиною й автоматом, автоматом і автоматом.

В обох аспектах категорію «інформація» включено в науку інформатику, яка вивчає інформаційні процеси в соціосередовищі, зокрема такі пізнавальні компоненти, як:

– структура й загальні властивості самої інформації;

– її роль у проектуванні (моделюванні) та безпосередньому здійсненні соціальної діяльності;

– вплив на об'єкти й суб'єктів цієї діяльності;

– різні системи збирання, перероблення, зберігання та використання інформації в конкретних видах діяльності тощо.

Закон України «Про інформацію» (ст. 1) та Цивільний кодекс України (ст. 20) визначають інформацію як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Водночас у Законі України «Про телекомунікації» (ст. 1) зазначено, що інформація – це відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Способи і прийоми оволодіння інформацією дають змогу зробити висновок про існування двох її видів: гласної та негласної. За змістом інформація поділяється на такі види:

– інформація про фізичну особу;

– інформація довідково-енциклопедичного характеру;

– інформація про стан довкілля (екологічна інформація);

– інформація про товар (роботу, послугу);

– науково-технічна інформація;

– податкова інформація;

– правова інформація;

– статистична інформація;

– соціологічна інформація та ін.

Найпоширенішою в правоохоронній діяльності є правова інформація, що визначається як будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

Одним із різновидів правової інформації, що використовується в ОРД, є оперативно-розшукова інформація. Одне з перших і упродовж тривалого часу домінуючих у теорії ОРД визначень поняття оперативно-розшукової інформації було запро-

поновано Д. Гребельським, який сформулював його як *сукупність даних про осіб, причетних до підготовки і вчинення злочинів, факти злочинних виявів, стан оперативно-розшукових сил і засобів, а також про умови, в яких відбувається діяльність ОВС щодо боротьби зі злочинністю.*

Пізніше Г. Синілов до змісту поняття оперативно-розшукової інформації відніс *відомості, які свідчать про задумані, підготовлювані або вчинені злочини, про осіб, що становлять оперативний інтерес, а також про причини й умови, які сприяють учиненню злочинів.*

Надалі низка авторів включили в це поняття також *відомості, які характеризують: оперативну обстановку; психологічні риси осіб, підозрюваних у готуванні та вчиненні злочинів; поточні профілактичні й оперативно-розшукові заходи; види та способи вчинення злочинів; прикмети злочинців, викрадених речей; дані про злочини, які задумуються та підготовлюються, та інші компоненти.*

С. Овчинський розкриває множинний характер оперативно-розшукової інформації і, зокрема, виокремлює такі важливі методологічні аспекти:

– відбивальний, що розкриває роль інформації в процесах відображення об'єктивного світу;

– гносеологічний, що дає уявлення про інформацію як засобу пізнання;

– аксіологічний, що формує ціннісні концепції інформації для різних сфер соціальної діяльності;

– семантичний, що з'ясовує зміст і значення інформації;

– комунікативний, що розкриває психологічні та організаційно-психологічні закономірності та механізми інформаційного зв'язку в соціальних комунікаціях, тощо[1].

У поширених наукових положеннях про поняття й сутність оперативно-розшукової інформації її головна цінність справедливо вбачається в тому, що вона є об'єктивним відображенням мінливого соціального середовища й обстановки, у яких здійснюється ОРД. Ця інформація відбиває також

---

[1] Овчинский С. С. Оперативно-розыскная информация / С. С. Овчинский; под ред. А. С. Овчинского и В. С. Овчинского. – М.: ИНФРА-М, 2000. – С. 19.

наслідки постійного впливу на це середовище особливої за своєю спрямованістю та змістом діяльності (і правомірної, і протиправної) різних соціальних суб'єктів.

На цьому перетині оперативно-розшукова інформація, по-перше, виникає, а по-друге, тут же вона продовжує «працювати», тобто просуватися й розвиватися, включаючись у процеси безпосереднього здійснення ОРД і відображаючи зміни, що відбуваються або безпосередньо в об'єктах ОРД, або на їх периферії.

Проведення ОРД на практиці поєднано з потребою, що постійно виникає в її суб'єктів, у розширенні предметного уявлення про безпосередні об'єкти ОРД, а також у цілеспрямованому інформаційному впливі на них згідно з основними цілями та завданнями зазначеної діяльності. Ця потреба стикається з не вирішеною остаточно проблемою визначення й використання адекватної за своїм змістом оперативно-розшукової інформації та її джерел.

Вирізняються дві головні функції оперативно-розшукової інформації: пізнавальна та дієва, що реалізуються в процесі безпосереднього здійснення ОРД.

Пізнавальну функцію оперативно-розшукової інформації традиційно пов'язують з інформаційно-аналітичним забезпеченням ОРД, що здебільшого зводиться до вивчення й оцінки оперативної обстановки. Зміст останньої традиційно розглядається зазвичай крізь призму кримінологічної характеристики злочинів. Це вивчення ґрунтується на отриманні розгорнутих кримінологічних знань про стан, структуру, динаміку злочинів, їх причини й інші детерміністичні чинники.

Пізнавальна функція оперативно-розшукової інформації реалізується неоднаково за спрямованістю, предметним змістом та обсягами отримуваних, перероблюваних і використовуваних відомостей залежно від загального або видового вивчення оперативної обстановки.

У першому випадку пізнання слугує більш віддаленим організаційним цілям ОРД, а інформація має водночас загальний, зокрема й прогностичний характер.

Результати загального аналізу оперативної обстановки дозволяють розкрити й оцінити загальний стан злочинност-

ті, її структуру й динаміку, зокрема й рівень поширеності тих чи інших видів злочинів, зіставити виявлені тенденції з об'єктивними змінами соціального середовища на різних мікро- й макрорівнях тощо. Разом це створює інформаційно-аналітичні передумови для розроблення перспективних (річних, п'ятирічних) планів протидії злочинності, зміцнення оперативних позицій у певних регіонах, економічних зонах тощо.

Основними джерелами інформації для проведення такого аналізу слугують офіційні статистичні дані, інформаційні огляди, у тому числі такі, що стосуються діяльності інших державних органів, установ та організацій, програми соціального, економічного розвитку районів, міст, областей.

У другому випадку ми маємо справу з організаційно-управлінським рівнем використання оперативно-розшукової інформації на окремих видових напрямах протидії злочинності, зокрема для попередження та розкриття окремих видів злочинів, розшуку злочинців та ін.

До сфери видового аналізу оперативної обстановки включаються: відомості про поширеність серійних тяжких та особливо тяжких злочинів; обіг у злочинному середовищі вогнепальної зброї, боєприпасів, вибухових речовин та пристроїв; міжрегіональне й транснаціональне переміщення злочинного елемента, зокрема учасників організованих груп і злочинних організацій; появу етнічних злочинних угруповань тощо.

Установлюються та вивчаються, крім того:

– найбільш типові форми й способи вчинення окремих видів злочинів;

– соціальні та психологічні чинники формування особистості злочинця, що вчиняє окремі види злочинів;

– конкретні життєві ситуації та обставини, які у взаємозв'язку з суб'єктивними особистісними характеристиками можуть призвести до вчинення окремих видів злочинів конкретними категоріями осіб;

– оперативні контингенти, які через ймовірну злочинну поведінку повинні перебувати на оперативно-розшуковому або профілактичному обліку;

– основні показники ОРД за напрямами попередження та розкриття окремих видів злочинів тощо.

Видовий аналіз оперативної обстановки має також на меті повніше та глибше виявлення та вивчення специфічних причин та умов, які сприяють вчиненню окремих видів злочинів, включаючи їхній взаємозв'язок із криміногенними чинниками навколишнього середовища, а також загалом аналіз і оцінку рівня оперативно-профілактичного спостереження за криміногенним середовищем.

До джерел інформації під час проведення цього виду аналізу насамперед мають бути віднесені традиційні відомості інформаційно-аналітичного призначення, зокрема:

– первинні носії зафіксованих відомостей про зареєстровані, виявлені, попереджені та припинені злочини, відкриті кримінальні провадження (журнали реєстрації, статистичні картки та ін.);

– форми обліку та реєстрації заяв і повідомлень громадян, посадових осіб, громадських організацій; письмових доручень слідчих; вказівок прокурора; ухвал слідчого судді, суду (у межах кримінальних проваджень);

– публікації в засобах масової інформації та мережі Інтернет;

– закінчені й розглянуті судами матеріали кримінальних проваджень та реалізовані (архівні) ОРС;

– аналітичні узагальнення, інформаційні довідки, доповідні записки, статистичні звіти за окремими напрямами боротьби зі злочинністю з застосуванням оперативно-розшукових засобів і методів.

За необхідності можуть також використовуватися методи соціологічного опитування населення, інтерв'ювання працівників оперативних підрозділів, зокрема й отримання експертних оцінок найбільш досвідчених оперативників тощо.

Дійова функція інформації полягає в практичному інформаційному забезпеченні проведення ОРД. Саму інформацію дієвого призначення слід диференціювати на так звану первинну та вторинну оперативно-розшукову інформацію.

Отримання й використання первинної оперативно-розшукової інформації – це початковий етап інформаційно-аналітичного забезпечення організаційно-тактичних завдань ОРД і зводиться до оперативно-пошукової роботи в певному

соціальному середовищі, у певних верствах населення, на певних промислових та інших господарських об'єктах, у певних інфраструктурних утвореннях з метою:

– отримання та перевірки первинних відомостей про окремих осіб і групи, у поведінці та вчинках яких виявляються ознаки підготовки або вчинення злочинних діянь, а також для встановлення причетності цих осіб і груп до злочинів, вчинених невідомими особами;

– установлення осіб, поінформованих про злочинну діяльність об'єктів, що становлять оперативний інтерес, про майно, грошові кошти й цінності, здобуті ними злочинним шляхом, а також про інші факти й обставини, що є носіями доказової інформації;

– установлення місцезнаходження осіб, підозрюваних у вчиненні злочинів, а також таких, що переховуються від осіб, які переховуються від органів досудового розслідування, слідчого судді, суду або ухиляються від відбування кримінального покарання тощо.

Ці рекомендації випливають із чинного законодавства. Зокрема йдеться про ст. 1 Закону про ОРД, котра визначає завданням ОРД пошук і фіксацію фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена КК України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави. Практичне виконання вказаної вимоги пов'язане з «оперативним відпрацюванням» соціального середовища та його певних (криміногенних) елементів, що передбачає здійснення заходів ОРД.

Вторинна оперативно-розшукова інформація – це відомості, збирання й використання яких проводиться, як правило, у межах ОРС. Насамперед це дані, які підтверджують наявність правових підстав заведення зазначених справ. Однак для ухвалення остаточного рішення про проведення ОРД таких підстав мало. На це рішення впливають багато інших чинників інформаційного характеру, як, наприклад:

– достатність вихідних даних для об'єктивної оцінки самої потреби в здійсненні ОРД, а також визначення об'єктів

оперативної розробки, конкретних завдань, адекватних заходів ОРД і доцільності їхнього проведення;

– наявність відомостей, які підтверджують надійність джерел отримання вихідної інформації та достовірний її характер;

– наявність реальних шляхів і можливостей поповнення гласних і негласних джерел оперативно-розшукової інформації для забезпечення перспективи розвитку оперативної розробки фігурантів в ОРС, отримання об'єктивних даних про особу, поведінку, зв'язки розроблюваних осіб, а також про характер, спрямованість, цілі та способи здійснення ними злочинної діяльності тощо.

Для виявлення й підтвердження відповідних ознак потрібними є збирання, вивчення й оцінка відомостей про явно виражену злочинну поведінку конкретних осіб і груп; про характер і кримінальну спрямованість цієї поведінки, зокрема і про наявність у діях імовірних об'єктів ОРД ознак конкретних злочинів; про особистісну характеристику, колишню злочинну діяльність, злочинні зв'язки та інше найближче оточення цих об'єктів тощо.

Отримання таких відомостей, по-перше, значно підвищує правову значущість вихідної інформації, по-друге, вони необхідні для відшукання оперативних підходів до об'єкта розробки, для встановлення з ним або його близькими зв'язками контактів, тобто створення сприятливих передумов для успішного виконання завдань оперативної розробки.

Відтак оперативно-розшукова інформація на цьому організаційно-тактичному рівні ОРД становить насамперед ті вихідні знання, які дозволяють ухвалити правильні й безпомилкові рішення щодо правової обґрунтованості фактичної необхідності та можливості здійснення ОРД у певних умовах і стосовно конкретних об'єктів.

Однак на цьому ж рівні зазначена інформація є й інструментальною складовою безпосереднього оперативно-розшукового процесу. Її функцією значною мірою стає інформаційний вплив на розроблювані об'єкти та їхнє оточення для спонукання до визначених соціальних відносин і різних дій. Ці відносини та дії, як відомо, можуть свідчити про причетність фігурантів до конкретних злочинів, указувати на співучасників та інші злочинні зв'язки об'єктів оперативної розробки, вияв-

ляти сліди та знаряддя злочинів, речові докази, місця укриття злочинців, що переховуються, а також сховища цінностей, здобутих злочинним шляхом, розкривати причини й умови, які сприяють вчиненню злочинів, тощо.

Реалізація дієвої функції оперативно-розшукової інформації передбачає, з одного боку, отримання необхідних, тактично значущих для оперативної розробки відомостей, а з іншого боку, включення їх у порядку зворотного зв'язку в процес цієї розробки у вигідному для неї аспекті. У цьому полягає принципова схема «роботи» оперативно-розшукової інформації в ОРД, тобто впливу її на безпосередні об'єкти оперативної розробки.

Говорячи про отримання оперативними підрозділами тактичних відомостей, варто зауважити, що традиційні способи збирання їх негласними джерелами наштовхуються на доволі дієві контрзаходи з боку об'єктів ОРД. У сучасному злочинному середовищі це помітно виявляється в посиленні консолідації кримінальних елементів і конспірації їхньої злочинної діяльності, у підвищенні рівня поінформованості про методи ОРД, а також у здійсненні цілеспрямованих організаційних заходів щодо протидії витоку інформації зі свого середовища.

Тому сьогодні великого значення набуває опосередковане отримання оперативно-розшукової інформації в суміжних зі злочинним середовищем сферах, які охоплюють:

– інтимні зв'язки лідерів, членів організованих злочинних груп та інших осіб, наближених до цих груп;

– сімейно-побутові, родинні стосунки учасників злочинних груп;

– сфери проведення лідерами й членами груп дозвілля, зокрема місця перебування й осіб, які беруть у ньому участь;

– сфери задоволення споживацьких інтересів, особистого обслуговування тощо.

Зміст цієї інформації може бути найрізноманітнішим: від висвітлення способу життя, витрати коштів, отримання подарунків, вияву інтересу до окремих об'єктів, органів і фізичних осіб з боку розроблюваних (тих, що перевіряються) фігурантів до обговорення ними конкретних злочинних задумів, планів, наслідків скоєного, шляхів реалізації майна, здобутого злочинним шляхом, тощо.

Для збирання опосередкованої інформації в середовищі, яке становить інтерес, найчастіше використовуються природні життєві умови, звичні форми соціального спілкування тощо. Однак ці процеси можна активізувати в потрібному для ОРД напрямі, чому сприяє метод оперативного спілкування, який становлять специфічні інформативні, регулятивні та дієві компоненти. Цей метод дає змогу регулювати умови та форми міжособистісного, внутрішньогрупового та міжгрупового спілкування, створювати найбільш сприятливі умови для отримання цінної оперативно-розшукової інформації.

Існують три соціальні сфери, які насичують інформацією заходи ОРД організаційно-тактичного характеру щодо попередження, виявлення і припинення злочинів, розшуку злочинців, а також щодо виявлення й усунення причин та умов, що сприяють вчиненню злочинів:

1) середовище, у якому формуються оперативні контингенти й черпаються резерви їх поповнення (окремі особи та неформальні об'єднання з антигромадською або протиправною спрямованістю; місця концентрації таких осіб та об'єднань тощо);

2) середовище, у якому виявляються (діють) окремі особи та групи, підготовлюючи або вчиняючи злочини, переховуючись від органів досудового розслідування, прокуратури, суду або відбування кримінального покарання (громадські місця, підприємства, організації та установи, які становлять для них кримінальний інтерес: «чорні» ринки цінностей, автомобілів; підпільні гральні заклади; кубла для приїжджого злочинного елемента тощо);

3) сфери сімейно-побутових стосунків та особистого обслуговування об'єктів ОРД (родичі; нічні клуби, ресторани, кафе, інші розважальні заклади; повії; постачальники наркотиків; працівники та завсідники більярдних; обслуговуючий персонал лазень, саун, басейнів; масажисти, лікарі й інші особи, чиїх послуг потребують злочинці, та ін.).

Якщо перші дві сфери – це сфери суто злочинної діяльності оперативних контингентів, то третя – це місця або їх проживання, або звичного проводження часу.

І, нарешті, необхідно окреслити ще одну важливу функцію оперативно-розшукової інформації, а саме те, що вона знач-

ною мірою становить результат або підсумок ОРД. У цій якості оперативно-розшукова інформація реалізується у процесі ОРД згідно з її цілями та завданнями, які стоять перед оперативною розробкою конкретних об'єктів.

Це може бути інформація, необхідна для:

а) вирішення окремих тактичних завдань, наприклад для встановлення оперативним працівником психологічного контакту з особою, яка становить оперативний інтерес, спонукання об'єкта розробки до відвідання певних місць тощо;

б) досягнення цілей попередження, виявлення і припинення злочинів, розшуку злочинців, що переховуються;

в) забезпечення стратегічних цілей боротьби зі злочинністю, зокрема виявлення й усунення причин та умов, які сприяють вчиненню злочинів.

Ефективність використання оперативно-розшукової інформації в ОРД залежить від рівня її систематизації, концентрації та циркуляції, що врешті-решт забезпечує та зберігає її «тривалу» цінність. Сутність цієї ідеї закладена в автоматизованих інформаційно-пошукових системах.

В оперативно-розшуковому інформаційному процесі, як і в будь-якому іншому, діє принцип зворотного інформаційного зв'язку: що більше вихідних відомостей введено в обіг, то більше відповідей, що цікавлять, буде отримано з усіх упорядкованих джерел інформації. Це є особливо важливою умовою для процесу накопичення й руху негласної інформації, яка надходить від негласних джерел.

Наукові спостереження свідчать, що цей процес ще не забезпечує всіх практичних потреб ОРД. Однією з причин є те, що інформація, яка надходить до оперативних підрозділів, здебільшого використовується для вирішення локальних завдань, хоча значна її частина може бути реалізована неодноразово, багатопланово, кількома виконавцями й навіть оперативними підрозділами різних регіональних рівнів.

Усуненню цього недоліку може сприяти реалізація ідеї централізованого накопичення та проходження оперативно-розшукової інформації за такими принциповими схематичними моделями:

– інформація набуває універсального оперативно-тактичного характеру і корисності для інших оперативних

співробітників, а також для інших оперативних підрозділів у межах окремих органів Національної поліції;

– інформація набуває інтерес для оперативних підрозділів інших органів поліції, зокрема в межах регіонів, міжрегіональних кордонів, загалом по країні або в транснаціональних масштабах.

Саме ці вимоги мають стати основою системи циркуляції оперативно-розшукової інформації для того, щоб ця система могла забезпечувати:

– доступ до цінної інформації, яка має оперативно-тактичне значення, усіх заінтересованих оперативних працівників незалежно від просторових і внутрішньовідомчих розмежувань суб'єктів ОРД;

– пошук необхідних оперативно-розшукових даних у якомога коротші строки;

– підготовку управлінських рішень та оперативно-тактичних рекомендацій за окремими напрямами ОРД на регіональному, міжрегіональному рівнях і загалом у країні.

Ураховуючи широке використання в науковій літературі та нормативних документах одночасно понять «інформаційно-аналітичне забезпечення», «інформаційне забезпечення», «інформаційно-аналітична робота», «аналітична робота», проведемо спочатку порівняльне дослідження термінів «забезпечення» та «робота».

Термін «забезпечення» змістовно означає постачання чого-небудь у достатній кількості, а термін «робота» – заходи для виконання, здійснення чого-небудь.

У науковій літературі інформаційне забезпечення ОРД визначається як комплекс заходів, що здійснюються різними підрозділами правоохоронних органів, спрямованих на отримання з гласних та негласних джерел оперативно-значимої інформації, її фіксацію, зберігання, обробку, аналіз, а також використання первинних і збагачених даних з метою виконання оперативними підрозділами покладених на них функцій[2].

---

[2] Міжнародна поліцейська енциклопедія: у 10 т. / відп. редактори В. В. Коваленко, Є. М. Моісеєв, В. Я. Тацій, Ю. С. Шемшученко. – К.: Атіка, 2010. – Т. VI. Оперативно-розшукова діяльність поліції (міліції). – С. 349.

У юридичній літературі зазначається, що інформаційне забезпечення ОРД складається з трьох взаємопов'язаних компонентів:

1) *інформаційних систем,* у межах яких здійснюється збір, накопичення, системна обробка, зберігання й видача споживачу необхідної інформації;

2) *аналітичної роботи,* що полягає у здійсненні комплексу організаційних заходів і методичних прийомів з обробки та синтезу наявної оперативної та іншої інформації;

3) *управлінської діяльності,* яка забезпечує ухвалення необхідних рішень щодо стратегії і тактики протидії злочинності.

Інформаційні системи – це організаційно-технічні системи, в яких реалізуються технології обробки інформації з використанням технічних і програмних засобів. До складу інформаційних систем можуть входити інформаційні підсистеми, які містять банки даних, поєднані технологією обміну інформацією.

В ОРД засобом встановлення істини є аналітична робота. Термін «аналітичний» означає «стосується аналізу», заснований на застосуванні аналізу, тому можна використовувати словосполучення «аналітична робота» і «аналітична діяльність», як тотожні слову «аналіз».

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 з використанням географічного профілювання);

– *аналіз даних з відкритих джерел* (OSINT);

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

Для проведення аналізу застосовуються аналітичні інструменти, відповідне програмне забезпечення, а також наявні інформаційні ресурси.

Важливе значення в аналітичній роботі виконують аналітичні схеми. Складаються вони у непростих багатоепізодних справах, пов'язаних із діяльністю організованих злочинних груп, коли доводиться встановлювати способи вчинення ними злочинів, визначати зв'язки, які взаємно пересікаються між окремими учасниками злочину.

У науковій літературі управлінську діяльність у системі Національної поліції поділяють на внутрішньосистемну – спрямовану на упорядкування управлінських відносин, які виникають з питань організації самої системи та структури органів НПУ, та зовнішньосистемну управлінську діяльність, зміст якої зводиться до забезпечення співробітниками поліції функцій з охорони правовідносин[3].

У теорії та практиці ОРД із терміном «інформаційне забезпечення» вживається термін «інформаційно-аналітичне забезпечення», під яким розуміється кількісне (консолідація масивів інформації у вигляді баз і банків даних, упорядкування, систематизація), а також якісно-змістовне перетворення оперативної інформації (виробництво нових знань, ухвалення управлінських рішень) на основі інформаційної аналітики.

Головним завданням *інформаційно-аналітичного забезпечення* є систематичне і своєчасне надходження в оперативні підрозділи достовірної оперативної інформації.

У теорії та практиці ОРД вживається також термін «моніторинг» (від англ. *monitoring*, з лат. *monitor* – той, що наглядає і нагадує) – комплекс досліджень (спостереження, аналіз та інші методи пізнання) і контролю за станом чи процесами певного середовища прикладної системи, метою якого є попередження про появу шкідливих, небезпечних чи бажаних факторів (явищ) для існування цієї системи.

На теренах вітчизняної науки щораз частіше з інформаційно-аналітичним забезпеченням говорять про кримінальну розвідку. *Кримінальна розвідка* (оперативно-аналітична інформація) – це продукт збору, оцінки і інтерпретації інформації. Процес кримінальної розвідки є ланцюгом оперативних

---

[3] Голосніченко І. П. Адміністративне право України (основні категорії і поняття) / І. П. Голосніченко. – К.: ГАН, 2005. – С. 40–45.

дій або процедур, що призведуть до найточнішого і обґрунтованого висновку з цієї інформації.

За своїм характером кримінальна розвідка може бути загального характеру або спеціалізованою. Кримінальна розвідка загального характеру націлена на широкий спектр злочинних діянь, звичайно у сфері невеликих відомств або юрисдикцій. Спеціалізована кримінальна розвідка призначена для певного типу злочинної діяльності або об'єкту, як, наприклад, наркотики, промислове шпигунство або організована злочинність.

Кримінальна розвідка має тактичне і стратегічне застосування. Тактична кримінальна розвідка націлена на короткострокові завдання правоохоронних органів, передбачаючи негайні дії – затримання, накладення арешту, вилучення.

Своєю чергою, стратегічна кримінальна розвідка застосовується для більш масштабних довгострокових проблем і цілей, зокрема, для виявлення «крупних» фігур злочинного світу або синдикатів, прогнозування зростання видів злочинної діяльності та встановлення пріоритетів діяльності правоохоронних органів[4].

Консультативна місія ЄС підтримує впровадження в МВС і Національній поліції України моделі *поліцейської діяльності, керованої аналітикою* ***(Intelligence-Led Policing/ILP)***. ILP є моделлю поліцейської діяльності, згідно з якою оперативно-аналітична інформація/intelligence слугує підставою для проведення операцій/розслідувань, а не навпаки.

Розглянемо поняття «інформаційно-аналітична робота», яку у науковій літературі досліджують, по-перше, як елемент організації ОРД, тобто пошук, збирання, оцінка, аналіз, узагальнення даних, необхідних для ухвалення управлінського чи оперативного рішення; по-друге, як засіб отримання інформації в ОРД.

Інформаційно-аналітична робота в ОРД *– це передбачена законодавством України й урегульована відомчими*

---

[4] Основи оперативно-розшукової діяльності: навч. посібник / С. В. Албул, С. В. Андрусенко, Р. В. Мукоіда, Д. О. Ноздрін; за заг. ред. С. В. Албула. – Одеса: ОДУВС, 2016. – С. 167–168.

нормативними актами система заходів, спрямованих на збір, обробку, узагальнення, аналіз, зберігання та використання інформації, зокрема й обмеженого доступу, що має значення для вирішення завдань ОРД, в інтересах кримінального судочинства, безпеки громадян, суспільства і держави.

Виокремлюються три основні рівні інформаційно-аналітичної роботи в ОРД:

– *перший рівень* передбачає застосування її основ усіма працівниками оперативних та інформаційно-аналітичних підрозділів і певною мірою, іншими працівниками правоохоронних органів і негласними працівниками під час пошуку та фіксації фактичних відомостей про протиправну діяльність окремих осіб та груп, відповідальність за які передбачена КК України;

– *другий рівень* передбачає здійснення інформаційно-аналітичної роботи в процесі ведення ОРС та справ контрольного провадження, що здійснюється оперативними працівниками, які ведуть зазначені справи, а також спеціальними інформаційно-аналітичними підрозділами органів, уповноважених на здійснення ОРД;

– *третій рівень* – аналіз і прогнозування, що забезпечують ухвалення раціональних управлінських рішень у сфері ОРД і контроль за їх реалізацією, які проводяться організаційно-аналітичними структурами оперативних підрозділів правоохоронних органів та керівниками цих підрозділів.

Вирізняють такі складові поняття інформаційно-аналітичної роботи в ОРД та їх особливості:

1. *Інформаційно-аналітична робота в ОРД* – це система заходів (оперативно-розшукових, пошукових, розвідувальних, контррозвідувальних, організаційно-управлінських, технічних, аналітичних тощо), що передбачені законами України та врегульовані відомчими нормативними актами органів, уповноважених на здійснення ОРД, які визначають її порядок і умови.

2. *Суб'єктами* інформаційно-аналітичної роботи в ОРД є оперативні й інформаційно-аналітичні підрозділи та їх посадові особи та певною мірою інші працівники правоохоронних органів і негласні працівники.

3. *Об'єктами* інформаційно-аналітичної роботи в ОРД є фізичні та юридичні особи, корпоративні об'єкти, предмети, речовини, тварини, трупи, приміщення, споруди, ділянки місцевості, мережа Інтернет, явища, процеси, події, навички, зовнішні дії людини, радіоефір, трафіки зв'язків абонентів мобільного зв'язку тощо.

4. *Механізм* інформаційно-аналітичної роботи охоплює низку дій суб'єктів її здійснення (пошук, фіксацію, отримання, обробку, систематизацію, узагальнення, аналіз, прогнозування, зберігання та використання інформації).

5. *Предметом* інформаційно-аналітичної роботи в ОРД є характерні особливості чи ознаки об'єктів інформаційно-аналітичної роботи, зафіксовані на відповідних носіях або в пам'яті людей, або їх відображення.

6. *Основними засобами* інформаційно-аналітичної роботи в ОРД є: оперативна техніка та спеціальні технічні засоби, призначені для гласного та негласного отримання інформації; відповідні апаратно-програмні комплекси (автоматизовані інформаційно-пошукові, експертні та логіко-аналітичні системи тощо) і різні технічні пристрої, за допомогою яких здійснюється обробка, систематизація та аналіз оперативно-розшукових та інших відомостей фактографічного і криміналістичного характеру.

7. *Метою* інформаційно-аналітичної роботи є вирішення завдань ОРД, які полягають у пошуку та фіксації фактичних даних про протиправні діяння окремих осіб і груп, відповідальність за які передбачена КК України, та їх подальша обробка, систематизація, аналіз, прогнозування та використання з метою припинення правопорушень і в інтересах кримінального судочинства, безпеки громадян, суспільства і держави.

Важливу роль виконують принципи інформаційно-аналітичної роботи.

До *загальних принципів* інформаційно-аналітичної роботи в ОРД належать принципи верховенства права, законності, гуманізму; дотримання прав і свобод людини, конспірації; поєднання гласних і негласних методів і засобів; високої оперативності (наступальності); всебічності, повноти та об'єктивності; науковості; застосування досвіду і теоретичних знань інших суміжних наук.

Спеціальні принципи інформаційно-аналітичної роботи в ОРД пов'язані зі закономірностями, що випливають із сутності самого її процесу. До них належать: безперервність накопичення інформації, системність, узгодженість, варіантність, верифікованість, ефективність тощо.

Основними *інформаційними ресурсами*, що використовуються в процесі інформаційно-аналітичної роботи в ОРД, є:

– *оперативні обліки*, які складаються із оперативно-розшукових, оперативно-профілактичних та оперативно-довідкових обліків;

– *банки даних* криміналістичної, кримінологічної, адміністративної, статистичної інформації;

– *банки даних* інших міністерств, відомств, підприємств, установ та організацій, які не стосуються безпосередньо боротьби зі злочинністю;

– *банки даних* міських і обласних органів влади;

– *об'єкти* надання та отримання охоронних послуг;

– *оператори* мобільного зв'язку;

– *звернення та заяви* громадян, депутатські запити;

– *засоби* масової інформації, зокрема й Інтернет.

До *внутрішніх інформаційних ресурсів* належать бази даних: ІІПС Національної поліції, АІС оперативного призначення, ІП «Оперативно-довідкова картотека», ІП «Статистика», ІП «ІТТ», НАІС ЄДР МВС; Інтегрованої міжвідомчої автоматизованої системи обміну інформацією з питань контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон «Аркан»; фізичних та юридичних осіб, щодо яких надходили запити правоохоронних органів інших країн; паспортів громадян України для виїзду за кордон, іноземних громадян та осіб без громадянства; об'єкти надання та отримання охоронних послуг поліції охорони; криміналістичні обліки; відкриті джерела, ЗМІ, інформаційні ресурси Інтернет; звернення та заяви громадян, депутатські запити.

До *зовнішніх інформаційних ресурсів* належать банки даних інших правоохоронних органів; банки даних інших міністерств, відомств, підприємств, установ та організацій, які не стосуються безпосередньо боротьби зі злочинністю; банки даних обласних і міських органів влади; оператори мобільного зв'язку.

Важливу роль в інформаційно-аналітичній роботі в ОРД виконують *інформаційно-аналітичні технології*, які визначаються як сукупність методів, технологічних процесів і програмно-технічних засобів, інтегрованих з метою збирання, обробки, систематизації, узагальнення, аналізу, зберігання та використання інформації, зокрема й обмеженого доступу, що має значення для вирішення завдань ОРД, в інтересах досудового слідства, безпеки громадян, суспільства і держави.

У МВС створена і функціонує *єдина цифрова відомча телекомунікаційна мережа МВС (далі – ЄЦВТМ)*. ЄЦВТМ є сучасною логічно цілісною мультисервісною багаторівневою інформаційно-телекомунікаційною мережею МВС, що здійснює взаємодію із загальнодержавними телекомунікаційними мережами спеціального зв'язку та включає сукупність технічних засобів й обладнання мережі доступу і транспортної телекомунікаційної мережі для забезпечення передання інформації (даних), яка (які) належить (належать) до державних інформаційних ресурсів регіонального (між МВС, Національною гвардією України, центральними органами виконавчої влади, діяльність яких спрямовує та координує Міністр внутрішніх справ України, Автономною Республікою Крим, областями, містами Київ та Севастополь), районного та міського рівнів, для потреб користувачів, а також надає підключеним до неї віддаленим один від одного користувачам системи МВС весь різновид телекомунікаційних послуг і сервісів фіксованого телефонного, документального, радіозв'язку, аудіо- та відеоселекторного зв'язку тощо і у звичайних умовах, і під час особливого періоду чи запровадження в державі надзвичайного стану.

Основними завданнями інформатизації ОРД на сучасному етапі є:

– збирання, обробка й накопичення якісної та вірогідної інформації в базах даних за всіма напрямами діяльності оперативних підрозділів поліції;

– забезпечення оперативного доступу користувачів (оперативних працівників) до баз даних безпосередньо з робочих місць;

– використання сучасних аналітичних методів обробки оперативно-розшукової інформації;

– використання ресурсів невідомчих інформаційних систем з метою забезпечення правоохоронної діяльності багатовидовою інформацією;

– визначення перспективних напрямів та тенденцій розвитку сучасної злочинності;

– адаптація існуючих положень тактики і методики ОРД до умов сучасного інформаційного суспільства;

– розроблення, упровадження та використання спеціального програмного забезпечення.

1.3. Основні форми інформаційно-аналітичної роботи в оперативно-розшуковій діяльності

Форма інформаційно-аналітичної роботи – це зовнішнє вираження змісту. Вона визначає зовнішню «конфігурацію» інформаційно-аналітичної роботи, окремих її складових, характеризує їх реалізацію в просторі і в часі. Форму інформаційно-аналітичної роботи можна також розглядати як спосіб її існування.

Формою інформаційно-аналітичної роботи є внутрішня і зовнішня організація її системи. Інформаційно-аналітична робота у будь-якій сфері людського буття передбачає певні форми своєї реалізації, зумовлені особливостями застосовуваних засобів і методів, а також специфікою отриманих результатів.

Основними формами інформаційно-аналітичної роботи в ОРД є:

– отримання оперативно-розшукової інформації;

– систематизація оперативно-розшукової інформації;

– оперативно-розшукова ідентифікація;

– оперативно-розшукова діагностика;

– оперативно-розшукове прогнозування;

– аналітична розвідка.

1.3.1. Отримання оперативно-розшукової інформації

Отримання оперативно-розшукової інформації – *це одна із форм інформаційно-аналітичної роботи в ОРД, у межах якої відбувається пошук і фіксація відомостей про проти-*

правні діяння окремих осіб та груп, з використанням наявних сил, засобів і методів ОРД, в інтересах ОРД та досудового розслідування.

Отримання оперативно-розшукової інформації – це початковий етап інформаційно-аналітичної роботи і зводиться до оперативно-пошукової роботи в певному соціальному середовищі, у певних верствах населення, на певних промислових й інших господарських об'єктах, у певних інфраструктурних утвореннях тощо.

Пошук оперативно-розшукової інформації пропонується вести найперше у традиційному середовищі оперативних контингентів:

– раніше судимі особи, насамперед за злочини, учинені в складі злочинних груп;

– прямі співучасники, підсобники, збувальники, які проходили у кримінальних провадженнях про групові злочини і не притягнуті з різних причин до кримінальної відповідальності;

– кримінальні авторитети;

– особи, які ведуть чітко виражений антигромадський і протиправний спосіб життя;

– представники тіньового бізнесу, сумнівних торговельних, валютних структур тощо.

Інформаційне середовище охоплює бази даних державних і недержавних підприємств; інформаційні системи правоохоронних органів і спецслужб; оперативні обліки, архіви, перевірочні матеріали; окремих людей (їх досвід і знання), колективи; відомості, що циркулюють у розроблюваних злочинних угрупованнях. Це середовище розглядається не як джерело, з якого може бути отримана інформація, а як інформаційні ресурси, які потребують розробки.

Основний ресурс безпосередньо оперативно-розшукової інформації міститься в матеріалах, що накопичуються під час перевірки первинних відомостей про злочини та осіб, які їх вчинили (зокрема звернення і заяви громадян, повідомлення про кримінальні правопорушення, зниклих осіб, документи, що містять результати виконання доручень слідчих, прокурорів і суду, відповіді захисту, агентурні повідомлення, інші оперативно-службові документи).

Потужним ресурсом для добування оперативно-розшукової інформації в сучасних умовах є, зокрема, відомості, зосереджені в ЗМІ та мережі Інтернет, які є одними з найважливіших ресурсів оперативно-розшукової інформації.

До ресурсів оперативно-розшукової інформації належать також банки даних різних служб правоохоронних органів, податкових і митних служб, реєстраційних органів, фондів медичного та соціального страхування, медичних установ, банків і фінансових компаній, транспортних підприємств, авіа- та залізничних кас й багато інших.

Паралельно з пошуком і обробкою інформації в інформаційно-аналітичних підрозділах правоохоронних органів здійснюється пошук інформації в державних і недержавних інформаційно-аналітичних центрах. У процесі здобуття інформації можливе і надсилання офіційних письмових запитів керівникам підприємств, установ і організацій для надання ними відповідних відомостей, і особисте отримання цих відомостей оперативними працівниками під час здійснення оперативно-пошукових заходів.

До сучасних перспективних технологій та технічних засобів отримання оперативно-розшукової інформації належить аерофотозйомка з використанням безпілотних літальних апаратів і космічна розвідка. Зокрема вже є досвід використання повітряних і космічних апаратів для виявлення посівів різноманітних культур, які є сировиною для виробництва наркотиків, розробки родовищ корисних копалин без ліцензії, незаконної вирубки лісових насаджень тощо.

Оперативно-розшукова інформація про діяльність лідерів злочинних угруповань або про складні технології злочинного бізнесу:

– добувається із залученням низки різноманітних відкритих і оперативно-організаційних інформаційних ресурсів шляхом застосування спеціальних технічних засобів та комп'ютерних технологій, дозволених законом;

– проходить обробку, зокрема очистку (аудіо-, відео), ідентифікацію (голосів, слідів), структурування (текстових даних) за офіційно прийнятими методиками;

– аналізується шляхом застосування надійно апробованих потужних логіко-математичних методів аналітичного та імітаційного моделювання;

– візуалізується і озвучується на основі мультимедійних технологій, здійснюючи інформаційне «зшивання» кримінального провадження і наочне подання його в судовому процесі[5].

Складові елементи поняття отримання оперативно-розшукової інформації:

суб'єктами отримання оперативно-розшукової інформації є оперативні, оперативно-технічні, інформаційно-аналітичні підрозділи та їх посадові особи і певною мірою інші працівники Національної поліції та негласні працівники;

об'єктами отримання оперативно-розшукової інформації є фізичні та юридичні особи, корпоративні об'єкти, предмети, речовини, тварини, трупи, приміщення, споруди, ділянки місцевості, ЗМІ, мережа Інтернет, інформаційні системи та банки даних, явища, процеси, події, навички, зовнішні дії людини, радіоефір, трафіки зв'язків абонентів мобільного зв'язку тощо;

механізм отримання оперативно-розшукової інформації включає низку дій (пошук, добування, фіксацію, обробку інформації) з використанням наявних сил, засобів і методів ОРД;

предметом отримання оперативно-розшукової інформації є характерні особливості чи ознаки об'єктів отримання оперативно-розшукової інформації, зафіксовані на відповідних носіях або в пам'яті людей, або їх відображення;

метою отримання оперативно-розшукової інформації є вирішення завдань ОРД, які полягають у пошуку та фіксації відомостей про протиправні діяння окремих осіб і груп, з використанням наявних сил, засобів і методів ОРД, за якими після їх оцінки та аналізу ухвалюється рішення щодо подальшого використання отриманої інформації в інтересах ОРД та досудового розслідування.

1.3.2. Систематизація оперативно-розшукової інформації

Систематизація оперативно-розшукової інформації *– це одна із форм інформаційно-аналітичної роботи в ОРД, у межах якої здобуті відомості про протиправні діяння окремих*

---

[5] Овчинский А. С. Информация и оперативно-розыскная деятельность: монография / под ред. В. И. Попова. – М.: ИНФРА-М, 2002. – С. 56–57.

осіб та груп приводяться в систему за допомогою технічних і програмних засобів з метою подальшої їх оцінки, аналізу та використання отриманої інформації в інтересах ОРД та досудового розслідування.

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» обробка інформації в системі – це виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

Ефективного вирішення профілактичних і оперативно-тактичних завдань можна досягти тільки на основі систематизованої, комплексної інформації, що поєднує різні відомості, які отримані з різних логічно пов'язаних джерел.

Великий тлумачний словник сучасної української мови тлумачить поняття «систематизація» як приводити в систему. Відомості, які збираються оперативними підрозділами у процесі ОРД, необхідно систематизувати так, щоб у будь-який час без перешкод можна було розшукати потрібну інформацію для її використання в інтересах вирішення оперативно-тактичних і кримінально-процесуальних завдань.

Якість систематизованої інформації визначається низкою вимог, що висуваються до оперативно-розшукової інформації, а саме:

оптимальність, повнота;

точність;

лаконічність повідомлень;

логічність викладення;

цінність (корисність).

Система оперативно-розшукової інформації повинна:

– бути сукупністю банків даних оперативного, профілактичного та довідкового призначення, реалізованих на основі сучасних інформаційних і телекомунікаційних технологій;

– бути такою, що легко управляється, надійною і зрозумілою користувачам (оперативним працівникам);

– працювати в режимі, розрахованому на багато користувачів (оперативних працівників);

– швидко обробляти величезні масиви відомостей, миттєво відстежуючи зміни, що вносяться різними користувачами;

– легко змінюватися й модернізуватися, а також мати можливість вбирати кращі досягнення науки;

– обробляти різну, навіть найбільш неструктуровану інформацію, автоматично її впорядковуючи;

– відповідати жорстким вимогам безпеки інформації, органічно підтримувати різні рівні доступу до даних для різних користувачів.

Важливе значення для систематизації оперативно-розшукової інформації мають ***оперативні обліки****, які розглядаються як система реєстрації, накопичення, класифікації, зберігання та використання даних про осіб, предмети, події за їх прикметами та ознаками, призначена для ефективного забезпечення ОРД оперативних підрозділів правоохоронних органів, яка складається із АІС, картотек, ОРС, справ контрольного-наглядового провадження та інших документів оперативно-розшукового та довідкового призначення.*

Головне призначення оперативних обліків полягає в тому, що вони забезпечують:

– проведення оперативно-розшукових, пошукових та інших заходів у сфері попередження, розкриття та розслідування злочинів;

– зберігання оперативно значущої інформації упродовж тривалого часу;

– недопущення повторного збирання оперативно-розшукової інформації, яка вже зберігається у банках даних правоохоронних органів;

– можливість своєчасного використання раніше отриманих відомостей оперативними підрозділами з різними рівнями доступу;

– організацію ефективної взаємодії оперативних підрозділів між собою, а також з іншими підрозділами та правоохоронними органами;

– запобігання призначенню осіб, які підозрюються у вчиненні злочинів, на посади, робота на яких пов'язана з документами, що становлять державну таємницю.

Оперативні обліки складаються із оперативно-розшукових, оперативно-профілактичних та оперативно-довідкових обліків.

Оперативно-розшуковий облік призначений для інформаційного забезпечення ОРД оперативних підрозділів. Цей облік ведуть спеціально призначені працівники оперативних підрозділів, які мають право на здійснення ОРД.

Оперативно-профілактичний облік призначений для інформаційного забезпечення індивідуально-профілактичної роботи з особами з кримінального середовища. Цей облік ведеться оперативними підрозділами щодо криміногенних осіб, проти яких немає достатніх підстав для заведення ОРС.

Оперативно-довідковий облік призначається для вирішення таких основних завдань:

– установлення особи затриманих і заарештованих;

– отримання даних про злочинну діяльність у минулому осіб, стосовно яких здійснюється провадження в ОРС;

– перевірка первинних даних щодо кримінальної активності осіб, які потрапили в поле зору оперативних працівників;

– установлення місця знаходження архівних кримінальних справ і ОРС;

– установлення місць відбування покарання конкретних осіб;

– перевірка осіб, з якими буде встановлене конфіденційне співробітництво на засадах добровільності;

– установлення фактів затримання за бродяжництво та жебракування.

Складові поняття систематизації оперативно-розшукової інформації:

суб'єктами систематизації оперативно-розшукової інформації є оперативні, оперативно-технічні, інформаційно-аналітичні підрозділи та їх посадові особи;

об'єктами систематизації оперативно-розшукової інформації є здобуті відомості про протиправні діяння окремих осіб та груп;

механізм систематизації оперативно-розшукової інформації охоплює низку операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення,

реєстрацію, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

предметом систематизації оперативно-розшукової інформації є і відкрита інформація, й інформація обмеженого доступу, до якої належить конфіденційна, таємна та службова інформація, яка обробляється в інформаційних системах та банках даних;

метою систематизації оперативно-розшукової інформації є приведення в систему здобутих відомостей про протиправні діяння окремих осіб та груп за допомогою технічних і програмних засобів, з метою подальшої їх оцінки, аналізу та використання отриманої інформації в інтересах ОРД та досудового розслідування.

1.3.3. Оперативно-розшукова ідентифікація

Оперативно-розшукова ідентифікація *– це форма інформаційно-аналітичної роботи в ОРД, спрямована на встановлення тотожності об'єкта або особи за сукупністю загальних і окремих ознак шляхом їх порівняльного дослідження з використанням сил, засобів і методів ОРД.*

Будь-яке протиправне діяння залишає в навколишньому середовищі різні сліди (відображення). Під час розкриття злочину виникає закономірна необхідність встановити за цими слідами зв'язок людини, предмета або іншого об'єкта з розслідуваною подією. Одним із основних засобів відшукання істини в цьому разі є встановлення тотожності, або ідентифікація.

Великий тлумачний словник сучасної української мови тлумачить термін «ідентифікація» як засіб встановлення тотожності особи за сукупністю її загальних та окремих даних.

Основне завдання криміналістичної ідентифікації – встановлення фактів, що мають значення доказів у кримінальному судочинстві, у зв'язку з чим вихідним матеріалом для встановлення тотожності об'єктів можуть слугувати лише ті факти, які отримані та задокументовані відповідно до вимог кримінально-процесуального законодавства, що є гарантією об'єктивності й достовірності їх походження.

Оперативно-розшукова ідентифікація має аналогічну мету, тому зафіксовані у відповідних службових документах

її результати також можуть бути подані у встановленому законом порядку в розпорядження слідчого, прокурора або до суду.

Ідентифікація проводиться за спеціально відібраними стійкими властивостями, так званими «ідентифікаційними ознаками», за допомогою яких можна відрізнити об'єкт від інших, йому подібних. Ідентифікаційні ознаки можуть виявлятися на ідентифікуючих об'єктах у таких формах відображення властивостей ідентифікованих об'єктів:

різні сліди (сліди рук, ніг, знарядь злому, транспортних засобів тощо);

уявних образів (чуттєво-конкретних відображень), які з'являються у свідомості людей в результаті зорового або іншого сприйняття (прикмети злочинця, особливості ділянки місцевості, зафіксовані в пам'яті потерпілого, свідка тощо);

зображень, до яких можна віднести фотографії, аудіо- та відеозаписи;

трафіків зв'язків абонентів мобільного зв'язку на місці вчинення злочину;

характерних особливостей окремих частин предметів (фрагментів знарядь злому; осколків скла, вилучених на місці пригоди тощо) [6].

Дослідження предметів і документів здійснюється оперативним працівником або за його дорученням експертно-криміналістичними та іншими підрозділами правоохоронних органів, іншими організаціями і установами, а також приватними особами, зокрема й на конфіденційній основі.

Із особами, предметами і документами до переліку ідентифікованих об'єктів, тотожність яких може бути встановлена під час проведення цього заходу, відносять також тварин, трупи людей, приміщення, споруди, ділянки місцевості, речовини тощо.

Оперативне ототожнення осіб, предметів та речовин проводиться у випадках, коли пред'явлення для впізнання,

---

[6] Гинзбург А. Я. Опознание в следственной, оперативно-розыскной и экспертной практике : учебно-практическое пособие / А. Я. Гинзбург; под ред. проф. Р. С. Белкина. – М.: Ассоциация работников правоохранительных органов, 1996. – С. 58–61.

передбачене кримінально-процесуальним законодавством, неможливо здійснити з різних обґрунтованих причин, але сам акт пізнавання можливий, доцільний, необхідний і здійсним оперативно-розшуковим шляхом.

Оперативне ототожнення особи поділяється на види:

– *безпосереднє*, що проводиться за статичними (біометричні персональні дані) і динамічними (хода, жестикуляція, мімічка тощо) ознаками;

– *опосередковане* – за словесним портретом, фотороботом, скульптурним портретом тощо.

В ОРД широко використовується оперативне ототожнення предметів та речовин, зокрема, впізнання викрадених речей у процесі особистого пошуку та оперативного огляду місця, встановлення під час митного контролю творів мистецтва, призначених для незаконного вивозу за кордон, інших незадекларованих товарів тощо.

Наведення довідок – це оперативно-розшуковий захід, який спрямований на отримання інформації про фізичних осіб, факти та обставини, що мають значення для вирішення завдань ОРД, шляхом безпосереднього вивчення документів, матеріалів баз даних, спрямування запитів на підприємства, в установи та організації, іншим юридичним, а також фізичним особам, які мають у своєму розпорядженні або можуть володіти зазначеною інформацією[7].

Відповідно до п. 4 ст. 8 Закону про ОРД оперативні підрозділи мають право з дозволу слідчого судді в порядку, передбаченому КПК, витребовувати документи та дані, що характеризують діяльність підприємств, установ, організацій, а також спосіб життя окремих осіб, підозрюваних у підготовці або вчиненні злочину, джерело та розміри їх доходів.

Складові поняття оперативно-розшукової ідентифікації:

– *суб'єктами* оперативно-розшукової ідентифікації є оперативні, оперативно-технічні, інформаційно-аналітичні

---

[7] Халиков А. Н. Юридическое, техническое и информационно-аналитическое обеспечение оперативно-розыскной деятельности: учебное пособие / А. Н. Халиков, Е. Н. Яковец, Н. И. Журавленко; под редакцией А. Н. Халикова. – М.: Юрлитинформ, 2010. – С. 386.

підрозділи та їх посадові особи і певною мірою інші працівники Національної поліції та негласні працівники;

– *об'єктами* оперативно-розшукової ідентифікації є фізичні та юридичні особи, корпоративні об'єкти, предмети, речовини, тварини, трупи, приміщення, споруди, ділянки місцевості, мережа Інтернет, явища, процеси, події, навички, зовнішні дії людини, радіоефір, трафіки зв'язків абонентів мобільного зв'язку тощо;

– *предметом* оперативно-розшукової ідентифікації є ідентифікаційні ознаки, які можуть виявлятися на ідентифікуємих об'єктах у вигляді: різних слідів; уявних образів, які з'являються у свідомості людей внаслідок зорового або іншого сприйняття; зображень, до яких можна віднести фотографії, аудіо- та відеозаписи; трафіків зв'язків абонентів мобільного зв'язку на місці вчинення злочину; характерних особливостей окремих частин предметів;

механізм оперативно-розшукової ідентифікації охоплює низку послідовних дій суб'єкта його застосування: роздільне дослідження ознак ідентифікованого та ідентифікуючого об'єктів; їх порівняльне дослідження; оцінку результатів порівняння; прогноз подальших дій, ухвалення рішення;

метою оперативно-розшукової ідентифікації є емпіричне виявлення за заздалегідь відомими загальними ознаками об'єктів ідентифікації, а також отримання нових знань про ці об'єкти з метою припинення правопорушень та в інтересах кримінального судочинства, безпеки громадян, суспільства і держави.

1.3.4. Оперативно-розшукова діагностика

Оперативно-розшукова діагностика *– це форма інформаційно-аналітичної роботи в ОРД, спрямована на емпіричне виявлення криміногенних осіб, злочинів та пов'язаних з ними предметів, речовин і документів за заздалегідь відомими загальними ознаками, на підставі оцінки об'єктів, які розпізнаються, а також отримання нових знань про ці об'єкти з метою припинення правопорушень та в інтересах кримінального судочинства, безпеки громадян, суспільства і держави.*

Великий тлумачний словник сучасної української мови роз'яснює термін «діагностика» як загальну процедуру перевірки функціонування системи.

Суть будь-якої діагностики полягає в тому, що на основі розпізнавання об'єкта, схожого з уже відомими подібними об'єктами, визначаються його властивості, стан, зміни, зв'язки зі зовнішнім середовищем тощо. Принциповою відмінністю діагностики від ідентифікації є та обставина, що при ідентифікації робота на аналітичній стадії відбувається з урахуванням ступеня зіставлення двох об'єктів: шуканого і перевіряємого. У діагностиці перевіряємого об'єкта немає, його ще потрібно знайти. На аналітичній стадії діагностичного процесу йдеться про виокремлення ознак тільки шуканого об'єкта.

Сучасна діагностика в ОРД ґрунтується на трьох основних складових: уміння спостерігати, знання людської натури і здатність до розроблення версій.

До основних *видів оперативно-розшукової діагностики* належать:

– оперативне розпізнання;

– опитування, що проводиться з використанням технічних засобів;

– нетрадиційні методи, пов'язані з інструментальною діагностикою емоційного стану;

– оперативно-розшукова дія «розробка оперативно-розшукової версії»;

– діагностична складова ОРЗ «дослідження предметів і документів».

Надзвичайно важливим видом оперативно-розшукової діагностики є здійснення *моніторингу переговорів абонентів мобільного зв'язку* на території, прилеглій до місця вчинення злочину, з метою перевірки їх причетності до протиправних дій.

Одним із основних видів оперативно-розшукової діагностики вважається оперативне розпізнання (особистий пошук).

Особистий пошук – це оперативно-розшуковий захід, що полягає у безпосередньому застосуванні працівником оперативного підрозділу прийомів розпізнання злочинців, негласного спостереження, оперативної установки й агентурної

роботи для запобігання та викриття злочинів, розшуку зниклих злочинців і громадян, які пропали безвісти.

Оперативне розпізнання – це пізнавальна (емпірична) частина оперативного пошуку – діяльності, спрямованої на виявлення об'єктів, які становлять оперативний інтерес.

Пошукові заходи можуть здійснюватися:

– у криміногенних групах;

– у середовищі затриманих і заарештованих;

– у місцях найбільш можливого вчинення злочинів;

– на транспорті;

– на контрольних пунктах перетину кордону;

– на митних постах;

– у зонах дії надзвичайного стану;

– у радіоефірі;

– у мережі Інтернет тощо.

Об'єкти оперативного розпізнання заздалегідь не відомі оперативному працівнику, який здійснює їх встановлення (пошук). Однак він володіє інформацією про стереотипний перелік характерних ознак, які вирізняють їх серед інших подібних об'єктів. Цим даний вид кримінального аналізу відрізняється від ототожнення, під час якого ініціатору пошуку заздалегідь відомі ідентифікаційні ознаки встановлюваного об'єкта, що дає змогу в окремих випадках констатувати наявність тотожності останнього з наявним у оперативного працівника відображенням його ознак. У процесі оперативного розпізнання ініціатору достатньо лише виявити об'єкт, який за відповідними ознаками відноситься до відповідного класу.

Оперативне розпізнання особи, на відміну від ототожнення, не передбачає виявлення всього класичного переліку ознак зовнішності людини, що використовується, наприклад, при складанні словесного портрета (індивідуальні анатомічні особливості обличчя, голови, тулуба, кінцівок тощо). Розпізнаються, як правило, лише найбільш помітні або особливі прикмети – татуювання, сліди характерних травм, операцій, наслідки захворювань тощо.

До специфічних особливостей зовнішності фізичної особи та її одягу належать ознаки, що вказують на вчинений злочин. Це ознаки, які відображаються на тілі, одязі або наявні в жит-

лі кримінально активних осіб у вигляді слідів злочину (сліди боротьби з жертвою злочину, сліди крові, сліди сигналітичних речовин тощо).

Актуальність цієї групи ознак визначається положеннями кримінально-процесуального законодавства, що передбачає право уповноваженої службової особи без ухвали слідчого судді, суду затримати особу, підозрювану у вчиненні злочину, за який передбачене покарання у виді позбавлення волі, у випадках:

– якщо цю особу застали під час вчинення злочину або замаху на його вчинення;

– якщо безпосередньо після вчинення злочину очевидець, зокрема й потерпілий, або сукупність очевидних ознак на тілі, одязі чи місці події вказують на те, що саме ця особа щойно вчинила злочин (ст. 208 КПК).

Наступний вид функціональних ознак, що дають змогу розпізнати осіб, які становлять інтерес для ОРД, і які не пов'язані з вчиненням ними конкретних злочинів, – це їх професійні навички, уміння і звички, що характеризують можливу належність до кримінального середовища, зокрема:

– навички застосування стрілецької і холодної зброї та вибухової справи;

– навички виготовлення кліше для різних поліграфічних робіт;

– навички злому комп'ютерних систем та створення комп'ютерних «вірусів» тощо.

Складові поняття оперативно-розшукової діагностики:

суб'єктами оперативно-розшукової діагностики є оперативні, оперативно-технічні, інформаційно-аналітичні підрозділи та їх посадові особи і певною мірою інші працівники Національної поліції та негласні працівники;

– *об'єктами* оперативно-розшукової діагностики є криміногенні особи, події, факти, явища та пов'язані з ними предмети, речовини і документи, які становлять оперативний інтерес для оперативних підрозділів;

– *предметом* оперативно-розшукової діагностики є функціональні ознаки, які характеризують кримінально активних осіб, кримінальні правопорушення, події, факти, явища та пов'язані з ними предмети, речовини і документи;

– *механізм* оперативно-розшукової діагностики охоплює низку послідовних дій суб'єкта його застосування: розпізнання, прогноз подальших дій, ухвалення рішення;

– *метою* оперативно-розшукової діагностики є емпіричне виявлення за заздалегідь відомими загальними ознаками об'єктів діагностики, а також отримання нових знань про ці об'єкти з метою припинення правопорушень та в інтересах кримінального судочинства, безпеки громадян, суспільства і держави.

1.3.5. Оперативно-розшукове прогнозування

Оперативно-розшукове прогнозування *– це форма інформаційно-аналітичної роботи в ОРД, яка полягає в організації процесу наукового передбачення майбутнього на основі оперативного аналізу минулого та сьогодення на підставі раніше зібраної оперативної інформації.*

В умовах протидії організованій, транснаціональній злочинності особливої актуальності набуває вміння передбачити розвиток криміногенної ситуації, запобігти розвитку подій у небажаному напрямку. Зазначені чинники вимагають від правоохоронних органів застосування відповідних заходів, засобів і методів боротьби зі злочинністю, впровадження сучасних прийомів і форм інформаційно-аналітичної роботи. сьогодні однією з таких форм є *оперативно-розшукове прогнозування*.

Прогнозування – це адміністративно-управлінська діяльність керівництва правоохоронного органу, яка здійснюється на основі аналізу стану оперативної обстановки, що дає можливість своєчасно виявити проблеми, тенденції, суперечності в організації боротьби зі злочинністю, правильно оцінювати та здійснювати пошук шляхів і засобів їх вирішення, обґрунтувати ухвалення управлінських рішень.

Великий тлумачний словник сучасної української мови визначає прогноз як передбачення на основі наявних даних напряму, характеру та особливостей розвитку й закінчення явищ і процесів у природі й суспільстві.

Оперативним підрозділам для виконання завдань оперативно-розшукової діяльності за наявності передбачених Законом про ОРД підстав при безпосередньому ви-

конанні своїх повноважень надається право здійснювати інформаційно-аналітичне прогнозування оперативної обстановки та криміногенної ситуації.

Прогнозування оперативної обстановки здійснюється шляхом висунення на основі інформації, що надходить, оперативно-розшукових версій про можливі дії осіб, схильних до скоєння правопорушень; про умови, що сприяють учиненню економічних і кримінальних правопорушень; про ймовірні методи приховування слідів учинених і здійснюваних злочинів тощо.

Основні види оперативно-розшукового прогнозування:

– *стратегічне прогнозування* тенденцій та чинників середовища функціонування, кримінологічної обстановки, сил та засобів правоохоронних органів, результативності протидії злочинності, громадської думки про стан середовища фукціонування, криміногенної ситуації, результативності діяльності правоохоронних органів;

– *оперативно-тактичне прогнозування*, що полягає у розробленні оперативно-розшукових версій розвитку ситуації, які сприяють здійсненню оперативно-розшукових заходів для вирішення конкретних завдань ОРД.

Під ***стратегічним прогнозуванням*** розуміється формування уявних моделей, що відображають:

– *імовірність розвитку* оперативної обстановки в будь-якому регіоні, на території окремі країни або низки держав;

– *можливість вияву* кримінальної активності великих організованих кримінальних структур, зокрема міжнародних, терористичних тощо;

– *перспективи появи* нових каналів незаконного постачання наркотиків, зброї, вибухових речовин та пристроїв, інших об'єктів, вилучених з цивільного обігу; нових потоків незаконної міграції;

– *вплив загальних* криміногенних процесів на тенденції розвитку злочинності в окремих регіонах;

– *вплив соціально-економічних*, демографічних, екологічних та інших чинників на тенденції та рівень злочинності;

– *тенденції розвитку* оперативної обстановки залежно від вжиття заходів, спрямованих на її стабілізацію тощо.

Основна мета ***оперативно-тактичного прогнозування*** полягає в розробленні та актуалізації оперативно-розшукових версій. До найперспективніших напрямів такого прогнозування належать такі:

– прогнозування ймовірної поведінки злочинних груп і неформальних об'єднань з антигромадською спрямованістю – для визначення необхідності, форм і методів профілактики;

– прогнозування індивідуальної злочинної поведінки – з тією ж метою;

– прогнозування ймовірної ситуації, яка може виникнути в період оперативної перевірки і розробки;

– прогнозування ймовірної поведінки осіб, які сприяють органам, уповноваженим на здійснення ОРД, у певних умовах.

Важливе значення для здійснення оперативно-розшукового прогнозування мають загальнонаукові та прикладні методи. До загальнонаукових методів належать: спостереження, опис, аналіз, синтез, індукція та дедукція, абстрагування, аналогія, порівняння, моделювання, експеримент тощо.

Методами, розробленими зарубіжною прогностикою, які застосовуються під час вирішення завдань інформаційно-аналітичної роботи, є:

– метод колективної експертної оцінки (*метод Дельфі*);

– метод колективної генерації ідей (*метод мозкової атаки*);

– метод складання сценаріїв (*метод Жерардена*);

– нормативні методи прогнозування (*метод Г. Лінстауна*).

Зазначені методи використовуються під час стратегічного і оперативно-тактичного прогнозування.

Із розглянутими методами у прогностиці використовуються і методи математичного моделювання, наприклад, прогнозування процесів злочинності за допомогою штучних нейронних мереж, що становлять математичні моделі, в основі яких є сучасні уявлення про будову мозку людини і здійснюваних у ньому процесах обробки інформації.

В оперативно-розшуковому прогнозуванні широко застосовуються методи статистичної екстраполяції, які ґрунтуються на припущенні про збереження в майбутньому минулих і сьогоднішніх тенденцій розвитку об'єкта прогнозування. Од-

нак екстраполяція даних за межі часового інтервалу дає змогу прогнозувати стан об'єкта тільки на найближче майбутнє.

Залежно від терміна оперативно-розшукове прогнозування може бути:

– для планування та проведення окремого заходу або оперативно-розшукової операції;

– короткострокове – квартал, півріччя, рік;

– середньострокове – до 5 років;

– довгострокове – 10–15 років.

Складові поняття оперативно-розшукового прогнозування:

– *суб'єктами* оперативно-розшукового прогнозування є оперативні, оперативно-технічні, інформаційно-аналітичні підрозділи та їхні посадові особи і певною мірою інші працівники Національної поліції та негласні працівники;

– *механізм* оперативно-розшукове прогнозування передбачає низку дій суб'єкта його застосування (аналіз, складання прогнозу, ухвалення рішення);

– *предметом* оперативно-розшукового прогнозування є відкрита інформація й інформація обмеженого доступу, до якої належить конфіденційна, таємна та службова;

– *метою* оперативно-розшукового прогнозування є наукове передбачення майбутнього на основі оперативного аналізу минулого та сьогодення на підставі раніше зібраної оперативної інформації.

1.3.6. Аналітична розвідка

Аналітична розвідка *– це особлива форма інформаційно-аналітичної роботи в ОРД, яка заснована на органічній єдності всіх форм цієї роботи і полягає у набутті нових знань про об'єкт чи явище на основі аналітичної обробки здобутої оперативно-розшукової інформації про осіб, події, предмети, що становлять оперативний інтерес.*

У перекладі з грецького слово «аналіз» (analysis) означає розкладання, розчленування. Аналіз може бути предметним, або логічним, уявним.

Розвідка полягає у здійсненні організаційних і технічних заходів щодо добування інформації про супротивника та обстановку, що склалася.

Як свідчить лінгвістичний аналіз, одним із значень іменника «розвідка» є слово «пошук» («розшук» або «обстеження чого-небудь зі спеціальною метою»). Тому словосполучення «аналітична розвідка» і «аналітичний пошук» цілком можна розглядати як синоніми.

Досвід роботи кримінальної поліції зарубіжних країн свідчить про неефективність традиційних агентурних і криміналістичних методів набуття оперативної обізнаності та визнає найрезультативнішим оперативно-розшуковим методом кримінальну розвідку, поєднану з поглибленими аналітичними дослідженнями, здійснюваними з використанням сучасних інформаційних технологій.

Про широке застосування аналітичної розвідки у практичній діяльності поліції та спецслужб західноєвропейських країн свідчить той факт, що, наприклад, у Скотланд-Ярді (Велика Британія) кількість оперативних працівників-аналітиків перевищує кількість інших оперативних працівників у 2,8 рази, у ФБР (США) – у 4,7 разів, у ЦРУ (США) – у 9 разів.

У межах аналітичної розвідки збирання первинної інформації може бути здійснено за такими способами:

– комп'ютерна розвідка у мережі Інтернет;

– комп'ютерна розвідка в автоматизованих банках даних та інформаційних системах різних форм власності;

– вивчення публікацій у ЗМІ;

– радіотехнічна розвідка (сканування радіоефіру) тощо.

Складовими поняття аналітичної розвідки є:

– *суб'єктами* аналітичної розвідки є працівники підрозділів кіберполіції, кримінальної розвідки, інформаційно-аналітичних підрозділів органів, уповноважених на здійснення ОРД. Окремі елементи аналітичної розвідки можуть здійснювати також інші працівники оперативних підрозділів;

– *об'єктом* аналітичної розвідки є інформаційне середовище (мережа Інтернет, публікації у ЗМІ, автоматизовані банки даних та інформаційні системи різних форм власності, радіоефір, трафіки зв'язків абонентів мобільного зв'язку тощо);

– *механізм* аналітичної розвідки охоплює низку дій (пошук, виявлення, збирання, обробка, систематизація, накопичення, узагальнення, зберігання, використання інформації та

отримання на основі її комплексного аналізу нових або додаткових відомостей про об'єкти, події, факти та явища, що становлять оперативний інтерес);

– *предметом* аналітичної розвідки є відкрита інформація й інформація обмеженого доступу (конфіденційна, таємна та службова);

– *метою* аналітичної розвідки є вирішення завдань ОРД, які полягають у пошуку, фіксації, обробці та використанні оперативно-розшукової інформації про осіб, події, предмети, що становлять оперативний інтерес, з метою припинення правопорушень та в інтересах кримінального судочинства, безпеки громадян, суспільства і держави.

За останні роки аналітична розвідка виокремилася у самостійний напрям діяльності структур, які гарантують безпеку господарюючих суб'єктів, а в поєднанні з іншими технологіями аналітичної обробки інформації вона утворює тут комплекс розвідувальних заходів.

Аналітична розвідка в ОРД відрізняється від аналітичної розвідки, яка застосовується комерційними структурами, своїми специфічними суб'єктами, інформаційною базою, цілями, завданнями та об'єктами дослідження. Водночас потрібно зазначити, що засоби, методи і способи їх здійснення в окремих випадках можуть збігатися.

Основна відмінність аналітичної розвідки від інформаційного пошуку полягає в тому, що, крім звичайної розвідки в інформаційному середовищі, вона спрямована на отримання нових знань про розвідуваний об'єкт або явище на підставі аналітичної обробки здобутої інформації та відомостей про відомі факти[8].

Аналітична розвідка – це компонент розвідувальної діяльності, який полягає у виявленні, оцінюванні, прогнозуванні соціальних процесів, подій, заходів на основі відомостей, одержуваних здебільшого з відкритих джерел, а також здобуваємих агентурною чи технічною розвідкою.

---

[8] Овчинский С. С. Оперативно-розыскная информация / С. С. Овчинский; под ред. А. С. Овчинского, В. С. Овчинского. – М.: ИНФА, 2000. – С. 328.

Для комплексної реалізації цих функцій використовується поєднання відповідних ідентифікаційних, діагностичних і прогностичних методик, повністю задіюються можливості інформаційних систем, завдяки чому аналітична розвідка перетворюється на своєрідну модель, що відображає характерні особливості всієї інформаційно-аналітичної роботи загалом.

Питання для самоконтролю:

1. Визначіть основні етапи історії розвитку інформаційно-аналітичної роботи у правоохоронних органах.

2. Дайте характеристику основних етапів розвитку інформаційно-аналітичної роботи в ОРД.

3. Визначіть загальне поняття інформації як соціальної категорії.

4. У чому полягають пізнавальна та дієва функції інформації в ОРД?

5. Охарактеризуйте поняття оперативно-розшукової інформації, особливості її отримання та використання у процесі здійснення ОРД.

6. Назвіть принципи отримання та використання оперативно-розшукової інформації.

7. У чому полягає поняття та сутність інформаційно-аналітичної роботи в ОРД?

8. Перерахуйте основні інформаційні ресурси, що використовуються в процесі інформаційно-аналітичної роботи в ОРД.

9. У чому полягають основні завдання інформатизації ОРД на сучасному етапі?

10. Назвіть основні форми інформаційно-аналітичної роботи в ОРД.

11. Дайте характеристику поняття та особливостей отримання оперативно-розшукової інформації.

12. Охарактеризуйте особливості систематизації оперативно-розшукової інформації.

13. Визначте основні поняття оперативно-розшукової ідентифікації.

14. Наведіть особливості оперативно-розшукової діагностики.

15. Поняття та особливості оперативно-розшукового прогнозування.

16. У чому полягають характерні особливості аналітичної розвідки?

Р о з д і л 2

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ РОБОТИ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ

2.1. Законодавче регулювання інформаційно-аналітичної роботи в оперативно-розшуковій діяльності

Правова основа інформаційно-аналітичної роботи в ОРД є складовою правової основи ОРД, яка визначається як сукупність правових норм, які закріплюють необхідність і створюють умови для досягнення завдань ОРД, безпосередньо визначають правові, організаційні і тактичні положення використання гласних і негласних сил, засобів і методів боротьби зі злочинністю.

Відповідно до ст. 3 Закону України «Про оперативно-розшукову діяльність» ***правову основу ОРД*** становлять Конституція України, Закон про ОРД, Кримінальний, Кримінальний процесуальний, Податковий та Митний кодекси України, закони України про прокуратуру, Національну поліцію, Національне антикорупційне бюро України, Державне бюро розслідувань, Службу безпеки, Державну прикордонну службу України, Державну кримінально-виконавчу службу України, державну охорону органів державної влади України та посадових осіб, статус суддів, забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві, державний захист працівників суду та правоохоронних органів, інші законодавчі акти та міжнародно-правові угоди і договори, учасником яких є Україна.

За своєю сутністю та змістом правова основа ОРД є сукупністю правових норм, котрі регламентують ОРД як окремий різновид правоохоронної діяльності, зокрема й специфічні правові та соціальні відносини, що виникають між її суб'єктами й іншими учасниками й об'єктами ОРД, а також між суб'єктами й іншими фізичними та юридичними особами, залученими

у процес цієї діяльності для гарантування безпеки людини й суспільства шляхом здійснення відповідних заходів ОРД.

Правові норми, що входять у цілісну систему правового регулювання ОРД, мають різноманітну юридичну чинність і, відтак, різне регулятивне значення.

З огляду на те, що інформаційно-аналітична робота є невід'ємною частиною ОРД, вона також повинна ґрунтуватися на дотриманні норм закону та підзаконних нормативних актів. Будь-яке неправомірне застосування оперативно-розшукових заходів не може бути виправдано ніякими оперативними, організаційними та іншими міркуваннями.

Нормативно-правовою основою інформаційно-аналітичної роботи в ОРД є система законодавчих актів, які визначають допустимість цієї роботи, а також підзаконних нормативних актів і правил, які регламентують її порядок і умови.

Ці норми та правила поділяються на дві групи:

– нормативні акти, які визначають загальні права та обов'язки суб'єктів інформаційно-аналітичної роботи в ОРД;

– підзаконні нормативні акти, які безпосередньо регламентують організацію інформаційно-аналітичної роботи в ОРД та застосування конкретних інформаційних систем.

Правові норми, що регламентують інформаційно-аналітичну роботу в ОРД, стосуються різних галузей права. До першої групи нормативних актів належать норми Конституції України, законів, Указів Президента України, постанов Верховної Ради та Кабінету Міністрів України, що встановлюють загальні принципи, цілі та завдання діяльності Національної поліції, зі змісту яких випливає допустимість інформаційно-аналітичної роботи в ОРД.

Найважливішу роль виконують положення ***Конституції України***, яка визначає Україну як суверенну, незалежну, демократичну, соціальну і правову державу. Маючи найвищу юридичну силу і пряму дію, Основний Закон встановлює правовий режим роботи з оперативною інформацією в ОРД.

Правовим принципом нашої держави є положення ч. 2 ст. 19 Конституції України, яка формулює загальновизнану в міжнародному праві норму: органи державної влади, їх посадові особи зобов'язані діяти лише на підставі, у межах повно-

важень та в спосіб, що передбачені Конституцією та законами України.

Законодавчими актами, які визначають основоположні засади інформаційно-аналітичної роботи в ОРД Національної поліції, є Закони України «Про Національну поліцію», «Про оперативно-розшукову діяльність», «Про організаційно-правові основи боротьби з організованою злочинністю», Кримінальний процесуальний кодекс України. Тобто, формування організаційно-правових основ інформаційно-аналітичної роботи в ОРД відбувається на законодавчому рівні.

Відповідно до ст. 25 ***Закону України «Про Національну поліцію»*** поліція у межах інформаційно-аналітичної діяльності:

– формує бази (банки) даних, що входять до єдиної інформаційної системи МВС України;

– користується базами (банками) даних МВС України та інших органів державної влади;

– здійснює інформаційно-пошукову та інформаційно-аналітичну роботу;

– здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями.

Поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень.

Під час наповнення баз (банків) даних інформацією щодо осіб, затриманих за підозрою у вчиненні правопорушень, поліція забезпечує збирання, накопичення мультимедійної інформації (фото, відео-, аудіозапис) та біометричних даних (дактилокартки, зразки ДНК).

Для забезпечення публічної безпеки і порядку поліція може закріплювати на форменому одязі, службових транспортних засобах, монтувати/розміщувати по зовнішньому периметру доріг і будівель автоматичну фото- і відеотехніку, а також використовувати інформацію, отриману із автоматичної фото- і відеотехніки, що знаходиться в чужому володінні, з метою: попередження, виявлення або фіксування правопорушення,

охорони громадської безпеки та власності, забезпечення безпеки осіб; забезпечення дотримання правил дорожнього руху. Інформація про змонтовану/розміщену автоматичну фототехніку та відеотехніку повинна бути розміщена на видному місці.

Відповідно до ст. 27 Закону України «Про Національну поліцію» поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади за обов'язковим дотриманням Закону України «Про захист персональних даних».

Інформація про доступ до бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про поліцейського, який отримав доступ, та про обсяг даних, доступ до яких було отримано.

Кожна дія поліцейського щодо отримання інформації з інформаційних ресурсів фіксується у спеціальному електронному архіві, ведення якого покладається на службу інформаційних технологій МВС України. В електронному архіві фіксуються прізвище, ім'я, по батькові та номер спеціального жетона поліцейського, вид отриманої інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації поліцейського, який отримував інформацію з реєстрів.

Поліція вживає всіх заходів для недопущення будь-яких порушень прав і свобод людини, пов'язаних з обробкою інформації. Поліцейські несуть персональну дисциплінарну, адміністративну та кримінальну відповідальність за вчинені ними дії, що призвели до порушень прав і свобод людини, пов'язаних з обробкою інформації.

МВС України у межах компетенції здійснює контроль за дотриманням вимог законів та інших нормативно-правових актів під час формування та користування поліцейськими інформаційними базами (банками) даних.

У ***Законі України «Про оперативно-розшукову діяльність»*** закріплені основоположні правові норми, які регламентують допустимість проведення ОРД, дотримання прав і свобод людини, взаємодії з органами управління і населенням, а також здійснено законодавче регламентування всієї оперативно-розшукової діяльності, унаслідок чого матеріали,

отримані у процесі її здійснення, мають значення даних, отриманих у передбаченому законом порядку.

Закон про ОРД визначає підстави для проведення оперативно-розшукових заходів (ст. 6). За наявності підстав для проведення ОРД заводиться оперативно-розшукова справа (ст. 9).

Відповідно до пп. 9, 14, 17 ст. 8 Закону про ОРД підрозділи, які здійснюють ОРД, мають право здійснювати аудіо-, відеоконтроль особи, зняття інформації з транспортних телекомунікаційних мереж, електронних інформаційних мереж згідно з положеннями ст.ст. 260, 263–265 КПК; отримувати від юридичних чи фізичних осіб безкоштовно або за винагороду інформацію про злочини, що готуються або вчинені, та про загрозу безпеці суспільства і держави; створювати і застосовувати автоматизовані інформаційні системи.

Підрозділи, що використовують автоматизовані інформаційні системи в ОРД, повинні забезпечити можливість видавати дані про особу на запит органів розслідування, прокуратури, суду. У місцях зберігання інформації повинна бути гарантована її достовірність та надійність охорони (ст. 9).

Одержані внаслідок оперативно-розшукової діяльності відомості, що стосуються особистого життя, честі, гідності людини, якщо вони не містять інформації про вчинення дій, заборонених законодавством України, не підлягають зберіганню і повинні бути знищені. Відомості, отримані внаслідок оперативно-розшукової діяльності, щодо підготовки до терористичних актів чи їх вчинення окремими особами та групами зберігаються до 5 років.

Не підлягають розголошенню результати ОРД, які відповідно до законодавства України становлять державну таємницю, а також відомості, що стосуються особистого життя, честі, гідності людини. За передання і розголошення цих відомостей працівники оперативних підрозділів, а також особи, яким ці відомості були довірені під час здійснення ОРД чи стали відомі по службі або роботі, підлягають відповідальності згідно з чинним законодавством, крім випадків розголошення інформації про незаконні дії, що порушують права людини.

Спостереження за особою, річчю або місцем, а також аудіо-, відеоконтроль місця може проводитися з метою встановлення даних про особу та про її зв'язки у разі, коли є факти, які

підтверджують, що нею готується тяжкий або особливо тяжкий злочин, для отримання відомостей, які вказують на ознаки такого злочину, для забезпечення безпеки працівників суду і правоохоронних органів та осіб, які беруть участь у кримінальному судочинстві, членів їхніх сімей та близьких родичів цих осіб, а також з метою отримання розвідувальної інформації в інтересах безпеки суспільства і держави.

Для одержання інформації забороняється застосовувати технічні засоби, психотропні, хімічні та інші речовини, які пригнічують волю або завдають шкоди здоров'ю людей та навколишньому середовищу.

Ст. 19 ***Закону України «Про організаційно-правові основи боротьби з організованою злочинністю»*** визначено основні положення інформаційного забезпечення боротьби з організованою злочинністю. Для вирішення завдань боротьби з організованою злочинністю спеціальні підрозділи СБУ та підрозділи органів Національної поліції мають право збирати, накопичувати і зберігати інформацію про події і факти, що свідчать про організовану злочинну діяльність, її причини та умови, про осіб, які беруть участь в організованій злочинній діяльності. З цією метою в МВС України і Головному управлінні по боротьбі з корупцією і організованою злочинністю СБУ створюються централізовані банки даних.

Порядок використання таких даних регулюється нормативними актами МВС України та СБУ, які вживають заходів щодо їх захисту. Відповідні банки даних створюються у спеціальних підрозділах по боротьбі з організованою злочинністю СБУ на місцях та підрозділах органів Національної поліції.

Відповідно до норм ***Кримінального процесуального кодексу України*** досудове розслідування кримінальних правопорушень в Україні здійснюється шляхом провадження гласних і негласних слідчих (розшукових) дій під процесуальним керівництвом прокурора.

Відповідно до вимог ст. 44 КПК виконання оперативними підрозділами доручень слідчого, прокурора щодо проведення НСРД покладається на уповноважені оперативні підрозділи, які на підставі свого завдання залучають до їх проведення відповідні оперативні та оперативно-технічні підрозділи. Прове-

дення більшості НСРД пов'язане із застосуванням спеціальних технічних засобів отримання інформації.

Відповідно до ***Положення про Міністерство внутрішніх справ України, затвердженого постановою Кабінету Міністрів України від 28 жовтня 2015 р. № 878***, Міністерство внутрішніх справ:

– забезпечує належне функціонування єдиної інформаційно-телекомунікаційної системи МВС, формує та підтримує в актуальному стані інформаційні ресурси, що входять до єдиної інформаційно-телекомунікаційної системи МВС, здійснює обробку персональних даних в межах повноважень, передбачених законом, забезпечує режим доступу до інформації, надає інформаційні послуги;

– здійснює інформаційну взаємодію з іншими державними органами, правоохоронними органами іноземних держав та міжнародними організаціями;

– забезпечує ведення обліку знарядь кримінального правопорушення та інших речових доказів, отриманих відповідно до закону від судів, органів, що здійснюють ОРД, органів досудового розслідування, а також натурних зразків або каталогів продукції, технічної документації та іншої інформації, необхідної для створення й оновлення методичної та нормативної бази судової експертизи.

МВС для виконання покладених на нього завдань має право отримувати в установленому порядку безоплатно від міністерств, інших центральних та місцевих органів виконавчої влади, органів місцевого самоврядування необхідні для виконання покладених на нього завдань інформацію, документи і матеріали; користуватися відповідними інформаційними базами даних державних органів, державною системою урядового зв'язку та іншими технічними засобами.

Відповідно до ***Положення про Національну поліцію, затвердженого постановою Кабінету Міністрів України від 28 жовтня 2015 р. № 877***, Національна поліція:

– у межах інформаційно-аналітичної діяльності формує бази (банки) даних, що входять до єдиної інформаційної системи МВС, користується базами (банками) даних МВС та інших державних органів, здійснює інформаційно-пошукову та

інформаційно-аналітичну роботу, а також оброблення персональних даних у межах повноважень, передбачених законом;

– здійснює моніторинг оперативної обстановки в державі, вивчає, аналізує і узагальнює результати та ефективність поліцейської діяльності, інформує у порядку та спосіб, які передбачені законом, органи державної влади, органи місцевого самоврядування, а також громадськість про здійснення державної політики у сферах забезпечення охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, підтримання публічної безпеки і порядку;

– використовує та надає іншим правоохоронним органам України доступ до інформаційно-телекомунікаційних систем і банків даних Інтерполу та Європолу, а також вносить до цих банків даних інформацію правоохоронних органів України.

Національна поліція для виконання покладених на неї завдань має право:

– одержувати в установленому законодавством порядку від державних органів та органів місцевого самоврядування, підприємств, установ, організацій незалежно від форми власності та їх посадових осіб, а також громадян та їх об'єднань інформацію, документи і матеріали, необхідні для виконання покладених на неї завдань;

– користуватися відповідними інформаційними базами даних державних органів, державною системою урядового зв'язку та іншими технічними засобами.

Відповідно до ***постанови Кабінету Міністрів України від 25 березня 1993 року № 220 «Про Національне центральне бюро Інтерполу»*** взаємодія правоохоронних органів України з компетентними органами зарубіжних держав щодо вирішення питань боротьби зі злочинністю, що має транснаціональний характер або виходить за межі країни, здійснюється лише через НЦБ Інтерполу.

До окремої групи законів, які безпосередньо не регламентують ОРД, але містять вимоги до інформаційно-аналітичного забезпечення, належать Закони України «Про інформацію», «Про Національну програму інформатизації», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про телекомунікації». Ці закони

застосовують для формування системи інформаційно-аналітичної роботи в ОРД.

Закон України «Про інформацію» закладає правове підґрунтя інформаційної діяльності, до основних видів якої належать створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації (ст. 9).

У цьому Законі дається визначення понять:

– *правової інформації*, до якої відносяться будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо;

– *інформації з обмеженим доступом*, яка за своїм правовим режимом поділяється на конфіденційну, таємну та службову. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень.

Закон України «Про Національну програму інформатизації» визначає загальні засади формування, виконання та коригування Національної програми інформатизації.

У цьому Законі дається визначення понять:

– *база даних* – як іменованої сукупності даних, що відображає стан об'єктів та їх відношень у визначеній предметній області;

– *інформаційна технологія* – цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування;

– *інформаційний продукт (продукція)* – документована інформація, яка підготовлена і призначена для задоволення потреб користувачів;

– *інформаційний ресурс* – сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо).

Закон України «Про державну таємницю» регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

До державної таємниці у сфері державної безпеки та охорони правопорядку Закон відносить, зокрема: інформацію про особовий склад органів, що здійснюють оперативно-розшукову або розвідувальну чи контррозвідувальну діяльність; про засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи і результати оперативно-розшукової, розвідувальної та контррозвідувальної діяльності; про осіб, які співробітничають або раніше співробітничали на конфіденційній основі з органами, що провадять таку діяльність; про склад і конкретних осіб, що є негласними штатними працівниками органів, які здійснюють оперативно-розшукову, розвідувальну і контррозвідувальну діяльність (ст. 8).

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

У Законі дається визначення понять:

– *інформаційна (автоматизована) система* – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

– *інформаційно-телекомунікаційна система* – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

– обробка інформації в системі – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

– *телекомунікаційна система* – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Згідно зі ст. 8 Закону інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися у системі із застосуванням комплексної системи захисту інформації

з підтвердженою відповідністю. Відповідальність за забезпечення захисту інформації в системі покладається на власника системи, який утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

У ***Законі України «Про телекомунікації»*** подано визначення таких понять:

– *дані* – інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки;

– *Інтернет* – всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами;

– *телекомунікаційна мережа* – це комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комунікації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого виду по радіо, проводових, оптичних, чи інших електромагнітних системах між кінцевим обладнанням;

– *транспортна телекомунікаційна мережа* – мережа, що забезпечує передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого виду між підключеними до неї телекомунікаційними мережами доступу;

– *трафік* – сукупність інформаційних сигналів, що передаються за допомогою технічних засобів операторів, провайдерів телекомунікацій за визначений інтервал часу, включаючи інформаційні дані споживача та/або службову інформацію.

Відповідно до ***Плану заходів з виконання Концепції реалізації державної політики у сфері профілактики правопорушень на період до 2015 року, затвердженого постановою Кабінету Міністрів України від 8 серпня 2012 р. № 767***, передбачено встановлення систем візуального спостереження за дотриманням правопорядку та забезпеченням безпеки громадян у громадських місцях, зокрема, місцях масового перебування населення на об'єктах залізничного, повітряного транспорту та зупинках громадського транспорту.

В ***Указі Президента України від 20 жовтня 2005 року № 1497 «Про першочергові заходи щодо впровадження новітніх інформаційних технологій»*** визначено, що розвиток

в Україні інформаційного суспільства та впровадження новітніх інформаційних технологій в усіх сферах суспільного життя, діяльності органів державної влади та органів місцевого самоврядування є одним із пріоритетних напрямів державної політики.

Згідно з вимогами ст. 4 ***Кодексу поведінки посадових осіб з підтримання правопорядку, прийнятого резолюцією 34/169 Генеральної Асамблеї ООН 17 грудня 1999 року*** визначено загальні принципи збереження конфіденційності відомостей, отриманих посадовими особами: відомості конфіденційного характеру, які отримані посадовими особами з підтримання правопорядку, зберігаються в таємниці, якщо виконання обов'язків чи вимоги правосуддя не вимагають іншого.

2.2. Законодавче регулювання дотримання прав людини у процесі інформаційно-аналітичної роботи в оперативно-розшуковій діяльності

Здійснення правоохоронними органами України владних повноважень щодо захисту конституційних прав і свобод людини є одним з найважливіших чинників, які характеризують ступінь демократичності та цивілізованості держави. У ст. 3 Конституції України визнано людину, її життя і здоров'я, честь і гідність, недоторканність і безпеку найвищою соціальною цінністю. Гарантування прав і свобод людини є головним обов'язком держави, вона відповідає перед громадянами за свою діяльність.

З огляду на положення КПК, Закон про ОРД, інші закони, постанови Кабінету Міністрів України, відомчі і міжвідомчі накази та інструкції, здійснення інформаційно-аналітичної роботи в ОРД безпосередньо стосується прав громадян, визначених у ст.ст. 27–32 Конституції України.

Зокрема межі здійснення інформаційних процесів установлюються спеціальними нормами Конституції, що гарантують повагу до гідності особи (ст. 28), право на свободу та особисту недоторканість (ст. 29), таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31), недоторканість житла (ст. 30).

Неприпустимість збору, збереження, використання та поширення інформації про приватне життя особи є однією з гарантій закріпленого у ст. 32 Конституції України права на недоторканість приватного життя людини. Особливого значення ця конституційна норма набуває через широке упровадження сучасних інформаційних і телекомунікаційних технологій в діяльність Національної поліції, що дає змогу накопичувати, зберігати і обробляти значні масиви інформації.

Ст. 34 Конституції закріплено право кожного вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або іншим способом, визначено створення необхідних правових основ роботи з інформацією.

Ст. 63 Основного Закону звільняє фізичних осіб від відповідальності за відмову від надання пояснень і показань стосовно себе і своїх найближчих родичів.

У разі, якщо під час здійснення ОРД стане відомо, що особа, про яку отримано конфіденційну інформацію, не причетна до протиправного діяння, така інформація має бути знищена у встановленому порядку. Якщо ж цього не зроблено, або в інших випадках порушення прав і свобод людини та громадянина, особа згідно зі ст.ст. 55, 56 Конституції України має право звернутися до суду за захистом своїх прав, а також має право на відшкодування матеріальної та моральної шкоди, завданої незаконними рішеннями, діями чи бездіяльністю працівників оперативних підрозділів.

У контексті захисту прав і свобод людини під час здійснення ОРД має значення презумпція невинуватості, яка закріплена у ст. 62 Конституції, де проголошується, що особа вважається невинуватою у вчиненні злочину і не може бути піддана кримінальному покаранню, доки її вину не буде доведено в законному порядку і встановлено обвинувальним вироком суду. Ніхто не зобов'язаний доводити свою невинуватість у вчиненні злочину.

Гарантія недоторканності приватного життя, особистої та сімейної таємниці міститься не тільки в нормах Конституції України, а й у галузевому законодавстві, яким встановлено конкретні підстави, умови і порядок отримання відомостей, що стосуються особистої та сімейної таємниці, чим створюються

перешкоди для втручання в приватне життя, насамперед з боку державних органів.

Спілкування є приватним, якщо під час нього інформація передається та зберігається за таких фізичних та юридичних умов, за яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб. Фізичними умовами, що можуть забезпечувати захист від втручання в спілкування, є обрані особами місце та час його здійснення, форма спілкування (вербальна, конклюдентна, письмова, графічна), форма обміну інформацією (безпосередня або опосередкована – листами, бандеролями, посилками, поштовими контейнерами, переказами, телеграмами, іншими матеріальними носіями передання інформації між особами), технічні засоби дротового та бездротового зв'язку та засоби писемності, створення графічних зображень, кодування інформації та її збереження тощо. Юридичними умовами, що забезпечують приватність спілкування, є гарантоване приписами Конституції України та інших нормативно-правових актів право будь-якої особи на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, невтручання у її особисте та сімейне життя, та можливість обмеження цих прав лише за рішенням суду (зокрема ст.ст. 31, 32 Конституції України; п. 7 ч. 1 ст. 7, ст.ст. 14, 15, 258, 260, 261, 263, 264 КПК; ст. 9 Закону України «Про телекомунікації»; ст. 6 Закону України «Про поштовий зв'язок»), та укладення угоди між особою та юридичною особою, що надає послуги телекомунікаційного, поштового зв'язку на території України для забезпечення її приватного спілкування[1].

Підставами, достатніми для втручання у приватне спілкування, є:

а) фактичні дані, отримані у передбаченому КПК порядку, що розмови особи або інші звуки, рухи, дії, пов'язані з її діяльністю або місцем перебування, поштово-телеграфна кореспонденція певної особи іншим особам або інших осіб їй, певна електронна інформаційна система можуть містити відомості про обставини, які мають значення для досудового розсліду-

---

[1] Кримінальний процесуальний кодекс України. Науково-практичний коментар / за заг. ред. професорів В. Г. Гончаренка, В. Т. Нора, М. Є. Шумила. – К.:Видавництво «Юстиніан», 2012. – С. 571–572.

вання, або речі і документи, що мають вагоме значення для досудового розслідування;

б) можливість отримання відомостей про зміст приватного спілкування тільки шляхом проведення слідчих (розшукових) дій, що включають втручання у приватне спілкування.

Право на недоторканність приватного життя пов'язане з правом людини на захист своєї честі та доброго імені, що вимагає недопущення:

– поширення без відома людини відомостей, що стосуються її особистого та сімейного життя, якщо ці відомості можуть підірвати репутацію людини в суспільстві;

– тенденційного висвітлення тих або інших рис особистості, що створює про неї однобічне уявлення;

– поширення відомостей про людину, її особисте та сімейне життя, професійну і політичну діяльність, які не відповідають дійсності[2].

Порушення зазначених вимог може спричинити застосування передбачених законом заходів захисту цивільних прав, аж до компенсації моральної шкоди (п. 1 ст. 3, ч. 3 ст. 13, п. 9 ч. 2 ст. 16, п. 4 ч. 2 ст. 23, ст. 301 ЦК України), а також кримінальну, адміністративну або іншу відповідальність (ст. 182 КК України; ст. 37 Закону України «Про друковані засоби масової інформації (пресу) в Україні»; ст. 49 Закону України «Про інформацію» тощо).

Під час виконання своїх завдань поліція забезпечує дотримання прав і свобод людини, гарантованих Конституцією та законами України, а також міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України, і сприяє їх реалізації.

Обмеження прав і свобод людини допускається виключно на підставах та в порядку, визначених Конституцією і законами України, за нагальної необхідності і в обсязі, необхідному для виконання завдань поліції.

Здійснення заходів, що обмежують права та свободи людини, має бути негайно припинене, якщо мета застосування

---

[2] Хараберюш І. Ф. Гарантії прав і свобод людини та громадянина від необґрунтованого застосування спеціальної техніки / І. Ф. Хараберюш // Проблеми правознавства та правоохоронної діяльності. – 2011. – № 1. – С. 176.

таких заходів досягнута або немає необхідності подальшого їх застосування.

Згідно з ч. 5 ст. 9 Закону про ОРД під час здійснення ОРД не допускається порушення прав і свобод людини. Окремі обмеження цих прав і свобод мають винятковий і тимчасовий характер й можуть застосовуватись лише за рішенням слідчого судді з метою виявлення, попередження чи припинення тяжкого або особливо тяжкого злочину у випадках, передбачених законодавством України, з метою захисту прав і свобод інших осіб, безпеки суспільства. Тобто органи, які здійснюють ОРД, під час проведення ОРЗ мають забезпечувати конституційні права людини та громадянина на недоторканність житла (ст. 30), таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31), невтручання в особисте та сімейне життя (ст. 32) тощо.

Згідно з ч. 3 ст. 8 Закону про ОРД окремі обмеження прав і свобод людини – це негласне обстеження публічно недоступних місць, житла чи іншого володіння особи, аудіо-, відеоконтроль особи, аудіо-, відеоконтроль місця, спостереження за особою, зняття інформації з транспортних телекомунікаційних мереж, електронних інформаційних мереж, накладення арешту на кореспонденцію, здійснення її огляду та виїмки, установлення місцезнаходження радіоелектронного засобу проводяться на підставі ухвали слідчого судді, постановленої за клопотанням керівника відповідного оперативного підрозділу або його заступника, погодженим з прокурором.

Ці заходи застосовуються виключно з метою запобігання вчиненню тяжкого або особливо тяжкого злочину, запобігання і припинення терористичних актів та інших посягань спеціальних служб іноземних держав та організацій, якщо іншим способом одержати інформацію неможливо.

У випадках, передбачених п. 4 ч. 1 ст. 8 Закону про ОРД, п. 5 ч. 2 ст. 7 Закону України «Про контррозвідувальну діяльність», за рішенням суду можуть бути витребувані документи та дані, що характеризують діяльність підприємств, установ, організацій, а також спосіб життя окремих осіб, підозрюваних у підготовці або вчиненні злочину, джерело та розміри їх доходів.

Накладення арешту на кореспонденцію полягає у затриманні установою зв'язку відправлення кореспонденції особи

(листів усіх видів, бандеролей, посилок, поштових контейнерів, переказів, телеграм, інших матеріальних носіїв передання інформації між особами) без її відома на підставі ухвали слідчого судді (ст. 261 КПК).

Накладення арешту на кореспонденцію надає право слідчому здійснювати огляд і виїмку цієї кореспонденції (ст. 262 КПК). Під час такого огляду слідчий може ухвалити рішення про: 1) відкриття цієї кореспонденції, зняття з неї копій чи отримання зразків з відповідних відправлень без вилучення їх вмісту з метою збереження конфіденційності накладення арешту на кореспонденцію та її огляду; 2) нанесення на виявлені речі та документи спеціальних позначок, обладнання їх технічними засобами контролю для забезпечення проведення інших НСРД; 3) заміну речей і речовин, що становлять загрозу для оточуючих чи заборонені у вільному обігу, на їх безпечні аналоги тощо[3].

Факт проведення цих дій обов'язково описується у протоколі огляду затриманої кореспонденції.

Зняття інформації з транспортних телекомунікаційних мереж є різновидом втручання у приватне спілкування, під час якого за допомогою спеціальних технічних засобів уповноваженими оперативно-технічними підрозділами Національної поліції та органів безпеки на підставі ухвали слідчого судді та за дорученням слідчого проводиться спостереження, відбір, фіксація змісту інформації, яка передається особою, а також одержання, перетворення і фіксація різних видів сигналів, що передаються каналами зв'язку (SMS, MMS, факс, модемний зв'язок), без відома осіб, що використовують засоби телекомунікації, для встановлення обставин, які мають значення для кримінального провадження[4].

Закон про ОРД, надаючи право оперативним підрозділам проводити заходи зі зняття інформації з каналів зв'язку, не містить норм, що розкривають сутність проваджуваних

---

[3] Кримінальний процесуальний кодекс України. Науково-практичний коментар / за заг. ред. професорів В. Г. Гончаренка, В. Т. Нора, М. Є. Шумила. – К.:Видавництво «Юстиніан», 2012. – С. 575.

[4] Там само. – С. 579.

ними дій. Окремі положення норм вказаного Закону тлумачить *Постанова Пленуму Верховного Суду України «Про деякі питання застосування судами України законодавства при дачі дозволів на тимчасове обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства» від 28 березня 2008 р. № 2 (із змінами, внесеними згідно з Постановою Верховного Суду № 8 від 4 червня 2010 р.)*. У п. 3 вказаної постанови зазначається, що зняття інформації з каналів зв'язку полягає у застосуванні технічного обладнання, яке дає змогу прослуховувати, фіксувати та відтворювати інформацію, що передавалася цим каналом зв'язку. Така інформація може включати дані і про взаємоз'єднання телекомунікаційних мереж, і про зміст інформації, яка була передана каналом зв'язку. Відтак відповідно до наданого роз'яснення отримання уповноваженими оперативними підрозділами інформації про з'єднання абонентів телекомунікацій навіть без розкриття змісту повідомлень, згідно зі змістом Закону про ОРД може здійснюватись лише за рішенням суду.

У кримінальному провадженні отримання інформації про з'єднання абонентів телекомунікацій без розкриття змісту повідомлень проводиться НСРД зі зняття інформації з транспортних телекомунікаційних мереж, яке може забезпечуватись спеціально уповноваженими підрозділами Національної поліції та СБ України, а також безпосередньо підприємствами (установами), що надають послуги зв'язку, які в установленому законом порядку з метою вирішення завдань кримінального провадження зобов'язані надавати органам досудового розслідування відомості про з'єднання абонентів телекомунікаційних каналів та мереж без розкриття змісту повідомлень.

Вищий спеціалізований суд України у своєму листі від 5 квітня 2013 р. № 223-558/0/4-13 «Про деякі питання здійснення слідчим суддею суду першої інстанції судового контролю за дотриманням прав, свобод та інтересів осіб під час застосування заходів забезпечення кримінального провадження» зауважує, що у КПК передбачено декілька процесуальних дій, які мають певну схожість. Зокрема у ст. 159 та п. 7 ч. 1 ст. 162 КПК передбачено такий захід забезпечення кримінального

провадження, як тимчасовий доступ до документів, які знаходяться в операторів та провайдерів телекомунікацій та містять інформацію про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалість, зміст (вихідні чи вхідні з'єднання, SMS, MMS тощо), маршрути передавання, а ст.ст. 263 та 268 КПК передбачено такі негласні слідчі (розшукові) дії, як зняття інформації з транспортних телекомунікаційних мереж та установлення місцезнаходження радіоелектронного засобу відповідно.

ВССУ наголошує, що у ст.ст. 159, 162 КПК передбачено отримання слідчим (прокурором) інформації про зв'язок, що відбувся в минулому (постфактум), зокрема й про місцезнаходження радіоелектронного засобу у певний день та час, водночас визначена у ст. 268 КПК негласна слідча (розшукова) дія – установлення місцезнаходження радіоелектронного засобу – передбачає локалізацію (моніторинг) місцезнаходження радіоелектронного засобу в режимі реального часу (тобто дає змогу отримати інформацію про те, де перебуває відповідний засіб на момент спостереження за ним, визначити маршрут його перебування).

Окремої уваги потребують персональні дані, які ***Законом України «Про захист персональних даних»*** віднесені, за винятком знеособлених персональних даних, до інформації з обмеженим доступом (ч. 2 ст. 5). Цей Закон прийнято відповідно до Конвенції про захист осіб стосовно автоматизованої обробки даних особистого характеру, ухваленої Радою Європи 28 січня 1981 р., та Додаткового протоколу до Конвенції щодо органів нагляду та транскордонних потоків даних, які ратифіковані Україною.

Законодавець визначає інформацію про фізичну особу (персональні дані) як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (ст. 2).

Конституційний Суд України, даючи офіційне тлумачення чч. 1, 2 ст. 32 Конституції України, вважає, що інформація про особисте та сімейне життя особи (персональні дані про неї) – це будь-які відомості чи сукупність відомостей про фізичну

особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних щодо виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може бути поширена тільки за їхньою згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини[5].

Закон України «Про захист персональних даних» встановлює режим обмеженого доступу до відомостей про фізичну особу, забороняє обробку персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, а також даних, що стосуються здоров'я чи статевого життя (ч. 1 ст. 7).

Водночас зазначене положення не застосовується, якщо обробка персональних даних стосується обвинувачень у вчиненні злочинів, вироків суду, здійснення державним органом повноважень, визначених законом, щодо виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом.

З метою забезпечення захисту персональних даних в Україні створено Державну службу з питань захисту персональних даних, на яку покладаються повноваження щодо ведення Державного реєстру баз персональних даних, та здійснення контролю за діяльністю володільців чи розпорядників баз персональних даних.

---

[5] Рішення Конституційного Суду України від 20 січня 2012 р. № 2-рп у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України // Офіційний вісник України. – 2012. – № 9. – С. 106. – Ст. 332.

2.3. Відомче нормативне регулювання інформаційно-аналітичної роботи в оперативно-розшуковій діяльності Національної поліції

Порядок і умови здійснення інформаційно-аналітичної роботи в ОРД визначаються відомчими нормативними актами. Основними нормативно-правовими актами, які регламентують інформаційно-аналітичну роботу в ОРД, є:

– Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, затверджена наказом Генпрокуратури, МВС, СБУ, Адміністрації Держприкордонслужби, Мінфіна, Мін'юста від 16 листопада 2012 р. № 114/1042/516/1199/936/1687/5;

– Інструкція про порядок ведення єдиного обліку в органах поліції заяв і повідомлень про вчинені кримінальні правопорушення та інші події, затверджена наказом МВС від 6 листопада 2015 р. № 1377, зареєстрованим у Міністерстві юстиції України 1 грудня 2015 р. за № 1498/27943;

– Інструкція з організації функціонування криміналістичних обліків експертної служби МВС України, затверджена наказом МВС від 10 вересня 2009 р. № 390, зареєстрованим у Міністерстві юстиції України 15 жовтня 2009 р. за № 963/16979;

– Положення про порядок ведення Єдиного реєстру досудових розслідувань, затверджене наказом ГПУ від 6 квітня 2016 р. № 139, зареєстрованим в Міністерстві юстиції України 5 травня 2016 р. за № 680/28810;

– Порядок взаємодії Генеральної прокуратури України та Міністерства внутрішніх справ України щодо обміну інформацією з Єдиного реєстру досудових розслідувань та інформаційних систем органів внутрішніх справ, затверджений наказом Генпрокуратури та МВС від 17 листопада 2012 р. № 115/1046;

– наказ МВС від 2 жовтня 2012 р. № 846, яким визначено ДІАЗ та відповідні підрозділи інформаційно-аналітичного забезпечення ГУМВС, УМВС відповідальними за ведення довідників організаційної структури Єдиного реєстру досудових розслідувань;

– положення про структурні підрозділи апарату Національної поліції.

Відповідно до вимог нормативно-правових актів МВС *основними завданнями інформаційно-аналітичної роботи в ОРД* Національної поліції є:

– вирішення основних завдань ОРД щодо пошуку та фіксації фактичних даних про протиправні діяння окремих осіб і груп, відповідальність за які передбачена КК України, з метою припинення правопорушень та в інтересах кримінального судочинства, безпеки громадян, суспільства і держави;

– формування єдиних оперативних обліків, передбачених Законом про ОРД та регламентованих нормативно-правовими актами МВС;

– формування автоматизованої інформаційної системи оперативного призначення (АІС ОП), інтегрованої інформаційно-пошукової системи ІІПС НП, спеціалізованих АІС;

– координація оперативно значущої інформації, необхідної оперативним підрозділам під час здійснення ними ОРД, шляхом здійснення інформаційно-аналітичної роботи;

– аналіз стану окремих напрямів ОРД в ініціативному порядку та за завданнями керівництва МВС, Національної поліції, ГУНП;

– організація інформаційної взаємодії оперативних підрозділів між собою та з іншими правоохоронними органами;

– інформаційно-статистичне забезпечення ОРД.

Використання автоматизованих інформаційних систем в інформаційно-аналітичній роботі в ОРД Національної поліції регламентується відомчими нормативно-правовими актами МВС, зокрема:

Інтегрована інформаційно-пошукова система Національної поліції (ІІПС). ІІПС створена на виконання Указу Президента України від 20 жовтня 2005 р. № 1497 «Про першочергові завдання щодо впровадження новітніх інформаційних технологій» та відповідно до Програми створення Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України, затвердженої наказом МВС від 7 червня 2006 р. № 571, з метою подальшого вдосконалення оперативно-службової діяльності ОВС із використанням сучасних інформаційних технологій.

ІІПС функціонує відповідно до Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ

України, затвердженого наказом МВС від 12 жовтня 2009 р. № 436, зареєстрованим у Міністерстві юстиції України 28 грудня 2009 р. за № 1256/17272 (зі змінами, внесеними наказом МВС від 16 травня 2013 р. № 460).

Метою створення ІІПС є об'єднання існуючих в органах та підрозділах Національної поліції інформаційних ресурсів у єдиний інформаційно-аналітичний комплекс із використанням сучасних інформаційних технологій, комп'ютерного та телекомунікаційного обладнання для підтримки оперативно-службової діяльності органів і підрозділів поліції, суттєвого зміцнення їх спроможності протидії та профілактики злочинності.

Відповідно до свого призначення ІІПС вирішує такі завдання:

– автоматизація процесів обліку отриманої інформації, обробки інформаційних запитів, пошук та відбір необхідної інформації;

– виконання інформаційно-пошукових заходів, проведення аналітичних досліджень;

– обмін інформацією між інтегрованими банками даних ІІПС відповідних рівнів та забезпечення постійного зв'язку між ними, уніфікація технологічних процедур опрацювання документів, збирання, реєстрації, накопичення та обробки інформації, що надходить до кожного з банків даних;

– постійне формування, оновлення та адміністрування банків даних ІІПС, забезпечення достовірності, оперативного доступу та збереження інформаційного ресурсу;

– формалізація технологічних процесів обробки інформації, визначення типових маршрутних технологічних схем для їх виконання;

– забезпечення надійного зберігання інформаційних обліків, максимально зручна їх систематизація;

– забезпечення комплексного захисту інформації та розмежування доступу до інформації, що зберігається в ІІПС;

– автоматизація збирання даних про результати виконання технологічних процесів щодо інформаційних обліків, формування аналітичних і статистичних звітів (довідок);

– інформаційне забезпечення управлінської діяльності, підготовка аналітично-довідкових матеріалів;

– наскрізний контроль (підрозділ контролю, керівник, безпосередній виконавець) за своєчасністю і повнотою надання первинних облікових та інформаційно-пошукових документів, проведення аналізу їх повноти, сумісності та об'єктивності.

Інформаційними ресурсами (об'єктами обліку) ІІПС є об'єктивно поєднаний набір відомостей, що безпосередньо стосується осіб, кримінальних та адміністративних правопорушень, а також інших подій, який накопичується в процесі службової діяльності НПУ в обсязі, структурі й порядку, що визначаються завданнями, покладеними на НПУ, відповідно до чинного законодавства.

До складу ІІПС входять такі інформаційні підсистеми: «Єдиний облік», «Злочин», «Затримані та доставлені», «Особа», «Розшук», «Пізнання», «Річ», «Антикваріат», «Угон», «Викрадені (втрачені) документи», «Кримінальна зброя», «Зареєстрована зброя», «Адміністративне правопорушення», «Мігрант», «Корупція», «Кримінальна статистика».

Інформаційна підсистема «Оперативно-довідкова картотека» («ОДК») створена відповідно до наказу МВС від 26 березня 2002 р. № 301. Порядок ведення оперативно-довідкових і дактилоскопічних фондів у цій підсистемі регламентується Інструкцією про порядок формування, ведення та використання оперативно-довідкового і дактилоскопічного обліку в органах внутрішніх справ та органах (установах) кримінально-виконавчої системи України, затвердженою наказом МВС та ДДУПВП від 23 вересня 2002 р. № 823/188. До складу інформаційної підсистеми «ОДК» входять підсистеми «Мігрант» та «Рубін-2002». ІП «Мігрант» призначена для обліку осіб, затриманих за порушення законодавства України про державний кордон та про правовий статус іноземців. ІП «Рубін-2002» реалізує технологію віддаленого оперативного доступу до банків даних з метою введення інформації і перевірки вимог на судимості.

Отримання відомостей з персонально-довідкового обліку за зверненнями державних органів, які здійснюють правоохоронні функції, здійснюється відповідно до Порядку доступу до відомостей персонально-довідкового обліку єдиної інформаційної системи Міністерства внутрішніх справ України, затвердженого наказом МВС від 29 листопада 2016 р. № 1256, за-

реєстрованого в Міністерстві юстиції України 10 січня 2017 р. за № 22/29890.

Автоматизовану систему обліку автотранспортних засобів України (АІС «Національний банк даних «Автомобіль») введено в експлуатацію наказом МВС від 28 лютого 1996 р. № 131. АІС «Національний банк даних «Автомобіль» призначена для вдосконалення інформаційного забезпечення МВС під час виконання ним завдань з попередження та розкриття злочинів, пов'язаних з незаконним заволодінням транспортними засобами або злочинів із використанням транспортних засобів, більш ефективній протидії незаконній легалізації в Україні транспортних засобів, увезених в Україну поза зоною митного контролю.

Наказ МВС від 28 лютого 1996 р. № 131 скасовано наказом МВС від 31 липня 2012 р. № 657.

Відповідно до Закону України від 24 вересня 2008 р. № 586-VI «Про внесення змін до деяких законодавчих актів України щодо вдосконалення регулювання відносин у сфері забезпечення безпеки дорожнього руху» та на виконання постанови Кабінету Міністрів України від 18 травня 2011 р. № 507 «Про затвердження Порядку використання коштів, передбачених у державному бюджеті для створення та впровадження Національної автоматизованої інформаційної системи департаменту Державної автомобільної інспекції» наказом МВС від 10 січня 2014 р. № 9 введено в експлуатацію ***Національну автоматизовану інформаційну систему Єдиного державного реєстру Міністерства внутрішніх справ стосовно зареєстрованих транспортних засобів та їх власників («НАІС ЄДР МВС»)***. НАІС ЄДР МВС призначена забезпечити обробку інформації (уведення, приймання, отримання, передавання, реєстрація, зберігання) та автоматизований доступ до інформаційних ресурсів (баз даних) суб'єктів системи.

Наказом МВС від 29 грудня 2011 р. № 975 уведено в експлуатацію ***автоматизовану інформаційно-пошукову систему відеофіксації транспортних засобів з розпізнаванням номерних знаків та перевіркою їх за розшуковими реєстрами «ВІДЕОКОНТРОЛЬ-Рубіж»***. Комплекс «ВІДЕОКОНТРОЛЬ-Рубіж» – це система цілодобового автоматизованого

моніторингу руху автотранспорту із одночасною можливістю здійснювати перевірки за наявними базами обліку МВС.

Криміналістичні обліки експертної служби регламентуються Інструкцією з організації функціонування криміналістичних обліків експертної служби МВС України, затвердженої наказом МВС від 10 вересня 2009 р. № 390, зареєстрованим у Міністерстві юстиції України 15 жовтня 2009 р. за № 963/16979. До криміналістичних обліків належать такі види: трасологічний облік; дактилоскопічний облік; балістичний облік; облік холодної зброї; облік грошових знаків, бланків документів, цінних паперів та пластикових платіжних карток; облік осіб за ознаками зовнішності; вибухотехнічний облік; пожежно-технічний облік; облік наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів; облік генетичних ознак людини; облік записів голосів та мовлення осіб; облік ідентифікаційних позначень транспортних засобів та реквізитів документів (підписів, печаток, штампів); облік матеріалів, речовин та виробів.

Відповідно до п. 3 Положення про ***інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон***, затвердженого наказом Адміністрації Держприкордонслужби, Держмитслужби, ДПА, МВС, МЗС, Мінсоцполітики, СБУ, СЗР України від 3 квітня 2008 р. № 284/287/214/150/64/175/266/75, система «Аркан» – це сукупність організаційно-розпорядчих заходів, програмно-технічних та телекомунікаційних засобів, що забезпечують обробку інформації (уведення, приймання, отримання, передавання, реєстрація, зберігання) щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон України, та автоматизований доступ до інформаційних ресурсів (баз даних) суб'єктів системи «Аркан».

Спільним наказом МВС, ГПУ, СБУ, Держприкордонслужби, Держмитслужби, ДПА від 9 січня 1997 р. № 3/1/2/5/2/2 затверджено Інструкцію про порядок використання правоохоронними органами можливостей НЦБ Інтерполу в Україні у попередженні, розкритті та розслідуванні злочинів. Відповідно до Інструкції НЦБ Інтерполу в Україні забезпечує співробітництво правоохоронних органів України та зарубіжних

країн і надає можливості для обміну оперативно-розшуковою, оперативно-довідковою та криміналістичною інформацією про підготовку і вчинення злочинів та причетних до них осіб, а також архівною та, в окремих випадках процесуальною інформацією.

Питання для самоконтролю

1. Що становить нормативно-правову основу інформаційно-аналітичної роботи в ОРД?
2. Чому найважливішу роль у регламентації інформаційно-аналітичної роботи в ОРД виконують положення Конституції України?
3. Дайте характеристику правових норм Закону України «Про Національну поліцію», які регулюють інформаційно-аналітичну роботу в ОРД Національної поліції.
4. Охарактеризуйте положення Законів України «Про оперативно-розшукову діяльність», «Про організаційно-правові основи боротьби з організованою злочинністю», Кримінальний процесуальний кодекс України, які регламентують використання автоматизованих інформаційних систем в ОРД.
5. Назвіть основні обов'язки та права Національної поліції щодо інформаційно-аналітичної діяльності відповідно до положень про Міністерство внутрішніх справ та Національну поліцію.
6. Охарактеризуйте правові основи інформаційної діяльності, що викладені в Законах України «Про інформацію», «Про Національну програму інформатизації», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про телекомунікації».
7. Назвіть положення Конституції України, які безпосередньо стосуються здійснення інформаційних процесів?
8. У яких випадках спілкування вважатиметься приватним?
9. Які підстави є достатніми для втручання у приватне спілкування?
10. У чому полягає накладення арешту на кореспонденцію?
11. Назвіть характерні особливості зняття інформації з транспортних телекомунікаційних мереж?
12. Яким нормативно-правовим актом регламентується захист персональних даних?
13. Назвіть особливості захисту персональних даних.
14. Які відомчі нормативні акти регламентують інформаційно-аналітичну роботу в ОРД Національної поліції?
15. Якими нормативними актами регулюється функціонування Інтегрованої інформаційно-пошукової системи Національної поліції (ІІПС НП)?

Р о з д і л 3

СУЧАСНІ ІНФОРМАЦІЙНО-АНАЛІТИЧНІ ТЕХНОЛОГІЇ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ

3.1. Комп'ютерна розвідка – новий захід оперативного (ініціативного) пошуку

В останні десятиліття широкого розповсюдження набула діяльність з гласного та негласного пошуку й добування інформації з відкритих і закритих інформаційних систем, баз і банків даних, контролю за повідомленнями, які передаються в комп'ютерних мережах, отримання персональних даних користувачів АІС та іншої цінної комп'ютерної інформації. Для характеристики подібної діяльності використовуються терміни «комп'ютерна розвідка», «комп'ютерний пошук», «аналітична розвідка», «аналітична розвідка засобами Інтернет», «комп'ютерний моніторинг», «кіберрозвідка» тощо.

Сутність комп'ютерної розвідки полягає в добуванні:

– комп'ютерної інформації, яка обробляється, зберігається та передається в інформаційних системах;

– даних і відомостей про характеристики (параметри) програмних, апаратних і програмно-апаратних комплексів, що застосовані в інформаційних системах;

– даних і відомостей про методи, способи і механізми захисту інформації, які застосовані в інформаційних системах;

– персональної інформації про користувачів інформаційних систем[1].

Термін «комп'ютерна інформація» неоднозначно трактується в законодавчих актах. Зокрема у диспозиціях ст.ст. 361–363

---

[1] Ємельянов С. Л. Сутність та методи комп'ютерної розвідки / С. Л. Ємельянов // Захист інформації: науково-технічний журнал. – 2010. – № 1. – С. 30–35; Варламов О. О. Компьютерная разведка и создание АС до класса защищенности 1Г на основе сертифицированного ПС «ЭЛАР Саперион» / О. О. Варламов // Штучний інтелект. – № 3. – 2008. – С. 137–144.

КК України йдеться про інформацію, яка зберігається, обробляється або розповсюджується за допомогою автоматизованих систем, комп'ютерних мереж або мереж зв'язку.

У ст. 2 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» зазначається, що об'єктами захисту є інформація, яка обробляється, і програмне забезпечення, яке призначене для обробки цієї інформації.

Водночас у деяких міжнародних нормативно-правових документах використовується термін «комп'ютерні дані»[2].

У сучасній теорії ОРД комп'ютерна розвідка визначається як оперативно-розшуковий захід зі здійснення цілеспрямованого пошуку у відкритій інформації з комп'ютерних систем та мереж з метою виявлення відомостей криміногенного та кримінального характеру[3].

Ст. 264 КПК запроваджена негласна слідча (розшукова) дія «Зняття інформації з електронних інформаційних систем», яка полягає у здійсненні на підставі ухвали слідчого судді пошуку, виявлення і фіксації відомостей, що містяться в електронній інформаційній системі або її частин, доступ до яких обмежений власником, володільцем або утримувачем системи розміщенням її у публічно недоступному місці, житлі чи іншому володінні особи або логічним захистом доступу, а також отримання таких відомостей без відома її власника, володільця або утримувача. Водночас п. 9 ст. 8 Закону про ОРД оперативним підрозділам надано право здійснювати зняття інформації з електронних інформаційних мереж згідно з положеннями ст.ст. 258, 264, 265 КПК.

За своїм складом електронні інформаційні системи можуть бути і локальними, в яких всі їхні компоненти (база даних, система управління базою даних, клієнтське програмне забезпечення) знаходяться на одному комп'ютері, і розподіленими, в яких компоненти розподілені по кількох комп'ютерах. Крім того, електронні інформаційні системи можуть бути

---

[2] Конвенція про кіберзлочинність // Офіційний вісник України. – 2007. – № 65. – С. 107. – Ст. 2535. – Офіц. пер.

[3] Овчинский С. С. Оперативно-розыскная информация / С. С. Овчинский; под ред. А. С. Овчинского, В. С. Овчинского. – М.: ИНФА, 2000. – С. 325.

відкритими і закритими для громадян, тобто доступ до них обмежений їх власником, володільцем або утримувачем шляхом розміщення файлових серверів та робочих станцій інформаційної системи у публічно недоступних місцях, житлі чи іншому володінні особи та встановленням систем логічного захисту доступу до електронної інформаційної системи з робочих станцій локальної мережі підприємства, установи, організації тощо, або з робочих станцій, зв'язаних з файловим сервером через мережу Інтернет[4].

Зняття інформації з електронних інформаційних систем або їх частин здійснюється без дозволу слідчого судді, якщо доступ до них не обмежується їх власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту (п. 2 ст. 264 КПК). У випадках, коли файловий сервер електронної інформаційної системи встановлений у публічно недоступному місці, житлі або іншому володінні особи, але доступ до баз даних, розміщених на ньому, не захищений системами логічного захисту доступу та можливий з робочих станцій, розташованих поза межами місць розміщення файлових серверів електронної інформаційної системи, зняття інформації з електронних інформаційних систем або її частин також допускається без дозволу слідчого судді. Водночас складається тільки протокол зняття інформації з електронних інформаційних систем з відповідними додатками до нього.

Провівши аналіз поняття «зняття інформації з електронних інформаційних систем або їх частин, якщо доступ до них не обмежується їх власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту» (далі – зняття інформації), виокремимо такі його складові елементи та їх особливості:

1) зняття інформації – це *оперативно-пошуковий захід*, який полягає у пошуку та отриманні оперативної інформації з комп'ютерних систем та мереж, доступ до яких не обмежується їх власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту;

---

[4] Кримінальний процесуальний кодекс України. Науково-практичний коментар / за заг. ред. професорів В. Г. Гончаренка, В. Т. Нора, М. Є. Шумила. – К.: Видавництво «Юстиніан», 2012. – С. 582.

2) зняття інформації здійснюють працівники оперативних та оперативно-технічних підрозділів (*суб'єкти* зняття інформації);

3) *механізм* зняття інформації передбачає пошук та отримання (реалізацію) оперативно-розшукової інформації в електронному вигляді за допомогою апаратних, програмних або апаратно-програмних засобів;

4) *об'єктом* зняття інформації є інформація з комп'ютерних систем та мереж, доступ до яких не обмежується їх власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту;

5) *предметом* зняття інформації є характерні особливості чи ознаки об'єктів зняття інформації, зафіксовані на відповідних носіях у комп'ютерних системах та мережах;

6) *метою* зняття інформації є вирішення завдань ОРД, які полягають у пошуку і фіксації фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена КК України, у комп'ютерних системах та мережах, з метою припинення правопорушень та в інтересах кримінального судочинства, безпеки громадян, суспільства і держави;

7) зняття інформації не *потребує дозволу* слідчого судді, оскільки воно не пов'язано з тимчасовим обмеженням прав особи.

Тобто комп'ютерна розвідка є різновидом зняття інформації з електронних інформаційних систем або їх частин, якщо доступ до них не обмежується їх власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту.

Отже, *комп'ютерна розвідка – це оперативно-пошуковий захід, який полягає у цілеспрямованому пошуку та отриманні інформації з комп'ютерних систем та мереж, доступ до яких не обмежується їхнім власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту, що здійснюється працівниками оперативних та оперативно-технічних підрозділів з метою виявлення відомостей криміногенного та кримінального характеру.*

Необхідність проведення комп'ютерної розвідки обумовлена особливостями сучасної організованої та транснаціональної злочинності. У нинішніх умовах комп'ютерні мережі,

насамперед Інтернет, щораз активніше використовуються злочинцями для створення нелегальних ринків збуту зброї, наркотиків, людських органів, порнографічної продукції, вибухових речовин та вибухових пристроїв, пропозицій щодо надання кілерських «послуг», а також є способом розповсюдження інформації щодо виготовлення саморобних вибухових пристроїв, пропаганди національної ворожнечі, тероризму, закликів до розв'язання війни.

Метою комп'ютерної розвідки є отримання інформації, яка міститься в комп'ютерних системах та мережах (на серверах). За критеріями криміногенності інформацію в мережі Інтернет умовно можна поділити на три групи:

1) інформація, розміщення якої на сайті становить *об'єктивну сторону певного складу злочину* (інформація, що становить державну таємницю; конфіденційна інформація, яка є власністю держави; інформація щодо технологій, які можуть бути використані для створення зброї, військової та спеціальної техніки; інформація, спрямована на розпалювання національної, расової чи релігійної ворожнечі та ненависті; розповсюдження матеріалів із закликами до агресивної війни або розв'язання воєнного конфлікту; інформація порнографічного характеру);

2) інформація, яка може свідчити про *факти злочинної діяльності* (незаконна економічна діяльність, створення фінансових пірамід, торгівля товарами, забороненими для вільного обігу, укладання сумнівних угод, переведення грошових коштів, протиправна професійна діяльність, торгівля людьми, незаконна торгівля органами або тканинами людей тощо);

3) інформація, яка містить *установочні дані щодо певних фізичних та юридичних осіб*, що можуть бути використані в ОРД (сфера економічної діяльності, укладені контракти, VIP-клієнти, афілійовані особи чи компанії, співробітники фірми та їх телефони, структури фірми, діючі філії).

Підставами для здійснення комп'ютерної розвідки є:

– застосування комп'ютерних систем і мереж для вчинення злочинів (зокрема, незаконне переміщення грошових коштів, розповсюдження дитячої порнографії тощо) та підтримання зв'язку у злочинному середовищі;

– *розповсюдження* через ресурси мережі Інтернет (електронна пошта, сервіси IP-телефонії, соціальні мережі тощо) інформації кримінального характеру;

– *зростання* кількості злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (ст.ст. 361–363 КК України);

– *наявність* інформації про фінансову діяльність підприємств в електронному вигляді в комп'ютерних системах, що становить оперативний інтерес;

– *розповсюдження* електронних періодичних видань у мережі Інтернет, які можуть містити інформацію, що становить оперативний інтерес;

– *здійснення* комерційної діяльності, зокрема й протизаконної, у комп'ютерних мережах загального користування;

– *функціонування* в мережі Інтернет форумів з обміну інформацією з різних питань суспільного життя, що становить оперативний інтерес.

До *основних напрямів* здійснення комп'ютерної розвідки належать:

1) *пошук* інформації, яка може свідчити про вчинення протиправних дій;

2) *збирання* інформації щодо певних об'єктів: фізичних та юридичних осіб, предметів та подій у зв'язку з їхнім відношенням до протиправної діяльності;

3) *здійснення* в комп'ютерній мережі активних заходів (оперативне опитування, оперативний експеримент, оперативна закупка тощо).

Серед *основних функцій* комп'ютерної розвідки є:

– здійснення моніторингу інформаційних ресурсів у мережі Інтернет з метою пошуку відомостей криміногенного та кримінального характеру;

– накопичення, фіксація, систематизація та аналіз інформації, отриманої під час комп'ютерної розвідки, з метою подальшого її використання оперативними підрозділами для вирішення завдань ОРД та досудового розслідування;

– здійснення ОРЗ у мережі Інтернет з метою протидії злочинності.

Програмними засобами, за допомогою яких здійснюється комп'ютерна розвідка, є мережеві пошукові системи Яндекс, Rambler, Yahoo!, Google, Aport, Meta тощо, які дають змогу здійснювати пошук необхідної інформації в комп'ютерних мережах за комбінацією ключових слів. Їх використання оперативний працівник здійснює через стандартний браузер (мережевий навігатор) типу Internet Explorer, Opera, Mozilla Firefox тощо, який інстальований на його комп'ютері.

Для пошуку інформації щодо фізичних осіб використовуються такі прийоми: здійснення прямого пошуку на сайтах за комбінацією ключових слів (наприклад, |Іванов Іван Іванович|, |Іванов Іван|, |Іванов І. І.|, |Іванов І.| тощо); використання можливостей так званих «білих сторінок», на яких розміщуються електронні телефонні довідники; застосування спеціальних пошукових програм щодо персональної інформації (наприклад, ZabaSearch).

Для здійснення комп'ютерної розвідки використовують *спеціалізовані розвідувальні програми* – прикладні програми, які виконують функції пошуку, отримання або аналізу інформації поза межами оперативних обліків – у корпоративних та банківських мережах, Інтернеті, а також на окремих комп'ютерах.

Розвідувальні програми відрізняються від інших програм пошуково-аналітичного призначення наявністю в них специфічних функцій, спрямованих на вирішення суто розвідувальних завдань (наприклад, Analyst's Notebook 6). До таких функцій належить, зокрема, пошук інформації за частковими параметрами, на основі нечіткої логіки, на основі діаграми зв'язків тощо. Перспективним вважається так званий інфомедійний пошук, який дає змогу в автоматичному режимі аналізувати інформацію, що міститься у відеоматеріалах, здійснюючи комплекс досліджень усного мовлення та зображень (розпізнавання мовлення, обличчя, переклад з однієї мови на іншу тощо). Отримана за допомогою спеціалізованих розвідувальних програм інформація зіставляється з наявною інформацією з оперативних обліків[5].

---

[5] Овчинский С. С. Оперативно-розыскная информация / С. С. Овчинский; под ред. А. С. Овчинского, В. С. Овчинского. – М.: ИНФА, 2000. – С. 221–223.

Під час здійснення ОРЗ у мережі Інтернет може використовуватися і універсальне, і спеціальне програмне забезпечення. Так, універсальні програми (ІПС, редактори, електронні таблиці тощо) загального призначення не тільки підвищують продуктивність праці та ефективність роботи з виявлення, розкриття та розслідування злочинів, а й піднімають її на якісно новий рівень.

Спеціалізовані програми дають змогу: контролювати процес спроб злому комп'ютерної системи або мережі; визначати індивідуальний почерк роботи програміста; визначати перелік електронних адрес та сайтів, з якими працював користувач; негласно реєструвати програми, з якими працює користувач; визначати загрози для комп'ютерної системи; здійснювати негласний контроль над програмістом; виявляти закриту і закодовану інформації в комп'ютерній системі; проводити ідентифікацію комп'ютерних систем; здійснювати дослідження слідів діяльності оператора; здійснювати діагностику пристроїв і систем телекомунікацій щодо можливості здійснення несанкціонованого доступу до них; досліджувати матеріальні носії; проводити дослідження комп'ютерних технологій для виявлення злочинних виявів (крекінг, хакінг, фрікінг тощо); досліджувати програми для ЕОМ і бази даних з метою виявлення програмних закладок, підпрограм класу «троянський кінь» тощо.

Удосконалення технології спостереження призвело до появи самостійних програмних комплексів із розширеними можливостями отримання інформації (Boss Everyware, Spector Pro, WinWhotWhere, Spy Agent, Keykey), які дозволяють визначити загальні функції: неправомірне заволодіння комп'ютерною інформацією; створення журналу подій; запис інформації, яка вводиться з клавіатури; фіксація зображень на екрані; облік використаних програм і відвідуваних сайтів.

Пошукові програмні засоби можуть мати широке застосування в ОРД. Водночас факт виявлення об'єктів (програмних закладок, програмного забезпечення для створення вірусів або здійснення злому комп'ютерних мереж тощо) може слугувати підставою для відкриття кримінального провадження і проведення розслідування. У процесуальній формі

пошукові програмні засоби можуть знаходити застосування під час проведення слідчих дій, а саме: слідчий огляд, виїмка предметів, документів та електронної поштової кореспонденції, слідчий експеримент, що виконуються з метою дослідчої перевірки показів[6].

У сучасних умовах протидії злочинності комп'ютерна розвідка:

1) стає одним із найбільш затребуваних оперативно-пошукових заходів, який полягає у пошуку та отриманні оперативної інформації з комп'ютерних систем та мереж, доступ до яких не обмежується їхнім власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту, з метою виявлення відомостей криміногенного та кримінального характеру;

2) не потребує дозволу слідчого судді, оскільки вона не пов'язана з тимчасовим обмеженням прав особи;

3) здійснюється працівниками оперативних або оперативно-технічних підрозділів шляхом отримання (реалізації) оперативно-розшукової інформації в електронному вигляді за допомогою апаратних, програмних або апаратно-програмних засобів.

3.2. Комп'ютерні засоби оперативно-розшукової ідентифікації

Особлива роль в ОРД та криміналістиці відводиться спеціалізованим комп'ютерним системам ідентифікації людини. Ці системи дають змогу отримувати й аналізувати за декількома пов'язаними параметрами інформацію, що прямо чи опосередковано може сприяти розкриттю злочину. Зокрема недавнім часом значного поширення в діяльності правоохоронних органів набули інформаційно-пошукові системи біометричної ідентифікації особи.

---

[6] Оперативно розыскная деятельность в сфере высоких технологий [Электронный ресурс]. – Режим доступа: http://it-sektor.ru/operativno-rozysknaya-deyatel-nost-v-sfere-vysokix-texnologiyi.html.

Біометрична ідентифікація – це засіб підтвердження особи; належності паспорта його власникові шляхом розпізнавання та зіставлення біометричних даних (кольору очей, малюнка сітківки ока, відбитків пальців, геометрії руки, рис обличчя тощо), що зафіксовані носіями цих даних, з особистими даними власника.

Розглянемо насамперед найбільш розповсюджені методи ідентифікації особи, які поділяються на дві групи: статичні й динамічні.

Статичні методи ґрунтуються на фізіологічній (статичній) характеристиці людини, зокрема:

1) *ідентифікація особи за відбитками пальців*. В основі цього методу біометричної ідентифікації є унікальність папілярного узору дистальної фаланги пальця (подушечки). Із зображення відбитка пальця, отриманого за допомогою спеціального сканера, формується цифровий код, який порівнюється з еталоном, що був сформований раніше і є у базі даних біометричної системи ідентифікації;

2) *ідентифікація особи за формою обличчя*. За допомогою телекамери та спеціального програмного забезпечення на зображенні обличчя виділяються контури очей, брів, носа, губ, вух, підборіддя або інші параметри обличчя відповідно до вибраного алгоритму й вираховуються відстані між ними. Отримане зображення перетворюється в цифрову форму, зберігається в базі даних і слугує еталоном;

3) *ідентифікація особи за формою руки* ґрунтується на розпізнаванні геометрії кисті руки, яка також є унікальною біометричною характеристикою особи. У цьому разі отримують тримірне зображення кисті руки (розміри долоні, довжина і ширина пальців, зміна їх висоти та контури суглобів), яке фіксується спеціальною ПЗЗ-камерою з інфрачервоним підсвіченням;

4) *ідентифікація особи за характеристиками ока*. Око людини має дві унікальні складові: райдужну оболонку та сітківку, структури яких такі ж індивідуальні, як і будь-які інші частини людського тіла;

5) *ідентифікація особи за розташуванням вен на лицьовій стороні долоні*. За допомогою інфрачервоної камери

зчитується малюнок вен на лицьовій стороні долоні або грона руки. Отримане зображення обробляється і за схемою розташування вен формується цифрова згортка;

6) *ідентифікація особи за ДНК*. Експерти використовують знайдені на місці злочину ДНК крові, сперми, шкіри, слини або волосся для ідентифікації злочинця. ДНК-аналіз вважається одним із методів розкриття злочинів, який дає змогу з точністю ідентифікувати особу злочинця й ефективно довести його причетність до вчинення протиправних дій. За допомогою ДНК-аналізу можна ефективніше розшукувати безвісно зниклих осіб та встановлювати особи невпізнаних трупів, ідентифікувати жертв авто- і авіакатастроф.

Динамічні методи біометричної ідентифікації ґрунтуються на поведінковій (динамічній) характеристиці людини, зокрема:

1) *ідентифікація за рукописним почерком*. До цифрового коду може входити інформація графічних параметрів підпису, час підпису та динаміка натискування на поверхню, на якій цей підпис виконується. Для реалізації цього методу застосовуються різні планшети, плоскі екрани;

2) *ідентифікація особи за голосом*. За допомогою різних комбінацій частотних та статичних голосових характеристик формується код ідентифікації. При наступному входженні в систему відбувається порівняння «голосів». Метод дає змогу ідентифікувати особу на значній відстані;

3) *ідентифікація за клавіатурним почерком*. Для здійснення ідентифікації використовується комп'ютерна клавіатура та певне ключове слово. Основна характеристика, за якою формується еталон, – це динаміка набору ключового слова.

За даними International Biometric Group (див. рис. 3.1) домінують живе сканування (38,3 %), методи ідентифікації особи за відбитками пальців (28,4 %), за формою обличчя (11,4 %)[7].

---

[7] The Most Trusted Report on the Biometrics Industry [Электронный ресурс]. – Режим доступа: https://ibgweb.com/products/reports/bmir-2009-2014.

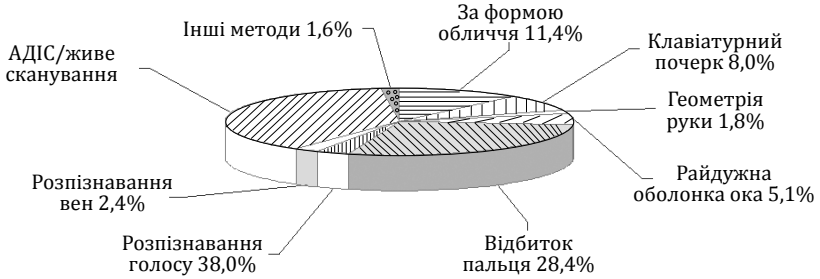

Рис. 3.1. Сегментація ринку біометричного продукту

Біометрію особи як основну технологію ідентифікації запроваджено Новоорлеанською угодою після подій 11 вересня 2001 р. у США, її учасниками стали 188 країн світу.

Однією із актуальних проблем сьогодення є введення національних посвідчень (паспортів) громадян. У понад ста країнах запроваджують так звані біометричні паспорти (ID cards). Біометричний паспорт відрізняється від звичайного тим, що в нього вбудований спеціальний чіп, який містить двомірну фотографію його власника, а також його дані: прізвище, ім'я, по батькові, дату народження, номер паспорта, дату його видачі та закінчення терміну дії. Також на чіпі є біометрична інформація: скан сітківки ока, відбитки пальців тощо.

Під електронними або біометричними проїзними документами розуміються всі документи, які дають змогу перетинати державний кордон (громадянські, службові та дипломатичні паспорти, візи, посвідчення особи, особи без громадянства, біженця, дозволи на постійне проживання тощо), та до яких вмонтовано електронний носій біометричної та іншої інформації – мікрочіп. Практично «ID cards» з ідентифікаційним чіпом дозволяють вмістити такий обсяг інформації, який дає можливість ідентифікувати особу.

Біометричні технології, такі як розпізнавання людини за відбитками пальців, долоней і губ, райдужною оболонка ока, за формою голови, голосовими даними, здатні значно спростити пошук злочинців.

Зважаючи на вимоги Євросоюзу щодо впровадження біометричних паспортів для надання безвізового режиму для

громадян України та на вимоги ІСАО щодо обов'язкового переходу країн-членів організації на використання машинозчитувальних проїзних документів, Верховна Рада України 20 листопада 2012 р. прийняла Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус», яким запроваджено в Україні документи, до безконтактного електронного носія яких вноситься інформація про біометричні параметри особи, додаткові (факультативні) біометричні дані, а також дані щодо забезпечення захисту інформації.

Відповідно до п. 2 ст. 3 зазначеного Закону *біометричні дані* – це сукупність даних про особу, зібраних на основі фіксації її характеристик, що мають достатню стабільність та істотно відрізняються від аналогічних параметрів інших осіб (основні біометричні дані, параметри – відцифрований підпис особи, відцифрований образ обличчя особи, додаткові біометричні дані, параметри – відцифровані відбитки пальців рук).

З метою забезпечення виконання вимог вказаного Закону постановою Кабінету Міністрів України від 13 березня 2013 р. № 185 затверджено єдині зразки бланків документів, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи, та порядок централізованого оформлення, видачі, обміну, пересилання, вилучення, повернення державі, знищення зазначених документів.

У червні 2006 року міністри внутрішніх справ, юстиції і генеральні прокурори країн «вісімки» виступили за відпрацювання єдиних критеріїв до документів з біометричними даними. Акцентовано на питанні забезпечення сумісності систем ідентифікації документів нового покоління, що засвідчують особу, та їх взаємного зчитування.

У країнах Європейського Союзу впровадження в обіг проїзних документів здійснюється на підставі Правил із заходів безпеки та біометричної автентифікації, прийнятих Радою Європи 13 грудня 2004 р. за № 2252/2004, відповідно до яких всі нові паспорти ЄС повинні бути машинозчитувальними і мають охоплювати з 2006 року цифрові фотографії власника, а з 2009 – відбитки пальців. Біометрична інформація збе-

рігається на чіпі (електронний носій інформації) в паспорті і в національних базах даних, зокрема у Шенгенській інформаційній системі II (SIS II).

Автентифікація – це процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора. Тобто, автентифікація – це шлях встановлення вірогідності інформації, пред'явленої користувачем у разі звернення його до системи та відкриття йому доступу, якщо він має на це право.

Нині в країнах Європи, Ізраїлі та США найбільш поширеними є два способи біометричної автентифікації: 1) за відбитками пальців; 2) за двомірним зображенням обличчя. Біометрична автентифікація за відбитками пальців вважається найбільш точною, а за двомірним зображенням обличчя може застосовуватися навіть негласно.

Крім високої надійності, на користь цих способів біометричної автентифікації також свідчить можливість їх використання майже у кожній країні. За відсутності в тій чи іншій країні бази даних щодо проїзних документів як джерела порівняльних зразків для верифікації чи ідентифікації пред'явників проїзних документів можуть виступати наявні бази даних кримінальної інформації, в яких містяться і відбитки пальців, і двомірні зображення обличчя осіб, причетних до скоєння правопорушень. Зазначені способи біометричної автентифікації вже сьогодні застосовуються у Великобританії, Ізраїлі, Латвії, Молдові, Німеччині та США. З червня 2009 р. у Греції та Фінляндії запроваджено біометричну автентифікацію за відбитками пальців, а в Чехії – за відбитками пальців і за двомірним зображенням обличчя[8].

Розширення практики застосування біометричної автентифікації в країнах Євросоюзу пов'язується із запровадженням обов'язкової біометричної автентифікації іноземців (негромадян Європейського Союзу) під час отримання ними шенгенських віз.

---

[8] Мовчан А. В. Зарубіжний досвід застосування біометричної ідентифікації людини у протидії транснаціональній злочинності / А. В. Мовчан, Д. А. Мовчан // Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. – Луганськ, 2009. – № 1. – С. 180–181.

Сьогодні практика обов'язкової біометричної автентифікації іноземців при отриманні ними віз або при в'їзді на територію країни є у Великобританії, Ізраїлі та США. Водночас у Великобританії скануються всі десять пальців, в Ізраїлі – лише вказівні, а в США – як вказівні (пункти пропуску через державний кордон), так і всі десять (дипломатичні установи за кордоном).

У найбільших пунктах перетину державного кордону Німеччини функціонують пілотні проекти з перевірки власників віз за відбитками пальців і двомірним зображенням обличчя (проект BioDev).

Недавніми роками поступово набирає поширення біометрична автентифікація за райдужною оболонкою ока. Зокрема у межах проекту «Trusted Traveler» («Надійний мандрівник») у найбільших пунктах перетину державного кордону Великобританії здійснюється додатковий контроль осіб, які в'їжджають на територію цієї країни, за вказаною біометричною характеристикою. У Німеччині цей спосіб біометричної автентифікації застосовується в міжнародному аеропорту м. Франкфурт. Такий контроль може здійснюватися лише гласно, але, на відміну від перевірки за відбитками пальців, він не викликає в особи, що перевіряється, асоціацій з перевіркою потенційних правопорушників, тому сприймається нею значно спокійніше.

Здійснення біометричної автентифікації є можливим завдяки використанню спеціальних носіїв інформації – мікрочіпів, вмонтованих у ті чи інші проїзні документи. Зазвичай на мікрочіп записуються відомості про сам проїзний документ, відомості про власника проїзного документу, біометричні дані власника проїзного документу чи посилання на місце їхнього розміщення у відповідній базі даних.

Для перевірки за біометричними характеристиками осіб, що в'їжджають на територію країни, використовують такі бази даних:

біометричної інформації (Великобританія, Греція, Ізраїль, Норвегія, Японія);

кримінальної інформації (наприклад, Automatic Fingerprints Identification Systems – автоматизовані системи ідентифікації відбитків пальців (Колумбія, Німеччина, США));

біометричної і кримінальної інформації (Латвія, Фінляндія).

Виокремлюються такі основні переваги впровадження паспортів з біометричною інформацією:

– використання захищених персональних даних підвищує довіру до документа з боку міграційних і прикордонних служб;

– цим документом не можна скористатися сторонній людині;

– новий паспорт дозволяє підвищити ефективність боротьби з тероризмом і незаконною міграцією.

Надійність біометричних паспортів України забезпечується, зокрема, такими захисними можливостями:

– внутрішні сторінки паспорта захищені водяними знаками з гербом і зображеннями на історичну тематику;

– для захисту застосовуються жовто-блакитні волокна, номера сторінок продубльовані водяними знаками;

– номер паспорта на другій сторінці надруковано червоним кольором;

– сторінка з даними власника містить зображення, які видно лише під певним кутом;

– фото власника паспорта виконано за допомогою лазерного гравіювання;

– інформація на електронному носії зашифрована;

– при спробі відкріплення ідентифікаційного чіпу він перестане працювати[9].

Системи біометричної ідентифікації складаються із центральної бази даних і польових терміналів. Бази даних призначені для зберігання фотографій, реєстрації електронних відбитків пальців і долонь, ідентифікаційного пошуку за біометричними даними, мобільної автоматичної ідентифікації. Польовий термінал – це портативний блок біометричної ідентифікації, з'єднаний з центральною базою даних по каналах радіозв'язку.

---

[9] Особенности биометрического паспорта [Электронный ресурс]. – Режим доступа: http://vesti-ukr.com/infografika/81796-osobennosti-biometricheskogo-pasporta.

У зв'язку з простотою перевірки відповідності обличчя пред'явника двомірному цифровому зображенню офіційного власника проїзного документа спеціальні прилади для контролю цієї біометричної характеристики особи здебільшого не застосовуються. Проте в міжнародному аеропорту Риги (Латвія) Служба охорони державного кордону цієї країни випробовує експериментальну систему контролю осіб за двомірним зображенням обличчя. На початку березня 2013 р. стартував експеримент зі застосування біометричних технологій в аеропорту Хітроу (Великобританія). Для перевірки пред'явників проїзних документів за відбитками пальців у Великобританії, Ізраїлі та США застосовують спеціальні сканери.

Через запровадження біометричного контролю іноземців, які в'їжджають до країн Європейського Союзу, подібні сканери будуть встановлені в пунктах перетину кордону Євросоюзу.

За весь період застосування біометричних технологій створено велику кількість дактилоскопічних сканерів отримання папілярних узорів пальців рук людини з використанням різних технологій, але майже всім цим сканерам притаманна одна негативна особливість – неможливість визначити природне походження об'єкта сканування, тобто відрізнити справжній папілярний узор пальця від штучного (муляжу). Отже, існує ймовірність протизаконного використання папілярних узорів пальців рук однієї людини, отриманих з будь-яких предметів, іншою, що дає можливість певним особам ідентифікувати себе як іншу людину.

Зокрема у 2002 році аспірант національного університету Йокогами Ц. Мацумото опублікував результати своїх досліджень про те, як він з використанням желатину і пластикового шаблону виготовив «підроблений палець», який успішно «проходив» через сканер у чотирьох випадках із п'яти.

У першому методі Мацумото виготовив зліпок з пальця «жертви», для чого було використано харчовий желатин і формувальний пластик, що застосовується авіа- та судомоделістами. Желатинову смужку-відбиток можна непомітно приліпити до власного пальця і обманути комп'ютерну систему доступу навіть у присутності охоронця.

Більш ефективним виявився інший метод Мацумото, за яким обробляється один із залишених на різних предметах

відбитків пальця «жертви». Знявши відбиток пальця з предмета, дослідники поліпшили його якість за допомогою ціанакрилатного адгезиву (парів супер-клею) і сфотографували результат цифровою камерою. Потім контрастність знімка була оптимізована за допомогою графічного редактора, після чого знімок роздрукували на прозорій плівці. Для виготовлення об'ємного відбитка Мацумото скористався методом фотолітографії: на світлочутливу друковану плату-заготовку спроектували «палець» з плівки і витравили відбиток на міді. Ця плата стала формою для желатинового «фальшивого пальця», який обманював практично всі з випробуваних біометричних систем – і з оптичними, і з ємнісними сенсорами. Після деякого тренування желатиновий зліпок дозволив дослідникам обманювати і новітніші системи, обладнані «детекторами живого пальця», що реагують на вологість або електричний опір[10].

Проведене у ДНДІ МВС України дослідження засвідчило, що в сучасних методах біометричної ідентифікації використовуються оптичні, електрооптичні, ємнісні, радіочастотні, ультразвукові, температурні, натискні, оптоволоконні сканери для отримання папілярних узорів пальців рук людини.

Під час дослідження здійснено порівняння можливостей отримання відбитків живих пальців і їх муляжів на прикладі: електрооптичного сканера «ДактоБАТ» (Україна); оптичного сканера «Futronic FS88» (Гонконг); протяжного термосканера «Ufis110» (Німеччина); ємнісного сканера «Pocket PC» (Росія) і долонного оптичного сканера «DactyScan84» (Італія).

За результатами проведених випробувань встановлено, що дактилоскопічні сканери, робота яких заснована на використанні оптичних, температурних і ємнісних датчиків, технічно не можуть відрізнити муляжі від живих пальців рук людини, тобто мають низьку селективність (вибірковість).

Електрооптичний дактилоскопічний сканер «ДактоБАТ» відрізняє муляж, нанесений на будь-яку поверхню, від живого

---

[10] Михайлов М. А. Проблема идентификации личности выходит за пределы, определяемые предметом криминалистики / М. А. Михайлов // Ученые записки Таврического национального университета им. В. И. Вернадского. Серия «Юридические науки». – № 2. – Т. 20 (59).– 2007. – С. 156.

пальця й може бути використаний для достовірного дактилоскопіювання осіб безфарбовим методом з метою отримання зображень відбитків папілярних узорів пальців рук в електронному вигляді для проведення оперативних перевірок за дактилообліками й ідентифікації, а також у будь-якій іншій сфері життєдіяльності, що потребує використання біометричних технологій ідентифікації особи.

Крім того, електрооптичний дактилоскопічний сканер «ДактоБАТ» дає можливість отримувати трьохвимірне зображення папілярних узорів пальців рук людини, що розширює можливості ідентифікації, та отримувати просторове розміщення біологічно активних точок.

Фахівці вважають, що нині є сканери, які виявляють більшість муляжів. Найефективнішими вважаються сканери фірми Lumidigm (США) і NEC (Японія). Перший сканер використовує багатоспектральне випромінювання, проникаюче під шкіру, а другий використовує не тільки зображення відбитка пальця, а й малюнок вен.

У сканерах компанії «Сонда Технолоджі» для захисту від муляжів використовується вимір пульсу. Крім того, потрібно враховувати, що при накладанні на палець муляжних плівок різко знижується освітленість[11].

Експерт в області інформаційної безпеки М. Роджерс провів експеримент, у процесі якого він спробував «зламати» дактилоскопічний модуль Touch ID смартфона iPhone 6. Біометричний сканер iPhone 6 вбудований в кнопку Home, для його використання необхідно попередньо створити резервний код ідентифікації і ввести зразки відбитків тих пальців, за допомогою яких користувач буде розблоковувати телефон.

Для «злому» Touch ID Роджерс сфотографував відбиток пальця власника iPhone, потім обробив фотографію в «фотошопі» – підчистив і інвертував за кольором. Далі йому знадобилися плівка і лазерний принтер з роздільною здатністю 1200 dpi і товстим шаром тонера. Перед тим, як прикласти

---

[11] Биометрия 2013: пора отказываться от банковских карт. Мечта? [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/post/174397/.

«зліпок» до кнопки iPhone, на паперову копію відбитка наноситься латексне молочко або білий столярний клей. Подібну техніку Роджерс застосовував для обходу сканера безпеки iPhone 5s.

Експерт з'ясував, що Touch ID другого покоління надійніший, ніж оригінальний модуль iPhone 5s. У нього вища роздільна здатність і ширша область сканування. Виготовлений зліпок повинен бути товстішим, щоб не проглядався чужий палець. Крім того, необхідна більш чітка фотографія папілярного узору.

Обійти захист iPhone 6 в домашніх умовах практично неможливо. Спосіб «злому» Touch ID набагато складніший застосовуваного для обману сканерів «силіконового» зліпка пальця, тобто від звичайних підробок сканер смартфона захищений[12].

Водночас існують також організаційні методи боротьби з муляжами:

– по-перше, необхідно встановлювати сканери по можливості в публічних місцях;

– по-друге, для платіжних систем застосовувати спеціальний сканер, де використовується подвійне прикладання пальця, причому, другий раз сканер підказує який саме палець потрібно докласти;

– по-третє, використовувати так званий «тривожний палець» – його потрібно прикладати під примусом, у результаті рахунок буде заблокований і сигнал тривоги піде правоохоронцям.

Для надійності та боротьби з помилковими спрацьовуваннями обов'язково слід використовувати два пальці. Під час проведення міжнародних тестів, де відбитки були отримані за допомогою оптичних сканерів, зафіксована ймовірність помилкового спрацьовування приблизно на рівні однієї помилки на тисячу випадків, при використанні двох пальців – одна помилка на мільйон випадків.

---

[12] Обновленный Touch ID в iPhone 6 сложнее взломать, чем сканер отпечатков iPhone 5s [Электронный ресурс]. – Режим доступа: http://www.macdigger.ru/iphone-ipod/touch-id-2-v-iphone-6-slozhnee-vzlomat-chem-skaner-otpechatkov-iphone-5s.html.

Відповідно до Плану заходів зі створення системи контролю іноземців та осіб без громадянства, що в'їжджають на територію України, з фіксуванням їх біометричних даних, затвердженого розпорядженням Кабінету Міністрів України від 12 березня 2008 р. № 439-р, передбачено впровадження біометричних технологій в інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон (система «Аркан») і у відповідні відомчі системи.

За інформацією Державної прикордонної служби, усі 157 пунктів міжнародного прикордонного контролю в Україні вже обладнані пристроями для зчитування біометричних паспортів у межах підготовки до безвізового режиму з Європейським союзом та підключені до баз даних Інтерполу[13].

Розпізнавання за зображенням обличчя. Розпізнавання за допомогою біометричних технологій передбачає порівняння раніше виділеного біометричного зразка зі знову отриманими біометричними даними.

Робота всіх біометричних систем заснована, як правило, на типовому алгоритмі, який узагальнено можна уявити так:

– *запис* – фізичний або поведінковий зразок запам'ятовується системою;

– *виділення шаблону* – унікальна інформація виділяється зі зразка і створюється біометричний шаблон;

– *порівняння* – збережений зразок порівнюється з поданим;

– *співпадіння/неспівпадіння* – система вирішує, чи збігаються біометричні зразки й виносить рішення.

Принцип роботи автоматизованої системи ідентифікації особи заснований на спеціальному алгоритмі переводу зображень у цифровий формат, водночас здійснюється програмний пошук обличчя в кадрі та визначення характерних ознак його будови – так званих «реперних точок» (форма очей,

---

[13] Біометричні паспорти тепер можуть зчитувати на всіх прикордонних пунктах України [Електронний ресурс]. – Режим доступу: http://www http://hromadske.ua/posts/biometrychni-pasporty-teper-mozhut-zchytuvaty-na-vsikh-prykordonnykh-punktakh-ukrainy.

скули, ширина перенісся, губ тощо). Відтак кожне обличчя описується унікальним набором параметрів.

Для ідентифікації з високим ступенем точності достатньо близько 40 характеристик, тоді як система задає декілька тисяч оціночних параметрів. Фотографія та цифровий опис обличчя заносяться до бази даних, за якою надалі здійснюється пошук.

Ефективність біометричних систем ідентифікації особи, що використовують методи автоматизованої обробки зображення обличчя, визначається дотриманням низки обов'язкових вимог, які забезпечують кількісні та якісні характеристики базової фототеки.

Основними джерелами біометричних шаблонів автоматизованих систем ідентифікації особи є:

– фотопортрет обличчя, поданий у цифровому вигляді;

– фотографія портретного типу (для подальшого сканування);

– цифровий «відеопотік» (окремий фрагмент у вигляді медіафайлу або відеосигнал, який надходить у режимі on-line).

Перспективним для оперативно-розшукової ідентифікації вважається використання відеоінформації з камер спостереження, встановлених на вулицях та інших місцях (супермаркети, магазини, ринки, банківські установи, обмінні пункти валюти, вокзали, станції та вагони метрополітену, аеропорти, стадіони, спортивні комплекси, АЗС, розважальні заклади, ресторани, навчальні заклади, офіси фірм тощо), відеокамер банкоматів, автомобільних відеореєстраторів тощо.

Сучасні системи біометричної ідентифікації особи нового покоління спроектовані як багатофакторні – ідентифікація буде проводитися за сукупністю різних біометричних параметрів, список яких в майбутньому можна буде збільшити.

Зокрема розробка системи Next Generation Identification (NGI) призначена замінити застарілу систему автоматичного розпізнавання відбитків пальців, яка тривалий час була головною біометричної базою даних ФБР.

Система NGI містить набагато більше інформації, ніж попередні системи: відбитки пальців, знімки райдужної оболонки ока, фотографії шрамів і татуювань осіб, якими зацікавились

правоохоронні органи США, а також зображення обличчя людей. Крім фотографій затриманих поліцією осіб, до бази даних NGI належать фото і біометричні дані людей, які працюють у сферах, пов'язаних з підвищеною відповідальністю, зокрема, банківських службовців[14].

Застосування систем відеоспостереження особливо актуально під час проведення масових спортивних, культурних, суспільно-політичних та інших заходів за участю великої кількості учасників і глядачів.

Напередодні чемпіонату Європи з футболу 2012 року у громадських місцях приймаючих міст ЄВРО 2012 в Україні встановлено 179 камер відеоспостереження (Київ – 35; Донецьк – 75; Харків – 40; Львів – 29).

У межах реалізації програми «Безпечне місто» ГУМВС України у м. Києві напередодні чемпіонату ЄВРО 2012 введено в експлуатацію автоматизовану систему централізованого управління нарядами патрульної служби «ЦУНАМІ», яка включає:

– геоінформаційну систему (електронну карту міста);
– систему супутникового GPS-позиціювання та мобільного комунікаційного обладнання;
– систему відеоспостереження;
– систему колективного відображення.

При надходженні повідомлення про злочин до служби «102» на монітор оператора виводиться інформація про номер абонента та статистичні дані про цей номер. У разі визначення адреси встановлення цього телефонного номера, на монітор оператора виводиться інформація з баз даних «АРМОР». Ця інформація разом з номером телефона заявника автоматично передається на робоче місце диспетчера-чергового.

Сьогодні у м. Києві в межах програми «Безпечне місто» встановлено 4 тисячі відеокамер: 3423 камери – на об'єктах соціальної інфраструктури міста (у школах, дитячих садках, поліклініках, лікарнях, музеях та театрах), 339 камер – у центрі

---

[14] Новая система распознавания лиц и биометрической идентификации ФБР готова к эксплуатации [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/company/nordavind/blog/236993/.

міста та на автомобільних мостах через річку Дніпро, на Майдані Незалежності встановлена унікальна камера панав'ю з оглядом у 360 градусів. Завдяки функції розпізнавання державних номерних знаків забезпечено можливість безперервного контролю транспортних потоків, пошуку викрадених автомобілів.

Смарткамери мають свій, заздалегідь запрограмований сценарій інцидентів, у разі виникнення яких система автоматично інформує ситуаційний центр, що дає змогу забезпечити оперативну реакцію відповідних служб[15].

Безпрецедентні заходи безпеки були вжиті при проведенні Чемпіонату світу з футболу 2014 року в Бразилії. З метою забезпечення ефективного захисту громадян, туристів та їх майна на автостанціях Бразилії BRT MOVE було встановлено понад 300 одиниць 1.3-мегапіксельних мережевих відеокамер спостереження Hikvision DS-2CD864F-E з функцією WDR. Ці відеокамери спостереження, які мають можливість функціонувати в умовах низької освітленості, демонструють ефективне отримання зображень в кольоровому і чорно-білому режимі. Крім того, функція 3D цифрового шумозаглушення і наявність режиму «день/ніч» забезпечують високу якість зображення з роздільною здатністю 1280x960 незалежно від часу доби.

За допомогою мегапіксельних зображень, одержуваних цією камерою, співробітники служби безпеки можуть ідентифікувати підозрілих людей і предмети на автовокзалах та в їх околицях. Також, за необхідності, отримані відеозображення можуть бути надані для судово-медичних експертиз[16].

Крім того, для забезпечення безпеки Чемпіонату світу з футболу поліція Бразилії придбала окуляри Ex-Eye з відеокамерами, дисплеєм на зразок Google Glass і портативними

---

[15] Презентація загальноміської системи відеонагляду: 4 тисячі відеокамер наглядають за безпекою міста [Електронний ресурс]. – Режим доступу: https://www.facebook.com/ilyasagaidak?fref=ts.

[16] IP видеонаблюдение от Hikvision обеспечивает безопасность на Чемпионате мира по футболу 2014 в Бразилии [Електронний ресурс]. – Режим доступу: http://www.worldvision.su/news/novosti-tehniki/ip-videonablyudenie-ot-hikvision-obespechivaet-bezopasnost-na-chempionate-mira-po-futbolu-2014-v-brazilii-606.html.

комп'ютерами на базі Intel Atom, підключеними до бездротової мережі, які можуть записувати відео, розпізнавати обличчя і шукати збіги в базі даних з мільйонів осіб злочинців, терористів і футбольних хуліганів.

Розробником системи є ізраїльська компанія Ex-Sight. За кілька десятих часток секунди особи, що потрапили в кадр, розпізнаються, і для кожного з них формується «відбиток», що містить біометричні характеристики. Кожен такий відбиток займає всього 2,4 кілобайт, що дає змогу доволі швидко сканувати великі бази даних. Крім осіб, система вміє розпізнавати автомобільні номери[17].

Зважаючи на те, що процес ідентифікації передбачає встановлення тотожності невідомого об'єкта відомому на підставі збігу ознак, будь-якому фотозображенню, що буде брати участь у процесі біометричного впізнання, повинні бути встановлені унікальні атрибути. Відтак фотозображення перед виділенням унікальної інформації для створення біометричного шаблона (процес кодування) заноситься до інтегрованого банку даних з обов'язковою прив'язкою до категорійного об'єкта обліку.

Як свідчить аналіз, більшість систем, що використовують біометричні технології, функціонально обмежені виконанням завдань ідентифікації або верифікації об'єкта, без можливості отримання більш повної інформації про об'єкт аналізу, що значно знижує ефективність використання подібних систем.

Водночас ідентифікація з використанням фотозображень у системі «АРГУС» дає змогу здійснювати ідентифікацію осіб криміногенних категорій, невідомих хворих, невпізнаних трупів громадян, біометричні шаблони яких попередньо були внесені до інтегрованого банку даних. Результатом відповіді на поданий системі запит на ідентифікацію є набір фотозображень і список осіб, які мають найбільшу відповідність і максимальну схожість з фотозображенням, наданим для пошуку,

---

[17] Чемпионат мира по футболу в Бразилии будут охранять роботы, беспилотники и полицейские в очках, распознающих лица [Електронний ресурс]. – Режим доступу: http://habrahabr.ru/company/ nordavind/blog/180587/.

а також розгорнуте досьє на кожний об'єкт аналізу і відповідні дані[18].

Верифікація дозволяє здійснювати порівняння двох фотозображень з метою визначення ступеня схожості та відповіді на запитання «Ви дійсно той, за кого себе видаєте?» Крім того, користувач має можливість здійснити поглиблений аналіз з використанням можливостей АІС «Сова» та АІС «АРМОР».

Водночас розглянута система біометричної ідентифікації містить низку прогалин, зокрема, не вдається досягти необхідної точності ідентифікації при впізнанні невпізнаних трупів з ознаками значних змін зовнішнього стану, чи окремих частин тіла, а також встановлення особи злочинця за словесним описом.

Прикладом поєднання всіх видів оперативно-розшукової ідентифікації є створення та впровадження в практичну діяльність правоохоронних органів комплексів оперативних (розшукових) перевірок для встановлення особи, які у термін до 10 хвилин з використанням супутникового зв'язку здійснюють такі операції: встановлення особи затриманих, підозрюваних, обвинувачених, осіб, які скоїли адмінправопорушення, та їх зображень, а також на основі дослідження відбитків пальців рук; наведення довідок в АІПС про знаходження осіб у розшуку, про скоєні ними раніше правопорушення, про наявність документів, що засвідчують особу тощо.

Комплекси оперативних (розшукових) перевірок забезпечують отримання цифрових фотозображень, безфарбове дактилоскопування фігурантів, формування запитів в банки даних та отримання результатів перевірки і в стаціонарних, і в польових умовах. За відсутності каналів зв'язку перевірка може проводитись за локальною базою даних.

Конструктивно мобільний комплекс виконано у вигляді валізи, яка комплектується комп'ютером-ноутбуком зі спеціалізованим програмним забезпеченням, цифровим фотоапаратом, планшетним і дактилоскопічним сканерами, засобами

---

[18] Задорожный Ю. А. Проблемы информатизации органов внутренних дел / Ю. А. Задорожный // Вісник Луганського державного університету внутрішніх справ. – 2007. – № 2. – С. 221–222.

супутникового зв'язку, фотопринтером, батареєю підвищеної ємності та автомобільним перетворювачем напруги.

Комплекс дозволяє фотографувати й дактилоскопувати затриманих осіб, формувати запити до банків даних, які містять зображення обличчя, відбитки пальців і установочні дані, відправляти запити по каналах зв'язку, отримувати результати перевірок.

Ефективність застосування систем біометричної ідентифікації в правоохоронній діяльності залежить від багатьох чинників. Наприклад, поліція графства Лестершир (Великобританія) заявила про успішне впровадження системи NeoFace компанії NEC. Позитивний результат цього експерименту обумовлений високою якістю зображень в базі даних поліцейського управління графства, в якій на момент впровадження системи зберігалося 92 тис. записів. Для формування цієї бази було придбано спеціальне програмне забезпечення.

Водночас лондонські поліцейські вважають, що за зображенням, знятим у вуличних умовах, проводити ідентифікацію набагато складніше й ефективність її значно знижується. Якщо в аеропортах якість зображення доволі висока, то вже в супермаркетах можуть спостерігатися збої. Результат розпізнавання може бути негативним, якщо камера не мегапіксельна, освітлення компромісне, ракурс зйомки не фронтальний, а на задньому плані є джерела світла. Системи розпізнавання за зображенням особи, що знаходяться на озброєнні лондонської поліції, за півтора року роботи зуміли ідентифікувати ледь десяток розшукуваних. Для порівняння: штатні лондонські розпізнавані упізнають протягом тижня до півтори сотні людей. При розслідуванні так званих «лондонських бунтів» (серпень 2011 року), один із суперрозпізнавачів зумів впізнати 180 осіб, у той час як система зуміла знайти лише один збіг[19].

Важливе значення для оперативно-розшукової ідентифікації розроблюваних осіб має інформація щодо наявності у них терміналів рухомого (мобільного) зв'язку, адже сьогодні більшість громадян України, зокрема й криміногенні особи,

---

[19] Мнения правоохранителей о распознавании лиц разделились [Електронний ресурс]. – Режим доступу: http://www.secnews.ru/digest/ 21049.htm.

постійно користуються засобами мобільного зв'язку. За даними Державної служби статистики, кількість користувачів мобільного зв'язку в Україні становить 57624,0 тис. абонентів[20].

За інформацією Scientific Reports, вчені можуть ідентифікувати особу навіть за обмеженою інформацією щодо переміщення терміналу мобільного зв'язку. Аналіз даних дослідження про переміщення 1,5 млн мобільних телефонів протягом 15 місяців показав, що для унікального визначення одного користувача мережі достатньо знати чотири місця, в яких він з'являється в конкретний час доби. Зазначений критерій дозволив дослідникам успішно розпізнати 95% осіб із загальної вибірки[21].

З метою автоматизації аналізу інформації, отриманої за наслідками моніторингу місця вчинення злочину, використовується спеціалізоване програмне забезпечення, зокрема, програмні продукти, розроблені компаніями i2 Limited, Visual Analytics і Xanalys. Так, Analyst's Notebook – це програмний продукт компанії i2 Limited, призначений для аналізу системи пов'язаних об'єктів і динаміки послідовних подій. Об'єкти на діаграмі можуть бути подані не тільки як піктограми, але й у вигляді фотографій, файлів, аудіо-, відеозаписів тощо.

Одним із перспективних напрямів використання систем біометричної ідентифікації особи є здійснення пошукових заходів у кіберпросторі. Адже соціальні мережі – це величезний архів оцифрованих зображень, які цілком піддаються комп'ютерній обробці за допомогою відповідних систем. Водночас об'єктом дослідження може бути не лише зображення користувача, а також особи, які були зафіксовані на передньому чи задньому плані зображення. Маючи зображення особи, яка становить оперативний інтерес, за допомогою біометрії можливо встановити її місцезнаходження, зв'язки, або хоча б напрям для подальшого пошуку.

---

[20] Транспорт і зв'язок України – 2015. Статистичний збірник. – К.: Державна служба статистики України, 2015. – С. 181.

[21] Ученые идентифицировали людей по перемещению их телефонов [Електронний ресурс]. – Режим доступу: http://lenta.ru/news/2013/03/27/mobility/.

Отже, використання сучасних інформаційно-пошукових систем ідентифікації особи спроможне значно спростити пошук та ідентифікацію злочинців і терористів. До характерних особливостей оперативно-розшукової ідентифікації належать:

1) *оперативно-розшукова ідентифікація* – розглядається як процес досягнення абсолютної тотожності за відображенням індивідуальних ідентифікаційних ознак, а також як процес встановлення групової належності об'єктів на підставі дослідження їх групових ознак;

2) *оперативно-розшукова ідентифікація* – передбачає проведення одного з таких оперативно-розшукових та оперативно-пошукових заходів:

– оперативне ототожнення осіб, предметів та речовин;

– отримання довідково-аналітичної інформації;

– дослідження предметів і документів (у частині проведення ідентифікаційних досліджень);

– зняття інформації з транспортних телекомунікаційних мереж;

– зняття інформації з електронних інформаційних мереж;

– установлення місцезнаходження радіоелектронного засобу;

– радіотехнічна розвідка;

3) як *об'єкти оперативно-розшукової ідентифікації* розглядаються:

– індивідуально-визначені тіла, що мають стійку зовнішню будову (особи, предмети, тварини, трупи людей, приміщення, споруди, ділянки місцевості);

– речовини (порошкоподібні, рідкі, газоподібні);

– явища, процеси, події, навички, мережа Інтернет, трафіки зв'язків абонентів мобільного зв'язку, зовнішні дії особи, тобто об'єкти, які взагалі не мають матеріального втілення;

4) оперативно-розшукову ідентифікацію здійснюють працівники оперативних, оперативно-технічних, інформаційно-аналітичних підрозділів і певною мірою інші працівники поліції та негласні працівники (*суб'єкти оперативно-розшукової ідентифікації*);

5) *метою оперативно-розшукової ідентифікації* є вирішення завдань ОРД, які полягають у пошуку, отриманні та фіксації фактичних даних про протиправні дії окремих осіб та груп, що мають безпосереднє відношення до процесу доказування у кримінальних провадженнях.

3.3. Застосування інформаційно-аналітичних технологій для вирішення завдань оперативно-розшукової діагностики

Одним із основних видів оперативно-розшукової діагностики є *оперативне розпізнавання*, яке зі змістовного боку є пізнавальною (емпіричною) складовою оперативного пошуку – діяльності, спрямованої на виявлення об'єктів, які становлять інтерес для кримінального аналізу. В етимологічному значенні поняття «пошук» тлумачиться через терміни «шукання», «розшукування».

Науковці визначають *оперативний пошук* як систему розвідувально-пошукових заходів, що здійснюються її уповноваженими суб'єктами для отримання та перевірки первинної інформації щодо осіб, предметів і подій, які становлять оперативний інтерес для оперативних підрозділів з метою встановлення ознак злочину чи спростування інформації про нього. Оперативний пошук здійснюється і особисто суб'єктами пошуку (особистий пошук), і з залученням до нього відповідних сил і засобів, зокрема й інформаційних систем, відео- та аудіозапису, кіно- та фотозйомки тощо[22].

Об'єктами особистого пошуку є особи, факти, події, явища, предмети, документи, що становлять оперативний інтерес для оперативних підрозділів, зокрема:

1) *особи:*

– підозрювані у вчиненні злочинів, їх плануванні чи в готуванні або підбурюванні до них та їхні зв'язки;

– від поведінки яких можна очікувати вчинення злочину;

– які знаходяться в розшуку;

---

[22] Погорецький М. А. Пошукові ознаки об'єктів оперативного пошуку: поняття та сутність / М. А. Погорецький, В. П. Шеломенцев // Вісник Академії управління МВС. – К., 2010. – № 4. – С. 115–116.

– психічно хворі, які схильні до скоєння правопорушень;

– які володіють інформацією, що має оперативно-розшукове значення;

– які спроможні систематично надавати допомогу правоохоронним органам чи сприяти виконанню оперативно-розшукових завдань;

2) *факти, події, явища:*

– подія злочину;

– обставини, що сприяють учиненню злочинів;

– мережа Інтернет;

– радіоефір;

– трафіки зв'язків абонентів мобільного зв'язку;

3) *предмети, документи:*

– майно, отримане злочинним шляхом;

– знаряддя та засоби вчинення злочину;

– інші предмети, які мають оперативно-розшукове значення або можуть бути речовими доказами тощо[23].

Оперативне розпізнавання за ознаками зовнішності особи поділяється на три групи:

1) за ознаками статі, віку, зросту, комплекції тіла, типу зовнішності, статури, ходи, деталей одягу та побуту, які дають можливість розпізнати особу серед натовпу;

2) за ознаками, що переважають у зовнішності особи, а саме: асиметрія в будові голови, обличчя і його частин, характерний вираз обличчя, особливості одягу та інших елементів зовнішності;

3) за ознаками, які індивідуалізують зовнішній вигляд особи, за якими проводиться її остаточна ідентифікація.

Залежно від пошукових властивостей ознаки, за якими здійснюється оперативне розпізнання, поділяються на дві групи. До першої з них належать ознаки, які дозволяють установити групову належність об'єкта розпізнання. В основі такого розпізнання є загальні ознаки поведінки, найбільш характерні для осіб, що становлять оперативний інтерес, а також ознаки, загальні для групи злочинів.

---

[23] Оперативне розпізнавання: монографія / В. А. Некрасов, В. Я. Мацюк, Н. Є. Філіпенко, Л. В. Родинюк. – К.: КНТ, 2007. – С. 35.

До другого різновиду пошукових ознак належать ті, за якими встановлюється тотожність (індивідуальні ознаки). Тобто йдеться про ознаки, характерні конкретній особі або предмету.

Свої особливості має розпізнавання з метою розкриття злочинів, що здійснюється шляхом розшуку викраденого майна. Знаючи його характерні ознаки, оперативні працівники мають можливість розпізнати їх у числі інших речей. Оцінюючи поведінку «продавця», можна припустити, що має місце збут краденого. Наприклад, настороженість або спроби здійснити оборудку потай від оточуючих осіб. Ретельніше спостереження й перевірка дозволяють ідентифікувати майно як викрадене під час вчинення конкретного злочину.

Варто зазначити, що злочини виявляються здебільшого за динамічними (функціональними) ознаками, які характеризуються специфічним алгоритмом кримінальної дії (бездіяльності). Прикладом може слугувати оперативне розпізнавання підготовки вчинення кишенькової крадіжки в місцях масового скупчення людей, де кожний учасник злочинної групи виконує певну рольову функцію, зокрема, навмисно створюється тиснява в громадському транспорті, штовханина серед пасажирів, хоча це не зумовлено необхідністю.

Іншим видом встановлення факту вчинення злочинного діяння є емпіричне розпізнавання його матеріальних слідів на місці події, наприклад, виявлення ножових ран на тілі потерпілого; візуальне виявлення фактів підробки документів, що здійснюється з метою незаконного переміщення товару через митний кордон; виявлення на вході в приміщення зламаного замка в момент, коли відбувається крадіжка; виявлення слідів вибухових речовин тощо. Ознаки тих чи інших триваючих злочинів можна виявити у різних інформаційних середовищах, зокрема в кіберпросторі.

Як уже зазначалося, існує чітка диференціація функціональних і ознак, що характеризують злочинні навички фізичних осіб, і функціональних ознак, властивих злочинним діянням. У першому випадку об'єктом розпізнання є безпосередньо особи, які демонструють певний набір скелетно-м'язових рухів. У другому випадку це процес (дія або бездіяльність з боку

людей), закономірний результат цього процесу, а також причинний зв'язок між ними. Причому необхідно докласти зусиль для розпізнання кожного з цих елементів окремо, незалежно один від одного, що дає змогу здійснити попередню кваліфікацію злочину за його об'єктивною стороною. Тобто йдеться про кримінально-правову оцінку розшукової інформації.

Об'єкти розпізнання (предмети, речовини і документи) поділяються на такі категорії:

1) предмети і речовини, незаконний обіг яких тягне за собою кримінальну відповідальність (зброя, боєприпаси, вибухові речовини та пристрої, наркотичні засоби, психотропні речовини та їх прекурсори тощо);

2) знаряддя та засоби вчинення злочину;

3) інші предмети, речі та документи, залучені до вчинення злочинів;

4) предмети, речовини і документи – носії слідів злочинного діяння.

Розпізнавання терористичних загроз. Учинені в останні роки терористичні акти на об'єктах транспортної галузі різних країн свідчать про необхідність перегляду систем їх комплексної безпеки.

За даними Державної служби статистики в Україні лише в метро протягом року перевозиться 726 млн пасажирів (Київ – 504, Харків – 215, Дніпро – 7), для перевезення пасажирів використовується 1190 вагонів метрополітену (Київ – 824, Харків – 321, Дніпро – 45)[24].

Водночас за останні десятиліття здійснено низку терористичних актів у метрополітені найбільших міст світу. Зокрема 25 липня 1995 р. на станції метро в центрі Парижа вибухнув газовий балон, начинений цвяхами, водночас вісім людей загинули і 117 були поранені. У результаті теракту 3 грудня 1996 р. – четверо загиблих, 100 поранених.

20 березня 1995 р. терористи з радикального руху «Аум Сінрікьо» на п'яти станціях токійського метро застосували отруйний газ зарин. Внаслідок газової атаки загинуло 12 осіб, 5,5 тис. отримали отруєння.

---

[24] Транспорт і зв'язок України. Статистичний збірник. – К.: Державна служба статистики України, 2015. – С. 181.

Вранці 7 липня 2005 р. в лондонському метро з інтервалом в 50 сек. сталися три вибухи, через годину смертник підірвав автобус. У результаті терактів загинули 52 людини, 700 отримали поранення.

У московському метрополітені скоєно 8 терористичних актів, під час здійснення яких 116 осіб загинуло, 419 – поранено. 11 квітня 2011 року на станції метро «Жовтнева» в Мінську скоєно терористичний акт, у результаті якого 15 людей загинуло, 203 – поранено[25].

З огляду на те, що аеропорти, вокзали, станції метрополітену є місцем масового перебування людей, проблеми своєчасної ідентифікації терористів і вибухових пристроїв є надзвичайно актуальними в сучасних умовах. Одним з напрямів підвищення безпеки пасажирів є застосування сучасних біометричних систем. Подібні системи вже впроваджуються в аеропорту Хітроу (Великобританія), аеропорту імені Джона Кеннеді (США) і в інших транспортних вузлах.

Біометрична інформаційно-пошукова система відеоспостереження дозволяє в автоматичному режимі проводити ідентифікацію в потоці людей, здійснюючи перевірку отриманих зображень за базами даних осіб, які перебувають у розшуку. Виділені зображення осіб передаються на сервери розпізнавання (які можуть бути як локальними, так і віддаленими), в яких здійснюється миттєва, за частки секунди, перевірка зображень осіб з фотографіями розшукуваних терористів, злочинців, правопорушників. У разі подібності фотозображення людини, знятого відеокамерою в натовпі людей, з розшукуваною особою, система сповіщає в установленому порядку уповноважений правоохоронний орган, який і приймає рішення про подальші оперативні заходи. Відтак система вирішує такі завдання – розпізнавання осіб в потоці людей, пошук осіб у відеоархіві, пошук осіб у базі даних, що містить фотозображення та персональні дані[26].

---

[25] Теракты в московском метро: длинная история взрывов [Электронный ресурс]. – Режим доступа: http://www.chuchotezvous.ru/social-disasters/24.html.

[26] «Сова-видеопоток» [Электронный ресурс]. – Режим доступа: http://www.ladacom.ru/site/node/18.

Водночас однією з головних проблем під час впровадження та експлуатації систем біометричної ідентифікації за зображенням особи є складні умови роботи. На ефективність роботи алгоритмів ідентифікації, а отже, і на ефективність пошуку в потоці людей безпосередньо впливають такі чинники, як умови освітленості (рівень і рівномірність освітлення), ракурси осіб, якість контрольних фотографій, швидкість, щільність і напрямок потоку людей і низка інших чинників.

Свого часу компанією «Комплексні технології безпеки» презентовано систему «Спартан 300», що призначена для виявлення у натовпі людей, поведінка яких відхиляється від норми. Розробники системи позиціонують її як універсальний автоматичний інструмент контролю пасажирських потоків на транспорті. Для аналізу потоку пасажирів використовується штучна нейронна мережа, яку розробники системи відпрацювали на базових емоціях Пола Екмана. Оператор такої системи бачить людський потік, в якому обличчя звичайних людей укладені в зелену рамку, а обличчя людей у зміненому стані – у червону.

З метою попередження терористичних загроз на об'єктах транспортної інфраструктури передбачено розгортання при вході в пасажирську зону станцій метрополітену та залізничних вокзалів доглядової зони (стаціонарний рамочний металодетектор, стаціонарний рентгенівський сканер для предметів, стаціонарний сканер для пасажирів, вибухозахисний контейнер, локалізатор вибухових речовин, експрес-аналізатори вибухових речовин тощо).

Для проведення оперативних та пошукових заходів підрозділи поліції використовують рентгенотелевізійні комплекси «Шмель-240 ТВ», «Колибри-150 ТВ», доглядові відеокомплекси «Шмель-В1», «Шмель-В2», «Шмель-3N», портативні металодетектори SPHINX BM-612, MD-3003 B1, GARNET SUPERWAND, PD140 C.E.I.A, сканери «Ватсон», комбіновані доглядові пристрої, пошукові радіометри тощо. На думку фахівців-вибухотехніків, 95% завдань, які стоять перед ними, вирішуються комплексом «Шмель-240 ТВ».

У боротьбі з «поштовим» тероризмом найчастіше використовуються стаціонарні рентгенотелевізійні установки

«Калан-2М», «Калан-4», портативні рентгенотелевізійні установки «Норка», настільні рентгенотелевізійні установки XR-PSCAN, які дають змогу оглядати і виявляти вибухові та інші потенційно небезпечні речовини в багажі, листах, бандеролях, контейнерах, у залишених сумках, пакетах тощо.

У разі виявлення знарядь злочину та інших предметів «подвійного» призначення можуть застосовуватися спеціальні технічні засоби. Наприклад, для розпізнавання вибухових речовин використовуються ручні детектори, які виявляють сліди вибухових речовин (зокрема аналізатори парів вибухових речовин «Пилот-М», Е-3500 тощо), детектори годинникових механізмів «Анкер-4Е», «Анкер-Е», набори спреїв «Поиск-ХТ». У зв'язку з поширенням останніми роками пластикової вибухівки, яка фактично не має запаху, найбільш ефективним способом її виявлення, крім маркування, є пошук інших компонентів, які, як правило, застосовуються у вибухонебезпечних посилках, – батарей, детонаторів, проводів тощо.

Одним із надійних способів виявлення вибухових і деяких наркотичних речовин є застосування службово-розшукових собак, здатних розпізнати ті чи інші предмети і речовини за їх запаховими слідами.

Успіх оперативного розпізнання предметів, викрадених під час вчинення злочинів корисливої спрямованості або тих, які незаконно переміщуються через митний кордон, залежить від наявності в оперативних працівників професійних навичок, пов'язаних з проведенням оглядів, обшуків та спостереженням.

До документів – об'єктів оперативного розпізнання слід віднести лише ті з них, які мають очевидний зв'язок з правопорушеннями (наприклад, однозначно належать підозрюваному, несуть на собі явні ознаки підробки, позначені сигналітичними речовинами тощо), а також виявляються й оцінюються емпіричним шляхом. Важливе місце займає оперативне розпізнання грошових знаків і цінних паперів, що мають ознаки підробки.

Поліцейський скринінг. Одним із напрямів діагностики є здійснення так званого «поліцейського скринінгу». Скринінг (від англ. *screening*) – означає відбір фактів, явищ із багатьох

однорідних, які в процесі дослідження виявляють необхідні, шукані властивості.

Зокрема з метою забезпечення належного проведення в Україні та Польщі чемпіонату Європи з футболу ЄВРО 2012 було залучено значну кількість представників служб охорони, стюардів, волонтерів, ЗМІ, обслуговуючого персоналу тощо. Тому особливої актуальності для правоохоронних органів України набуло питання попередження можливості потрапляння на об'єкти ЄВРО 2012 осіб, які могли б становити потенційну загрозу безпеці його проведення. З цією метою була запроваджена система акредитації, одним із елементів якої стала перевірка осіб, які її отримували, за обліками правоохоронних органів або так званий «поліцейський скринінг».

Метою поліцейського скринінгу є мінімізація ризиків щодо інших осіб та об'єктів ЄВРО 2012 шляхом виключення осіб, які могли б становити загрозу безпеці проведення чемпіонату, з числа аплікантів на акредитацію.

Вихідні персональні дані кожного апліканта на акредитацію для здійснення відповідних перевірок за банками даних Інтерполу, МВС та СБУ містили унікальний ідентифікаційний номер особи на ЄВРО 2012, її прізвище, ім'я, стать, дату народження, громадянство, місце роботи, категорію акредитації, тип, номер і термін дії ідентифікаційного документа.

Оцінювання результатів скринінгу здійснювалося з урахуванням відповідних критеріїв, тобто специфічних ознак відомостей, отриманих під час перевірки персональних даних аплікантів на акредитацію за обліками МВС, СБУ та Генерального секретаріату Інтерполу, що зумовлено різним рівнем можливого ризику з боку аплікантів на акредитацію у зв'язку з різними відомостями про цих осіб, які можуть міститися у відповідних банках даних, а також різним рівнем доступу цих осіб на об'єкти чемпіонату.

Використання скринінгу аплікантів на акредитацію може успішно використовуватись під час підготовки та проведення найвагоміших міжнародних спортивних заходів, таких як Олімпійські ігри, чемпіонати світу та Європи з футболу тощо.

Оперативне розпізнання події злочину, пов'язане з наявністю в осіб, причетних до його вчинення, засобів

мобільного зв'язку. Відповідно до ст. 8 Закону про ОРД оперативним підрозділам для виконання завдань ОРД за наявності передбачених законом підстав надається право зняття інформації з транспортних телекомунікаційних мереж, електронних інформаційних мереж (п. 9), здійснювати установлення місцезнаходження радіоелектронного засобу (п. 12).

Під зняттям інформації з транспортних телекомунікаційних мереж розуміється спостереження, відбір та фіксація змісту інформації уповноваженими оперативними підрозділами із використанням у встановленому законодавством порядку відповідних технічних засобів, а також одержання, перетворення і фіксація різних видів сигналів, що передаються каналами зв'язку.

Зняття інформації із транспортних телекомунікаційних мереж забезпечує контроль, конспіративне перехоплення та фіксацію з використанням технічних засобів телефонних розмов, що передаються засобами стаціонарного та рухомого (мобільного зв'язку), а також інших даних, що передаються каналом зв'язку, що контролюється (SMS, MMS, факс, модемний зв'язок).

В ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому разі додатково повинні бути зазначені ідентифікаційні ознаки, які дають змогу унікально ідентифікувати абонента спостереження, транспортну телекомунікаційну мережу, кінцеве обладнання, на якому може здійснюватися втручання у приватне спілкування, а саме:

– номер абонента в телефонній мережі загального користування у форматі код країни – код зони або оператора – номер абонента в мережі;

– міжнародний ідентифікаційний номер мобільного терміналу (IMEI);

– міжнародний ідентифікаційний номер мобільного абонента (IMSI)[27].

Зняття інформації з транспортних телекомунікаційних мереж з метою контролю та фіксації інформації, що передається

---

[27] Кримінальний процесуальний кодекс України. Науково-практичний коментар: у 2 т. / за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. – Х.: Право, 2012. – С. 389.

через Інтернет та іншими мережами передачі даних, може здійснюватись за ідентифікаційними ознаками аналогічними тим, за якими проводиться контроль за телефонними розмовами. Зняття інформації з каналів зв'язку може здійснюватись за такими ознаками:

– за адресою електронної пошти у форматі «ім'я поштової скриньки @ домен.домен верхнього рівня» (наприклад, info@ssu.gov.ua);

– адресою в мережі передачі даних з комутацією пакетів, у тому числі IP-адреса для мережі Інтернет у форматі ххх.ххх. ххх.ххх (наприклад, 010.011.012.130);

– апаратною адресою (MAC-адреса) пристрою, приєднаного до мережного середовища[28].

За результатами зняття інформації з транспортних телекомунікаційних мереж може бути зафіксована інформація, що вказує на ознаки кримінального правопорушення в діях підозрюваного, обвинуваченого, а також відомості про протиправну діяльність окремих осіб, що контактували із цими особами через канали телекомунікаційної мережі у проміжок проведення ОТЗ.

За результатами проведення зняття інформації з транспортних телекомунікаційних мереж складається протокол, у якому зазначаються: місце і час проведення цього ОТЗ, правові підстави здійснення, описуються отримані результати або розшифровуються окремі епізоди звукозапису розмов, що містять інформацію, яка має значення для ОРД та кримінального провадження.

Безпосереднє виконання ОТЗ зі зняття інформації з транспортних телекомунікаційних мереж покладається на уповноважені підрозділи органів Національної поліції та органів СБУ.

Ч. 1 ст. 9 Закону України «Про телекомунікації» вказує, що охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційна безпека телекомунікаційних мереж гарантуються Конституцією та законами України.

---

[28] Кримінальний процесуальний кодекс України. Науково-практичний коментар: у 2 т. / за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. – Х.: Право, 2012. – С. 389.

З огляду на викладене, КПК покладає на керівників та працівників операторів телекомунікаційного зв'язку обов'язок сприяти виконанню дій із зняття інформації з транспортних телекомунікаційних мереж, вживати необхідних заходів щодо нерозголошення факту проведення таких дій та змісту отриманої інформації, а також з метою забезпечення подальшого використання у кримінальному судочинстві, зберігати отриману інформацію в незмінному вигляді.

Вирішення проблеми створення й впровадження сучасних систем безпеки, засобів зовнішнього контролю (спостереження) та швидкого реагування в діяльність правоохоронних органів та інших органів державної влади з метою запобігання терористичних загроз та протидії злочинності полягає у комплексному, поетапному вирішенні проблемних питань у цій сфері шляхом упровадження організаційних засад функціонування загальнодержавної системи зовнішнього контролю (спостереження) та швидкого реагування на всіх рівнях, підвищення ефективності управління з боку органів державної влади та органів місцевого самоврядування з питань протидії злочинності, зміцнення законодавчої, нормативно-правової, науково-технічної та ресурсної бази, що сприятиме зниженню рівня терористичної загрози в Україні.

Для вирішення зазначених проблем Кабінетом Міністрів України схвалено Концепцію Державної цільової правоохоронної програми встановлення сучасних систем безпеки, застосування засобів зовнішнього контролю (спостереження) та швидкого реагування на період до 2016 року, основною метою якої є підвищення ефективності діяльності правоохоронних органів та інших органів державної влади у сфері боротьби зі злочинністю та запобігання тероризму шляхом розроблення та впровадження новітніх систем безпеки, засобів зовнішнього контролю (спостереження) та швидкого реагування.

У межах виконання Державної цільової правоохоронної програми необхідно здійснити заходи за такими пріоритетними напрямами:

1) організаційно-правовий:

– підвищення ефективності управління та діяльності із запобігання терористичної загрози шляхом внесення змін

до законодавчих та нормативно-правових актів у сфері протидії тероризму з метою оптимізації структур суб'єктів боротьби з тероризмом та підвищення відповідальності за стан цієї діяльності керівників усіх рівнів управління;

– прийняття регіональних програм встановлення сучасних систем безпеки, застосування засобів зовнішнього контролю (спостереження) з елементами аналітичної обробки інформації;

– формування організаційної структури системи державних органів забезпечення антитерористичної безпеки, що входять до складу суб'єктів боротьби з тероризмом, розподіл їх функцій;

– комплексне забезпечення життєдіяльності частин (структурних елементів) системи: кадрове, фінансове, матеріальне, технічне, інформаційне тощо;

– підготовка сил та засобів системи до їх застосування згідно з призначенням;

– вироблення стратегії та планування конкретних заходів щодо забезпечення антитерористичної безпеки;

2) організаційно-технічний:

– створення систем відеоспостереження з елементами аналітичної обробки інформації за центральними, криміногенно-активними та людними місцями міст; у закритих об'єктах (супермаркети, навчальні заклади, вокзали, аеропорти, стадіони, станції та вагони метро; за станом транспортних комунікацій);

– організація системи відслідковування рухомих об'єктів з використанням глобальної системи позиціонування (GPS/ГЛОНАСС);

– встановлення систем безпеки на об'єктах транспортної інфраструктури шляхом розгортання під час входу в пасажирську зону станцій метрополітену, залізничних вокзалів доглядової зони (стаціонарний рамочний металодетектор, стаціонарний рентгенівський сканер для предметів, стаціонарний сканер для пасажирів, вибухозахисний контейнер, локалізатор вибухових речовин, експрес-аналізатори вибухових речовин тощо);

– упровадження в діяльність чергових частин органів НПУ апаратно-програмних комплексів;

– організація систем цифрового радіозв'язку та проводового зв'язку;

– організація каналів передачі даних (безпроводових – WI–FI, WI–MAX, 3G, 4G; проводових та оптичних).

3.4. Автоматизація оперативно-розшукового прогнозування

Оперативно-розшукове прогнозування має свій особливий статус у системі міжгалузевих співвідношень юридичної прогностики. З огляду на специфіку ОРД, інтереси її прогнозної галузі пов'язані з інтересами прогнозування матеріально-правової, кримінально-процесуальної й оперативно-розшукової сфери.

Взаємодія розглянутих прогнозів полягає в:

1) попередженні та виявленні специфічними методами і засобами події злочинів, а також осіб, які їх вчинили;

2) розшуку осіб, які переховуються від правосуддя;

3) організації діяльності правоохоронних органів щодо попередження, припинення, розкриття та розслідування злочинів.

Головні особливості прогнозування полягають у такому:

– основна мета розробки прогнозу – виявлення можливих наслідків настання якої-небудь події, явища або визначення можливих шляхів і перспектив настання цих наслідків;

– можливе розроблення кількох варіантів прогнозу, які нерідко суперечать один одному;

– для розроблення оперативно-розшукових прогнозів необхідне використання додаткових, суто прогностичних знань;

– остаточний результат прогнозу – приписи та рекомендації, перевірка істинності яких здійснюється безпосередньо в процесі їх реалізації на практиці;

– процес розробки прогнозу має динамічний, безперервний характер, оскільки фігуруючі в ньому об'єкти знаходяться в пермаментному русі, спрямованому в майбутнє[29].

У процесі оперативно-розшукового прогнозування вирізняють три основних етапи:

– *на першому етапі* здійснюється різноаспектний аналіз об'єктів прогнозування, виділення їх ознак, найбільш значущих для проведених досліджень;

– *другий етап* передбачає формування вихідних гіпотез, основне призначення яких полягає у встановленні зв'язків між різними об'єктами; у поясненні причин їх виникнення; у реконструкції картини минулого й формуванні картини майбутнього;

– *на третьому етапі* отримані внаслідок гіпотетичного дослідження дані інтерпретуються з використанням специфічних методів і засобів прогнозування[30].

Відтак з'являється відповідна система знань, що дає змогу визначати можливі наслідки настання будь-яких подій, явищ або описувати можливі шляхи та перспективи настання цих наслідків, передбачати майбутні характеристики досліджуваних об'єктів тощо. Потрібно зазначити, що перехід від гіпотези до прогнозу означає рух від абстрактного передбачення до конкретного. Отже, попередній етап прогностичних досліджень в ОРД безпосередньо пов'язаний з побудовою гіпотези, тобто з діагностикою.

Вибір методу прогнозування залежить від низки чинників, серед яких найважливішими є широта охоплення прогнозованого об'єкта, дальність прогнозу, його багатофакторність тощо. Багато залежить і від того, які фахівці, учені, практичні працівники залучаються до розроблення прогнозу і яка технічна база водночас використовується.

Нині теорія ОРД поки не має спеціальних методів оперативно-розшукового прогнозування. Тому найбільш оптимальним вважається адаптація існуючих методів прогнозування,

---

[29] Горшенин Л. Г. Основы теории криминалистического прогнозирования: монография / Л. Г. Горшенин – М.: Акад. МВД РФ, 1993. – С. 98–101.

[30] Бестужев-Лада И. В. Поисковое социальное прогнозирование: перспективные проблемы общества. Опыт систематизации / И. В. Бестужев-Лада. – М.: Наука, 1984. – С. 88.

розроблених у межах загальної теорії прогностики й суміжних юридичних прогностик (криміналістичної і кримінологічної), до потреб ОРД.

Науковці виокремлюють низку основних категорій методів прогнозування, які доцільно адаптувати до специфіки ОРД, і пропозиції щодо їх класифікації. За ступенем належності до прогностичної діяльності ці методи умовно поділяються на спеціальні та прогностичні.

Першу групу становлять методи різних наук, які використовуються в процесі прогнозування (соціологічний, історичної аналогії, математичний, кібернетичний, статистичний тощо). Важливе значення серед спеціальних методів набувають математичні методи, які використовуються при обробці результатів вимірювань, аналітичного порівняння, опису ознак і характеристик прогнозованих оперативно-розшукових об'єктів. Крім того, вони необхідні для опису, вимірювання, порівняння майбутніх умов прогнозованого об'єкта. Математичні методи передбачають також використання комп'ютерної техніки в процесі розроблення оперативно-розшукових прогнозів. На практиці розроблено кілька програмних продуктів, що дають змогу здійснювати прогностичну оцінку стану оперативно значущих об'єктів за допомогою комп'ютерної обробки інформації[31].

В юридичній літературі стверджується, що інколи правоохоронні органи дійсно застосовують відповідні прогностичні методики (реальна прогностика), а іноді під виглядом оперативно-розшукового прогнозування здійснюються інші аналітичні заходи (псевдопрогностика), які не мають жодного стосунку до наукових методів прогнозування.

До групи реальної прогностики належать:

1) *аналіз окремих елементів механізму злочину (аналітичний пошук з елементами прогнозування)*. Зокрема використання методики, заснованої на застосуванні методу Г. Лінстауна, для підготовки щомісячних аналітичних довідок про злочини, пов'язані з підпалами автомобілів, знищенням або

---

[31] Горшенин Л. Г. Основы теории криминалистического прогнозирования: монография / Л. Г. Горшенин. – М.: Акад. МВД РФ, 1993. – 123 с.

пошкодженням чужого майна (шляхом підпалу), хуліганством (шляхом підпалу) тощо. На основі аналізу отриманої інформації пропонується орієнтувати підрозділи патрульної поліції на виявлення підозрілих осіб під час патрулювання території у проміжок часу з 24.00 до 5.00 год. ранку (у зазначений час зазвичай відбуваються підпали і саме в цей проміжок слід очікувати вчинення інших аналогічних злочинів);

2) *застосування методу Г. Лінстауна в комплексі з так званими технічними методами прогнозування.* Наприклад, підготовка огляду про злочини, пов'язані з викраданням сумок, барсеток і грошових коштів із автомобілів, а також з нападами на перевізників грошових коштів, учинених на території певної адміністративної дільниці. За допомогою матриць, виконаних у формі Excel-таблиць, аналізуються час, місце, спосіб учинення злочинів, номери і марки автомобілів злочинців тощо. Під час підготовки підсумкового матеріалу може бути здійснений геоінформаційний аналіз отриманих відомостей, пов'язаний із систематизацією місць, де відбувалися крадіжки, проживання злочинців, можливого відвідування тощо;

3) *застосування геоінформаційної системи для прогнозування та моделювання ситуацій щодо боротьби зі злочинністю й тероризмом (ГІС »Дзеркало»)*. Як математичні методи, що застосовуються у зазначеній системі при обробці інформації та подальшому прогнозуванні, обрані методи: Беллмана-Заде, сумарних переваг і недоліків, правило Борда, принцип Парето, метод аналізу ієрархій, правило послідовних вчинків тощо. Із математичними система допускає застосування і методу експертних оцінок;

4) *застосування математичних методів на базі комп'ютерних технологій.* Зокрема О. Г. Бєлоглазовим розроблена методика прогнозування вбивств на замовлення, виявлення замовників і об'єктів убивств на замовлення на основі аналітичного моделювання конфліктних процесів у злочинному середовищі. Технологічною основою цієї методики стало виявлення рольових функцій учасників організованих злочинних груп. Розроблено також варіант вирішення цієї задачі з використанням електронної комп'ютерної таблиці Excel шляхом

побудови математичної моделі конфлікту на основі динаміки зв'язків конфліктуючих осіб[32].

Розвиток оперативно-розшукового прогнозування найперше визначається подальшим удосконаленням відповідних комп'ютерних програмних продуктів, які дають змогу підвищити його швидкість, широту і точність. Водночас вирішальне значення відводиться людському фактору – професійному інтелекту аналітика, оскільки без участі останнього будь-яка техніка, навіть найдосконаліша, буде безсила.

До групи псевдопрогностики можна віднести:

1) *емпіричне передбачення*, що видається за оперативно-розшукове прогнозування: передбачення індивідуальної злочинної поведінки, наприклад, передбачення поведінки осіб, засуджених за вчинення тяжких, особливо тяжких злочинів, які звільнилися з місць позбавлення волі. Такі особи часто виявляються непотрібними ні суспільству, ні сім'ї. Учиняти злочини з використанням транспорту або високотехнологічних знарядь злочинів вони не можуть через відсутність грошових коштів і необхідних навичок, тому змушені вчиняти ті злочини, за які були раніше засуджені (розбої, грабежі, квартирні крадіжки, шахрайство, збут наркотиків тощо). Водночас виділяється категорія осіб, звільнених з місць позбавлення волі, які досягли певної ваги у злочинній ієрархії – стали злочинними «авторитетами» або особами, до них наближеними. Такі особи, звільнившись, як правило, знову стають членами ОЗУ, а деякі можуть зайняти в них провідне місце[33];

2) *прогнозування окремих показників стану злочинності (кримінологічне прогнозування).* Оскільки як базова використовується лише інформація ЗМІ і офіційної статистики

---

[32] Белоглазов Е. Г. Методология обеспечения аналитической разведки криминальных процессов и явлений: автореферат дис. на соиск. уч. степ. д-ра техн. наук: 05.13.01 / Е. Г. Белоглазов. – М.: РАГС при Президенте РФ, 2007. – С. 33.

[33] Агеев В. В. Анализ и совершенствование частных методик оперативно-розыскного прогнозирования в деятельности подразделений оперативно-разыскной информации / В. В. Агеев // Информатизация и информационная безопасность правоохранительных органов. – М.: Академия управления МВД России, 2011. – С. 207–212.

про зареєстровані злочини на території, що обслуговується, без урахування латентної складової злочинності, у цьому разі може йтися лише про здійснення кримінологічного аналізу й прогнозування оперативної обстановки загалом або окремого виду злочинності;

3) *використання оперативного розпізнання в ході інформаційного пошуку з використанням апаратно-програмних комплексів.* Зокрема використання програмно-технічного комплексу «Розшук-Магістраль» дає змогу для будь-якого поїзда, що знаходиться в дорозі або відправляється через певний час, здійснювати аналіз усіх його пасажирів з метою виявлення осіб, з боку яких можна очікувати вчинення злочинів, пов'язаних з незаконним перевезенням наркотичних засобів – так званий «прогноз на поїзд». Утім, цей алгоритм аналогічний оперативному розпізнанню кишенькового злодія в місцях скупчення громадян, який здійнюється у процесі пошукових заходів та його супровід до моменту вчинення злочину. Подібні види аналізу слід кваліфікувати як оперативно-розшукову діагностику, що здійснюється емпіричним шляхом, але не в кримінальному середовищі, а в інформаційних масивах;

4) *здійснення ініціативних оперативно-аналітичних досліджень*, які іноді іменують оперативно-розшуковим прогнозуванням. Висновки, що формулюються у цих дослідженнях, не містять інформації «про ймовірний розвиток» тих чи інших об'єктів прогнозування. Тому за змістом ці матеріали є результатами інших видів інформаційно-аналітичної роботи;

5) *підготовка інформаційно-аналітичних матеріалів штабного характеру*. Ця діяльність не належить до оперативно-розшукового прогнозування, тому що не відповідає вимогам відомчих нормативних актів.

Отже, значна частина діяльності, яка здійснюється підрозділами правоохоронних органів як оперативно-розшукове прогнозування, такою не є.

Серед інших спеціальних методів, які можуть бути використані при оперативно-розшуковому прогнозуванні, особливе місце займають статистичні методи. Вони широко застосовуються під час кримінологічного й криміналістичного прогнозування. В оперативно-розшуковій практиці ці методи

поки використовуються рідко, хоча в перспективі за ними велике майбутнє.

Практично всі статистичні методи полягають у побудові та аналізі динамічних рядів характеристик об'єкта прогнозування. Серед соціологічних методів найбільш прийнятними для оперативно-розшукового прогнозування є анкетування та опитування. Вони застосовуються для збору інформації про об'єкти оперативно-розшукового прогнозування, а також для оцінки його ефективності.

Метод історичної аналогії заснований на встановленні аналогії об'єкта прогнозування з однаковим за природою об'єктом, який випереджає перший у своєму розвитку. Утім, висновки цього методу має лише ймовірнісний характер і мають невеликий ступінь достовірності.

Друга група методів прогнозування, які здебільшого запозичені з вітчизняної та зарубіжної прогностики, поділяється на нормативні та пошукові методи. Нормативні методи дають змогу прогнозувати можливі шляхи досягнення бажаного стану об'єкта на основі заздалегідь заданих критеріїв, цілей, норм, а пошукові методи – можливий стан прогнозуємого процесу, події або параметрів.

До *пошукових методів* належать: метод Дельфі (метод колективної експертної оцінки), метод колективної генерації ідей (мозкова атака), метод складання сценаріїв (метод Л. Жерардена), метод прогнозування за допомогою економічних моделей, методи екстраполяції.

Серед *нормативних методів* найбільш відомі: метод блок-схеми послідовності виконання завдань (метод Г. Лінстауна), «Дерево цілей», побудови морфологічних моделей тощо. Проте аналіз практики оперативно-розшукового прогнозування свідчить про те, що нині ці методи застосовуються доволі рідко.

Застосування *методу Дельфі* ґрунтується на виявленні узгодженої думки експертної групи шляхом автономного та анонімного опитування експертів за декілька турів при повідомленні їм результатів попереднього туру для додаткового обґрунтування оцінки та формування статистичної характеристики групової відповіді. Об'єктивність застосування цього

методу допомагає забезпечувати поєднання фахівців різного профілю за професійним, територіальним та іншими критеріями.

Ефективне використання методу Дельфі забезпечується певними умовами:

– має бути передбачена ефективна система контактів між експертами;

– необхідний їх вільний доступ до відповідної інформації;

– ці відомості мають бути підготовлені заздалегідь;

– інформацію, яка не становить інтерес, потрібно виключати з розгляду;

– необхідно чітко сформулювати мету прогнозування;

– слід врахувати можливість оцінки зробленого прогнозу на основі його практичної реалізації.

За дотримання цих умов і доволі високої кваліфікації експертів їхні висновки можуть мати певну схожість. Якщо ж ці думки різняться, необхідно визначити причини їх неузгодженості. У разі, коли висновки одного з експертів істотно відрізняються від інших висновків, його не слід включати в корпоративний прогноз доти, доки не буде знайдено розумний компроміс.

Метод колективної генерації ідей (мозкова атака) також ґрунтується на максимальному використанні досвіду експертів у різних галузях знань і вимагає досягнення єдиної думки з досліджуваного питання. Консенсус і в цьому разі досягається на основі індивідуального мислення, але з урахуванням таких правил:

а) забороняється оцінка висунутих ідей;

б) обмежується час кожного виступу, але допускається багаторазовий виступ одного і того ж учасника обговорення;

в) обов'язково фіксується все сказане;

г) стимулюється розвиток будь-якої ідеї;

ґ) між учасниками підтримується вільна дискусія.

Названі методи застосовуються і у стратегічному, і в оперативно-тактичному прогнозуванні. Вони належать до так званих методів експертної оцінки або логічної екстраполяції.

Вивчення та аналіз практики оперативно-розшукового прогнозування дає можливість стверджувати, що на прак-

тиці найчастіше застосовуються інтуїтивні (експертні) методи оперативно-розшукового прогнозування. Водночас технічний прогрес не стоїть на місці, уже розроблені спеціальні комп'ютерні програмні продукти для оперативно-розшукового прогнозування, які в перспективі здатні значно підвищити його ефективність і які потрібно якомога ширше впроваджувати у практику оперативно-розшукового прогнозування.

Крім того, в оперативно-розшуковому прогнозуванні застосовуються й різні методи статистичної екстраполяції, які ґрунтуються на припущенні про збереження в майбутньому минулих і сьогоднішніх тенденцій розвитку об'єкта прогнозування. Основу цих методів становить вивчення часових рядів (ряди динаміки, складені на базі вихідних статистичних даних про злочинність, результати діяльності оперативних підрозділів тощо) і побудова графіка (функції), який характеризує тенденцію (динаміку) розвитку процесу загалом. Утім, екстраполяція даних за межі часового проміжку дозволяє прогнозувати стан об'єкта тільки на найближче майбутнє.

Ще одну групу прогностичних методів становлять методи побудови прогнозних моделей: метод складання сценаріїв, метод формування економічних моделей, метод Г. Лінстауна тощо.

Метод складання сценаріїв (метод Л. Жерардена) полягає в складанні та аналізі можливих варіантів альтернативних ситуацій, які можуть бути в майбутньому. Він сприяє виявленню шляхів еволюції систем у послідовності проміжків часу та визначенню тих критичних рівнів напруженості, за яких соціальні сили змінюють або зупиняють існуючі тенденції розвитку прогнозованого об'єкта.

Прогноз реалізується за такими етапами:

1) опис структури системи в будь-який момент і перевірка її внутрішньої узгодженості в цей час;

2) розгляд еволюції системи за певний проміжок на основі зафіксованих станів її структури, що визначаються природним рухом подій або впливом певних зовнішніх чинників, що відповідають тим чи іншим тенденціям у кримінальному середовищі.

У цьому разі як однією з умов передбачається, що ретроспективні тенденції в кримінальному середовищі зберігають свій вплив протягом наступних п'яти років. Відтак при використанні цього методу необхідно мати достатній попередній проміжок часу (близько 15–20 років) для того, щоб результати змін, які відбуваються, стали на цьому фоні досить добре видимими.

Метод Л. Жерардена краще використовувати у стратегічному прогнозуванні.

Метод прогнозування за допомогою економічних моделей використовує як вихідну інформацію об'єктивні відомості про тенденції зміни прогнозованих об'єктів і суб'єктивні думки експертів про можливі перспективні шляхи та результати розвитку прогнозуємої галузі економіки, а також окремих економічних структур, зокрема й – пов'язаних з криміналом.

Модель об'єкта прогнозування становить систему рівнянь, що виражають різні взаємозв'язки між змінами, які впливають на економічні аспекти діяльності. У процесі реалізації цього методу відкриваються відповідні можливості використання математичної логіки, теорії графів, матричного аналізу тощо.

Метод передбачає здійснення трьох основних умов:

а) визначення (побудова, знаходження) моделі об'єкта;

б) експерементування з моделлю, встановлення зв'язків між її елементами;

в) перенесення (через симетричність відносин між об'єктом і його моделлю) висновків про властивості і відносини між елементами моделі на об'єкт.

В *основі методу блок-схеми послідовності виконання завдань* (метод Г. Лінстауна) лежить системний аналіз, головним призначенням якого є відображення елементів будь-якої системи і вивчення взаємозв'язків між ними. Суть методу Г. Лінстауна полягає у схематичному зображенні всіх альтернативних шляхів вирішення якого-небудь завдання. На кожному шляху виявляються істотні етапи та пов'язані з ними труднощі й витрати. Наприклад, з його допомогою можна скласти блок-схему прогнозованої підготовки квартирної крадіжки – визначити фактори, що перешкоджають або, навпаки, сприяють її вчиненню; розрахувати фізичні, моральні й матеріальні витрати, на які змушений робити підозрюваний тощо.

Водночас позитивний ефект від застосування цього методу можливий лише в тому разі, якщо зовнішні чинники, які впливають на стан злочинності в тому чи іншому регіоні, є стабільними. Це дозволяє використовувати стандартні блок-схеми для кожної території, що обслуговується, або об'єкта з урахуванням їх своєчасної актуалізації. Порівняння блок-схем різних видів правопорушень та механізмів їх здійснення дає змогу виявляти стійкі тенденції та закономірності, що склалися в зонах обслуговування, вивчення яких сприяє вдосконаленню діяльності правоохоронних органів у вирішенні завдань ОРД.

Цілком очевидно, що цей метод може використовуватися і в стратегічному, і в оперативно-тактичному прогнозуванні. В останньому випадку він найбільш актуальний при складанні соціально-психологічного портрета підозрюваного, який передбачає створення прогностичної моделі скоєння подальших протиправних діянь.

Наприклад, В. А. Образцов і С. Н. Богомолова використовують метод Г. Лінстауна для прогнозування місця і часу вчинення чергового злочину маніяком-ґвалтівником. Дослідники зазначають, що незважаючи на те, що місце вчинення злочину є як би довільним, заданим самим маршрутом жертви, у свідомості злочинця місце злочину й вимоги до нього бувають вибрані заздалегідь. Уже після першого злочину можна охарактеризувати бажані йому місця злочинів. Тому можливо й необхідно визначити подібні місця на місцевості і взяти їх під нагляд. Злочинець обов'язково «обходить» територію, нерідко повертаючись на місце злочину[34].

Аналогічний підхід і до процесу прогнозування часового чинника, пов'язаного з нападами. Не будучи чимось випадковим, цей фактор несе доволі багато інформації про злочинця, особливо якщо вдається виявити закономірності, за якими він вибирає той чи інший час для нападів. Закономірності вибору часу вчинення злочину встановлюються за двома напрямами:

---

[34] Образцов В. А. Российские серийные убийцы. Типовой портрет / В. А. Образцов, С. Н. Богомолова [Электронный ресурс]. – Режим доступа: http://ord.com.ua/categ_1/artic le_31537.html.

визначення часу доби (години, хвилини) та періодичності здійснення нападів (місяці, дні).

Доведено, що на вибір часу доби вчинення злочину впливає ймовірність появи жертви в місці, зручному для нападу. На періодичність здійснення злочинів впливають характер та рівень нереалізованих потреб злочинця, що, своєю чергою, залежить від погодних умов, пори року, фази місяця, режиму роботи, навчання тощо.

Піки збільшення кількості подібних злочинів обумовлені насамперед появою на вулиці одночасно найбільшої кількості потенційних жертв:

14–15 год. – час закінчення занять у школах;

16–17 год. – закінчення занять у групах продовженого дня, училищах, вищих навчальних закладах;

18–19 год. – закінчення робочого дня;

22 год. – повернення з вечірніх гулянь, з гостин.

Під час вивчення часу нападу злочинця на його жертви важливо зауважувати на те, в які дні тижня вони відбувалися, чим ці дні відрізняються від інших для даної території.

Із розглянутими методами в прогностиці використовуються і *методи математичного моделювання*, наприклад, прогнозування процесів злочинності за допомогою штучних нейронних мереж, які становлять математичні моделі, в основі яких лежать сучасні уявлення про будову мозку людини і здійснюваних у ньому процесах обробки інформації.

З аналізу описаних методів вбачається, що більшість з них одночасно спрямовані на вирішення і стратегічних, і тактичних завдань боротьби зі злочинністю. Майже всі методи, які застосовуються в оперативно-розшуковому прогнозуванні, ґрунтуються на кримінологічному або криміналістичному прогнозуванні. Насамкінець усі вони належать до так званих методів соціального прогнозування, що засновані на трьох розглянутих взаємопов'язаних групах способів отримання інформації про майбутнє.

Крім того, існують специфічні методи, властиві виключно оперативно-розшуковому прогнозуванню, які засновані на так званій нетрадиційній прогностиці. Ідеться, зокрема, про використання метода прогнозування функціонування і стійкості об'єктів на основі космічних ритмозадаючих факторів.

3.5. Здійснення оперативно-розшукових заходів у мережі Інтернет

Відкриті джерела інформації вважаються найбільш ємними і найбільш затребуваними інформаційними каналами. Відомий фахівець ЦРУ Ш. Кент, якого в США вважають засновником «аналітичної розвідки», стверджував, що в мирний час до 80% інформації, необхідної для ухвалення рішення, доступні саме з відкритих джерел.

Пізніше колишній керівник розвідувального управління Міністерства оборони США С. Уілсон зазначив, що до 90% розвідувальних даних беруться з відкритих та відносно відкритих джерел і тільки 10% – за рахунок роботи інших видів розвідки.

Останнім часом значного впливу на суспільне життя в нашій країні набули глобальні інформаційні мережі (насамперед мережа Інтернет), які отримали в науковій літературі назву «кіберпростір» (*cyberspase*).

Термін «кіберпростір» є сполученням слів – «кібер» і «простір». Слово «кібер» (від грецького *κυβερ*) означає над. Під простором розуміють необмежену протяжність; вільний великий простір, просторінь. Проте події у кіберпросторі відбуваються не на фізичних ділянках місцевості, а у певному специфічному середовищі. Дослідники вбачають, що кіберпростір доцільно розглядати саме як «кібернетичний простір», що створений на основі принципів та методів кібернетики[35].

Водночас у законодавчих та підзаконних правових актах поняття кіберпростору практично не регламентовано, що негативно впливає на ефективність забезпечення прав і законних інтересів особи, суспільства і держави у «віртуальному» просторі.

У проекті закону «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України» кібернетичний простір (кіберпростір)

---

[35] Погорецький М. А. Поняття кіберпростору як середовища вчинення злочину / М. А. Погорецький, В. П. Шеломенцев // Науково-практичний журнал «Інформаційна безпека людини, суспільства, держави». – К., 2009. – № 2. – С. 78.

визначається як середовище, яке виникає внаслідок функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, кібернетична безпека – як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі.

Водночас термін «Інтернет» тлумачиться як «всесвітня асоціація комп'ютерних мереж, інтегрована мережна «павутина», яка складається з різних фізичних неоднорідних комунікаційних мереж, об'єднаних в єдину логічну архітектуру».

Також слід зазначити, що користувачами Інтернету є не лише законослухняні громадяни, а й особи, що виношують злочинні наміри. Кіберпростір використовується злочинними та терористичними угрупованнями для незаконної торгівлі наркотиками, зброєю, розповсюдження дитячої порнографії, підготовки та здійснення терористичних актів і збройної агресії проти України, проведення різні екстремістської діяльності (зокрема, пропаганди тероризму, насильства, жорстокості, расової, національної, релігійної нетерпимості), порушення авторських прав, а також промислового шпигунства, конкурентної розвідки тощо.

Крім того, кримінальні структури активно використовують мережу Інтернет для спілкування між собою, поширення своїх злочинних ідей (зокрема терористичних і екстремістських) серед населення, для пошуку, збору і передання кримінальної інформації.

Джерелами кібернетичних загроз можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері інформаційних технологій злочинці, іноземні державні органи, терористичні та екстремістські угруповання, транснаціональні корпорації та фінансово-промислові групи тощо. Зростає загроза використання кібернетичних засобів як з середини країни, так і з-за меж її кордонів.

Сучасна кіберзлочинність характеризується високою латентністю; використанням новітніх технологій, сучасним апаратним та програмним забезпеченням; організованістю, міжрегіональними та міжнародними зв'язками; використанням інформаційних ресурсів, які територіально розташовані у різних країнах.

Подальшій криміналізації кіберпростору сприяє низка характерних особливостей «віртуального» середовища:

1) *транснаціональність* Інтернету (відсутність кордонів, митниць, територіальна роз'єднаність груп людей);

2) *уявна анонімність* користувачів (як імена у мережі використовуються псевдоніми (нікнейми));

3) *значна кількість* користувачів, до яких легко можна довести свої ідеї, організувати їх для проведення якої-небудь акції, формувати громадську думку, навмисно дезінформувати, збирати інформацію;

4) *законодавча неврегульованість* цього середовища[36].

Недавнім часом об'єктами кібератак та кіберзлочинів дедалі частіше стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які забезпечують безпеку, оборону, захист від надзвичайних ситуацій, а також сервери їх офіційних Інтернет-представництв і електронної пошти.

Кількість злочинів, що вчиняється у кіберпросторі, зростає пропорційно числу користувачів комп'ютерних мереж. За оцінками Інтерполу темпи зростання злочинності в глобальній мережі Інтернет є найбільшими, порівняно з іншими видами злочинів, включаючи торгівлю наркотиками та зброєю. Щорічно глобальна кіберзлочинність обходиться планеті в 114 млрд доларів, кіберзлочинність уже ввійшла до переліку найбільш серйозних загроз з тих, з якими доводиться стикатися поліції[37].

За даними НБУ, на території України на 1 січня 2016 р. зареєстровано 98 банківських установ, що здійснюють емісію платіжних карток, функціонує 33334 банкомати, 194478

---

[36] Демянчук Е. В. Борьба с преступлениями экстремистской и террористической направленности, совершаемые с использованием сети «Интернет» / Е. В. Демянчук // Научный портал МВД России. – М., 2009. – № 1. – С. 99–100.

[37] Зима Л. М. Протидія кіберзлочинності у банківській сфері: стан, проблеми та шляхи їх вирішення / Л. М. Зима // Протидія злочинам, які вчиняються з використанням комп'ютерних мереж: тези доповідей міжнарод. наук.-практ. конф. (м. Севастополь, 1-2 жовт. 2010 р.). – Суми: ДВНЗ «УАБС НБУ», 2010. – С. 74–75.

платіжних терміналів, в обігу знаходиться понад 59 млн платіжних карток, зареєстровано 43 млн держателів платіжних карток, сума операцій із використанням платіжних карток за рік становить 1233 млрд грн.

Для здійснення платіжних операцій за допомогою мережі Інтернет використовуються системи на основі банківських карток, смарт-карток, інтернет-банкінгу або «електронних» грошей. Найбільш популярними платіжними системами, які використовуються в мережі Інтернет, є: WebMoney Transfer, E-Gold, PayPal, Яндекс, Інтернет-гроші, Portmone.

Вирізняються чотири групи відомостей, які найчастіше піддаються нападу з використанням шкідливих програм:

1) доступ до різних фінансових операцій (онлайн-банкінг, платіжні картки, електронні гроші), інтернет-аукціонів тощо;

2) доступ до поштових скриньок, які є складовою ICQ-акаунтів, як і всі знайдені на комп'ютері адреси електронної пошти;

3) паролі, коди доступу до інтернет-пейджерів, сайтів тощо;

4) паролі, коди до онлайн-ігр[38].

Останніми роками спостерігається тенденція до збільшення шахрайських дій у мережі Інтернет, зокрема й отримання персональної інформації (паролів, банківських рахунків або дампів з інформацією про власників кредитних карт тощо), шляхом розсилки електронних листів від імені банку, які містять посилання на підроблені сайти, що імітують роботу справжніх – так званого «фішингу». Цьому сприяло стрімке розповсюдження Інтернет-аукціонів, «фінансових пірамід», використання небанківських електронно-платіжних систем.

Зафіксовано непоодинокі факти несанкціонованого списання коштів з рахунків підприємств, учиненого шляхом втручання в роботу систем віддаленого обслуговування клієнтів. Зокрема у Дніпропетровській області викрито групу осіб, які з використанням мережі Інтернет здійснювали втручання

---

[38] Яппаров Р. М. Информационные технологии и компьютерные преступления в сети Интернет / Р. М. Яппаров // Информационные технологии, связь и защита информации МВД России. – М.: ВНИИ МВД России, 2012.

в роботу автоматизованої електронної системи Інтернет-магазину «WebMoney.ua». Зловмисниками шляхом несанкціонованої зміни інформації було сформовано 58 підроблених платіжних доручень, за якими з електронного гаманця зазначеного магазину перераховано на свій електронний гаманець понад 1 млн грн[39].

Службою безпеки України припинено діяльність групи кібершахраїв, якими за останні п'ять років викрадено понад 250 млн доларів США. Хакери за допомогою вірусу отримували доступ до систем інтернет-банкінгу, після чого переводили кошти компаній на рахунки підставних фірм. Тільки в Україні від їхніх дій потерпіли більше 30 компаній[40].

В умовах глобальної нестабільності значного розповсюдження набуло використання кіберпростору для здійснення конкурентної розвідки та промислового шпигунства. Завдяки високим технологіям шпигувати за чужими промисловими секретами стало набагато простіше, ніж 10–15 років тому. Підприємці швидко засвоїли, що, вивідуючи комерційні секрети, можна оптимізувати процес входження на ринок, потіснити конкурентів, раніше за інших вивести новий товар, заволодіти новими технологіями і суттєво зекономити час і кошти.

Подальший розвиток науково-технічного прогресу, збільшення потоку патентів і жорсткість конкурентної боротьби роблять викрадення чужих комерційних таємниць особливо прибутковою і перспективною справою. Як результат, втрати Німеччини від промислового шпигунства оцінюють у 20 млрд євро щорічно, втрати США – від 100 млрд доларів.

Сучасні ІТ-технології дають можливість на відстані відстежувати діяльність конкурентів, зокрема: сервіс SEMrush дозволяє аналізувати конкурентні сайти, джерела трафіку, ключові слова, за якими конкуренти просуваються в Google;

---

[39] Зима Л. М. Протидія кіберзлочинності у банківській сфері: стан, проблеми та шляхи їх вирішення / Л. М. Зима // Протидія злочинам, які вчиняються з використанням комп'ютерних мереж : тези доповідей Міжнарод. наук.-практ. конф. (м. Севастополь, 1-2 жовт. 2010 р.). – Суми: ДВНЗ «УАБС НБУ», 2010. – С. 76–77.

[40] Обезврежена группа хакеров [Электронный ресурс]. – Режим доступа: http://kommersant.ua/doc/2160535.

SemanticForce моніторить інформаційне поле і медійну активність конкурентів не тільки в соціальних мережах, а й в онлайн-виданнях, відстежує активність співробітників компанії. Крім того, для конкурентної розвідки використовують хмарні технології, SaaS системи і серверні ферми Google.

Колишній агент ЦРУ Едвард Сноуден наглядно показав усьому світу, що сервери багатьох популярних сайтів постійно перебувають під контролем.

Однією з ключових проблем, які в умовах глобалізації інформаційного обміну та широкого впровадження інформаційних технологій у всіх сферах життєдіяльності суспільства постали перед усіма державами світу, є проблема захисту інформації, що обробляється в інформаційно-телекомунікаційних системах. У цих умовах великі корпорації для захисту конфіденційної інформації застосовують комплексні системи захисту. Зокрема локалізувати небезпеку можна шляхом встановлення спеціальних захисних екранів і фільтрів на вході в локальну мережу. Найефективніше взагалі не підключати комп'ютери з важливою інформацією ні до локальної, ні до глобальної мережі. Для нових розробок зазвичай використовують комп'ютери, в яких немає технічної можливості вставити флеш-накопичувач, а всередині їх немає жорсткого диску (вони підключені до серверів, розташованих в окремому захищеному приміщенні). Обмін інформацією з іншими користувачами здійснюється за допомогою одного комп'ютера, а робота з кресленнями, програмним кодом тощо – на іншому, не підключеному до мережі Інтернет.

За сучасних умов використання мережі Інтернет оперативними підрозділами правоохоронних органів є необхідною умовою успіху у сфері боротьби зі злочинністю. Водночас потрібно відрізняти організацію боротьби з кіберзлочинами та організацію здійснення ОРЗ шляхом використання кіберпростору, оскільки останні можуть проводитись як у справах про кіберзлочини, так і у справах про злочини, учинені у звичайному середовищі.

Моніторинг соціальних сайтів у мережі Інтернет дає можливість перевірити наявні або зібрати нові відомості про конкретну особу, отримати фотографії різних років її

життя, виявити зв'язки (родинні, дружні, комерційні, злочинні) та контакти, встановити місце перебування та роботи. Принцип функціонування таких мереж допускає здійснення безпосереднього контакту з конкретною особою або виявлення її зв'язків з іншими особами. Ця діяльність є новим напрямом здійснення ОРЗ, що потребує розроблення та впровадження відповідної тактики їх проведення.

Зважаючи на це, можна окреслити основні напрями використання мережі Інтернет:

1) виявлення осіб, які становлять оперативний інтерес;

2) пошук конкретних осіб, встановлення їх фізичного місцезнаходження;

3) налагодження негласних зв'язків з подальшим входженням у безпосередній контакт;

4) пошук викрадених речей та встановлення причетних до цього осіб;

5) здійснення психологічного впливу на учасників кримінальних структур шляхом ведення активної роботи на форумах і чатах[41].

Перспективним напрямом є використання в інтересах ОРД різноманітних інформаційних систем, насамперед баз даних, які функціонують у мережі. Пошук інформації в мережі Інтернет здійснюється з використанням спеціальних пошукових систем: Google, Yandex, Yahoo, Aport, Rambler, Altavista, List тощо. Найбільш ефективний пошук інформації можливий при відпрацюванні за кількома пошуковими системами. Усі пошукові системи, з одного боку, схожі, з іншого – відрізняються обсягом обробляємої ними інформації й особливостями «мови пошуку». Найчастіше співробітники правоохоронних органів у своїй роботі користуються двома пошукачами – Google і Yandex.

Викриття злочинця, який активно використовує комп'ютерні засоби в повсякденному житті, серед іншого й для

---

[41] Воронов И. А. Теоретические основы использования информационных и поисковых систем глобальной сети Интернет в оперативно-розыскной деятельности / И. А. Воронов // Вісник ЛДУВС ім. Е. О. Дідоренка. – Луганськ, 2009. – № 1. – С. 200.

досягнення злочинних цілей, потребує системного аналізу інформації в інформаційно-телекомунікаційних мережах. Для ефективного пошуку інформації використовують такі ресурси:

– *сервери служби Whois*, які містять інформацію про належність певної IP-адреси до конкретного провайдера (наприклад: http://www.allwhois.com, http://www.internic.net/whois.html, http://www.ripe.net/db/whois/whois.html, http://www.ripn.net:8080/nic/whois, http://smart-ip.net тощо);

– *електронну пошту* (E-mail), що забезпечує обмін поштовими повідомленнями з будь-яким абонентом цієї мережі;

– *соціальні мережі*, які надають можливість спілкування користувачам зі спорідненими інтересами (наприклад, «ВКонтакте», «Одноклассники», Facebook, Twitter, Instagram тощо);

– *блоги* (англ. blog, від «web log», «мережний журнал або щоденник подій») – веб-сайти, основний зміст яких становлять записи, які регулярно доповнюються, зображення або мультимедіа;

– *сайти знайомств* – інтернет-сервери, що надають користувачам Інтернету послуги з віртуального спілкування з іншими користувачами;

– *веб-форуми* – клас веб-додатків для організації спілкування відвідувачів веб-сайту;

– *чати* (англ. chat – розмова) – засіб спілкування користувачів мережі в режимі реального часу;

– *сервіси IP-телефонії*, що надають послуги з передавання телефонних розмов абонентів за протоколом IP шляхом застосування інформаційно-телекомунікаційних мереж (одними із найпоширеніших сервісів таких послуг є Skype та Viber);

– *сервіс YouTube*, який надає послуги відеохостингу користувачам, які можуть добавляти, переглядати і коментувати ті чи інші відеозаписи;

– *файлові сервери*, на яких можуть бути розміщені будь-які типи файлів (зокрема: RapidShare, MegaUpload.com, FileFactory.com, iFolder, Ex.ua). Найчастіше файли розміщуються на таких серверах анонімно, що створює умови для розміщення компрометуючих матеріалів, порушення авторських прав, учинення злочинів.

Найбільш популярними інтернет-браузерами для персональних комп'ютерів у 2016 році залишались Google Chrome, Яндекс Браузер, Opera, Firefox і Internet Explorer[42].

Залежно від виду ресурсу та його призначення реквізитами пошуку можуть бути індивідуальний номер абонента, вік, стать, ім'я, прізвище, псевдонім, номер електронної пошти, місто або країна проживання. Досить часто встановлення навіть факту використання певного ресурсу особою, яка становить оперативний інтерес, може значно підвищити поінформованість оперативних працівників про обставини злочину, а також сприяти отриманню додаткових відомостей, важливих для розкриття злочину, висунення додаткових версій або створення легенди в процесі оперативної розробки. Перевірка доменного імені з використанням різних інтернет-сайтів дозволяє встановити, на чиє ім'я і в якій країні зареєстрований сайт.

Візитівкою комерційної організації в Інтернеті є її корпоративний сайт, на якому зазвичай розміщена інформація про місцезнаходження, посадових осіб та банківські реквізити організації.

Для здійснення пошуку в мережі Інтернет працівники оперативних підрозділів можуть також використовувати такі сайти: каталог товарів і послуг (price.ua, rozetka.ua); автобазар (rul.ua); працевлаштування (trud.ua); дошка оголошень (emarket.ua); продажа, аренда нерухомості (agent.ua, domik.net); інтернет-аукціон (aukro.ua); продажа автомобілів (infocar.ua); бажаючих познайомитися (love.join.com.ua, love.bigmir.net); послуг сексуального характеру (xmodel.com.ua, x-kiev.ua) тощо. Інтернет-сайти www.nomer.org, http://spravkaru.net, http://spb.telkniga.com дозволяють отримувати інформацію з телефонних довідників низки міст України та СНД.

Роботу з інформаційними системами, які зберігають значний обсяг інформації, полегшують вбудовані програмні функції пошуку конкретної особи, відбору всіх контактів, груп друзів,

---

[42] Кращі браузери 2016 — рейтинг. Який найбільш швидкий, зручний? [Електронний ресурс]. – Режим доступу: http://vidpoviday.com/krashhi-brauzeri-2016-rejting-yakij-najbilsh-shvidkij-zruchnij.

встановлення періодичності відвідування ресурсів Інтернету. Утім, основний недолік цих програм полягає в тому, що вони втрачають певну кількість корисної інформації і цим дають неповну картину того, що відбувається. Крім того, ці програми здебільшого призначені для потреб комерційних організацій, а до специфіки завдань, що стоять перед правоохоронними органами, не адаптовані.

На вибір тактики здійснення пошукових заходів у мережі Інтернет впливає: необхідність залучення спеціальних знань у галузі інформаційних технологій під час проведення ОРЗ; «інтелектуальна» протидія розкриттю злочинів з боку осіб, які їх вчинили; значний обсяг даних (в електронній формі), які необхідно опрацювати під час розкриття злочину; дефіцит часу і динамічність обстановки.

З метою вирішення зазначених проблем розроблено технології, які поліпшують пошук і використання інформації оперативного характеру й дозволяють збирати відомості про кримінальних «авторитетів», їхні зв'язки, минуле, сьогодення і прогнозоване майбутнє, сприяють активному відпрацюванню мережі Інтернет з метою отримання інформації, що становить оперативний інтерес.

Правоохоронні органи нині використовують Інтернет не лише як додаткове джерело інформації, а і як спеціальний засіб здійснення психологічного впливу на учасників кримінальних структур шляхом ведення активної роботи на форумах і чатах. Зокрема можна навмисно дезінформувати учасників екстремістських організацій щодо місця і часу проведення несанкціонованих акцій протесту. Так, з метою формування громадської думки в соціальних мережах, на замовлення Служби зовнішньої розвідки Російської Федерації розроблено програми для «дослідження методів розвідки Інтернет-центрів і регіональних сегментів соціальних мереж» (шифр «Диспут»), «дослідження методів негласного управління в Інтернеті» (шифр «Монітор-3»), «засобів просування спеціальної інформації в соціальних мережах» (шифр «Шторм-12»).

Інноваційною технологією пошуку викрадених речей та встановлення причетних до цього осіб є вивчення пропозицій Інтернет-магазинів та аукціонів. Пошук доцільно починати

з виявлення регіонального об'єкта збуту. Подальшим етапом є аналіз товарів за категоріями, і врешті-решт, пошук конкретної марки приладу або речі. У багатьох випадках на відповідних ресурсах розміщується зображення товару, наводяться його характеристики, за наявності вказуються дефекти, що, по суті, і є пошуковими ознаками. Останній етап передбачає безпосередній контакт з особою, яка розмістила таку інформацію. Окремі Інтернет-магазини обов'язково вимагають вводити паспортні дані та ідентифікаційний код особи, яка пропонує товар на продаж.

Потрібно зазначити, що більшість ОРЗ здійснюється і у звичайному середовищі, і в кіберпросторі. За сучасних умов правоохоронні органи використовують Інтернет не лише як додаткове джерело інформації, а й як спеціальний засіб здійснення ОРЗ шляхом використання кіберпростору.

Досліджуючи закордонний досвід використання кіберпростору з оперативно-розшуковою метою, варто згадати спеціальні правоохоронні системи. Зокрема у Росії функціонує спеціальна система СОРМ, яка розшифровується як «Система оперативно-розыскных мероприятий» і поділяється на дві підсистеми: СОРМ-1 і СОРМ-2[43].

Перша призначена для контролю телефонного зв'язку, друга аналізує Інтернет-трафік. Відповідно до нормативних документів Інтернет-провайдер за свої кошти зобов'язаний встановити обладнання, програмне забезпечення і виділену лінію для місцевого підрозділу ФСБ, а також провести навчання співробітників. Все це дає змогу останнім відстежувати, перехоплювати й переривати зв'язок будь-якого клієнта цього провайдера. Принцип функціонування СОРМ-2 ґрунтується на обробці й накопиченні інформації за ключовими словами. Якщо є підстави підозрювати певну особу в учиненні тяжкого або особливо тяжкого злочину, то відповідно до законодавства Росії СОРМ настроюється на постійне стеження за трафіком підозрюваного. Системи, подібні СОРМ, існують у багатьох інших країнах, наприклад, у США це Carnivore.

---

[43] Нормативные правовые акты по СОРМ [Электронный ресурс]. – Режим доступа: http://www.libertarium.ru/sormlawdocs.

Питання для самоконтролю

1. У чому полягає сутність комп'ютерної розвідки?

2. Назвіть елементи поняття «зняття інформації з електронних інформаційних систем або їх частин, якщо доступ до них не обмежується їх власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту».

3. Охарактеризуйте підстави для здійснення комп'ютерної розвідки.

4. Назвіть основні напрями здійснення та основні функції комп'ютерної розвідки.

5. Дайте характеристику найбільш розповсюджених методів ідентифікації особи.

6. Основні положення біометричної ідентифікації особи.

7. Назвіть шляхи підвищення надійності дактилоскопічних сканерів.

8. Охарактеризуйте напрями підвищення ефективності систем біометричної ідентифікації за зображенням особи.

9. Проблеми підвищення достовірності інформації у кіберпросторі.

10. У чому полягає сутність оперативного розпізнання?

11. Назвіть основні напрями розпізнання терористичних загроз.

12. Охарактеризуйте основні засоби розпізнання терористичних загроз.

13. Для чого використовується «поліцейський скринінг» осіб?

14. Особливості оперативного розпізнання події злочину, пов'язане з наявністю в осіб, причетних до його вчинення, засобів мобільного зв'язку.

15. Основні напрями виконання Державної цільової правоохоронної програми встановлення сучасних систем безпеки, застосування засобів зовнішнього контролю (спостереження) та швидкого реагування

16. Особливості оперативно-розшукового прогнозування.

17. Охарактеризуйте основні методи прогнозування, які використуваються оперативними підрозділами правоохоронних органів.

18. У чому полягають особливості сучасної кіберзлочинності?

19. Назвіть напрями використання мережі Інтернет оперативними підрозділами.

20. Охарактеризуйте інформаційні ресурси мережі Інтернет, які використовуються оперативними підрозділами поліції.

Р о з д і л 4

ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ РОБОТИ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ

4.1. Поняття та елементи організації інформаційно-аналітичної роботи в оперативно-розшуковій діяльності

Ефективність ОРД залежить від повсякденної організаційної діяльності її суб'єктів. Складність і важливість завдань, які нині мають правоохоронні органи, зумовлюють необхідність подальшого вдосконалення організації цієї діяльності.

У сучасних умовах розвитку суспільства, зокрема і кримінального, особливого значення набуває інформаційно-аналітичне забезпечення ОРД. Водночас стрімкий розвиток сучасних інформаційних і телекомунікаційних технологій вимагає нових підходів до організації інформаційно-аналітичної роботи в ОРД.

Під *організацією ОРД* розуміється найбільш доцільна за цих умов система використання наявних сил, засобів і методів ОРД у боротьбі зі злочинністю, призначена для вирішення конкретних функцій (завдань).

Організація ОРД є окремим випадком соціальної організації, яка, своєю чергою, є окремим виявом більш загальних процесів самоорганізації матеріальних систем у природі[1].

Організація як одна із функцій управління має на меті підвищення рівня організованості системи управління шляхом:

– створення, підтримання функціонування та подальшого розвитку організаційних структур управління;

---

[1] Орлов Ю. Ю. Поняття та елементи організації оперативно-розшукової діяльності / Ю. Ю. Орлов // Науковий вісник Київського національного університету внутрішніх справ. – К., 2006. – № 5. – С. 179.

– здійснення організуючого впливу суб'єкта на об'єкт управління з метою впорядкування та узгодженості зв'язків між елементами системи;

– забезпечення взаємодії частин системи тощо[2].

Оскільки ОРД існує не автономно від інших соціальних процесів, а у зв'язку з подіями кримінального характеру, ОРД є відкритою соціальною системою.

ОРД як вид правоохоронної діяльності формувалася так, що організаційно-тактичні рекомендації щодо попередження, виявлення та розкриття злочинів, розшуку осіб, які переховуються від органів розслідування, слідчого судді чи суду, розроблялися й визначалися нормативними актами в поєднанні з правовими нормами застосування засобів ОРД.

ОРД є системою спеціально організованих для цієї мети оперативних підрозділів, які застосовують властиві їм форми, засоби та методи ОРД, тому під системою застосування оперативно-розшукових сил, методів та засобів розуміють систему управління у сфері ОРД – систему суб'єктів ОРД. Тобто існуючу систему оперативних підрозділів розуміють як систему управління у сфері ОРД[3].

Поняття організації ОРД характеризує стан цієї системи – її структуру, місце і роль кожного державного органу та їх оперативних підрозділів у цій системі, їх функції, повноваження, а також підстави, умови і напрями взаємодії при здійсненні ОРД тощо.

Об'єктом у системі управління у сфері ОРД є відносини, які виникають у процесі протидії злочинності з використанням оперативно-розшукових сил, методів і засобів.

Суб'єктами управління у сфері ОРД є керівники відповідних правоохоронних органів (начальники, їх заступники з оперативної роботи), керівники оперативних служб правоохоронних органів, а також керівники окремих оперативних підрозділів.

---

[2] Погорецький М. А. Поняття організації оперативно-розшукової діяльності / М. А. Погорецький, В. П. Шеломенцев // Кримський юридичний вісник. – 2010. – № 1 (8). – С. 33.

[3] Там само. – С. 34.

Процес управління складається з інформаційно-аналітичної роботи, визначення завдань, прогнозування, планування, організації, корегування, обліку й контролю.

Організація ОРД складається із сукупності таких елементів:

1) вивчення, аналіз і оцінка оперативної обстановки;

2) планування ОРД;

3) розстановка наявних сил і засобів відповідно до оперативної обстановки;

4) організація взаємодії в процесі ОРД;

5) контроль за ОРД.

Одним із основних елементів організації ОРД є стан оперативної обстановки. У широкому розумінні оперативну обстановку розглядають як сукупність факторів зовнішнього і внутрішнього середовища правоохоронних органів, які визначають основні умови їх функціонування[4].

Під *оперативною обстановкою* розуміється сукупність різноманітних явищ і процесів, що органічно пов'язані, постійно змінюються і визначають характер та інтенсивність оперативно-розшукових зусиль органів і підрозділів правоохоронних органів, спрямованих на попередження, припинення, розкриття злочинів, розшук злочинців і безвісти зниклих осіб.

Процес управління, з одного боку, передує створенню певної організаційної структури у сфері ОРД, з іншого – забезпечує її найбільш ефективне функціонування.

Завдання управління полягає в упорядкуванні ОРД як системи, її планомірному удосконаленні та увідповідненні зі сучасними вимогами, інтеграції різноманітних компонентів (підсистем) ОРД, встановленні науково обґрунтованих, найбільш доцільних відносин між ними.

Метою організації ОРД є створення сприятливих умов для найефективнішого вирішення її завдань. Як результат цієї діяльності на певний період слід розглядати відповідний стан системи управління у сфері ОРД.

---

[4] Погорецький М. А. Поняття організації оперативно-розшукової діяльності / М. А. Погорецький, В. П. Шеломенцев // Кримський юридичний вісник. – Сімферополь, 2010. – № 1 (8). – С. 36.

Організація ОРД не зводиться лише до вибору тактичних прийомів і методів, а передбачає вирішення низки питань щодо інформаційно-аналітичного забезпечення, планування, управління силами й засобами, взаємодії суб'єктів ОРД та координації їх дій.

Функціональний аспект організації ОРД стосується здійснення процесу управління цією діяльністю і передбачає, крім реалізації оперативно-розшукової тактики, організацію інформаційного та ресурсного забезпечення ОРД, проведення аналітичної роботи, довгострокове та поточне планування, забезпечення взаємодії оперативних підрозділів, контроль та аналіз їх діяльності, розроблення заходів з підвищення ефективності ОРД та забезпечення дотримання прав людини під час цієї діяльності тощо.

Реалізація основних форм інформаційно-аналітичної роботи в ОРД передбачає різний вияв функціонального аспекту організації ОРД.

Одним із напрямів наукової організації праці й управління в системі оперативних підрозділів правоохоронних органів є використання сучасних інформаційних і телекомунікаційних технологій.

Організація інформаційно-аналітичної роботи в ОРД – це система використання наявних сил, засобів і методів, спрямованих на постійний, цілеспрямований збір, обробку, узагальнення, аналіз, зберігання та використання оперативно-розшукової інформації, що здійснюється інформаційно-аналітичними, оперативно-технічними та оперативними підрозділами правоохоронних органів, з метою вирішення завдань ОРД та досудового розслідування.

Основними елементами організації інформаційно-аналітичної роботи в ОРД є:

– *визначення функцій (завдань)* оперативних підрозділів на стратегічному і тактичному рівнях щодо організації інформаційно-аналітичного забезпечення ОРД;

– *формування організаційної структури* організаційно-аналітичних підрозділів оперативних служб залежно від спеціалізації та рівня;

– *підбір, розстановка особового складу* оперативних підрозділів та навчання його основним формам інформаційно-аналітичної роботи в ОРД;

– *збирання, накопичення, систематизація та аналіз* інформації, необхідної для виконання функцій (завдань) оперативних підрозділів щодо протидії злочинності;

– *інформаційно-аналітичне забезпечення* ухвалення управлінських рішень, організації та контролю виконання прийнятих рішень щодо діяльності оперативних підрозділів під час виконання завдань, які стоять перед ними;

– *організація взаємодії й обміну* оперативно-розшуковою інформацією оперативних підрозділів між собою та з іншими правоохоронними органами;

– *упровадження в практичну діяльність* оперативних підрозділів сучасних інформаційних і телекомунікаційних технологій, новітніх оперативно-технічних засобів.

4.2. Організація інформаційно-аналітичної роботи в оперативних підрозділах Національної поліції

Організаційна структура управління інформаційно-аналітичною роботою в оперативних підрозділах Національної поліції. Під організаційною структурою управління розуміється сукупність посад, з'єднаних за допомогою організаційних зв'язків; сукупність організаційно оформлених груп людей, поєднаних відповідними зв'язками та управлінськими відносинами[5]. Ці зв'язки та відносини виявляються насамперед при виробленні та реалізації управлінських рішень.

В організаційній структурі управління посади суб'єктів управління є її *елементами*, а зв'язки між ними – *міжелементними внутрішньосистемними зв'язками*.

Організаційна структура управління певною системою визначається цілями, завданнями та функціями цієї системи, принципами та методами управління нею.

---

[5] Основи управління в органах внутрішніх справ: навч. посібник / О. М. Бандурка, В. М. Бевзенко , В. М. Василенко та ін.; МВС України, Харк. нац. ун-т внутр. справ. – Х.: ХНУВС, 2010. – С. 24.

Розподіл конкретних цілей на стратегічні й тактичні відображає динаміку довгострокових та найближчих інтересів учасників управлінських процесів.

Реальні часткові цілі, яких належить досягти для одержання головного результату діяльності, становлять зміст завдань, поставлених перед органами Національної поліції. Завдання і функції виконуються заради досягнення мети управління.

Функції – це окремі періоди (стадії), напрями управлінської діяльності, пов'язані єдиною остаточною метою, заради досягнення якої й здійснюється процес управління. За загальним значенням функції управління класифікуються на функції цільові та організаційні.

Інформаційно-аналітична функція передбачає збір, обробку, аналіз і оцінку інформації з метою підвищення ефективності діяльності, вона містить усі дії щодо оперування інформацією. Усі ці дії спрямовані на досягнення однієї мети – створення умов для реалізації інших функцій управління. Розглянута функція відображає природу управління, тому що цілеспрямований організуючий вплив ґрунтується на інформації та її оцінці.

Стратегічні й тактичні цілі втілюються у цільових функціях – прогнозуванні й плануванні.

Під *прогнозуванням* розуміється наукове визначення ймовірних шляхів і результатів майбутнього розвитку явищ, процесів і подій (формування злочинних організацій, готування та вчинення злочинів тощо), оцінки показників, що характеризують ці явища та процеси для порівняно віддаленого майбутнього. Прогнозування в ОРД є невід'ємною складовою загального передбачення, що поєднує всі різновиди способів отримання інформації про майбутній розвиток подій.

Планування – це обрання цілей і рішень, необхідних для їх досягнення, заздалегідь ухвалене рішення про те, хто, що, коли і як буде робити, процес підготовки на перспективу рішення про те, що, ким, як і коли має бути виконано.

Для виконання заходів, передбачених плануванням, і досягнення бажаного стану об'єкта управління необхідно здійснити низку організаційних функцій: загальноорганізаційну, координаційну, матеріально-технічного забезпечення, фінансово-економічну, обліку й контролю, кадрового забезпечення,

політико-правового забезпечення, соціального забезпечення та соціального захисту, мотивації тощо.

Залежно від покладених на той чи інший підрозділ функцій (завдань) визначається його організаційна структура. Кожній функції (завданню) має відповідати визначена структурна одиниця у складі підрозділу. Невідповідність виконуваних функцій організаційній структурі підрозділу призводить до дублювання в його роботі або до невиконання певних функцій.

У системі Національної поліції інформаційно-аналітичне забезпечення ОРД здійснюється підрозділами ДІПКП «102», ДОТЗ, ДОС, УРТЗІ та відповідними підрозділами ГУНП. Крім того, інформаційно-аналітична робота в ОРД у різних формах здійснюється іншими оперативними підрозділами НПУ та Робочого апарату Укрбюро Інтерполу.

Система підрозділів інформаційно-аналітичного забезпечення. *Департамент інформаційної підтримки та координації поліції* «102» НПУ є структурним підрозділом апарату центрального органу управління поліції, який організовує і здійснює заходи, передбачені законодавством України, що спрямовані на інформаційно-аналітичне та інформаційно-пошукове забезпечення правоохоронної діяльності та захист персональних даних при їх обробці в структурних підрозділах апарату НПУ, ГУНП України в Автономній Республіці Крим та м. Севастополі, областях, м. Києві, міжрегіональних територіальних органах НПУ, їх структурних (відокремлених) підрозділах.

ДІПКП «102» є головним підрозділом у системі інформаційно-аналітичного забезпечення діяльності органів і підрозділів Національної поліції та здійснює організаційно-методичне керівництво з цих напрямів.

До *основних завдань ДІПКП «102»* належить:

1. Організація інформаційно-аналітичної та інформаційно-пошукової діяльності поліції.

2. Формування баз (банків) даних, що входять до єдиної інформаційної системи МВС України.

3. Участь у реалізації в межах компетенції поліції державної політики у сфері інформатизації, координація виконання державних програм з цього напряму апаратом НПУ.

4. Організація за дорученням керівництва Національної поліції міжвідомчої та міждержавної інформаційної взаємодії, необхідної для виконання покладених на поліцію повноважень.

5. Координація діяльності органів і підрозділів поліції щодо забезпечення наповнення та підтримання в актуальному стані персонально-довідкового та дактилоскопічного обліків.

6. Проведення спеціальних перевірок стосовно осіб, що претендують на заміщення посад, які передбачають зайняття відповідального або особливо відповідального становища, та посад з підвищеним корупційним ризиком щодо наявності судимості, її зняття, погашення.

7. Створення відповідно до законодавства спільно з зацікавленими підрозділами апарату поліції власних баз (банків) даних, необхідних для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчих інформаційно-аналітичних систем, необхідних для виконання покладених на поліцію повноважень.

До *основних функцій ДІПКП «102»* належить:

1. Забезпечення відповідно до законодавства розроблення та запровадження в системі поліції оперативно-розшукових, персонально-довідкових, статистичних та інших інформаційно-аналітичних систем для забезпечення ОРД органів та підрозділів поліції.

2. Координація наповнення та підтримка в актуальному стані баз (банків) даних, що входять до єдиної інформаційної системи МВС України.

3. Забезпечення впровадження інформаційних підсистем для функціонування служб «102», управління силами та засобами реагування патрульної поліції, інших підрозділів, задіяних для підтримання публічної безпеки та порядку.

4. Централізоване ведення та супроводження баз (банків) даних, що формуються в процесі здійснення ОРД, знаходяться на обліку органів і підрозділів поліції, крім підрозділів внутрішньої безпеки.

5. Забезпечення адміністрування серверних програмно-апаратних комплексів та реєстрації і адміністрування користувачів сегмента мережі Інтернет апарату НПУ.

6. Забезпечення функціонування, адміністрування серверних програмно-апаратних комплексів, реєстрації та адміністрування користувачів поштових систем у відомчій корпоративній мережі органів та підрозділів поліції.

7. У межах компетенції проведення спеціальної перевірки відомостей стосовно претендентів на посади до центральних органів державної влади України щодо наявності судимостей, її зняття, погашення.

8. Формування статистичної звітності про результати роботи органів і підрозділів поліції, стан протидії корупції та застосування адміністративної практики органами і підрозділами поліції.

9. Здійснення відповідно до вимог Закону України «Про захист персональних даних» обробки персональних даних згідно зі завданнями та функціями, покладеними на поліцію Законом України «Про Національну поліцію» та іншими законами[6].

З метою координації наповнення та підтримки в актуальному стані баз (банків) даних, що входять до єдиної інформаційної системи (ЄІС) МВС України ДІПКП «102» постійно взаємодіє з Департаментом інформаційних технологій МВС України.

ДІТ МВС України формує та веде централізовані електронні та карткові оперативно-довідкові та дактилоскопічні обліки, бази (банки) даних, які входять до ЄІС МВС, структура та порядок використання якої визначаються окремим положенням.

До *основних завдань ДІТ МВС України* належить:

1) формування та забезпечення реалізації політики інформаційного забезпечення діяльності системи МВС;

2) забезпечення належного функціонування, формування, підтримки в актуальному стані та контролю процесів використання ЄІС МВС;

---

[6] Про затвердження Положення про Департамент інформаційної підтримки та координації поліції «102» Національної поліції України: наказ Національної поліції України від 30 грудня 2015 р. № 228.

3) організація забезпечення режиму доступу та захисту відомчих інформаційних ресурсів та персональних даних при їх обробці в системі МВС;

4) упровадження технологій електронного урядування в системі МВС;

5) організація інформаційного забезпечення та інформаційної взаємодії в системі МВС;

6) забезпечення інформаційної взаємодії з іншими державними органами, громадськими організаціями, фізичними та юридичними особами, правоохоронними органами іноземних держав та міжнародними організаціями;

7) упровадження передових інформаційних технологій, залучення програм та проектів міжнародної технічної допомоги для забезпечення інформатизації діяльності МВС.

ДІТ МВС України відповідно до покладених на нього завдань:

1) безпосередньо розробляє та погоджує розроблені в системі МВС проекти нормативно-правових актів з питань інформаційного забезпечення та обробки персональних даних;

2) координує виконання державних програм з інформатизації в системі МВС;

3) організовує і здійснює заходи, спрямовані на забезпечення правової охорони та легалізації програмного забезпечення в системі МВС;

4) організовує та контролює процес інтегрування на рівні МВС баз (банків) даних системи МВС;

5) вживає заходів з актуалізації інформаційних ресурсів ЄІС МВС відповідно до поточних завдань МВС;

6) формує та підтримує в актуальному стані інформаційні ресурси, що входять до ЄІС МВС;

7) надає доступ до інформаційних ресурсів ЄІС МВС авторизованим користувачам відповідно до режимів доступу та рівня захисту, визначених нормативно-правовими актами МВС;

8) забезпечує безпосередній оперативний доступ працівників системи МВС та інших державних органів до відповідних державних реєстрів, баз даних інших державних органів;

9) забезпечує формування електронних версій для персональних обліків, що входять до ЄІС МВС та ведуться у паперовому вигляді;

10) забезпечує інформаційно-аналітичну підтримку процесу ухвалення керівництвом МВС управлінських рішень, готує статистичні, аналітичні та прогнозні матеріали;

11) організовує і здійснює заходи, спрямовані на захист відомчих інформаційних ресурсів та персональних даних при їх обробці в системі МВС;

12) аналізує загрози безпеці персональним даним, що обробляються в системі МВС;

13) здійснює документальну фіксацію фактів порушення процесу обробки та захисту персональних даних;

14) організовує функціонування системи електронного документообігу в МВС;

15) організовує роботу із сертифікації ключів, забезпечує надання послуг електронного цифрового підпису в системі МВС та обслуговує сертифікати ключів;

16) здійснює в межах своїх повноважень обробку персональних даних;

17) готує проекти спільних наказів про обмін інформаційними ресурсами між МВС та іншими державними органами, порядок користування інформаційними ресурсами ЄІС МВС іншими державними органами;

18) здійснює інформаційне супроводження діяльності Головного центру з надання сервісних послуг МВС та територіальних центрів з надання сервісних послуг МВС;

19) надає в установленому порядку відомості щодо інформаційного забезпечення системи МВС на запити та звернення народних депутатів України, органів виконавчої влади, органів місцевого самоврядування, об'єднань громадян, фізичних та юридичних осіб, взаємодіє в межах повноважень з громадськими організаціями з питань інформатизації діяльності системи МВС;

20) проводить – за письмовими запитами уповноважених органів – перевірки фізичних осіб щодо їх перебування на відповідних обліках ЄІС МВС;

21) забезпечує проведення спеціальних перевірок стосовно осіб, які претендують на зайняття посад, які передбачають зайняття відповідального або особливо відповідального становища, та посад з підвищеним корупційним ризиком;

22) надає за зверненнями державних органів офіційні повідомлення, передбачені чинним законодавством;

23) надає в межах компетенції та в порядку, визначеному законодавством України, інформаційні послуги фізичним та юридичним особам;

24) організовує опрацювання звернень до інформаційних ресурсів ЄІС МВС;

25) забезпечує надання громадянам інформації про притягнення до кримінальної відповідальності, відсутність (наявність) судимості або обмежень, передбачених кримінально-процесуальним законодавством;

26) забезпечує функціонування веб-порталу МВС;

27) вивчає можливості використання сучасних програмно-технічних платформ в інформаційно-аналітичній діяльності системи МВС та розробляє пропозиції щодо їх упровадження;

28) забезпечує інтеграцію наявних програмно-апаратних платформ у центрі обробки даних;

29) організовує роботу із залучення та реалізації проектів міжнародної технічної допомоги для інформатизації діяльності системи МВС[7].

Система оперативних підрозділів. Основні форми інформаційно-аналітичної роботи в ОРД здійснюються також оперативними підрозділами кримінальної та спеціальної поліції, підрозділами внутрішньої безпеки.

До *основних напрямів* інформаційно-аналітичної роботи в ОРД Національної поліції належать:

– формування та аналіз баз даних про злочини та осіб, які їх учинили, прогнозування нових методів учинення злочинів;

– вивчення та оцінка стану злочинності;

– вивчення стану та ефективності використання оперативно-розшукових сил, засобів і методів у боротьбі зі злочинністю;

– підготовка на основі наявної інформації аналітичних матеріалів, експрес-інформацій, пропозицій тощо.

---

[7] Про затвердження Положення про Департамент інформаційних технологій Міністерства внутрішніх справ України: Наказ МВС від 14 грудня 2015 року № 1572.

Суб'єктами інформаційно-аналітичної роботи в ОРД є оперативні підрозділи карного розшуку, захисту економіки, БЗПТЛ, протидії наркозлочинності, кіберполіції, з виявлення небезпечних матеріалів та екологічних злочинів, кримінальної розвідки, оперативної служби, ОТЗ, внутрішньої безпеки, спеціальної поліції.

Організація інформаційно-аналітичної роботи в оперативних підрозділах апарату Національної поліції регламентується відповідними функціями цих підрозділів, зокрема:

Департамент карного розшуку:

– вивчення та аналіз стану злочинності, чинників, що її обумовлюють, прогнозування криміногенної ситуації. Розроблення та внесення пропозицій керівництву Національної поліції щодо визначення пріоритетних напрямів діяльності підрозділів карного розшуку та ефективних засобів і методів виконання покладених на них завдань;

– участь у наукових, кримінологічних і соціологічних дослідженнях, розробленні на їх основі державних програм боротьби зі злочинністю. Підготовка інформаційно-аналітичних, методичних і прогностичних матеріалів щодо підвищення ефективності протидії злочинності;

– на підставі комплексного аналізу оперативної обстановки та наявної в підрозділах карного розшуку територіальних органів поліції оперативної інформації підготовка управлінських рішень щодо активізації роботи з протидії груповій і організованій злочинності та вжиття ОРЗ з притягнення правопорушників до кримінальної відповідальності;

– здійснення контролю за дотриманням підпорядкованими підрозділами порядку прийняття, реєстрації, обліку і розгляду заяв, повідомлень та іншої інформації про злочини та події, ужиття заходів для покращання цієї роботи;

– із підрозділом інформаційно-аналітичного забезпечення – організація створення та поповнення АІС оперативно-розшукового і профілактичного призначення. Забезпечення функціонування, своєчасного поповнення та належного використання оперативно-розшукових обліків;

– організація взаємодії з підрозділами центрального органу управління поліцією, територіальними органами поліції,

міністерствами, іншими центральними органами виконавчої влади, установами, громадськими організаціями, а також правоохоронними органами зарубіжних країн і міжнародними організаціями у вирішенні питань боротьби зі злочинністю;

– безпосередня робота з джерелами оперативної інформації та за ОРС. Аналіз ефективності використання негласного апарату, проведення оперативних розробок у боротьбі зі злочинністю, вивчення процесів, які відбуваються в злочинному середовищі, та вироблення на цій основі пропозицій керівництву Національної поліції з покращення ОРД за зазначеними напрямами;

– здійснення поточного та перспективного планування оперативно-службової діяльності Департаменту, узагальнення позитивного досвіду у сфері протидії злочинності, розроблення методичних рекомендацій і посібників, їх упровадження в практичну діяльність підрозділів карного розшуку тощо[8].

Департамент захисту економіки:

– аналіз стану економічної злочинності, чинників, що її зумовлюють, прогнозування криміногенної ситуації в соціально-економічній сфері держави та окремих її регіонах, розроблення і внесення пропозицій керівництву НПУ щодо організації діяльності підрозділів захисту економіки;

– взаємодія зі структурними підрозділами Національної поліції, іншими органами державної влади, підприємствами, установами, організаціями, зокрема громадськими, а також із правоохоронними органами іноземних держав і міжнародними організаціями щодо вирішення питань боротьби зі злочинністю;

– аналіз ефективності використання сил, засобів та оперативно-пошукових обліків у боротьбі зі злочинністю, визначення основних напрямів й тактики ОРД, пов'язаної з виявленням злочинів у сфері економіки, надання пропозицій керівництву Національної поліції щодо підвищення ефективності ОРД;

– розроблення і реалізація програм, комплексних та цільових оперативно-профілактичних операцій, а також інші

---

[8] Про затвердження Положення про Департамент карного розшуку Національної поліції України: Наказ Національної поліції України від 14 листопада 2015 р. № 90.

заходи, спрямовані на активізацію протидії злочинності за визначеними пріоритетними напрямами;

– участь у наукових дослідженнях і розробленні за їх результатами державних програм боротьби зі злочинністю, а також у підготовці інформаційно-аналітичних, методичних матеріалів щодо стану та підвищення ефективності протидії злочинам у сфері економіки;

– контроль за дотриманням працівниками ДЗЕ НПУ порядку приймання та реєстрації заяв і повідомлень про кримінальні правопорушення та іншої інформації;

– організація діловодства, зокрема за матеріалами негласних заходів ОРД, контроль за дотриманням правил роботи з шифротелеграмами, створення необхідних умов для забезпечення режиму секретності;

– взаємодія з органами досудового розслідування, підрозділами, що здійснюють ОРД, а також із науково-дослідними установами системи Національної поліції під час здійснення оперативно-службової діяльності, зокрема за конкретними злочинами;

– надання відповідним структурним підрозділам Національної поліції пропозицій щодо створення та вдосконалення наявних АІС, забезпечення своєчасного поповнення та належного використання оперативно-пошукових обліків[9].

Департамент боротьби зі злочинами, пов'язаними з торгівлею людьми:

– аналіз і узагальнення результатів та ефективності діяльності підрозділів БЗПТЛ із запобігання вчиненню, виявлення, припинення і розкриття кримінальних правопорушень, пов'язаних з торгівлею людьми, нелегальною міграцією, а також правопорушень у сфері суспільної моралі шляхом збирання, узагальнення, систематизації наявної інформації, вивчення чинників, що їх обумовлюють, прогнозування криміногенної ситуації на загальнодержавному та регіональному рівнях; розроблення та внесення за їх результатами пропозицій керівництву Національної поліції щодо підвищення ефективності

---

[9] Про затвердження Положення про Департамент за хисту економіки Національної поліції України: Наказ Національної поліції України від 7 листопада 2015 р. № 81.

організації діяльності підрозділів БЗПТЛ, зокрема ОРД, роботи з джерелами оперативної інформації та за ОРС;

– здійснення взаємодії зі структурними підрозділами центрального органу управління Національної поліції, органами досудового розслідування, науково-дослідними установами МВС, іншими органами державної влади, а також співпраця з правоохоронними органами іноземних держав і міжнародними організаціями в розв'язанні питань протидії кримінальним правопорушенням, пов'язаним з торгівлею людьми, нелегальною міграцією (підроблення документів, печаток, штампів та бланків, а також збут чи використання підроблених документів, печаток, штампів, зловживання владою або службовим становищем, службове підроблення. Статті 358, 364, 366 КК України), та правопорушеннями у сфері суспільної моралі;

– звертання в межах своєї компетенції із запитами до органів правопорядку (правоохоронних органів) інших держав або міжнародних організацій поліції відповідно до закону, міжнародних договорів України, установчих актів та правил міжнародних організацій поліції, членом яких є Україна, та виконання запитів зазначених вище органів;

– узагальнення позитивного досвіду протидії торгівлі людьми, кримінальним правопорушенням, пов'язаним з нелегальною міграцією, а також правопорушенням у сфері суспільної моралі, розроблення методичних рекомендацій і посібників;

– організація та здійснення ОРД, спрямованої на виявлення та припинення кримінальних правопорушень, пов'язаних з торгівлею людьми, нелегальною міграцією, а також правопорушень у сфері суспільної моралі, та комплексне використання джерел оперативної інформації, можливостей оперативних підрозділів та застосування ОТЗ під час провадження в ОРС, контроль за використанням коштів, призначених для проведення цієї роботи;

– організація та здійснення діловодства, зокрема й за матеріалами негласних заходів ОРД. Забезпечення дотримання правил криптографічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої визначена законом;

– відповідно до законодавства України користування базами (банками) даних Національної поліції та МВС, а також інших державних органів, внесення пропозицій щодо створення нових та вдосконалення діючих АІС; забезпечення своєчасного поповнення та належного використання оперативно-пошукових обліків[10].

Департамент протидії наркозлочинності:

– організація та проведення оперативно-розшукових заходів із виявлення і документування тяжких та особливо тяжких кримінальних правопорушень, пов'язаних з незаконним обігом наркотичних засобів, психотропних речовин і прекурсорів, насамперед учинених злочинними групами осіб, які мають міжрегіональні та міждержавні зв'язки, особливо в їх організованих формах;

– розроблення та реалізація програм протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та запобігання поширенню наркоманії;

– проведення на території України операцій щодо виявлення осіб, які займаються розповсюдженням наркотиків, зокрема у навчальних закладах країни та в місцях масового проведення дозвілля молоді, а також інших комплексних заходів, спрямованих на перекриття каналів незаконного надходження наркотиків;

– проведення антинаркоманійної пропаганди через засоби масової інформації;

– участь у міжнародному співробітництві з питань організації протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та проблем поширення наркоманії[11].

Департамент кіберполіції:

– здійснення передбачених чинним законодавством заходів зі збирання й узагальнення інформації стосовно об'єктів,

---

[10] Про затвердження Положення про Департамент боротьби зі злочинами, пов'язаними з торгівлею людьми Міністерства внутрішніх справ України: Наказ МВС України від 14 жовтня 2014 р. № 1074.

[11] Про затвердження Положення про Департамент протидії наркозлочинності Національної поліції України: Наказ Національної поліції України від 17 листопада 2015 р. № 95.

у тому числі об'єктів сфери телекомунікацій, інтернет-послуг, банківських установ і платіжних систем з метою попередження, виявлення та припинення кримінальних правопорушень;

– забезпечення в порядку, передбаченому законодавством України, формування й наповнення інформаційних масивів даних, АІС відповідно до потреб службової діяльності;

– вивчення позитивного вітчизняного та зарубіжного досвіду боротьби з кримінальними правопорушеннями у сфері протидії кіберзлочинності та внесення пропозицій керівництву Національної поліції щодо його впровадження;

– створення та забезпечення функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі;

– аналіз та систематизація даних про кримінальні правопорушення, учинені у сфері протидії кіберзлочинності та з використанням високих технологій, що надходять від громадян каналами кол-центрів, електронними листами та терміналами зворотного зв'язку;

– відповідно до чинного законодавства збирання, узагальнення, систематизація та аналіз інформації про криміногенні процеси та стан боротьби зі злочинністю за напрямом діяльності Департаменту на загальнодержавному та регіональному рівнях, оцінювання результатів за окремими показниками службової діяльності, надання, відповідно до законодавства України, звітів про результати роботи та відповідну інформацію керівництву Національної поліції, МВС, органам державної влади з питань попередження та протидії кіберзлочинам;

– налагодження та підтримка взаємодії і партнерських відносин з органами державної влади, іншими правоохоронними органами, приватним сектором та правоохоронними органами іноземних держав, міжнародними установами та організаціями у сфері протидії кіберзлочинності для ефективного

виконання завдань ДКП, а також підвищення довіри населення до органів Національної поліції[12].

Департамент внутрішньої безпеки:

– здійснення, в межах компетенції, заходів щодо аналізу та проведення необхідних перевірок з питань дотримання органами та підрозділами Національної поліції:

– режиму збереження інформації з обмеженим доступом;

– порядку організації роботи щодо доступу на режимні об'єкти;

– вимог щодо запобігання прийняття на службу в Національну поліцію осіб, які мають злочинні або корисливі наміри;

– збирання, накопичення, систематизація та аналіз інформації щодо негативних явищ і тенденцій у органах та підрозділах Національної поліції, а також ужиття заходів щодо попередження їх розвитку;

– координація дій та участь у заходах щодо виявлення, попередження, припинення та документування протиправних посягань на життя і здоров'я працівників Національної поліції, учинення яких пов'язано з виконанням ними службових обов'язків;

– здійснення оперативного обслуговування органів та підрозділів Національної поліції з метою своєчасного отримання даних про факти кримінальних та корупційних правопорушень, що готуються або вчинені працівниками Національної поліції, а також даних, необхідних для виконання інших завдань за напрямками роботи ДВБ;

– аналіз результатів роботи ДВБ, визначення напрямків удосконалення їх діяльності щодо виявлення, попередження та припинення кримінальних та корупційних правопорушень в службовій діяльності органів та підрозділів Національної поліції;

– здійснення у межах компетенції взаємодії та обміну інформацією з органами та підрозділами Національної поліції, іншими правоохоронними органами, міністерствами,

---

[12] Про затвердження Положення про Департамент кіберполіції Національної поліції України: Наказ Національної поліції України від 10 листопада 2015 р. № 85.

органами влади з питань попередження та виявлення кримінальних та корупційних правопорушень серед працівників Національної поліції[13].

Система режимно-секретних органів складається з Управління режиму та технічного захисту інформації апарату НПУ, а також управлінь (відділів) режиму та технічного захисту інформації ГУНП в областях.

До *основних функцій* режимно-секретних органів, які регламентують інформаційно-аналітичну роботу в ОРД, належать:

– розроблення та реалізація заходів, спрямованих на забезпечення охорони державної таємниці, збереження службової інформації, посилення режиму секретності в системі Національної поліції, запобігання розголошенню секретної інформації, випадкам утрати її матеріальних носіїв, здійснення контролю за станом режиму секретності, технічного та криптографічного захисту інформації в органах і підрозділах поліції;

– виявлення та закриття каналів витоку інформації з обмеженим доступом у процесі службової діяльності органів і підрозділів Національної поліції;

– здійснення у межах компетенції контролю за дотриманням структурними підрозділами апарату Національної поліції, органами і підрозділами Національної поліції: вимог щодо побудови і функціонування системи та порядку виконання заходів з ТЗІ, проведення експертизи комплексної системи захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах; вимог щодо забезпечення безпеки та функціонування спеціальних видів зв'язку, поводження з шифротелеграмами;

– супроводження створення комплексної системи захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах;

– забезпечення реалізації визначеної державної політики у сфері захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

---

[13] Про затвердження Положення про Департамент внутрішньої безпеки Національної поліції України: Наказ Національної поліції України від 9 листопада 2015 р. № 83.

– організація та здійснення контролю за умовами обробки інформації в автоматизованих системах і телекомунікаційних мережах та станом її захищеності;

– дослідження об'єктів інформаційної діяльності, інформаційних систем щодо безпеки інформації (вивчення і аналіз проектної та програмної документації, технологічних процесів, інформаційних потоків, умов функціонування об'єктів інформаційної діяльності, інформаційних систем з метою визначення загрози безпеці інформації щодо її витоку, блокування та порушення цілісності);

– опрацювання та погодження ескізних, технічних та робочих проектів документації щодо створення автоматизованих систем класу «2» і «3», супроводження робіт з їх створення, удосконалення та введення в експлуатацію;

– організація та проведення державних експертиз комплексних систем захисту інформації в автоматизованих системах класу «1» органів та підрозділів Національної поліції;

– організація експлуатації та експлуатація засобів криптографічного захисту, зокрема й в інформаційно-телекомунікаційних системах, мережах передачі даних, автоматизованих системах;

– супроводження процесів проектування та впровадження інформаційно-телекомунікаційних систем, мереж передачі даних, автоматизованих систем, у яких захист інформації здійснюється з використанням засобів криптографічного захисту[14].

Правоохоронні органи України можуть використовувати можливості Робочого апарату Укрбюро Інтерполу для отримання інформації, яка міститься у банках даних Генерального секретаріату Інтерполу.

Функції Робочого апарату Укрбюро Інтерполу, які регламентують інформаційно-аналітичну роботу в ОРД:

– обмін інформацією з Генеральним секретаріатом Інтерполу, Європолом, органами правопорядку та іншими органами державної влади України, а також з компетентними органами іноземних держав з питань боротьби зі злочинністю;

---

[14] Про затвердження Положення про Управління режиму та технічного захисту інформації Національної поліції України: Наказ Національної поліції України від 27.11.2015 № 122.

– отримання від компетентних органів іноземних держав запитів про проведення перевірок, оперативно-розшукових та інших заходів на території України і організація їх виконання органами правопорядку та іншими органами державної влади України;

– інформування компетентних органів іноземних держав про результати виконання їх запитів органами правопорядку та іншими органами державної влади України;

– надсилання до компетентних органів іноземних держав запитів органів правопорядку та інших органів державної влади України про проведення перевірок, оперативно-розшукових та інших заходів на їх території;

– інформування органів правопорядку та інших органів державної влади України про результати виконання їх запитів компетентними органами іноземних держав;

– отримання від Європолу запитів з питань, визначених Угодою між Україною та Європейським поліцейським офісом про стратегічне співробітництво ратифікованою Законом України від 05 жовтня 2010 року № 2576-VI, організація їх виконання органами правопорядку та іншими органами державної влади України та інформування Європолу про результати їх виконання;

– надсилання до Європолу запитів органів правопорядку та інших органів державної влади України з питань, визначених Угодою між Україною та Європейським поліцейським офісом про стратегічне співробітництво, та інформування їх про результати виконання;

– внесення до Генерального секретаріату Інтерполу клопотання про публікацію циркулярних повідомлень Інтерполу;

– забезпечення обміну інформацією між органами правопорядку та іншими органами державної влади України та компетентними органами іноземних держав, а також з Генеральним секретаріатом Інтерполу щодо ідентифікації невідомих осіб та невпізнаних трупів;

– здійснення обміну інформацією з розвідувальними органами України з питань, що стосуються протидії злочинності;

– отримання в установленому порядку доступу до інформаційних систем та банків даних органів правопорядку

та інших органів державної влади України, використання їх у своїй діяльності;

– використання інформаційних систем та банків даних Генерального секретаріату Інтерполу, Європолу, організація та забезпечення надання в установленому порядку доступу до них органам правопорядку та іншим органам державної влади України;

– забезпечення наповнення в установленому порядку банків даних Інтерполу та Європолу інформацією, наданою органами правопорядку та іншими органами державної влади України;

– створення і використання власних автоматизованих інформаційних систем;

– складання на підставі інформації органів правопорядку та інших органів державної влади України звітів, інформаційно-аналітичних матеріалів з питань боротьби зі злочинністю, надсилання їх до компетентних органів іноземних держав, Інтерполу та Європолу;

– здійснення інформаційно-аналітичного забезпечення органів правопорядку та інших органів державної влади України з питань боротьби зі злочинністю на підставі матеріалів компетентних органів іноземних держав, Інтерполу та Європолу;

– координація діяльності підрозділів Укрбюро Інтерполу територіальних органів поліції[15].

4.3. Організація використання інформаційних систем підрозділами Національної поліції

Відповідно до Закону України «Про Національну поліцію» поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень, визначених цим Законом.

Національна поліція в межах інформаційно-аналітичної діяльності:

1) формує бази (банки) даних, що входять до єдиної інформаційної системи МВС України;

---

[15] Про затвердження Положення про Робочий апарат Укрбюро Інтерполу: Наказ Національної поліції України від 21 грудня 2015 р. № 193.

2) користується базами (банками) даних МВС України та інших органів державної влади;

3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу;

4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями.

Національна поліція наповнює та підтримує в актуальному стані такі бази (банки) даних, що входять до єдиної інформаційної системи МВС України, стосовно:

1) осіб, щодо яких поліцейські здійснюють профілактичну роботу;

2) виявлених кримінальних та адміністративних правопорушень, осіб, які їх учинили; руху кримінальних проваджень; обвинувачених, обвинувальний акт щодо яких направлено до суду;

3) розшуку підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання або вироку суду;

4) розшуку безвісно зниклих;

5) установлення особи невпізнаних трупів та людей, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком;

6) зареєстрованих в органах поліції кримінальних або адміністративних правопорушень, подій, які загрожують особистій чи публічній безпеці, надзвичайних ситуацій;

7) осіб, затриманих за підозрою у вчиненні правопорушень (адміністративне затримання, затримання згідно з дорученнями органів правопорядку, затримання осіб органами досудового розслідування, адміністративний арешт, домашній арешт).

Під час наповнення баз (банків) даних затриманих та доставлених осіб поліція забезпечує збирання, накопичення мультимедійної інформації (фото, відео-, аудіозапис) та біометричних даних (дактилокартки, зразки ДНК);

8) осіб, які скоїли адміністративні правопорушення, провадження у справах за якими здійснюється поліцією;

9) зареєстрованих кримінальних та адміністративних корупційних правопорушень, осіб, які їх учинили, та результатів розгляду цих правопорушень у судах;

10) іноземців та осіб без громадянства, затриманих поліцією за порушення визначених правил перебування в Україні;

11) викрадених номерних речей, цінностей та іншого майна, які мають характерні ознаки для ідентифікації, або речей, пов'язаних із учиненням правопорушень, відповідно до заяв громадян;

12) викрадених (втрачених) документів за зверненням громадян;

13) знайдених, вилучених предметів і речей, зокрема й заборонених або обмежених в обігу, а також документів з ознаками підробки, які мають індивідуальні (заводські) номери;

14) викрадених транспортних засобів і транспортних засобів, які розшукуються у зв'язку з безвісним зникненням особи, виявлених безгосподарних транспортних засобів, а також викрадених, втрачених номерних знаків;

15) виданих дозвільних документів у сфері безпеки дорожнього руху та дозволів на рух окремих категорій транспортних засобів;

16) зброї, що перебуває у володінні та користуванні фізичних і юридичних осіб, яким надано дозвіл на придбання, зберігання, носіння, перевезення зброї;

17) викраденої, втраченої, вилученої, знайденої зброї, а також добровільно зданої зброї із числа тієї, що незаконно зберігалася;

18) бази даних, що формуються в процесі здійснення ОРД відповідно до закону[16].

Інформація про доступ до бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про поліцейського, який отримав доступ, та про обсяг даних, доступ до яких було отримано.

Кожна дія поліцейського щодо отримання інформації із зазначених інформаційних ресурсів фіксується у спеціальному електронному архіві, ведення якого покладається на службу інформаційних технологій МВС України.

В електронному архіві фіксуються прізвище, ім'я, по батькові та номер спеціального жетона поліцейського, вид отриманої

---

[16] Про Національну поліцію: Закон України від 2 липня 2015 р. № 580-VIII // Відомості Верховної Ради України. – 2015. – № 40–41. – Ст. 379.

інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації поліцейського, який отримував інформацію з реєстрів.

Національна поліція вживає всіх заходів для недопущення будь-яких порушень прав і свобод людини, пов'язаних з обробкою інформації.

Поліцейські несуть персональну дисциплінарну, адміністративну та кримінальну відповідальність за вчинені ними діяння, що призвели до порушень прав і свобод людини, пов'язаних з обробкою інформації.

МВС України у межах компетенції здійснює контроль за дотриманням вимог законів та інших нормативно-правових актів під час формування та користування поліцейськими інформаційними базами (банками) даних.

З метою об'єднання існуючих в системі МВС України ІПС в єдиний інформаційно-аналітичний комплекс із використанням сучасних інформаційних технологій, комп'ютерного та телекомунікаційного обладнання та підтримки оперативно-службової діяльності поліції, значного зміцнення їх спроможності протидії та профілактиці злочинності, створена і функціонує ***Інтегрована інформаційно-пошукова система Національної поліції («ІІПС»)***.

До складу ІІПС входять такі інформаційні підсистеми:

ІП «Єдиний облік» – база даних, у якій обліковуються відомості про події, кримінальні та адміністративні правопорушення, надзвичайні події, викладені в заявах (повідомлення, рапорти), що зареєстровані в чергових частинах органів НПУ;

ІП «Затримані та доставлені» – база даних, у якій обліковуються особи, затримані та доставлені до органу НПУ для встановлення особистості та з'ясування обставин учиненого правопорушення;

ІП «Особа» – база даних, у якій обліковуються особи, які вчиняють протиправні діяння, становлять групу ризику, стосовно яких здійснюється профілактична робота;

ІП «Розшук» та «Пізнання» – бази даних, у яких обліковуються підозрювані, обвинувачені та підсудні, що переховуються від органів досудового розслідування, слідчого судді чи суду; засуджені до покарання у вигляді позбавлення волі,

які ухиляються від виконання кримінального покарання; безвісти зниклі особи; невпізнані трупи; невідомі хворі та діти, які не можуть повідомити інформацію про себе; особи, які переховуються від правоохоронних органів інших країн, держав – членів Інтерполу;

ІП «Річ» – база обліку речей, викрадених, вилучених у громадян (належність яких не встановлена), з ознаками підроблення, заборонених або обмежених у цивільному обігу, знайдених або вилучених з камер схову вокзалів, портів, аеропортів та зданих до органів НПУ. База даних «Річ» складається з підсистем «Номерна річ», «Антикваріат»;

ІП «Угон» – база даних, у якій обліковуються відомості про транспортні засоби (автомобілі, мотоцикли, мопеди, плавзасоби), які розшукуються органами НПУ, правоохоронними органами держав-учасниць СНД;

ІП «Викрадені (втрачені) документи» – база даних, у якій обліковуються відомості щодо документів (бланків документів) викрадених, утрачених, вилучених (з ознаками підробки) у громадян і службових осіб, не зданих паспортів померлих громадян, паспортів осіб, які знаходяться в розшуку, та які мають індивідуальні заводські (фабричні) номери і знаходяться у державному обігу;

ІП «Зареєстрована зброя» – база даних, що містить інформацію про вогнепальну та холодну зброю, яка використовується фізичними та юридичними особами легально та зареєстрована в дозвільній системі органів НПУ;

ІП «Кримінальна зброя» – база відомостей про зброю, викрадену, утрачену, знайдену, добровільно здану до органів НПУ, вилучену працівниками НПУ з числа тієї, що незаконно зберігалася, незалежно від її технічного стану, що має індивідуальні заводські (фабричні) номери або номери деталей;

ІП «Адміністративні правопорушення» – база даних, у якій обліковуються відомості про зареєстровані в органах НПУ адміністративні правопорушення, за матеріалами яких уповноваженими на те працівниками НПУ складено протоколи про адміністративні правопорушення.

Крім того, в ІП «Адміністративні правопорушення» обліковуються відомості про притягнення окремих осіб до

відповідальності через учинення ними кримінальних правопорушень, правову кваліфікацію таких порушень та орган досудового розслідування, яким здійснюється кримінальне провадження;

ІП «Мігрант» – база даних, у якій обліковується інформація про осіб, затриманих за порушення законодавства України про державний кордон, про правовий статус іноземців та осіб без громадянства;

ІП «Корупція» – база даних, у якій обліковуються відомості про зареєстровані корупційні правопорушення, за матеріалами яких уповноваженими працівниками органів НПУ у сфері протидії корупції складено протоколи про вчинення корупційних правопорушень, а осіб, які вчинили ці правопорушення, рішеннями судів притягнуто до відповідальності за корупційні правопорушення.

Основою системи функціонування ІІПС є територіальні вузли, які розміщені та функціонують безпосередньо в територіальних (відокремлених) відділах поліції з підключенням виділеними або комутованими каналами зв'язку до баз даних регіональних (обласних) вузлів ІІПС. Інформаційні ресурси інформаційних підсистем ІІПС центрального вузла формуються шляхом об'єднання інформаційних ресурсів інформаційних підсистем ІІПС регіональних (обласних) вузлів.

Центральні та регіональні інформаційні підсистеми ІІПС формуються на засадах якісно нового рівня обробки та надання інформації кримінального характеру шляхом зведення (інтеграції) інформаційних обліків до єдиної системи, яка відображає причинно-наслідкові зв'язки між об'єктами обліків.

Серед інформаційно-пошукових систем, які найчастіше використовують працівники оперативних підрозділів Національної поліції, необхідно також виділити ***АІПС «АРМОР»*** (рос. – Автоматизированное рабочее место оперативного работника). Система «АРМОР» була розроблена фахівцями УМВС України в Луганській області та прийнята за базову у всіх обласних управліннях МВС України з 2003 року. Нині система «АРМОР» поєднала у собі понад п'ятидесят автоматизованих підсистем, зокрема: ІП «Адреса»; ІП «Адмінпрактика»; ІП «Документ»; ІП «Розшук»; ІП «Розшук-Україна»; ІП «Запити»; ІП «Фото»; ІП «Сонда»

(дактилокарти); ІП «Юридичні особи»; ІП «Угон»; ІП «Мігрант»; ІП «Злочин»; ІП «Загублені документи» тощо.

Для інформаційно-аналітичного забезпечення оперативно-розшукової діяльності оперативних підрозділів Національної поліції функціонує ***АІС оперативного призначення (АІС ОП),*** яка має два рівня – регіональний (обласний) і центральний. На регіональному рівні здійснюється збір, обробка, зберігання інформації та її використання для інформаційно-аналітичного забезпечення роботи оперативних підрозділів. Своєю чергою, на центральному рівні накопичується інформація обласного рівня і та, що надходить з оперативних підрозділів.

Із обліками спеціального призначення (АІС ОП), які формують і використовують оперативні підрозділи Національної поліції, створені обліки загального користування, які ведуть слідчі, криміналістичні підрозділи, сервісні центри, поліція охорони тощо. Крім оперативних обліків, відповідно до напряму функціонування галузевих служб Національної поліції розрізняють кримінологічні, криміналістичні, адміністративні обліки.

Інформаційна підсистема «Оперативно-довідкова картотека» («ОДК») єдиної інформаційної системи МВС України. ІП «ОДК» містить відомості стосовно осіб, яким повідомлено про підозру в учиненні кримінального правопорушення, та осіб, яких засуджено за вчинення кримінального правопорушення.

Персонально-довідковий облік – це систематизований банк (база) даних ІП «ОДК» єдиної інформаційної системи МВС України стосовно осіб, яким повідомлено про підозру в учиненні кримінального правопорушення, та осіб, яких засуджено за вчинення кримінального правопорушення.

До складу ІП «ОДК» входять підсистеми «Мігрант», яка призначена для обліку осіб, затриманих за порушення законодавства України про державний кордон та про правовий статус іноземців, та «Рубін-2002», яка реалізує технологію віддаленого оперативного доступу до банків даних з метою введення інформації та перевірки вимог на судимості.

ІП «ОДК» містить обліки оперативно-довідкової картотеки та дактилоскопічні обліки ДІТ та ДНДЕКЦ МВС і забезпечує:

зберігання, накопичення, введення, облік та видачу в установленому порядку органам НПУ, СБУ, прокуратурі, судам та іншим правоохоронним органам оперативно-довідкової інформації на осіб (зокрема й іноземців та осіб без громадянства), які вчинили злочини на території України, були заарештовані, засуджені, затримані за бродяжництво, уникають слідства та суду; ідентифікацію осіб, які приховують свої біографічні дані від правоохоронних органів; пошук злочинців за слідами, виявленими на місці злочину.

Підставою перевірки осіб за персонально-довідковим обліком є проведення слідчих (розшукових) дій та НСРД у межах досудового розслідування та проведення оперативно-розшукових заходів за ОРС в порядку, визначеному кримінальним процесуальним законодавством та законодавством про ОРД.

У вимозі на перевірку зазначається:

– підстава перевірки (із зазначенням номера кримінального провадження або ОРС);

– установчі дані особи, яка перевіряється;

– прізвище, ініціали та посада ініціатора звернення;

– найменування та місцезнаходження органу ініціатора звернення.

Вимога формується окремо на кожну особу, яка перевіряється за персонально-довідковим обліком.

Вимоги подаються до підрозділів інформаційної підтримки НПУ. Їхнє засекречування здійснюється у випадках, коли це зумовлено службовою необхідністю з дотриманням вимог законодавства про захист інформації.

У підрозділі інформаційної підтримки НПУ вимоги вносяться з робочих місць віддаленого доступу до електронної форми запиту для надсилання на перевірку за персонально-довідковим обліком.

Надання відомостей з персонально-довідкового обліку на електронний запит здійснюється ДІТ у строк до 10 робочих днів, за винятком виконання вимог щодо осіб, стосовно яких вирішується питання про обрання запобіжного заходу – тримання під вартою, що виконуються протягом доби.

Інформаційна підсистема «ITT custody records» у складі Інформаційного порталу Національної поліції України. ІП «ITT custody records» забезпечує відстеження порядку тримання осіб в ізоляторах тимчасового тримання ГУНП для здійснення оперативного реагування на випадки порушення їх прав і законних інтересів, протиправних дій працівників поліції стосовно них, а також формування та ведення статистичних даних.

Завдання ІП «ITT custody records»:

– відстеження порядку тримання та переміщення осіб, утримуваних в ІТТ та забезпечення оперативного реагування на випадки порушень їхніх прав і законних інтересів;

– здійснення інформаційно-пошукових заходів, підготовки аналітично-довідкових матеріалів;

– автоматизація процесу обліку осіб, утримуваних в ІТТ та формування статистичних даних;

– наскрізний контроль (підрозділ контролю, територіальний орган поліції, безпосередній виконавець) за дотриманням прав і законних інтересів осіб під час їх поміщення, тримання та звільнення з ІТТ, своєчасним введенням інформації та її достовірності.

Національна автоматизована інформаційна система Єдиного державного реєстру Міністерства внутрішніх справ стосовно зареєстрованих транспортних засобів та їх власників («НАІС ЄДР МВС»). НАІС ЄДР МВС призначена для отримання інформації про зареєстровані транспортні засоби та їх власників.

Органи та підрозділи Національної поліції здійснюють пошук у Реєстрі відомостей про зареєстровані транспортні засоби та їхніх власників відповідно до Порядку ведення Реєстру, щонайменше за одним з таких критеріїв:

– прізвище, ім'я, по батькові (за наявності) власника та дата його народження;

– реєстраційний номер облікової картки платника податків або серія та номер паспорта власника (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідному контролюючому

органу і мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта);

– повне найменування юридичної особи;

– ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України (код згідно з ЄДРПОУ);

– номерний знак запитуваного транспортного засобу.

Крім зазначених, також можуть застосовуватися інші критерії пошуку, відповідно до повноважень користувача, визначених законом[17].

Автоматизована інформаційно-пошукова система відеофіксації транспортних засобів з розпізнаванням номерних знаків та перевіркою їх за розшуковими реєстрами «ВІДЕОКОНТРОЛЬ-Рубіж». Комплекс «ВІДЕОКОНТРОЛЬ-Рубіж» – це система цілодобового автоматизованого моніторингу руху автотранспорту із одночасною можливістю здійснювати перевірки за наявними базами обліку МВС.

Криміналістичні обліки МВС України. Обліки складаються з оперативно-пошукових та інформаційно-довідкових колекцій. В експертно-криміналістичних підрозділах ведуться ручні або автоматизовані картотеки: фотознімків (колекцій) відбитків пальців рук, слідів взуття, транспортних засобів, знарядь учинення злочинів, мікрочасток, вилучених з місць подій; гільз, куль, набоїв, підроблених грошових знаків, документів, медичних рецептів на наркотичні та сильнодіючі лікарські препарати тощо.

Оперативно-пошукові колекції призначені для отримання інформації про особу, яка причетна до вчинення злочину; ідентифікації особи, знаряддя злочину (транспортного засобу, зброї, обладнання тощо, які використовувалися під час учинення злочину); установлення спільної родової (групової) належності матеріалів та речовин; інших фактичних даних, які свідчать про вчинення злочинів конкретною особою; отримання іншої інформації щодо вчинених злочинів та запобігання їм.

---

[17] Деякі питання надання інформації про зареєстровані транспортні засоби та їх власників: Постанова Кабінету Міністрів України від 25 березня 2016 р. № 260 // Урядовий кур'єр від 7 квітня 2016 р. № 66.

Колекції формуються з об'єктів (їх копій, зображень) та (або) відомостей про них, вилучених або отриманих під час огляду місця події, проведення інших слідчих дій, оперативно-розшукових заходів тощо, а також отриманих під час криміналістичної реєстрації дактилокарт, фото- та відеозображень, записів голосів і мовлення осіб, ДНК-профілів.

Інформаційно-довідкові колекції призначені для використання об'єктів, уміщених до них, під час проведення експертних досліджень, створення науково-дослідних та дослідно-конструкторських розробок, оновлення методичної та нормативної бази судової експертизи, підготовки орієнтовної інформації, узагальнення відомостей про причини й умови вчинення злочинів та інших правопорушень з метою запобігання їм.

Колекції формуються з об'єктів, що становлять інтерес для оперативно-службової, науково-дослідної та методичної діяльності, є речовими доказами у кримінальних справах (кримінальних провадженнях), за якими закрито провадження і щодо яких є рішення суду про їх уміщення до колекцій, а також об'єктів, отриманих від установ, організацій, підприємств незалежно від форми власності.

Національна поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади за обов'язковим дотриманням Закону України «Про захист персональних даних», зокрема:

1) *Державної прикордонної служби* (Інтегрована міжвідомча автоматизована система обміну інформацією з питань контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон «Аркан») щодо:

– громадян України, іноземців та осіб без громадянства, зареєстрованих у пунктах пропуску через державний кордон;

– осіб, затриманих за порушення вимог законодавства про державний кордон;

– осіб, яким заборонено в'їзд в Україну;

– іноземців та осіб без громадянства, зокрема й тих, яким оформлено посвідку на постійне проживання в Україні;

– транспортних засобів, що перетнули державний кордон;

– документів, що дають право на в'їзд до та виїзд з України;

2) *Державної міграційної служби* щодо:

– реєстрації місця проживання або місця перебування особи;

– документів, що посвідчують особу, підтверджують громадянство України або спеціальний статус особи;

– імміграції в Україну;

– осіб, які отримали або претендували на отримання статусу біженця чи особи, яка потребує додаткового захисту, осіб, які набули (припинили) громадянство України, та осіб, яким надано (скасовано) дозвіл на імміграцію в Україну.

Організація доступу до інформаційних ресурсів МВС, ДМС та Держприкордонслужби визначається Порядком організації доступу до інформаційних ресурсів під час інформаційної взаємодії між Міністерством внутрішніх справ України, Державною міграційною службою України та Державною прикордонною службою України, затвердженим наказом МВС від 26 вересня 2013 р. № 920, зареєстрованим у Міністерстві юстиції України 16 жовтня 2013 р. за № 1771/24303.

Органи Національної поліції відповідно до покладених на них завдань та повноважень, передбачених законом, в обсягах і порядку, встановлених законодавством та підзаконними міжвідомчими нормативно-правовими актами МВС України та держателів відповідних реєстрів, можуть використовувати інформацію:

– Державного реєстру фізичних осіб-платників податків;

– Єдиного державного реєстру нормативно-правових актів;

– Єдиного реєстру громадських формувань;

– Єдиного державного демографічного реєстру;

– Державного реєстру актів цивільного стану громадян;

– Єдиного реєстру нотаріусів;

– Єдиного реєстру довіреностей;

– Державного реєстру обтяжень рухомого майна;

– Єдиного державного реєстру юридичних осіб та фізичних осіб - підприємців;

– Єдиного державного реєстру осіб, які вчинили корупційні правопорушення;

– Єдиного реєстру підприємств, щодо яких порушено провадження у справі про банкрутство;

– Єдиного державного реєстру виконавчих проваджень;
– Державного реєстру речових прав на нерухоме майно;
– Єдиного реєстру досудових розслідувань;
– Державного реєстру друкованих засобів масової інформації та інформаційних агентств як суб'єктів інформаційної діяльності;
– Єдиного державного реєстру судових рішень;
– Єдиного державного реєстру підприємств та організацій України;
– Державного реєстру виборців;
– Реєстру позичальників;
– Реєстру документів дозвільного характеру;
– Єдиного ліцензійного реєстру;
– Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування.

Інформаційні ресурси Інтерполу. Використання банків даних Інтерполу є однією із форм міжнародного поліцейського співробітництва. Банки даних Генерального секретаріату Інтерполу створені з метою забезпечення всебічної взаємодії правоохоронних органів держав-членів Інтерполу.

Формування банків даних Інтерполу здійснюється за рахунок інформації, яку надають правоохоронні органи держав-членів Інтерполу на добровільних засадах. Право власності на цю інформацію належить лише тим державам, які її надали.

У Генеральному секретаріаті Інтерполу створені та функціонують такі банки даних:

1. Банк даних «Особи» (ASF Nominal database) – містить інформацію про осіб, які розшукуються за вчинення злочинів, безвісно відсутніх, осіб, які підлягають ідентифікації, зокрема невпізнані трупи та ін.

Крім того, Генеральний секретаріат за допомогою системи I-24/7 надає доступ до банку даних циркулярних повідомлень Інтерполу.

Циркулярні повідомлення Інтерполу (картки Інтерполу) запроваджені у 1946 році з метою організації міжнародного розшуку злочинців, осіб зниклих безвісти, ідентифікації невпізнаних трупів тощо.

Картки (циркулярні повідомлення) поділяються на такі категорії:

«розшукується» («червоні картки» або «повідомлення з червоним кутом») – виставляються на злочинців, які підлягають арешту з подальшою видачею країні-ініціатору розшуку. Ці повідомлення містять повний текст ордеру (санкції) на арешт і детальний опис вчиненого злочину;

«встановлення місцезнаходження» («блакитні картки») – виставляються для збору інформації про зазначену в них особу, а саме про її місцеперебування тощо;

«попередження» («зелені картки») – інформують про «професійних» злочинців, які діють на території декількох країн;

«невпізнаний труп» («чорні картки») – містять детальний опис знайдених трупів, а також відбитки пальців, у разі їх наявності;

«зниклий безвісти» («жовті картки») – містять інформацію про осіб, зниклих безвісти.

У зазначеному банку даних міститься інформація про усі зазначені циркулярні повідомлення в електронному вигляді.

Крім того, система I-24/7 надає можливість безпосередньо в режимі реального часу формувати та надсилати запит про розповсюдження циркулярних повідомлень.

2. Банк даних викрадених транспортних засобів (ASF Stolen vehicles database) – містить інформацію про транспортні засоби, викрадені на території держав-членів Інтерполу.

3. Банк даних викрадених/втрачених документів (ASF Stolen/Lost Travel Documents and Stolen Administrative Blank Documents Database) – містить інформацію про викрадені/втрачені ідентифікаційні документи, а також викрадені/втрачені бланки адміністративних документів.

4. Банк даних викрадених творів мистецтва (ASF Stolen Works of Art) – містить інформацію про твори мистецтва, предмети антикваріату, інші культурні цінності, викрадені на території держав-членів Інтерполу.

5. Банк даних ДНК-профілів (DNA Profiles Database) – містить інформацію про ДНК, вилучені з місць вчинення злочинів на території держав-членів Інтерполу та від злочинців.

6. Банк даних відбитків пальців рук (Fingerprints Database) – містить відбитки пальців рук, вилучені з місць вчинення злочинів на території держав-членів Інтерполу та від злочинців.

7. Банк даних порнографічних зображень, створених із залученням неповнолітніх (INTERPOL Child Abuse Image Database), дає змогу ідентифікувати зображення порнографічного характеру за «авторством» та місцем розміщення в мережі Інтернет.

8. Банк даних підроблених платіжних карток (Counterfeit Payment Cards Database) – містить зображення підроблених платіжних карток та їх елементів (лицьової та зворотної сторін, емблем, голограм, підписів власників тощо) та іншу релевантну інформацію щодо підроблення платіжних карток.

Отримання інформації або перевірка тих чи інших відомостей за банками даних Інтерполу здійснюється:

– *безпосередньо*, в режимі on-line – через телекомунікаційну систему Інтерполу I-24/7 (банки даних щодо осіб, транспортних засобів, документів, творів мистецтва);

– *шляхом надсилання запиту* до Генерального секретаріату Інтерполу (банки даних ДНК, порнографічних зображень, відбитків пальців).

Для забезпечення цільового використання правоохоронними органами держав-членів банків даних Інтерполу, їх функціонування організовано так, що країна-власник інформації щодо об'єкта, розміщеного в банку даних Інтерполу, автоматично отримує повідомлення про факт перевірки цього об'єкта іншою державою (відповідно національним центральним бюро Інтерполу, певним правоохоронним органом тощо). Отримання такого повідомлення для країни-власника інформації є підставою звернутись до країни, що перевіряла об'єкт в банку даних, для з'ясування підстав проведення відповідної перевірки, запитування відомостей про місцезнаходження об'єкта тощо.

Використання можливостей НЦБ Інтерполу для отримання інформації з банків даних Генерального секретаріату Інтерполу здійснюється згідно з Інструкцією про порядок використання правоохоронними органами можливостей НЦБ Інтерполу в Україні у попередженні, розкритті та розслідування злочинів, затвердженою наказом МВС, ГПУ, СБУ, Держкомітету

у справах охорони державного кордону, Держмитслужби, ДПА від 9 січня 1997 р. № 3/1/2/5/2/2.

Перевірка інформації за банками даних Генерального секретаріату Інтерполу здійснюється на підставі запиту правоохоронного органу України, надісланого до НЦБ Інтерполу в порядку, передбаченому зазначеною Інструкцією.

Підставою для спрямування такого запиту можуть бути матеріали кримінального провадження, оперативно-розшукова справа, матеріали перевірки тощо.

Зазвичай перевірки здійснюються за банками даних розшукуваних осіб та викрадених транспортних засобів.

Більшість перевірок за банком даних розшукуваних осіб здійснюється згідно з Порядком провадження за заявами про надання дозволу на імміграцію і поданнями про його скасування та виконання прийнятих рішень, затвердженого постановою Кабінету Міністрів України від 26 грудня 2002 р. № 1983.

Інформація банку даних Генерального секретаріату Інтерполу викрадених транспортних засобів міститься у відповідних автоматизованих інформаційно-пошукових системах МВС України.

Перевірки за вказаним банком даних через НЦБ Інтерполу зазвичай здійснюються територіальними органами поліції під час проведення перевірок за фактами виявлення розшукуваних автомобілів у порядку, передбаченому Інструкцією про порядок здійснення підрозділами Державтоінспекції МВС державної реєстрації, перереєстрації та обліку транспортних засобів, оформлення і видачі реєстраційних документів, номерних знаків на них, затвердженої наказом МВС від 11 серпня 2010 р. № 379 (із змінами).

4.4. Організація інформаційної взаємодії оперативних підрозділів та обміну оперативно-розшуковою інформацією

В умовах протидії організованій, міжрегіональній злочинності особливої актуальності набувають питання інформаційної взаємодії оперативних підрозділів з іншими підрозділами Національної поліції, правоохоронними органами України

і міжнародними правоохоронними органами, державними установами та організаціями, недержавними установами і підприємствами, а також організації обміну оперативно-розшуковою інформацією.

Питання інформаційної взаємодії та координації діяльності оперативних підрозділів виконує важливу роль насамперед у випадках, коли злочинність має різнобічний характер, глибоко законспірована, а їй протистоїть діяльність розгалуженої мережі правоохоронних органів, що потребує впорядкування, взаємозв'язку, узгодженості дій, відповідної підпорядкованості та маневру силами і засобами.

У Великому тлумачному словнику сучасної української мови термін «взаємодія» тлумачиться як взаємний зв'язок між предметами у дії, а також погоджена дія між ким-, чим-небудь.

Взаємодія підрозділів у сфері інформаційно-аналітичної роботи в ОРД – це заснована на законах та підзаконних нормативних актах, погоджена за цілями, місцем і часом та належно організована діяльність суб'єктів інформаційно-аналітичної роботи щодо обміну або надання оперативно-розшукової інформації.

Взаємодія поділяється на внутрішню і зовнішню. Одна передбачає співпрацю з іншими підрозділами Національної поліції, інша – взаємодію з державними органами, підприємствами, установами, іншими правоохоронними органами, населенням тощо.

Головну роль у внутрішній взаємодії виконують оперативні підрозділи Національної поліції, оскільки саме вони отримують і передають один одному значну частину первинної оперативно-розшукової інформації.

Відповідно до вимог нормативно-правових актів попередження, виявлення і припинення злочинів досягається шляхом поєднання зусиль усіх органів і підрозділів Національної поліції, забезпечення належного рівня їх взаємодії, отримання, збирання, накопичення та використання інформації про осіб, причетних до їх учинення, а також події і факти, які можуть сприяти попередженню та виявленню злочинів, що є невід'ємним завданням для всіх працівників поліції.

Оперативні підрозділи забезпечують збирання, накопичення, систематизацію отриманої інформації та здійснюють її перевірку з метою встановлення осіб, причетних до вчинення злочинів, а також подій і фактів, які можуть сприяти їх розкриттю.

Порядок інформаційної взаємодії органів і підрозділів Національної поліції у попередженні, виявленні та розслідуванні кримінальних правопорушень регламентується нормативно-правовими актами МВС, зокрема:

– Інструкцією з організації взаємодії органів досудового розслідування з іншими органами та підрозділами внутрішніх справ, затвердженою наказом МВС від 14 серпня 2012 р. № 700 (зі змінами);

– Інструкцією про порядок ведення єдиного обліку в органах поліції заяв і повідомлень про вчинені кримінальні правопорушення та інші події, затвердженою наказом МВС від 6 листопада 2015 р. № 1377, зареєстрованого в Міністерстві юстиції України 1 грудня 2015 р. за № 1498/27943;

– Інструкцією з організації функціонування криміналістичних обліків експертної служби МВС України, затвердженою наказом МВС від 10 вересня 2009 р. № 390, зареєстрованим у Міністерстві юстиції України 15 жовтня 2009 р. за № 963/16979.

Окрім інформаційної взаємодії оперативних підрозділів між собою та з іншими підрозділами Національної поліції, успішній організації ОРД сприяє належна організація інформаційної взаємодії з іншими правоохоронними органами, серед яких: прокуратура, СБУ, НАБУ, держприкордонслужба, органи фіскальної служби, кримінально-виконавча служба тощо.

Наразі немає єдиної інформаційної системи правоохоронних органів та відповідного порядку обміну інформацією. Зазначені питання регламентуються зазвичай спільними нормативно-правовими актами, зокрема:

– Інструкцією про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, затвердженою наказом ГПУ, МВС, СБУ, Адміністрації Держприкордонслужби, Мінфіна, Мін'юста від 16 листопада 2012 р. № 114/1042/516/1199/936/1687/5;

– Інструкцією про взаємодію правоохоронних органів у сфері боротьби з організованою злочинністю, затвердженою наказом МВС та СБУ від 10 червня 2011 р. № 317/235, зареєстрованим у Міністерстві юстиції України 7 липня 2011 р. за № 822/19560;

– Інструкцією про порядок взаємного використання систем відеоспостереження Служби безпеки України, Управління державної охорони України, Міністерства внутрішніх справ України та Національної поліції України, затвердженою наказом СБУ, УДО, МВС від 12 вересня 2016 р. № 475/265/917;

– Інструкцією про порядок організації обміну інформацією між структурними підрозділами Міністерства внутрішніх справ України, Служби безпеки України, Державної податкової адміністрації України, Державної прикордонної служби України, Державної митної служби України в діяльності з виявлення та припинення корупційних діянь в правоохоронних органах, затвердженою наказом МВС, СБУ, ДПА, Адміністрації Держприкордонслужби, Держмитслужби України від 23 березня 2009 р. № 124/936/139/199/250, зареєстрованим у Міністерстві юстиції України 22 липня 2009 р. за № 670/16686.

Інформаційний взаємообмін АІС між правоохоронними органами України здійснюється відповідно до:

– Порядку організації доступу до інформаційних ресурсів під час інформаційної взаємодії між Міністерством внутрішніх справ України, Державною міграційною службою України та Державною прикордонною службою України, затвердженого наказом МВС від 26 вересня 2013 ро. № 920, зареєстрованого в Міністерстві юстиції України 16 жовтня 2013 р. за № 1771/24303;

– Інструкції про порядок формування, ведення та використання оперативно-довідкового та дактилоскопічного обліку в органах внутрішніх справ та органах (установах) кримінально-виконавчої системи України, затвердженої наказом МВС та ДДУПВП від 23 серпня 2002 р. № 823/188;

– Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон, затвердженого наказом Адміністрації Держприкордонслужби,

Держмитслужби, ДПА, МВС, МЗС, Мінпраці, СБУ, СЗР від 3 квітня 2008 р. № 284/287/214/150/64/175/266/75;

– Інструкції про Порядок взаємодії Генеральної прокуратури України та Міністерства внутрішніх справ України щодо обміну інформацією з Єдиного реєстру досудових розслідувань та інформаційних систем органів внутрішніх справ, затвердженої наказом ГПУ та МВС від 7 листопада 2012 р. № 115/1046;

– Порядку доступу до відомостей персонально-довідкового обліку єдиної інформаційної системи Міністерства внутрішніх справ України, затвердженого наказом МВС від 29 листопада 2016 р. № 1256, зареєстрованого в Міністерстві юстиції України 10 січня 2017 р. за № 22/29890;

– спільного Наказу Мін'юсту та МВС від 8 жовтня 2012 р. № 1480/22030 «Про організацію роботи щодо інформаційної взаємодії Міністерства юстиції України, Міністерства внутрішніх справ України та Державної виконавчої служби України».

Організація інформаційної взаємодії МВС з іншими правоохоронними органами України стосовно розшуку осіб, які переховуються від слідства та суду, регламентується спільними наказами МВС та ДПА від 1 вересня 1999 р. № 658/475, СБУ та МВС від 3 травня 2012 р. № 169/391.

Відповідно до Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» підрозділи органів Національної поліції взаємодіють на безоплатній основі з інформаційно-довідковими службами Державної служби статистики, Генеральної прокуратури, Міністерства юстиції, Верховного Суду України, Державної фіскальної служби України, банківських, фінансових та інших органів і установ, а також одержують від них всю інформацію про реальні вияви організованої злочинної діяльності. Порядок збирання, накопичення, опрацювання та надання такої інформації регламентується положеннями про ці органи та установи, відповідними законодавчими актами.

Розділ 5 зазначеного Закону містить низку важливих норм, які регламентують інформаційну взаємодію органів прокуратури, Національної поліції, Служби безпеки України у сфері боротьби з організованою злочинністю. Пп. 3–6 ст. 16

Закону визначають умови, за яких здійснюється обмін і передача оперативної інформації, документів і матеріалів, які стосуються боротьби з організованою злочинністю.

Ст. 18 цього Закону встановлює обов'язки державних органів, що мають контрольні повноваження, здійснення яких може оптимізувати спільні зусилля відомств у сфері боротьби з організованою злочинністю.

У випадках, коли серед учасників злочинних угруповань є громадяни іноземних держав або суб'єкт злочину, учиненого на території України, перебуває за її межами, або є достовірні дані про виїзд розшукуваних осіб за кордон, а також під час розшуку злочинців чи проведення інших ОРЗ, виникає потреба звертатися за допомогою до міжнародних правоохоронних організацій, зокрема НЦБ Інтерполу в Україні.

Відповідно до ст. 5-1 Закону про ОРД та згідно з Інструкцією про порядок використання правоохоронними органами можливостей НЦБ Інтерполу в Україні у попередженні, розкритті та розслідуванні злочинів, затвердженої наказом МВС, ГПУ, СБУ, Держприкордонслужби, Держмитслужби, ДПА від 9 січня 1997 р. № 3/1/2/5/2/2, Робочий апарат Укрбюро Інтерполу забезпечує співробітництво правоохоронних органів України та зарубіжних країн і надає можливості для обміну оперативно-розшуковою, оперативно-довідковою та криміналістичною інформацією про підготовку і вчинення злочинів та причетних до них осіб, а також архівною та, в окремих випадках, процесуальною інформацією.

Відповідно до ст. 19-1 Закону України «Про Національне антикорупційне бюро України» з метою забезпечення взаємодії НАБУ з органами Національної поліції, СБУ та іншими правоохоронними органами у штатних розписах центральних апаратів зазначених органів передбачаються посади осіб, до функціональних обов'язків яких входить здійснення взаємодії з НАБУ.

Обмін оперативною інформацією між НАБУ та органами Національної поліції, СБУ, іншими правоохоронними органами щодо спільних заходів здійснюється за письмовим розпорядженням керівників відповідних підрозділів.

Умови і порядок обміну інформацією між НАБУ та органами Національної поліції, СБУ, органами, уповноваженими законом

на проведення досудового розслідування, регулюються спільним нормативно-правовим актом НАБУ та відповідних органів.

Найактуальнішим положенням для розвитку інформаційно-аналітичного забезпечення правоохоронних органів є положення про створення загальнодержавних інформаційних систем, упровадження національних стандартів з питань криптографічного захисту інформації та створення інформаційно-аналітичної системи правоохоронних органів.

Указом Президента України від 31 січня 2006 р. № 80 передбачено створення Єдиної комп'ютерної інформаційної системи правоохоронних органів з питань боротьби зі злочинністю (ЄКІСПО) з участю РНБО, СБУ, МВС, Держприкордонслужби, Держмитслужби, ДПА та ГПУ.

Створення інтегрованої міжвідомчої інформаційно-телекомунікаційної системи правоохоронних органів має сприяти реалізації державної політики з питань боротьби зі злочинністю, а саме:

– забезпечити створення умов для поліпшення координації організаційних, профілактичних, оперативно-розшукових заходів;

– підвищити ефективність інформаційно-аналітичного забезпечення правоохоронної діяльності за рахунок удосконалення інформаційної взаємодії шляхом використання сучасних захищених інформаційно-телекомунікаційних систем і проведення стандартизованих (уніфікованих) процедур обміну інформацією.

Загальним недоліком інформаційних систем правоохоронних органів є вузьковідомчий характер накопичення і отримування інформації, відсутність можливості отримання та об'єднання у стислі терміни інформації з різних відомчих джерел, неможливість у більшості випадків її комплексного отримання в режимі «on-line» з інформаційних баз даних різних державних і недержавних структур.

Створення інтегрованої міжвідомчої інформаційно-телекомунікаційної системи має передбачати не фактичне об'єднання існуючих відомчих інформаційних ресурсів, а бути пов'язаним з переходом на принципово новий рівень

інформаційно-аналітичного забезпечення правоохоронних органів, що усуне існуючі негативні фактори низької ефективності інформаційної взаємодії. Єдина система повинна мати такі ознаки: інтегровані бази даних, в яких концентрується інформація про правопорушників, правопорушення тощо; комплексність інформаційного обслуговування всіх правоохоронних органів у режимі електронної телекомунікації в умовах реального масштабу часу. Можливість спільного використання інформаційних ресурсів, зокрема й інформації з обмеженим доступом, потребує чіткого нормативно-правового визначення процедури отримання інформації.

Формування інтегрованої бази даних правоохоронних органів України надасть змогу зробити значний крок до усунення міжвідомчого та внутрівідомчого розмежування, підвищити ефективність розкриття та розслідування злочинів, особливо таких, що мають міжрегіональні та міжнародні ознаки, а також учинених організованими злочинними угрупованнями. Однією з найбільш перспективних систем у цьому контексті є геоінформаційна, яка становить ефективний інструментарій для аналізу взаємодії об'єктів та пов'язаних з ними подій у рамках визначених територіальних меж і часових інтервалів.

В Україні вже є приклади створення об'єднаних інформаційних систем, зокрема: щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон; у сфері запобігання та протидії легалізації (відмивання) доходів, одержаних злочинним шляхом, і фінансування тероризму.

Отже, пріоритетними напрямами розвитку взаємодії оперативних підрозділів під час здійснення інформаційно-аналітичної роботи в ОРД на сучасному етапі є:

– подальше вдосконалення нормативного регулювання питань взаємодії оперативних підрозділів;

– створення єдиної інформаційно-аналітичної системи правоохоронних органів з питань боротьби зі злочинністю;

– забезпечення оперативного доступу до інформаційних систем правоохоронних органів та надійного захисту інформації в АІПС;

– удосконалення системи підготовки фахівців-аналітиків;

– спільне видання й обмін спеціальною науковою та навчально-методичною літературою;

– узагальнення і впровадження позитивного досвіду спільної роботи.

4.5. Конфлікти у сфері інформаційно-аналітичного забезпечення оперативно-розшукової діяльності

Оперативно-розшукова діяльність – як система гласних і негласних пошукових, розвідувальних та контррозвідувальних заходів, спрямованих на захист громадян, суспільства і держави від злочинних посягань, а також як функціональна структура, що складається із суб'єктів ОРД, об'єктів ОРД, заходів, засобів і методів ОРД, – визначають конфліктну сутність цієї діяльності. Особливо це визначається на рівні оперативно-тактичного забезпечення окремих заходів ОРД, для яких характерні міжособистісні конфлікти різної тривалості й гостроти, джерелами яких є не лише звичайні суперечності, а нерідко й відкрите протиборство між оперативними працівниками й злочинцями[18].

Термін *«конфлікт»* походить від латинського слова *«konflictus»* (зіткнення), що визначає протиборство сторін, сил, думок, ідей тощо. У повсякденному спілкуванні термін «конфлікт» застосовується щодо широкого кола явищ – від збройних сутичок і протистояння різних соціальних груп до службових чи сімейних суперечок, до проблем кожної особистості, які супроводжують її протягом усього життя.

Конфлікти є у всіх галузях суспільного життя, зокрема й в галузі права. У таких випадках ми маємо справу із правовим або юридичним конфліктом. *Юридичний конфлікт* – це різновид соціального конфлікту, під яким розуміють протиборство

---

[18] Психологія оперативного спілкування в діяльності оперативних підрозділів органів внутрішніх справ: навч.-практ. посібник / Б. І. Бараненко, В. А. Глазков, О. С. Звонок та ін.; за ред. Е. О. Дідоренка; МВС України, Луган. держ. ун-т внутр. справ. – Луганськ: РВВ ЛДУВС, 2007. – С. 85.

двох або декількох суб'єктів, обумовлене протилежністю (несумісністю) їх інтересів, потреб, систем цінностей або знань[19].

Уникнути конфліктів в інформаційно-аналітичній роботі в ОРД та їхніх наслідків, інколи негативних, доволі складно, тому й виникає потреба вивчення їх сутності, причин, меж, динаміки, досвіду вирішення, прогнозування та запобігання. Зважаючи на те, що інформаційний конфлікт є не, як формою соціального конфлікту, джерела конфліктів в інформаційно-аналітичній роботі необхідно шукати в соціальних конфліктах.

До головних причин, що викликають конфлікти в інформаційній сфері, науковці відносять прагнення до отримання певної свободи в інформаційному («віртуальному») просторі без урахування розбіжностей індивідуальної та суспільної моралі, життєвих цінностей, суперечності між очікуваннями, практичними намірами і вчинками осіб, нерозуміння людьми своїх дій стосовно один одного, усілякі непорозуміння, логічні помилки та семантичні труднощі в процесі комунікації, недоліки і «неякісність» інформації тощо[20].

Завдяки своєму міжгалузевому характеру, інформаційні конфлікти, як правило, пов'язані з різними галузями законодавства – адміністративним, цивільним, трудовим, сімейним, фінансовим, кримінальним, кримінально-процесуальним чи виправно-трудовим правом.

За правовими нормами інформаційні конфлікти можуть мати й забороняючий, і зобов'язуючий чи уповноважуючий характер. Зокрема порушення забороняючої норми призводить до інформаційного конфлікту держави в особі правоохоронних органів з фізичною або юридичною особою, що скоїли правопорушення, і навпаки. У разі порушення зобов'язувальних норм можливий інформаційний конфлікт між державою (в особі правоохоронних органів) і зобов'язаною особою, причому і зобов'язана особа має виконувати норму, і працівник

---

[19] Гуменюк Л. Й. Соціальна конфліктологія: навч. Посібник / Л. Й. Гуменюк. – Львів: Львівський державний університет внутрішніх справ, 2013. – С. 226.

[20] Боер В. М. Информационное право: учеб. пособие / В. М. Боер, О. Г. Павельева. – СПб., 2006. – Ч. 1: ГУАП. – С. 83–84.

правоохоронного органу повинен вимагати від цієї особи її виконання, а якщо ні, то він сам вступає в конфлікт із державою. Порушення уповноважуючої норми призводить до конфлікту між уповноваженим суб'єктом правоохоронного органу та приватною особою, інформаційні права якої можуть бути порушені діями першого. Зокрема такі інформаційно-правові конфлікти виникають через зловживання посадовими особами правоохоронних органів своїми службовими обов'язками та можливостями, наприклад, щодо обігу публічної або приватної інформації[21].

За територіальними ознаками інформаційні конфлікти можуть мати внутрішньогруповий, внутрішньодержавний або міжнародний характер.

Зважаючи на те, що діяльність правоохоронних органів не застрахована від помилок, некомпетентності, відсутності спеціальних знань та навичок, перевищення службових повноважень, можуть виникнути інформаційно-правові конфлікти не тільки між особою (фізичною чи юридичною) та правоохоронними органами, а й між окремими правоохоронними та правозастосовними органами, наприклад, між органами адвокатури та слідства, між органами прокуратури та адвокатури, між структурними підрозділами окремого правоохоронного органу тощо.

Конфліктні ситуації, що виникають в інформаційній сфері, обумовлені, насамперед, різним сприйняттям людьми ситуації, що склалася, інтерпретацією намірів і поводження, ухвалення відповідних рішень, а інколи «віртуальним» характером виникаючих правовідносин. По-перше, виникненню конфліктної ситуації в сфері інформаційних відносин передує настання загрози для досягнення обраної мети хоча б одному з учасників взаємодії; по-друге, будь-якому конфліктові передує спірна ситуація.

Конфліктна ситуація в інформаційній сфері також визначається об'єктивними обставинами і може бути створена

---

[21] Бєляков К. І. Інформаційний конфлікт та юридична відповідальність: сутність і співвідношення / К. І. Бєляков // Правова інформатика. – 2013. – № 2 (38). – С. 40.

навмисно однією зі сторін для досягнення певної мети у майбутньому (можливо, з метою скоєння правопорушення)[22].

У визначенні меж конфлікту виділяють три аспекти: просторовий, часовий та внутрішньосистемний.

Просторові межі визначають територію, на якій відбувається конфлікт. Вони можуть бути і мінімальними, і глобальними. Просторові межі інформаційного конфлікту мають значення для вибору адекватної форми впливу з метою врегулювання внутрішньогрупового, внутрішньодержавного або міжнародного конфлікту.

Часові межі інформаційного конфлікту визначають його тривалість у часі (початок, розвиток, загасання та закінчення), що має значення для кваліфікації дій учасників конфлікту та вирішення питання про юридичну відповідальність. Важливість їх виявлення визначається експертною оцінкою дій учасників конфлікту в певний момент часу, роллю і відповідальністю осіб, що приєдналися до конфлікту на різних його етапах.

Початок конфлікту визначається об'єктивними (зовнішніми) актами поведінки, спрямованими проти іншого учасника конфлікту, за умов, що останній усвідомлює ці акти як спрямовані проти нього та їм протидіє.

Прикладом виникнення та розростання конфліктів можуть слугувати так звані чати або соціальні мережі в Інтернеті, які найчастіше мають віртуальний характер.

Закінчення конфлікту – це процес припинення всіх активних дій протиборчих сторін, незалежно від причини початку конфлікту. Воно може виявлятися в різних формах: конфлікт може бути вичерпаний (наприклад, за примиренням сторін), а може припинитися через вихід однієї зі сторін із боротьби. Можливою формою припинення конфлікту є втручання третьої сили.

Внутрішньосистемні межі визначаються тим, що майже будь-який конфлікт відбувається у певній обумовленій системі,

---

[22] Бєляков К. І. Інформаційний конфлікт та юридична відповідальність: сутність і співвідношення / К. І. Бєляков // Правова інформатика. – 2013. – № 2 (38). – С. 40.

чи то сім'я, група співробітників, держава тощо. Конфлікт між сторонами, що входять до однієї системи, може бути більш глибоким, широким або частковим, обмеженим.

Визначення таких меж дає змогу, по можливості, чітко визначити кількість і ступінь залучення людей у конфлікт. Розширення цієї межі вказує на ускладнення структури конфлікту та необхідність пошуку інших способів вирішення конфлікту. Так само знання їх необхідне для впливу на реалізацію процесів щодо попередження конфліктів.

Крім безпосередньо протидіючих сторін учасниками конфлікту можуть бути і такі особи, як підбурювачі, підсобники, свідки, які самі в ньому не задіяні, а також радники, прихильники і противники тих чи інших суб'єктів, що конфліктують між собою. Усі ці особи (організації) є елементами системи. Межі системи залежать від того, наскільки широке коло учасників буде до нього включено[23].

За соціологічною класифікацією суб'єкти інформаційного конфлікту поділяються на три рівні: *індивіди, соціальні групи, держави (народи).* Із правових позицій виділяються дві групи суб'єктів: фізичні та юридичні особи.

Саме на зазначених етапах та їх межах, як правило, виникають проблеми правового регулювання завдяки їх можливої невизначеності, що є характерною особливістю конфліктів в інформаційній сфері. Науковці справедливо наголошують, що розвиток сучасних інформаційних технологій призводить до шумового забруднення інформаційного простору. Водночас таке забруднення відбувається не лише внаслідок постійного збільшення кількості інформації. Наріжною проблемою інформаційного суспільства є інформація протиправного змісту, зокрема: порнографічна; що ганьбить честь і гідність особи; розпалює міжнаціональну ворожнечу; містить заклики до екстремізму, сепаратизму, тероризму тощо[24].

---

[23] Конфліктологія: навч. посібник / Л. М. Герасіна, М. П. Требін, В. Д. Воднік та ін. – Х.: Право, 2012. – С. 22–24.

[24] Золотар О. О. Про поняття «інформаційний шум» у правовідносинах / О. О. Золотар // Інформація і право. – 2012. – № 1 (4). – С. 71.

Якщо йдеться про протиборство юридичних осіб, то конфлікт обов'язково набуває юридичного характеру, тому що між цими суб'єктами складаються (або вже існують) правові відносини; крім того, вирішити такий конфлікт найвірогідніше можна лише шляхом застосування правових норм.

Для інформаційної сфери більш характерними є ситуації, коли конфлікт розгортається між фізичними особами, які, будучи громадянами, зазвичай є суб'єктами певних правовідносин. Це накладає помітний відбиток на їхню поведінку в конфлікті.

Учасник конфлікту, що перебуває в тих або інших правових відносинах, повинен порівнювати свою поведінку з існуючими нормами права, пам'ятати, що певний розвиток подій може становити оперативний інтерес для правоохоронних органів. Суб'єкт конфлікту згодом може стати учасником цивільного, адміністративного або кримінального процесу як позивач, відповідач, потерпілий, підозрюваний, обвинувачений або свідок. Така перспектива загрожує багатьом суб'єктам інформаційних конфліктів й може призвести до юридичної відповідальності. У деяких випадках юридичний аспект конфлікту залишається вибірковим, тобто стосується не всіх, а лише окремих його учасників.

Розглядаючи *причини інформаційних конфліктів*, потрібно зазначити, що деякі з них зумовлені особливими, специфічними мотивами, однак є й загальні, характерні для всіх різновидів, зокрема:

– *ціннісні (морально-етичні)* причини, які обумовлені особистісними системами переконань, принципів поводження, цілей, бажань тощо;

– *структурні (управлінські)* причини, до яких належать взаємозалежність діяльності, неправильний розподіл відповідальності, недосконалість структур і норм управління, недостатня узгодженість прав і функцій;

– *комунікативні причини*, які включають поведінку суб'єктів, що не відповідає очікуванням оточуючих осіб;

– *суб'єктивні причини*, які обумовлені обмеженістю кола осіб, що мають законні права доступу до інформаційних ресурсів чи технологій.

Зазначені причини зумовлюють так звані «інформаційні правопорушення» – крайню форму конфліктної ситуації, що утворюються в різних сегментах інформаційної діяльності та виникаючих правовідносинах, які полягають у певних діях її суб'єктів[25].

Як відомо, обіг інформації складається з певних етапів, зокрема: створення, зберігання, поширення, споживання та знищення. У процесі створення інформаційних ресурсів конфлікти виникають завдяки володінню інформаційними ресурсами об'єктом (носієм) інформації, а саме: в момент виникнення права власності на інформаційний продукт, під час визначення кола суб'єктів такої власності чи під час забезпечення правового захисту конфіденційної інформації, права на таємницю, а також забезпечення реалізації конституційного права на інформацію інших осіб. Зазначені причини можуть розглядатися як привід для виникнення конфліктів і на етапах зберігання та знищення інформації.

До конфліктів на етапі створення інформаційних ресурсів належать ситуації, які визначаються як «інформаційні нормативно-правові» (юридичні помилки, колізії правових норм), спричинені в процесі нормотворення недосконалістю текстів законодавчих актів щодо регулювання інформаційних відносин та юридичної техніки їх застосування.

На стадії поширення інформації виникають певні інформаційні причинні бар'єри (технологічні і психологічні), що зумовлюють інформаційно-правові конфлікти.

Конфлікти під час споживання інформаційних ресурсів можуть виникати як наслідок відсутності потреби в окремих з них, перспективи їх подальшого використання, що, своєю чергою, викликає певні проблеми правових можливостей[26].

Сутність інформаційного конфлікту полягає в тому, що це найбільш гострий спосіб вирішення суперечностей в інтере-

---

[25] Бєляков К. І. Інформаційний конфлікт та юридична відповідальність: сутність і співвідношення / К. І. Бєляков // Правова інформатика. – 2013. – № 2 (38). – С. 44.

[26] Там само. – С. 45.

сах, цілях, поглядах, що виникають в інформаційній сфері та в процесі соціальної комунікації, протидії суб'єктів інформаційних відносин, порушенні їх прав та обов'язків, у процесі обігу та захисту інформаційних ресурсів, як правило, супроводжується використанням інформаційних технологій та виходить за межі моралі, соціальних правил і правових норм, створюючи протиправну ситуацію – інформаційне правопорушення.

Розвиток конфліктної ситуації до фази порушення норм чинного законодавства чи міжнародно-правових актів, призводить до скоєння протиправних суспільно небезпечних діянь (дій або бездіяльності) – правопорушення, як крайньої форми інформаційного конфлікту, подальшого проведення передбачених законом процесуальних дій і притягнення винних до юридичної відповідальності.

В інформаційно-правовій конфліктології поняття *«інформаційне правопорушення»* визначається як конфліктна ситуація, що склалася внаслідок протиправних суспільно небезпечних діянь (дій або бездіяльності) суб'єкта інформаційної сфери, пов'язаних з негативними наслідками впливу інформації, використанням інформаційних технологій, порушенням інформаційних прав і свобод людини, що несуть за собою юридичну відповідальність у вигляді санкцій, передбачених чинним законодавством та нормами міжнародного права[27].

У сфері інформаційно-аналітичного забезпечення ОРД виокремлюються три основні аспекти конфліктів:

1) *нормативно-правові* (прогалини та суперечності на рівні законодавчих, відомчих нормативних актів);

2) *організаційно-управлінські суперечності*;

3) *конфлікти на організаційно-тактичному рівні* отримання та використання оперативно-розшукової інформації.

Нормативно-правові аспекти інформаційних конфліктів. Науковці виокремлюють *інформаційні нормативно-правові конфлікти*, що виникають через суперечливість норм

---

[27] Бєляков К. І. Інформаційний конфлікт та юридична відповідальність: сутність і співвідношення / К. І. Бєляков // Правова інформатика. – 2013. – № 2 (38). – С. 45.

права та становлять окремий різновид інформаційних конфліктів – конфліктні ситуації, в яких безпосередніх учасників взагалі немає, а сам конфлікт відбувається на рівні нормативних визначень, зумовлених недосконалістю текстів законодавчих актів щодо регулювання інформаційних відносин та юридичної техніки їх застосування. Якщо соціальна значущість текстуальної офіційної норми права нижче, то вона або не одержує правового значення, або з часом перестає функціонувати і застосовуватися та втрачає правовий характер. Вирішення текстуальних інформаційних конфліктів у законодавстві можливе і за допомогою правових процедур, і через соціальний вибір між двома конкуруючими текстами, що стає справою часу[28].

Вирізняються суперечності між двома або кількома нормативними актами, між нормами права та правозастосовною практикою, суперечності між декількома правозастосовними актами, розбіжності в розумінні правових норм. Деякі правові акти можна тлумачити неоднозначно, що спричиняє протиріччя в правозастосовній діяльності різних гілок влади та призводить до правових колізій.

Організаційно-управлінські суперечності інформаційних конфліктів

Впровадження автоматизованих інформаційно-аналітичних систем у діяльність правоохоронних органів створює реальні умови для вдосконалення ОРД. Однак невідповідність здійснюваних аналітичних досліджень, форм і методів оперативної роботи вимогам сьогодення та їх неадекватність сучасним суспільним відносинам, розвитку злочинних угруповань та їх проникненню в соціально-економічні й адміністративно-правові сфери діяльності зумовлює необхідність подальшого реформування інформаційно-аналітичної роботи в оперативних підрозділах Національної поліції.

---

[28] Бєляков К. І. Інформаційний конфлікт та юридична відповідальність: сутність і співвідношення / К. І. Бєляков // Правова інформатика. – 2013. – № 2 (38). – С. 41.

Відсутність єдиного інформаційно-аналітичного середовища зумовлює неналежний рівень інформаційно-аналітичного забезпечення діяльності органів Національної поліції.

Національна поліція потребує створення на базі єдиного інформаційного поля підрозділів поліції із залученням інформаційних ресурсів інших органів державної влади та управління повного розвідувально-аналітичного циклу з метою ефективної обробки здобутої оперативним шляхом інформації, удосконалення якості наявних та отримання нових знань, необхідних для ухвалення оптимальних управлінських рішень.

Якість систематизованої інформації визначається низкою вимог, що висуваються до оперативно-розшукової інформації, а саме:

1) *оптимальність, повнота*. У практиці ОРД не визначено єдиних критеріїв повноти з багатьох питань, віднесених до компетенції Національної поліції (зокрема: підстави постановки громадян на різні види обліку; межі вивчення осіб, які перебувають на тому чи іншому обліку; набору відомостей, необхідних для визначення моменту оперативно-розшукового та профілактичного втручання тощо), що спричиняє певні складнощі у забезпеченні цієї вимоги;

2) *точність інформації*, яка пов'язана з достовірністю, об'єктивно правильним відображенням подій, явищ, стану об'єкта, середовища, що його оточує;

3) *лаконічність повідомлень* при максимальному навантаженні, яка підвищує їх насиченість, скорочує час на передачу та сприйняття інформації. Утім, лаконічність не повинна досягатися за рахунок повноти, достовірності та деталізації;

4) *логічність викладення* передбачає послідовність, доведеність, переконливість, відсутність непотрібних деталей, пропорційність місця, відведеного в повідомленні того чи іншого питання, значущість цього питання, зрозумілість мети, досягненню якої має слугувати повідомлення, однозначність інформації, яка повинна зберігати свій зміст, сенс та форми вираження для того, щоб вона однаково розумілася всіма працівниками оперативних підрозділів;

5) *цінність (корисність)* оперативно-розшукової інформації, яка вимірюється за допомогою її кількості, тобто,

згідно зі статистичною теорією, інформацію несе лише те повідомлення, яке зменшує, знімає наявну непевність.

Для багатьох органів Національної поліції типовою є несистемність, а звідси і надмірність інформації, яку неможливо обробити. Надходячи до оперативних працівників, вона часто недооцінюється ними з погляду потреб інших оперативних підрозділів і навіть інших співробітників у власному підрозділі. Несвоєчасне передання зацікавленим адресатам корисної інформації знижує значущість повноти та достовірності, оскільки вона втрачає актуальність.

Між повнотою і оперативністю інформації існує об'єктивна суперечність. Що повнішою є інформація, то більше часу та зусиль необхідно витратити на її отримання, обробку та аналіз, що знижує ступінь оперативності. Одним із головних шляхів вирішення цієї проблеми є вдосконалення інформаційно-аналітичної роботи, зокрема, техніки та технології обробки інформації, а також професійної підготовки працівників.

В умовах глобальної інформатизації суспільства вкрай актуальною є проблема ідентифікації особи в мережі Інтернет. Багато інтернет-сайтів для зручності користувачів використовують систему ідентифікації за допомогою процедур «реєстрація/авторизація». Проблема використання подібного механізму ідентифікації користувача полягає в тому, що інформація про користувача надається лише ним самим, не проходячи процедури верифікації. У більшості випадків користувачі в мережі Інтернет використовують псевдоніми (нікнейми).

Водночас потреба суспільства у підвищенні достовірності інформації вимагає розроблення механізмів ідентифікації користувачів у мережі. У реальному житті ми легко можемо отримати інформацію про особу, з якою маємо справу: при особистому спілкуванні ми можемо скласти уявлення про людину за зовнішнім виглядом, за необхідності можемо вимагати чи попросити надати необхідні документи, які містять перевірену інформацію. У мережі Інтернет таких можливостей у більшості випадків немає.

Одним із шляхів вирішення цієї проблеми є пропозиція запровадити так звані цифрові ідентифікатори, які мають містити відомості про утримувача ідентифікатора (для фізичної

особи: прізвище, ім'я, по батькові, стать, вік; для юридичної особи: повна назва, код ЄДРПОУ) у зашифрованому вигляді.

Утім, спроби встановити контроль за мережею Інтернет викликають численні протести в суспільстві. Зокрема у березні 2011 р. у Франції державним офіційним друкованим органом «Журналь оффіс'єль» опубліковано постанову, згідно з якою інтернет-компанії зобов'язані надавати правоохоронним органам інформацію про номери телефонів, домашню та електронну адреси інтернет-користувачів, їх псевдоніми і паролі, відстежувати режим роботи користувачів в Інтернеті – її початок і завершення, участь у блогах, розміщення тих чи інших коментарів із зазначенням точного часу. Крім того, компанії зобов'язані відстежувати дії користувачів, якщо ті, приміром, міняють паролі, переходячи з одного поштового сервера на інший, або з яких-небудь причин відбувається втрата шуканої інформації[29].

Прийняття зазначеної постанови викликало хвилю критики в країні, зокрема, її скасування зажадала Французька асоціація громадських інтернет-послуг ASIC. Що стосується приватного життя французьких громадян, вони вважають, що постанова, яка була розроблена як засіб боротьби з терористичною загрозою, має надмірно широкий характер.

Постановою Уряду Російської Федерації від 31 липня 2014 р. № 758 внесено зміни до низки правових актів з питання впорядкування обміну інформацією з використанням інформаційно-телекомунікаційних мереж, зокрема, обов'язкова ідентифікація користувачів проводиться операторами зв'язку у трьох випадках:

1) при наданні універсальних послуг зв'язку щодо передачі даних та надання доступу до мережі Інтернет з використанням колективного доступу;

---

[29] Васев А. В. Информационно-правовое обеспечение, как одно из приоритетных направлений деятельности правоохранительных органов на современном этапе / А. В. Васев // Информатизация и информационная безопасность правоохранительных органов: матеріали XXI Всерос. науч. конф., 30–31 мая 2012 г.: сб. тр. – М.: Акад. управления МВД России, 2012. – 356 с.

2) при укладанні строкового договору про надання разових послуг з передачі даних у пунктах колективного доступу;

3) при укладанні строкового договору про надання разових телематичних послуг зв'язку в пунктах колективного доступу[30].

Водночас ідентифікація користувача повинна здійснюватися оператором зв'язку шляхом встановлення прізвища, імені, по батькові (за наявності) користувача, які підтверджуються документом, що засвідчує особу. Зазначена постанова викликала багато суперечок у ЗМІ, а її положення трактувалися як заборона на анонімне використання Wi-Fi.

Масові протести в суспільстві викликало прийняття Верховною Радою Закону України від 16 січня 2014 р. № 721-VII «Про внесення змін до Закону України «Про судоустрій і статус суддів» та процесуальних законів про додаткові заходи захисту безпеки громадян», яким, зокрема, дозволялося приймати рішення про обмеження доступу абонентів операторів телекомунікацій до ресурсів мережі Інтернет, через які здійснюється розповсюдження інформації, поширення якої суперечить закону, або через які здійснюється діяльність інформаційного агентства без передбаченого законом свідоцтва про державну реєстрацію інформаційного агентства[31].

Конфлікти на організаційно-тактичному рівні отримання та використання оперативно-розшукової інформації. Інформаційно-аналітична робота в ОРД зазвичай передує ухваленню рішень, висуненню версій, плануванню

---

[30] О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и в отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей»: Постановление Правительства Российской Федерации от 31.07.2014 № 758 [Электронный ресурс]. – Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201408050024? index=1&rangeSize=1.

[31] Про внесення змін до Закону України «Про судоустрій і статус суддів» та процесуальних законів про додаткові заходи захисту безпеки громадян: Закон України від 16 січня 2014 р. № 721-VII // Відомості Верховної Ради України. – 2014. – № 22. – С. 1906. – Ст. 801.

роботи. Тобто ретельний аналіз сприяє висуненню найбільш вірогідних версій і плануванню роботи щодо їх відпрацювання, дозволяє обирати шляхи отримання достовірної, повноцінної інформації. Проте ґрунтовний аналіз неможливо здійснити без необхідної інформації. Така інформація залежно від ситуації може бути отримана з матеріалів кримінальних проваджень та ОРС, архівних справ, а також із АІС оперативно-розшукового призначення та інших АІС, незалежно від їх прямого призначення та відомчої належності, мережі Інтернет, операторів мобільного зв'язку.

Результати загального аналізу оперативної обстановки дають змогу, зокрема, розкрити й оцінити загальний стан злочинності, її структуру й динаміку, у тому числі рівень поширеності тих чи інших видів злочинів, зіставити виявлені тенденції з об'єктивними змінами соціального середовища на різних мікро- й макрорівнях тощо. Разом це створює інформаційно-аналітичні передумови для розроблення перспективних (річних, п'ятирічних) планів протидії злочинності, зміцнення оперативних позицій у певних регіонах, економічних зонах тощо.

Нині правоохоронні органи для аналізу оперативної обстановки щораз ширше використовують можливості комп'ютерної техніки. Безумовно, саме впровадження автоматизованих інформаційно-аналітичних систем у діяльність правоохоронних органів створює реальні умови для вдосконалення ОРД.

Застосування сучасних комп'ютерних технологій дозволяє не тільки накопичувати й аналізувати оперативну, статистичну інформацію, але й безпосередньо здобувати її за допомогою електронних засобів, а також моделювати і прогнозувати розвиток ситуації

На цьому етапі характерною є така ознака, як *інформаційна невизначеність*, на виникнення якої впливають такі об'єктивні фактори, як суперечливість інформації, недостатність (дефіцит) інформації, неможливість отримання більш повної інформації, а також суб'єктивні – ненадійність джерел інформації, з яких її було отримано, недостатність можливостей оперативних джерел для перевірки інформації, недостатній досвід роботи та низький професіоналізм працівників оперативних підрозділів тощо.

Інформаційна невизначеність суттєво ускладнює пізнання всіх обставин (умов) проведення оперативно-розшукових заходів і визначення спроможності оперативного підрозділу досягти бажаних результатів. Тому на етапі проведення аналізу використовується увесь спектр засобів і методів ОРД, методів формальної та математичної логіки, теорії інформації, теорії ймовірності, логіко-математичного моделювання тощо[32].

Важливим принципом отримання й використання оперативно-розшукової інформації є принцип *інформаційної достатності*. Його вимоги, що полягають у повноті й оптимальності інформації, повинні враховуватись і на організаційно-управлінському, і на організаційно-тактичному рівнях здійснення ОРД. Водночас зазначимо, що у практиці ОРД ще не вироблено єдиних критеріїв достатності інформації, у тому числі для ухвалення рішень про застосування тих чи інших оперативно-розшукових заходів, засобів і методів, поставлення оперативних контингентів на різні види обліку тощо.

Говорячи про отримання оперативними підрозділами тактичних відомостей, слід зауважити, що традиційні способи збирання їх негласними джерелами наштовхуються на досить дієві контрзаходи з боку об'єктів ОРД. У сучасному злочинному середовищі це помітно виявляється в посиленні консолідації кримінальних елементів і конспірації їхньої злочинної діяльності, у підвищенні рівня поінформованості про методи ОРД тощо, а також у здійсненні цілеспрямованих організаційних заходів щодо протидії витоку інформації зі свого середовища.

В інформаційному конфлікті оперативно-розшуковим заходам оперативних підрозділів протиставляються відповідні контрзаходи злочинців, їх підсобників та заінтересованих осіб. Значення інформаційного конфлікту очевидне, оскільки саме поінформованість щодо рішень і конкретних дій протиборчої сторони обумовлює ефективність ОРД. Це визначає

---

[32] Психологія безпеки професійної діяльності в системі МВС України: навч.-практ. пос. / Б. І. Бараненко, Д. О. Бабічев, В. О. Криволапчук та ін.; за ред. Б. І. Бараненка, О. В. Шаповалова; МВС України, ДНДІ МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. – Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. – С. 120–121.

необхідність збирання оперативними підрозділами максимальної інформації про об'єкт оперативної розробки і водночас захисту себе від аналогічних дій у відповідь. Для подолання інформаційного конфлікту слід брати до уваги такі обставини: забезпечувати конспіративність, розподіляти інформацію між виконавцями для збереження загального змісту інформації від можливого витоку, використовувати лише перевірені канали зв'язку, запобігати можливості «зняття» інформації сторонніми особами за допомогою технічних засобів, використовувати технічні засоби збирання інформації та аналітичної розвідки, здійснювати заходи для дезінформації противника, перевіряти будь-яку інформацію, що надходить, проводити контррозвідувальні заходи з приводу можливих витоків інформації через корумпованих посадових осіб тощо[33].

Основні суперечності під час здійснення попереднього аналізу оперативної обстановки. Першим етапом попереднього аналізу оперативної обстановки є *інтерпретація інформації*, під якою мається на увазі виявлення справжнього значення тієї чи іншої інформації. Насамперед це стосується вербальної інформації, тому що почасти те чи інше висловлювання неправильно трактується. Це відбувається у випадках, коли фраза вирвана з контексту або неправильно зрозуміла іноземна мова, інтонація, жести, сленг тощо. У разі виникнення такої ситуації на допомогу працівникам інформаційно-аналітичного підрозділу доцільно запросити досвідченого фахівця, який зможе правильно інтерпретувати те чи інше повідомлення.

Мова, що використовується для опису інформації, може допускати неоднозначність її розуміння. Це створює певні труднощі при інтерпретації вербальної інформації, але в цьому випадку істинний сенс можна зрозуміти з контексту. Інформація, яка зберігається в комп'ютерних базах даних, як правило, позбавлена контексту, тому помилкова інтерпретація стає набагато ймовірнішою.

---

[33] Міжнародна поліцейська енциклопедія: у 10 т. / відп. ред. В. В. Коваленко, Є. М. Моісеєв, В. Я. Тацій, Ю. С. Шемшученко. – К.: Атіка, 2010. – Т. VI. Оперативно-розшукова діяльність поліції (міліції). – 1128 с. – С. 399.

Вся інформація поділяється на факти, особисті думки й аналітично оброблені дані. Змішування або неправильне визначення цих різних за своєю суттю видів інформації може призводити до помилок в інтерпретації і, як наслідок, до ухвалення неправильних рішень. Отже, процес інтерпретації потребує максимальної обережності та ретельності.

Виділення сторонньої інформації. Надлишок інформації, так само як і її недостатність (дефіцит), становлять серйозні проблеми і ускладнюють проведення інформаційно-аналітичної роботи. Тактика виділення декількох ключових деталей набагато ефективніша, ніж розподіл між багатьма розрізненими даними. Крім того, працівники інформаційно-аналітичних підрозділів можуть прагнути зберегти інформацію, яка не відноситься безпосередньо до справи, з надією, що вона може стати в нагоді в майбутньому. Така інформація має заноситись в банк даних так, щоб згодом її можна було легко знайти. Зі створенням такого інформаційного банку та його постійним поповненням завдання пошуку і збору вихідної інформації для аналізу буде значно полегшене. Проте надлишок інформації є серйозною проблемою, тому що значно уповільнює ведення інформаційно-аналітичної роботи, старіння і знецінення інформації при цьому відбувається дуже швидко. Крім того, надлишок сторонньої інформації є для керівника оперативного підрозділу сигналом того, що пошук і збір інформації організовані неефективно.

Оцінка інформації. Під оцінкою інформації розуміється метод ранжирування джерел інформації, самої інформації і способів її отримання.

Оцінка джерела здійснюється за такими критеріями:

- надійне джерело;
- зазвичай надійне джерело;
- доволі надійне джерело;
- не завжди надійне джерело;
- ненадійне джерело;
- джерело невстановленої надійності.

Оцінка інформації здійснюється за такими критеріями:

- підтверджена іншими фактами;
- ймовірно правдива;

– можливо правдива;
– сумнівна;
– неправдоподібна;
– достовірність не піддається визначенню.

Оцінка способу отримання інформації джерелом здійснюється за такими критеріями:

– отримав інформацію сам (сам бачив, сам чув тощо);
– отримав інформацію через постійне джерело (через негласного працівника, відкриті джерела тощо);
– отримав інформацію через разове джерело (випадково підслухана розмова, чутки тощо)[34].

На етапі оцінки інформації необхідно встановити, наскільки інформація може відповідати істині. Водночас потрібно враховувати, що можна отримати інформацію, яка не відповідає істині, таких типів:

– дезінформацію, доведену до відома джерела;
– навмисно або ненавмисно спотворену джерелом;
– довільно або мимоволі змінену в ході передачі.

При навмисній дезінформації застосовується явна брехня, напівправда, а також правдиві відомості, які в цьому контексті підштовхнуть осіб, які сприймають інформацію, до помилкових висновків.

Спотворення, що виникає в процесі передання вихідних даних, може відбуватися з багатьох причин:

– передання тільки частини повідомлення;
– переказ почутого своїми словами;
– факти, спотворені чиїмось суб'єктивним сприйняттям.

Для своєчасного виявлення спотвореної інформації, а також для успішної боротьби з ймовірною дезінформацією необхідно розрізняти факти і думки, враховувати суб'єктивні характеристики джерела і його передбачуване ставлення до наданого повідомлення. Слід чітко усвідомлювати, чи здатне джерело за своїм становищем мати доступ до повідомлених фактів. Для підстрахування необхідно мати дублюючі джерела інформації, використовувати дублюючі канали зв'язку і намагатися виключати всі зайві проміжні ланки передання

---

[34] Учебник по информационно-аналитической работе / И. Н. Кузнецов. – М., ООО Изд. Яуза, 2001. – 100 с.

інформації. Крім того, необхідно пам'ятати, що особливо легко сприймається та дезінформація, яка добре відповідає прийнятій раніше версії, тобто та, яку припускають або бажають отримати.

Наступним етапом є побудова попередніх версій, що пояснюють місце основних отриманих фактів у ланцюзі подій. Першим кроком є складання переліку відомостей, готових для аналізу. Це необхідно для подальшого ранжирування їх за ступенем важливості, крім того, це є певною гарантією того, що про відомості не забудуть. Отримані відомості повинні бути чітко класифіковані за ступенем достовірності джерела, самих відомостей і способу їх отримання. У переліку відомостей, готових для аналізу, найбільш важливі відомості спеціально позначаються. Матеріали з позначками «джерело невстановленої надійності» і «достовірність не піддається визначенню» не беруть участі в аналізі без крайньої необхідності.

Потім необхідно виявити всі можливі гіпотези, які можуть пояснювати головні події, і, розташувавши їх за ступенем ймовірності, по черзі перевіряти на збіг з усіма даними. Якщо виявлено значну розбіжність будь-якої попередньої гіпотези з отриманими відомостями, причому останні мають досить високі оцінки достовірності, то слід переходити до наступної гіпотези. На цьому етапі виникає одна з найсерйозніших проблем аналітичної роботи – суперечності у відомостях. Для її подолання необхідно порівняти оцінки інформації і джерела, дати отримання сумнівних відомостей. Вирішальне ж значення має інтуїція, знання і досвід самого співробітника інформаційно-аналітичного підрозділу.

Визначення потреби в додатковій уточнюючій інформації. Необхідно чітко розрізняти поняття «неповна інформація» і «прогалини в інформації». *Неповна інформація* означає відсутність відомостей, які не мають особливої важливості, що є природним, оскільки ніколи не можна отримати абсолютно всі відомості. А надто, така інформація була б надмірною і ускладнила б аналіз.

Прогалини в інформації означають відсутність відомостей, що є ключовими у цій ситуації або необхідними для усунення суперечностей. Такі відомості вкрай важливі для проведення аналізу.

Виявивши прогалини в інформації, потрібно визначити їх важливість для подальшого аналізу. Не можна до нескінченності відкладати складання аналітичного звіту під приводом того, що в інформації виявлено прогалини. На певному етапі слід визнати, що для вирішення завдання зібрано достатньо даних. Співробітники інформаційно-аналітичного підрозділу повинні прагнути до вирішення обраного завдання наявними засобами і в розумні терміни[35].

На основі виконання попередніх етапів приступають до *підготовки аналітичних звітів* з певного питання оперативно-розшукової діяльності, вироблення конкретних висновків і пропозицій. Підготовка звітів є основним обов'язком працівника інформаційно-аналітичного підрозділу, а готовий звіт є результатом функціонування системи інформаційно-аналітичної роботи в ОРД.

Підсумок інформаційно-аналітичної роботи залежить від:

– достовірності первинної інформації;

– якості вихідної інформації;

– кваліфікації оперативних працівників та фахівців-аналітиків;

– адекватності заходів, що застосовуються для протидії злочинності;

– своєчасності й ефективності ухвалених управлінських рішень.

У практичній діяльності оперативних підрозділів використовуються такі основні види аналізу оперативної обстановки та результатів оперативно-службової діяльності в боротьбі зі злочинністю:

– поточний (за добу, тиждень, місяць);

– за звітний період (квартал, півріччя, дев'ять місяців, рік);

– позачерговий;

– проблемний.

---

[35] Кузнецов И. Н. Информация: сбор, защита, анализ. Учебник по информационно-аналитической работе / И. Н. Кузнецов. – М., ООО Изд. Яуза, 2001. – 100 с.

Усі письмові звіти повинні містити глибокий аналіз і бути представлені в регламентованій (типовій, уніфікованій) формі. Споживачами аналітичних звітів є відповідальні за планування та ухвалення рішень посадові особи підрозділів правоохоронних органів, які мають право пред'являти певні вимоги до змісту та оформлення звітів. Аналітичний звіт повинен бути чітко, логічно і грамотно складений. Крім того, звіт повинен абсолютно відповідати місцю співробітника правоохоронного органу – споживача інформації в дозвільній системі доступу до конфіденційної інформації: за ступенем конфіденційності використовуваних в звіті відомостей, профілем професійних знань співробітника і службової необхідності інформації для конкретного напряму оперативно-розшукової діяльності. Потрібно враховувати також і те, що зовнішній вигляд звіту обов'язково буде впливати на сприйняття інформації, яка міститься в ньому.

Отже, результатом аналізу та оцінювання оперативно-розшукової ситуації є визначення можливості ухвалення відповідного рішення, а також важливих інформаційних елементів, що потребують додаткової перевірки та уточнення.

4.6. Організація підготовки фахівців у сфері інформаційно-аналітичної роботи для оперативних підрозділів Національної поліції

Органи і підрозділи Національної поліції в сучасних умовах мають потребу у фахівцях, які здатні забезпечити безпеку особи, суспільства й держави на новому технологічному рівні. Ефективно протидіяти злочинності під силу лише правоохоронцям, які досконало володіють законодавчою базою, мають належний рівень професійної підготовки, достатній досвід боротьби із сучасними видами злочинів.

Для виконання обраних завдань оперативні та інформаційно-аналітичні підрозділи повинні мати не тільки сучасне обладнання та програмне забезпечення, а й належно підготовлених фахівців, які б уміли їх ефективно застосовувати у боротьбі зі злочинністю.

Широке застосування комп'ютерних технологій у злочинній діяльності вимагає якісно нових підходів до підготовки фахівців, зокрема з протидії кіберзлочинності. Така підготовка має передбачати не лише навчання прийомам виявлення, розслідування та припинення комп'ютерних злочинів, але й насамперед озброєння фахівців сучасними знаннями, які дозволяють широко і ефективно застосовувати інформаційні технології на різних напрямах оперативно-розшукової, слідчої та іншої службової діяльності.

Працівники підрозділів кіберполіції мають бути і оперативниками, і фахівцями з комп'ютерної техніки. Крім того, зважаючи на транснаціональний характер кіберзлочинів і специфіку інформаційного середовища в мережі Інтернет, такі фахівці мають вільно володіти іноземними мовами, найперше англійською.

Наявність у професійній діяльності працівників поліції таких чинників сильного впливу, як небезпека, ризик, загроза для життя та здоров'я, вимагає проведення комплексу спеціально організованих заходів, спрямованих на профілактику деформуючих впливів.

Ця проблема потребує системного комплексного вирішення, першочерговими кроками якого має бути:

– підвищення авторитету працівників поліції;
– зміцнення правоохоронних зв'язків з населенням;
– підвищення професіоналізму поліцейських;
– використання засобів психологічної та медичної релаксації для нейтралізації стресових перевантажень;
– упровадження ефективної програми правового виховання населення.

Створення комплексів для комп'ютерної та аналітичної розвідки і оснащення ними інформаційно-аналітичних та оперативних підрозділів Національної поліції вимагає проведення відповідних науково-дослідних робіт, а також підготовки фахівців, які володіють і юридичними, і спеціальними технічними знаннями у сфері інформаційних технологій.

Оскільки інформатизація суспільства є основою виникнення складних високотехнологічних схем злочинної діяльності, надає їй найвищий рівень організованості, висуваються

нові вимоги до рівня кваліфікації кадрів правоохоронних органів, серед яких:

– готовність до постійного підвищення професіоналізму;
– високий рівень інформаційної грамотності;
– уміння використовувати сучасні інформаційні технології в ОРД;
– здатність до налагодження комунікацій;
– знання іноземних мов.

Навички інформаційно-аналітичної роботи потрібні не лише працівникам інформаційно-аналітичних підрозділів, а й усім суб'єктам ОРД, які виконують інформаційно-аналітичну роботу як спеціальну оперативно-розшукову функцію.

Навчальний процес у вищих навчальних закладах із специфічними умовами навчання має гнучко та своєчасно реагувати на зміни в правовому полі. Це вимагає від відомчих навчальних закладів удосконалення змісту та методики навчання, їхнє увідповіднення з реальними умовами і завданнями протидії злочинності.

Підготовка фахівців у сфері інформаційно-аналітичної роботи для оперативних підрозділів поліції може здійснюватись шляхом створення у вищих навчальних закладах із специфічними умовами навчання:

– відповідних спеціалізацій курсантів, у межах яких із юридичними спеціальними дисциплінами поглиблено вивчати спеціальні технічні дисципліни у сфері інформаційних технологій;
– відповідних груп слухачів-правоохоронців, які вже мають вищу технічну або економічну освіту у сфері інформаційних технологій, та поглиблено вивчати з ними спеціальні юридичні дисципліни.

Підготовка фахівців для інформаційно-аналітичних підрозділів та підрозділів кіберполіції може здійснюватись:

– шляхом відбору та прийняття на службу в поліцію досвідчених фахівців у галузі комп'ютерних технологій із цивільних організацій;
– у вищих навчальних закладах із специфічними умовами навчання зі спеціалізацією на старших курсах;

– шляхом перепідготовки випускників ІТ-спеціальностей цивільних ВНЗ на спеціальних курсах у вищих навчальних закладах із специфічними умовами навчання.

Випускник вищого навчального закладу із специфічними умовами навчання має бути максимально теоретично й практично підготовленим до виконання оперативно-службових завдань, уміти професіонально застосовувати отримані знання на практиці. Лише за умови переходу від універсальної підготовки до спеціалізованої вищі навчальні заклади із специфічними умовами навчання зможуть випускати фахівців, здатних забезпечити захист прав і законних інтересів громадян, ефективно боротися зі злочинністю.

Діяльність вищих навчальних закладів зі специфічними умовами навчання має спрямовуватися на підготовку фахівця, який не тільки має певні знання і професійні навички, але й характеризується відповідним рівнем сформованості моральних особистісних якостей, що може бути досягнуто лише шляхом послідовної цілеспрямованої виховної роботи.

Найпершим завданням галузевої освіти стає розроблення сучасних методів навчально-виховної роботи, в яких гармонійно поєднувалися б освоєння інформаційних технологій, формування високих моральних якостей, вироблення імунітету до скоєння правопорушень – «інформаційна культура».

Підготовка майбутніх правоохоронців зумовлює формування у курсантів таких якостей, як організованість, висока моральність, уміння самостійно діяти у складних умовах, що, своєю чергою, вимагає здійснення комплексу виховних заходів на всіх напрямах навчального процесу: у навчально-методичній, індивідуально-виховній роботі, психологічному та інформаційно-пропагандистському забезпеченні, культурній, просвітницькій та соціальній роботі.

Важливе місце займає спеціальна підготовка працівників поліції до дій в екстремальних умовах, і головне, в умовах оперативного ризику. Така підготовка має бути систематичною і проводитись протягом усієї службової діяльності.

Професійна діяльність працівників поліції реалізується в середовищі, яке вважається «зоною підвищеного ризику», що поєднано з реальною небезпекою для їхнього життя

та здоров'я, а також членів їхніх сімей. Існує прямий зв'язок між рівнем готовності працівника поліції до забезпечення особистої безпеки та рівнем набутих професійних знань, умінь і навичок.

Необхідною умовою досягнення високого рівня професіоналізму є формування в працівника поліції позитивної мотивації щодо реалізації себе за обраною професією.

Важливе значення для підготовки фахівців для Національної поліції має набуття практичних умінь з охорони публічного порядку та безпеки під час проходження практики та стажування.

Навички, отримані в патрульній поліції, є основними для всіх напрямів правоохоронної діяльності. Про це свідчить і зарубіжний досвід, коли підготовка офіцерів поліції здійснюється лише після набуття кандидатами практичного досвіду в патрульних підрозділах.

Важливим чинником удосконалення системи підготовки фахівців для інформаційно-аналітичних підрозділів є збільшення практичної складової підготовки курсантів. З цією метою передбачається:

– залучення керівників практичних підрозділів до роботи у складі комісій з оцінки результатів практики і стажування курсантів, участі в роботі Державних екзаменаційних комісій;

– залучення працівників поліції, які прибувають на навчання в системі післядипломної освіти, до проведення навчальних занять з курсантами у формі семінарів, круглих столів за напрямами їхньої діяльності та спеціалізації підготовки;

– проведення бінарних занять, коли заняття з курсантами та слухачами проводить не лише викладач, а й практичний працівник поліції.

У підготовці працівників поліції широко використовуються тренінгові технології, зокрема, мотиваційні тренінгові програми, що є сучасною формою підвищення професійної компетентності, стимулювання діяльності персоналу.

Через упровадження у практичну діяльність Національної поліції автоматизованих інформаційно-пошукових систем особливої актуальності набувають питання підготовки пра-

цівників поліції, насамперед оперативних та інформаційно-аналітичних підрозділів, до роботи з базами даних АІПС, які функціонують у системі МВС.

Визначення раціонального співвідношення прикладних і технічних аспектів викладання для спеціалізованої підготовки фахівців для підрозділів кіберполіції залежить від таких чинників:

– змістовних аспектів кожної дисципліни спеціалізації;
– методики викладання;
– рівня початкової підготовки курсантів, педагогічного і наукового рівня викладацького складу тощо.

Фахівці в галузі інформаційних технологій мають чітко знати напрями пошуку необхідної інформації та способи її інтеграції для вирішення поставлених задач, здобути навички отримання різнорідної інформації із застосуванням сучасних інформаційних технологій.

Головне завдання системи галузевої освіти МВС полягає у перетворенні її на високоефективну мобільну систему, здатну оперативно реагувати на потреби практичних підрозділів щодо підготовки фахівців у сфері інформаційно-аналітичної роботи для оперативних підрозділів, підвищення кваліфікації та перепідготовки працівників поліції, проведення наукових досліджень з актуальних проблем застосування сучасних інформаційних технологій у правоохоронній діяльності.

Питання для самоконтролю

1. Охарактеризуйте поняття та елементи організації ОРД.
2. Назвіть основні елементи організації інформаційно-аналітичної роботи в ОРД.
3. З чого складається організаційна структура інформаційно-аналітичної роботи в оперативних підрозділах Національної поліції?
4. Дайте характеристику системи інформаційно-аналітичного забезпечення Національної поліції.
5. Назвіть основні напрями інформаційно-аналітичної роботи в оперативних підрозділах поліції.
6. Хто є суб'єктами інформаційно-аналітичної роботи в ОРД?

7. Охарактеризуйте основні функції оперативних підрозділів Національної поліції, які регламентують інформаційно-аналітичну роботу в ОРД.

8. Назвіть основні функції режимно-секретних підрозділів щодо інформаційно-аналітичного забезпечення ОРД.

9. Дайте характеристику основних функцій Робочого апарату Укрбюро Інтерполу, які регламентують інформаційно-аналітичну роботу в ОРД.

10. Назвіть бази (банки) даних, що входять до єдиної інформаційної системи МВС, які наповнюються та підтримуються в актуальному стані Національною поліцією.

11. Які інформаційні підсистеми входять до Інтегрованої інформаційно-пошукової системи Національної поліції («ІІПС НП»)?

12. До яких інформаційних ресурсів інших органів державної влади Національна поліція має безпосередній оперативний доступ?

13. Які інформаційні системи використовуються оперативними підрозділами поліції поряд з обліками оперативного призначення?

14. З яких колекцій складаються криміналістичні обліки МВС України?

15. Дайте характеристику інформаційних ресурсів Інтерполу.

16. У чому полягає взаємодія підрозділів Національної поліції у сфері інформаційно-аналітичної роботи в ОРД?

17. Особливості інформаційної взаємодії підрозділів Національної поліції з іншими правоохоронними органами.

18. Для чого необхідне створення інтегрованої бази даних правоохоронних органів України?

19. Загальне поняття конфлікту як соціальної категорії.

20. Нормативно-правові аспекти інформаційних конфліктів.

21. Організаційно-управлінські суперечності інформаційних конфліктів.

22. Конфлікти на організаційно-тактичному рівні отримання та використання інформаційно-аналітичної інформації.

23. Основні етапи аналізу оперативно-розшукової інформації.

24. Основні вимоги до підготовки фахівців для підрозділів інформаційно-анілітичного забезпечення та кіберполіції.

25. Назвіть шляхи підготовки фахівців для підрозділів інформаційно-анілітичного забезпечення та кіберполіції.

ГЛОСАРІЙ

Автоматизоване робоче місце (АРМ) – місце користувача, обладнане персональним комп'ютером з установленим програмним забезпеченням, апаратом телефонного зв'язку, пристроєм відображення відомчого телебачення, пристроєм аудіо- або відеоселекторного зв'язку та підключене до локальної мережі.

Автентифікація – процедура встановлення вірогідності інформації, пред'явленої користувачем у разі звернення його до системи та відкриття йому доступу, якщо він має на це право.

Аналітична розвідка – особлива форма інформаційно-аналітичної роботи в ОРД, яка заснована на органічній єдності всіх форм цієї роботи і полягає у набутті нових знань про об'єкт чи явище на основі аналітичної обробки здобутої оперативно-розшукової інформації про осіб, події, предмети, що становлять оперативний інтерес.

База даних – іменована сукупність даних, що відображає стан об'єктів та їх відношень у визначеній предметній області (Закон України «Про Національну програму інформатизації» від 4 лютого 1998 р. № 74/98-ВР).

Безконтактний електронний носій – імплантована у бланк документа безконтактна інтегральна схема для внесення персональних даних, параметрів, у тому числі біометричних, що дає змогу здійснювати комплекс заходів, пов'язаних з верифікацією особи, та може використовуватися як засіб електронного цифрового підпису у випадках, передбачених законом (Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» від 20 листопада 2012 р. № 5492-VI).

Біометрична ідентифікація – засіб підтвердження особи; належності паспорта його власникові шляхом розпізнавання та зіставлення біометричних даних (кольору очей, малюнка сітківки ока, відбитків пальців, геометрії руки, рис обличчя тощо), що зафіксовані носіями цих даних, з особистими даними власника.

Біометричні дані – сукупність даних про особу, зібраних на основі фіксації її характеристик, що мають достатню стабільність та істотно відрізняються від аналогічних параметрів інших осіб (основні біометричні дані, параметри – відцифрований підпис особи, відцифрований образ обличчя особи, додаткові біометричні дані, параметри – відцифровані відбитки пальців рук) (Закон України «Про Єдиний державний

демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» від 20 листопада 2012 р. № 5492-VI).

Біометричні параметри – вимірювальні фізичні характеристики або особистісні поведінкові риси, що використовуються для ідентифікації (впізнання) особи або верифікації наданої ідентифікаційної інформації про особу (Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» від 20 листопада 2012 р. № 5492-VI).

Верифікація – порівняння даних (параметрів), у тому числі біометричних, для встановлення тотожності особи документам або інформації з Реєстру для підтвердження їх ідентичності (Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» від 20 листопада 2012 р. № 5492-VI).

Дані – інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки (Закон України «Про телекомунікації» від 18 листопада 2003 р. № 1280-IV).

Електронна пошта (E-mail) – ресурси інформаційно-телекомунікаційної мережі, що забезпечують обмін поштовими повідомленнями з будь-яким абонентом цієї мережі.

Електронні (біометричні) проїзні документи – документи, які дають змогу перетинати державний кордон (громадянські, службові та дипломатичні паспорти, візи, посвідчення особи, особи без громадянства, біженця, дозволи на постійне проживання тощо) та до яких вмонтовано безконтактний електронний носій біометричної та іншої інформації – мікрочіп.

Електронні гроші – електронні аналоги грошей, чекових книжок, цінних паперів, які випущені в обіг банком та забезпечені активами банку емітента.

Засоби оперативно-розшукової діяльності – сукупність передбачених чинним законодавством та відомчими нормативними актами спеціальних обліків, що забезпечують накопичення, обробку, зберігання та використання інформації про факти, предмети і осіб, що становлять оперативний інтерес, а також засобів оперативної техніки і службово-розшукового собаківництва, що використовуються оперативними підрозділами для попередження, виявлення і припинення злочинів (проект Закону України «Про оперативно-розшукову діяльність» реєстр. № 4778).

Зняття інформації з електронних інформаційних мереж (систем) без відома їх власника, володільця або утримувача – оперативно-розшуковий захід, що полягає у негласному пошуку,

виявленні шляхом фізичного та/або програмного доступу, відборі та фіксації інформації, що міститься в електронних інформаційних мережах (системах) або їх частинах, доступ до яких обмежується її власником, утримувачем або пов'язаний з подоланням системи логічного захисту (проект Закону України «Про оперативно-розшукову діяльність» реєстр. № 4778).

Зняття інформації з каналів зв'язку – оперативно-розшуковий захід, що полягає в негласному одержанні, фіксації із застосуванням відповідних технічних засобів, зокрема встановлених на транспортних телекомунікаційних мережах, обробці та відтворенні, у тому числі придатних для автоматизованої обробки засобами обчислювальної техніки, різних видів сигналів, які передаються через мережу Інтернет, інші мережі передачі даних, що контролюються (проект Закону України «Про оперативно-розшукову діяльність» реєстр. № 4778).

Зняття інформації з транспортних телекомунікаційних мереж –оперативно-розшуковий захід, що полягає у застосуванні технічного обладнання, яке дає змогу зафіксувати факт контакту у мережі, а також аудіовізуально сприймати, фіксувати та відтворювати інформацію, що передавалася цим каналом зв'язку, зокрема й її зміст (проект Закону України «Про оперативно-розшукову діяльність» реєстр. № 4778).

Ідентифікація – встановлення тотожності об'єктів на підставі тих чи інших ознак.

Ідентифікація особи – встановлення особи шляхом порівняння наданих даних (параметрів), у тому числі біометричних, з наявною інформацією про особу в реєстрах, картотеках, базах даних тощо (Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» від 20 листопада 2012 р. № 5492-VI).

Інтернет – всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та ґрунтується на Інтернет-протоколі, визначеному міжнародними стандартами (Закон України «Про телекомунікації» від 18 листопада 2003 р. № 1280-IV).

Інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів (Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 р. № 80/94-ВР).

Інформаційна технологія – цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації

незалежно від місця їх розташування (Закон України «Про Національну програму інформатизації» від 4 лютого 1998 р. № 74/98-ВР).

Інформаційний продукт (продукція) – документована інформація, яка підготовлена і призначена для задоволення потреб користувачів (Закон України «Про Національну програму інформатизації» від 4 лютого 1998 р. № 74/98-ВР).

Інформаційний ресурс – сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо) (Закон України «Про Національну програму інформатизації» від 4 лютого 1998 р. № 74/98-ВР).

Інформаційно-аналітична робота в ОРД – передбачена законодавством України й урегульована відомчими нормативними актами система заходів, спрямованих на збір, обробку, узагальнення, аналіз, зберігання та використання інформації, у тому числі обмеженого доступу, що має значення для вирішення завдань ОРД, в інтересах кримінального судочинства, безпеки громадян, суспільства і держави.

Інформаційно-аналітична функція – збір, обробка, аналіз і оцінка інформації з метою підвищення ефективності діяльності, яка містить усі дії щодо оперування інформацією.

Інформаційно-аналітичні технології в ОРД – сукупність методів, технологічних процесів і програмно-технічних засобів, інтегрованих з метою збирання, обробки, систематизації, узагальнення, аналізу, зберігання та використання інформації, у тому числі обмеженого доступу, що має значення для вирішення завдань ОРД, в інтересах досудового слідства, безпеки громадян, суспільства і держави.

Інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле (Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 р. № 80/94-ВР).

Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (Закон України «Про інформацію» від 2 жовтня 1992 р. № 2657-XII).

Інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (Закон України «Про захист персональних даних» від 1 червня 2010 р. № 2297-VI).

Кібернетична безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі (проект Закону України «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України» реєстр. № 2483).

Кібернетичний простір (кіберпростір) – середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем (проект Закону України «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України» реєстр. № 2483).

Комп'ютерна інформація – інформація, яка зберігається, обробляється або розповсюджується за допомогою автоматизованих систем, комп'ютерних мереж або мереж зв'язку (Кримінальний кодекс України від 5 квітня 2001 р. № 2341-III).

Комп'ютерна розвідка – оперативно-пошуковий захід, який полягає у цілеспрямованому пошуку та отриманні інформації з комп'ютерних систем та мереж, доступ до яких не обмежується їх власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту, що здійснюється працівниками оперативних та оперативно-технічних підрозділів, з метою виявлення відомостей криміногенного та кримінального характеру.

Контроль за телефонними розмовами – оперативно-розшуковий захід, що полягає в негласному спостереженні, відборі, фіксації, обробці та відтворенні з використанням технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, змісту телефонних розмов, а також інших відомостей та сигналів, які передаються телефонним каналом зв'язку, що контролюється (проект Закону України «Про оперативно-розшукову діяльність» реєстр. № 4778).

Контроль кореспонденції – оперативно-розшуковий захід, що полягає в негласному відборі за ідентифікаційними ознаками кореспонденції, на яку накладено арешт, її обробленні, знятті копій чи отриманні зразків та інформуванні підрозділу-ініціатора для прийняття рішення щодо подальших дій (проект Закону України «Про оперативно-розшукову діяльність» реєстр. № 4778).

Конфіденційна інформація – інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень.

Муляж – імітація статичного біометричного образу, наприклад, виготовлення дубліката папілярного узору пальця.

Наведення довідок – оперативно-розшуковий захід, який спрямований на отримання інформації про фізичних осіб, факти та обставини, що мають значення для вирішення завдань ОРД, шляхом безпосереднього вивчення документів, матеріалів баз даних, направлення запитів на підприємства, в установи та організації, іншим юридичним, а також

фізичним особам, які мають у своєму розпорядженні або можуть володіти зазначеною інформацією.

Накладення арешту на кореспонденцію – затримання установою зв'язку відправлення кореспонденції особи (листів усіх видів, бандеролей, посилок, поштових контейнерів, переказів, телеграм, інших матеріальних носіїв передання інформації між особами) без її відома на підставі ухвали слідчого судді (ст. 261 КПК).

Нормативно-правова основа інформаційно-аналітичної роботи в ОРД – система законодавчих актів, які визначають допустимість цієї роботи, а також підзаконних нормативних актів і правил, які регламентують її порядок і умови.

Обробка інформації в системі – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів (Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 р. № 80/94-ВР).

Оперативна обстановка – сукупність різноманітних явищ і процесів, що органічно пов'язані, постійно змінюються і визначають характер та інтенсивність оперативно-розшукових зусиль органів і підрозділів правоохоронних органів, спрямованих на попередження, припинення, розкриття злочинів, розшук злочинців і безвісти зниклих осіб.

Оперативна установка – оперативно-розшуковий захід, що полягає в діях оперативного працівника, спрямованих на збір інформації про особу, події або факти, які представляють інтерес для правоохоронних органів, шляхом проведення бесід з громадянами або посадовими особами, ознайомлення з документами та наведення довідок із зашифруванням своєї приналежності до оперативних підрозділів правоохоронних органів (проект Закону України «Про оперативно-розшукову діяльність» реєстр. № 4778).

Оперативне опитування – захід, який полягає в одержанні від опитуваної особи інформації, що може мати значення для вирішення завдань оперативно-розшукової діяльності, а також отримання даних від осіб про події та факти, що становлять оперативний інтерес (проект Закону України «Про оперативно-розшукову діяльність» реєстр. № 4778).

Оперативне розпізнання – пізнавальна (емпірична) частина оперативного пошуку – діяльності, спрямованої на виявлення об'єктів, які становлять оперативний інтерес.

Оперативні обліки – система реєстрації, накопичення, класифікації, зберігання та використання даних про осіб, предмети, події за їх

прикметами та ознаками, призначена для ефективного забезпечення оперативно-розшукової діяльності оперативних підрозділів правоохоронних органів, яка складається із автоматизованих інформаційних систем, картотек, оперативно-розшукових справ, справ контрольного-наглядового провадження та інших документів оперативно-розшукового та довідкового призначення.

Оперативно-розшукова діагностика – одна із форм інформаційно-аналітичної роботи в ОРД, спрямована на емпіричне виявлення криміногенних осіб, злочинів та пов'язаних з ними предметів, речовин і документів за заздалегідь відомими загальними ознаками, на підставі оцінки об'єктів, які розпізнаються, а також отримання нових знань про ці об'єкти, з метою припинення правопорушень та в інтересах кримінального судочинства, безпеки громадян, суспільства і держави.

Оперативно-розшукова діяльність – система гласних і негласних пошукових, розвідувальних та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів (Закон України «Про оперативно-розшукову діяльність» від 18 лютого 1992 р. № 2135-XII)

Оперативно-розшукова ідентифікація – одна із форм інформаційно-аналітичної роботи в ОРД, спрямована на встановлення тотожності об'єкта або особи за сукупністю загальних і окремих ознак шляхом порівняльного їх дослідження з використанням сил, засобів і методів ОРД.

Оперативно-розшукова справа – форма концентрації та систематизації матеріалів на особу або групу осіб (у тому числі невстановлених), стосовно яких є достовірні дані про підготовку до вчинення злочину, або осіб, які розшукуються (проект Закону України «Про оперативно-розшукову діяльність» реєстр. № 4778).

Оперативно-розшукове прогнозування – одна із форм інформаційно-аналітичної роботи в ОРД, яка полягає в організації процесу наукового передбачення майбутнього на основі оперативного аналізу минулого та сьогодення на підставі раніше зібраної оперативної інформації.

Оперативно-розшукові заходи – отримання та перевірка оперативної інформації щодо осіб і фактів, які представляють оперативний інтерес; визначення напрямів використання відомостей, отриманих у процесі роботи (проект Закону України «Про оперативно-розшукову діяльність» реєстр. № 4778).

Оперативно-технічні засоби – сукупність різних технічних засобів та науково-обґрунтованих прийомів їх правомірного використання у процесі оперативно-розшукової діяльності (проект Закону України «Про оперативно-розшукову діяльність» реєстр. № 4778).

Оперативно-технічні заходи – система дій підрозділів правоохоронних органів з негласного впровадження і застосування спеціальної техніки для вирішення завдань ОРД.

Організація інформаційно-аналітичної роботи в ОРД – система використання наявних сил, засобів і методів, скерованих на безперервний, цілеспрямований збір, обробку, узагальнення, аналіз, зберігання та використання оперативно-розшукової інформації, що здійснюється інформаційно-аналітичними, оперативно-технічними та оперативними підрозділами правоохоронних органів, з метою вирішення завдань ОРД та досудового розслідування.

Особистий пошук – оперативно-розшуковий захід, що полягає у безпосередньому застосуванні працівником оперативного підрозділу прийомів розпізнання злочинців, негласного спостереження, оперативної установки й агентурної роботи для запобігання та викриття злочинів, розшуку зниклих злочинців і громадян, які пропали безвісти (проект Закону України «Про оперативно-розшукову діяльність» реєстр. № 4778).

Отримання довідково-аналітичної інформації – захід, який полягає у відкритому збиранні інформації, зокрема й за допомогою запитів до підприємств, установ та організацій про осіб, які перевіряються на причетність у сприянні, підготовці, учиненні або участі в учиненні злочину, а також предмети і факти, що становлять оперативний інтерес (проект Закону України «Про оперативно-розшукову діяльність» реєстр. № 4778).

Отримання оперативно-розшукової інформації – одна із форм інформаційно-аналітичної роботи в ОРД, у межах якої відбувається пошук і фіксація відомостей про протиправні діяння окремих осіб та груп, з використанням наявних сил, засобів і методів ОРД, в інтересах оперативно-розшукової діяльності та досудового розслідування.

Пароль – випадкова послідовність символів, яка запам'ятовується користувачем, що становить його таємницю та використовується ним у процесі автентифікації.

Планування – обрання цілей і рішень, необхідних для їх досягнення, заздалегідь ухвалене рішення про те, хто, що, коли і як буде робити, процес підготовки на перспективу рішення про те, що, ким, як і коли має бути виконано.

Поліцейський скринінг – перевірка осіб, аплікантів на акредитацію, за обліками правоохоронних органів.

Правова інформація – будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок,

правопорушення і боротьбу з ними та їх профілактику тощо (Закон України «Про інформацію» від 2 жовтня 1992 р. № 2657-XII).

Приватне спілкування – спілкування, під час якого інформація передається та зберігається за таких фізичних та юридичних умов, за яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб.

Прогнозування – наукове визначення ймовірних шляхів і результатів майбутнього розвитку явищ, процесів і подій (формування злочинних організацій, готування та вчинення злочинів тощо), оцінки показників, що характеризують ці явища та процеси для порівняно віддаленого майбутнього.

Радіотехнічна розвідка – захід, який проводиться оперативно-технічними підрозділами та полягає в установленні постачальників послуг рухомого зв'язку, технічним обладнанням яких охоплюється певна територія або місце (проект Закону України «Про оперативно-розшукову діяльність» реєстр. № 4778).

Сайти знайомств – інтернет-сервери, що надають користувачам Інтернету послуги з віртуального спілкування з іншими користувачами.

Сервери служби Whois – ресурси інформаційно-телекомунікаційної мережі, що містять інформацію про належність певної IP-адреси до конкретного провайдера.

Сервіс IP-телефонії – ресурси, що надають послуги з передавання телефонних розмов абонентів за протоколом IP шляхом застосування інформаційно-телекомунікаційних мереж.

Сервіс YouTube – ресурс інформаційно-телекомунікаційної мережі, який надає послуги відеохостингу користувачам.

Систематизація оперативно-розшукової інформації – одна із форм інформаційно-аналітичної роботи в ОРД, у рамках якої здобуті відомості про протиправні діяння окремих осіб та груп приводяться в систему за допомогою технічних і програмних засобів з метою подальшої їх оцінки, аналізу та використання отриманої інформації в інтересах ОРД та досудового розслідування.

Скринінг **(від англ.** *screening***)** – відбір фактів, явищ із багатьох однорідних, які в процесі дослідження виявляють необхідні, шукані властивості.

Соціальні мережі – ресурси інформаційно-телекомунікаційної мережі, які надають можливість спілкування користувачам зі спорідненими інтересами.

Спеціалізовані розвідувальні програми – прикладні програми, які виконують функції пошуку, отримання або аналізу інформації поза межами оперативних обліків – у корпоративних та банківських мережах, Інтернеті, а також на окремих комп'ютерах.

Телекомунікаційна мережа – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комунікації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних, чи інших електромагнітних системах між кінцевим обладнанням (Закон України «Про телекомунікації» від 18 листопада 2003 р. № 1280-IV).

Телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб (Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 р. № 80/94-ВР).

Транспортна телекомунікаційна мережа – мережа, що забезпечує передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду між підключеними до неї телекомунікаційними мережами доступу (Закон України «Про телекомунікації» від 18 листопада 2003 р. № 1280-IV).

Трафік – сукупність інформаційних сигналів, що передаються за допомогою технічних засобів операторів, провайдерів телекомунікацій за визначений інтервал часу, включаючи інформаційні дані споживача та/або службову інформацію (Закон України «Про телекомунікації» від 18 листопада 2003 р. № 1280-IV).

Установлення місцезнаходження радіоелектронного засобу – оперативно-розшуковий захід, що полягає в негласному застосуванні технічних засобів для локалізації місцезнаходження радіоелектронного засобу, у тому числі ММ; кінцевого обладнання, активованого в мережах операторів рухомого (мобільного) зв'язку, без розкриття змісту повідомлень, що передаються, та інших радіовипромінювальних пристроїв (проект Закону України «Про оперативно-розшукову діяльність» реєстр. № 4778).

Форма інформаційно-аналітичної роботи – внутрішня і зовнішня організація її системи.

Чати (англ. *chat* – розмова) – засіб спілкування користувачів мережі в режимі реального часу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Нормативно-правові акти

1. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.
2. Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-III // Відомості Верховної Ради України. – 2001. – № 25–26. – Ст. 131.
3. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 р. № 4651-VI // Голос України від 19.05.2012. – № 90–91.
4. Кримінальний процесуальний кодекс України. Науково-практичний коментар: у 2 т. / за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. – Х.: Право, 2012. – .– Т. 1. – 768 с. – . – Т. 2. – 664 с.
5. Кримінальний процесуальний кодекс України. Науково-практичний коментар / за заг. ред. професорів В. Г. Гончаренка, В. Т. Нора, М. Є. Шумила. – К.: Вид-во «Юстиніан», 2012. – 1224 с.
6. Про Національну поліцію: Закон України від 2 липня 2015 р. № 580-VIII // Відомості Верховної Ради України. – 2015. – № 40–41. – Ст. 379.
4. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 р. № 2135-XII // Відомості Верховної Ради України. – 1992. – № 22. – Ст. 303.
5. Про організаційно-правові основи боротьби з організованою злочинністю: Закон України від 30 червня 1993 р. № 3341-XII // Відомості Верховної Ради України. – 1993. – № 35. – Ст. 358.
6. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. № 80/94-ВР // Відомості Верховної Ради України. – К., 1994. – № 31. – Ст. 286.
7. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
8. Про Національну програму інформатизації: Закон України від 4 лютого 1998 р. № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27–28. – Ст. 181.
9. Про державну таємницю: Закон України від 21 січня 1994 р. № 3855-XII // Відомості Верховної Ради України. – 1994. – № 16. – Ст. 93.
10. Про Концепцію Національної програми інформатизації: Закон України від 4 лютого 1998 р. № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27–28. – Ст. 182.
11. Про телекомунікації: Закон України від 18 листопада 2003 р. № 1280-IV // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.
12. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 9 січня 2007 р. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.

13. Про захист персональних даних: Закон України Закон від 1 червня 2010 р. № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481.
14. Про першочергові завдання щодо впровадження новітніх інформаційних технологій: Указ Президента України від 20 жовтня 2005 р. № 1497 // Урядовий кур'єр від 1 листопада 2005 р. – № 207.
15. Про затвердження Положення про Національну поліцію: Постанова Кабінету Міністрів України від 28 жовтня 2015 р. № 877 // Урядовий кур'єр від від 06.11.2015 № 207.
16. Про затвердження Положення про Міністерство внутрішніх справ України: Постанова Кабінету Міністрів України від 28 жовтня 2015 р. № 878 // Урядовий кур'єр від 6 листопада 2015 р. № 207.
17. Про Національне центральне бюро Інтерполу: Постанова Кабінету Міністрів України від 25 березня 1993 р. № 220 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/220-93-п.
18. Деякі питання надання інформації про зареєстровані транспортні засоби та їх власників: Постанова Кабінету Міністрів України від 25 березня 2016 р. № 260 // Урядовий кур'єр від 7 квітня 2016 р. № 66.
19. Про затвердження Плану заходів з виконання Концепції реалізації державної політики у сфері профілактики правопорушень на період до 2015 року: Постанова Кабінету Міністрів України від 8 серпня 2012 р. № 767 // Урядовий кур'єр від 5 вересня 2012 р. № 159.
20. Про деякі питання застосування судами України законодавства при дачі дозволів на тимчасове обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства: Постанова Пленуму Верховного Суду України від 28 березня 2008 р. № 2 (із змінами, внесеними згідно з Постановою Верховного Суду № 8 від 4 квітня 2010 р.) // Вісник Верховного суду України. – 2008. – № 4. – С. 4.
21. Про деякі питання здійснення слідчим суддею суду першої інстанції судового контролю за дотриманням прав, свобод та інтересів осіб під час застосування заходів забезпечення кримінального провадження: Лист Вищого спеціалізованого суду України від 5 квітня 2013 р. № 223-558/0/4-13 // Судовий Вісник. – 2013. – № 4.
22. Рішення Конституційного Суду України від 20 січня 2012 р. № 2-рп у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України // Офіційний вісник України. – 2012.– № 9. – С. 106. – Ст. 332.
23. Конвенція про кіберзлочинність // Офіційний вісник України. – 2007. – № 65. – С. 107. – Ст. 2535. – Офіц. пер.
24. Кодекс поведінки посадових осіб з підтримання правопорядку: резолюція 34/169 Генеральної Асамблеї ООН 17 грудня 1999 р. [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/995_282.
25. Про затвердження Інструкції про порядок ведення єдиного обліку в органах поліції заяв і повідомлень про вчинені кримінальні правопорушен-

ня та інші події: Наказ МВС від 6 листопада 2015 р. № 1377, зареєстрований в Міністерстві юстиції України 1 грудня 2015 р. за № 1498/27943.
26. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: Наказ ГПУ, МВС, СБУ, АДПС, Мінфіна, Мінюста від 16 листопада 2012 р. № 114/1042/516/1199/936/1687/5.
27. Про затвердження Інструкції про порядок використання правоохоронними органами можливостей НЦБ Інтерполу в Україні у попередженні, розкритті та розслідування злочинів: Наказ МВС, ГПУ, СБУ, Держкомітету у справах охорони державного кордону, Держмитслужби, ДПА від 9 січня 1997 р. № 3/1/2/5/2/2.
28. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України: Наказ МВС від 12 жовтня 2009 р. № 436 // Офіційний вісник України. – 2010. – № 101. – С. 409. – Ст. 3569.
29. Про затвердження Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів які перетинають державний кордон: Наказ АДПС, ДМС, ДПА, МВС, МЗС, Мінпраці, СБУ, Служби зовнішньої розвідки від 3 травня 2008 р. № 284/287/214/150/64/175/266/75, зареєстрований в Міністерстві юстиції України 12 травня 2008 р. за № 396/15087 // Офіційний вісник України. – 2008. – № 37. – С. 54. – Ст. 1249.
30. Про затвердження Положення про єдину цифрову відомчу телекомунікаційну мережу МВС: Наказ МВС від 4 липня 2016 р. № 596, зареєстрований в Міністерстві юстиції України 28 липня 2016 р. за № 1055/29185.
31. Про затвердження Інструкції з організації функціонування криміналістичних обліків експертної служби МВС України: Наказ МВС від 10 вересня 2009 р. № 390, зареєстрований в Міністерстві юстиції України 15 жовтня 2009 р. за № 963/16979.
32. Про затвердження Порядку взаємодії Генеральної прокуратури України та Міністерства внутрішніх справ України щодо обміну інформацією з Єдиного реєстру досудових розслідувань та інформаційних систем органів внутрішніх справ: Наказ ГПУ та МВС від 17 листопада 2012 р. № 115/1046.
33. Про затвердження Положення про порядок ведення Єдиного реєстру досудових розслідувань: Наказ ГПУ від 6 квітня 2016 р. № 139, зареєстрований в Міністерстві юстиції України 5 травня 2016 р. за № 680/28810 // Офіційний вісник України. – 2016. – № 46. – С. 48. – Ст. 1674.
34. Про затвердження Положення про Департамент карного розшуку Національної поліції України: Наказ НПУ від 14 листопада 2015 р. № 90.
35. Про затвердження Положення про Департамент захисту економіки Національної поліції України: Наказ НПУ від 7 листопада 2015 р. № 81.
36. Про затвердження Положення про Департамент кіберполіції Національної поліції України: Наказ НПУ від 10 листопада 2015 р. № 85.
37. Про затвердження Положення про Департамент внутрішньої безпеки Національної поліції України: Наказ НПУ від 9 листопада 2015 р. № 83.

38. Про затвердження Положення про Департамент протидії наркозлочинності Національної поліції України: Наказ НПУ від 17 листопада 2015 р. № 95.
39. Про затвердження Положення про Департамент боротьби зі злочинами, пов'язаними з торгівлею людьми Міністерства внутрішніх справ України: Наказ МВС України від 14 жовтня 2014 р. № 1074.
40. Про затвердження Положення про Департамент кримінальної розвідки Національної поліції України: Наказ НПУ від 3 грудня 2015 р. № 140.
41. Про затвердження Положення про Робочий апарат Укрбюро Інтерполу: Наказ НПУ від 21 грудня 2015 р. № 193.
42. Про затвердження Положення про Департамент інформаційних технологій Міністерства внутрішніх справ України: Наказ МВС від 14 грудня 2015 року № 1572.
43. Про затвердження Положення про Департамент інформаційної підтримки та координації поліції «102» Національної поліції України: Наказ НПУ від 30 грудня 2015 р. № 228.
44. Про затвердження Положення про Управління режиму та технічного захисту інформації Національної поліції України: Наказ НПУ від 27 листопада 2015 р. № 122.
45. Про організацію доступу до відомостей персонально-довідкового обліку єдиної інформаційної системи Міністерства внутрішніх справ України: Наказ МВС від 29 листопада 2016 р. № 1256, зареєстрований в Міністерстві юстиції України 10 січня 2017 р. за N 22/29890.

Спеціальна література

1. Мовчан А. В. Компьютерные системы биометрической идентификации. Актуальные проблемы применения в правоохранительной деятельности: монография / А. В. Мовчан. – Saarbrücken, Deutschland: LAP LAMBERT Academic Publishing, 2015. – 80 с.
2. Бєляков К. І. Інформаційний конфлікт та юридична відповідальність: сутність і співвідношення / К. І. Бєляков // Правова інформатика. – 2013. – № 2(38). – С. 38–46.
3. Боер В. М. Информационное право: учеб. пособие / В. М. Боер, О. Г. Павельева. – СПб., 2006. – Ч. 1: ГУАП. – 116 с.
4. Воронов И. А. Теоретические основы использования информационных и поисковых систем глобальной сети Интернет в оперативно-розыскной деятельности / И. А. Воронов // Вісник ЛДУВС ім. Е. О. Дідоренка. – 2009. – № 1. – С. 194–203.
5. Гуменюк Л. Й. Соціальна конфліктологія: навч. посібник / Л. Й. Гуменюк. – Львів: Львівський державний університет внутрішніх справ, 2013. – 400 с.
6. Задорожный Ю. А. Проблемы информатизации органов внутренних дел / Ю. А. Задорожный // Вісник Луганського державного університету внутрішніх справ. – 2007. – № 2. – С. 215–228.

7. Захаров В. П. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник / В. П. Захаров, В. І. Рудешко. – 2-ге вид., доп. – Львів: ЛьвДУВС, 2015. – 492 с.
8. Захаров В. П. Проблеми інформаційного забезпечення боротьби зі злочинністю: моногр. / В. П. Захаров. – Львів: Львів. держ.ун-т внутр. справ, 2008. – 472 с.
9. Інформатика та інформаційні технології: навч. посібник / Б. В. Щур, І. С. Керницький, В. В. Сеник та ін. – Львів: Львів. держ. ун-т внутр. справ, 2010. – 536 с.
10. Конфліктологія: навч. посібник / Л. М. Герасіна, М. П. Требін, В. Д. Воднік та ін. – Х.: Право, 2012. – 128 с.
11. Кузнецов И. Н. Информация: сбор, защита, анализ: учебник по информационно-аналитической работе / И. Н. Кузнецов. – М., ООО Изд. Яуза, 2001. – 100 с.
12. Лук'янчиков Є. Д. Методологічні засади інформаційного забезпечення розслідування злочинів: монографія / Є. Д. Лук'янчиков. – К.: Нац. акад. внутр. справ України, 2005. – 360 с.
13. Міжнародна поліцейська енциклопедія: У 10 т. / відп. редактори В. В. Коваленко, Є. М. Моісеєв, В. Я. Тацій, Ю. С. Шемшученко. – К.: Атіка, 2010. – Т. VI. Оперативно-розшукова діяльність поліції (міліції). – 1128 с.
14. Movchan A. V. Actual issues of the obtaining of investigation and search information under modern conditions / A. V. Movchan // Наука і правоохорона. – 2014. – № 1. – С. 92–96.
15. Мовчан А. В. Зарубіжний досвід застосування біометричної ідентифікації людини у протидії транснаціональній злочинності / А. В. Мовчан, Д. А. Мовчан // Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. – Луганськ, 2009. – № 1. – С. 179–184.
16. Мовчан А. В. Кібернетична безпека України в умовах глобальної нестабільності / А. В. Мовчан // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2015. – № 1. – С. 159–163.
17. Мовчан А. В. Характеристика основних форм інформаційно-аналітичної роботи в оперативно-розшуковій діяльності / А. В. Мовчан // Наука і правоохорона. – 2014. – № 4. – С. 241–247.
18. Негласні слідчі (розшукові) дії та особливості їх проведення оперативними підрозділами органів внутрішніх справ: навч.-практ. посіб. / Б. І. Бараненко, О. В. Бочковий, К. А. Гусева та ін.; МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. – Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2014. – 416 с.
19. Никифорчук Д. Й. Аналітична робота в оперативно-розшуковій діяльності: навч.-практ. посіб. / Д. Й. Никифорчук, О. Ю. Бусол, Г. М. Бірюков. – К.: НАВС, 2012. – 152 с.
20. Овчинский А. С. Информация и оперативно-розыскная деятельность: монография / под ред. В. И. Попова. – М.: ИНФРА–М, 2002. – 97 с.
21. Овчинский С. С. Оперативно-розыскная информация / под ред. А. С. Овчинского и В. С. Овчинского. – М.: ИНФРА–М, 2000. – 367 с.

22. Оперативне розпізнавання: монографія / В. А. Некрасов, В. Я. Мацюк, Н. Є. Філіпенко, Л. В. Родинюк. – К.: КНТ, 2007. – 216 с.
23. Оперативно-розыскная деятельность: учеб. / Под ред. К. К. Горяинова, В. С. Овчинского, Г. К. Синилова, А. Ю. Шумилова. – [2-е изд., доп. и перераб.]. – М.: ИНФРА–М, 2004. – 848 с.
24. Орлов Ю. Ю. Поняття та елементи організації оперативно-розшукової діяльності / Ю. Ю. Орлов // Науковий вісник Київського національного університету внутрішніх справ. – К., 2006. – № 5. – С. 178–187.
25. Основи оперативно-розшукової діяльності: навч. посіб. / С. В. Албул, С. В. Андрусенко, Р. В. Мукоіда, Д. О. Ноздрін; за заг. ред. С. В. Албула. – Одеса: ОДУВС, 2016. – 270 с. – з іл. (Серія: Теорія і практика ОРД).
26. Основи управління в органах внутрішніх справ: навч. посібник / О. М. Бандурка, В. М. Бевзенко, В. М. Василенко та ін. – Х. : Ха·рк. нац. ун-т внутр. справ, 2010. – 590 с.
27. Отримання та використання первинної оперативно-розшукової інформації оперативними підрозділами ОВС України: монографія / А. В. Баб'як, В. П. Сапальов, М. В. Стащак, В. В. Шендрик. – Львів: Каменяр, 2010. – 167 с.
28. Погорецький М. А. Поняття організації оперативно-розшукової діяльності / М. А. Погорецький, В. П. Шеломенцев // Кримський юридичний вісник. – 2010. – № 1 (8). – С. 30–39.
29. Психологія безпеки професійної діяльності в системі МВС України: навч.-практ. пос. / Б. І. Бараненко, Д. О. Бабічев, В. О. Криволапчук та ін.; за ред. Б. І. Бараненка, О. В. Шаповалова; МВС України, ДНДІ МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. – Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. – 200 с.
30. Психологія оперативного спілкування в діяльності оперативних підрозділів органів внутрішніх справ: навч.-практ. посібник / Б. І. Бараненко, В. А. Глазков, О. С. Звонок та ін.; за ред. Е. О. Дідоренка; МВС України, Луган. держ. ун-т внутр. справ. – Луганськ: РВВ ЛДУВС, 2007. – 552 с.
31. Словник спеціальних термінів правоохоронної діяльності / за ред. Я. Ю. Кондратьєва. – К.: Нац. акад. внутр. справ України, 2004. – 560 с.
32. Халиков А. Н. Юридическое, техническое и информационно-аналитическое обеспечение оперативно-розыскной деятельности: учеб. пособие / А. Н. Халиков, Е. Н. Яковец, Н. И. Журавленко; под ред. А. Н. Халикова. – М.: Юрлитинформ, 2010. – 472 с.
33. Хахановський В. Г. Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності: основні поняття та нормативно-правова база / В. Г. Хахановський // Науковий вісник ЛІВС. – 2003. – № 2 (1). – С. 191–195.
34. Яковец Е. Н. Проблемы аналитической работы в оперативно-розыскной деятельности органов внутренних дел: монография / Е. Н. Яковец. – М.: Издательский дом Шумиловой И. И., 2005. – 219 с.

Інтернет-ресурси

1. Офіційний веб-сайт Президента України [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/.
2. Офіційний веб-сайт Верховної Ради України [Електронний ресурс]. – Режим доступу: http://rada.gov.ua/.
3. Офіційний веб-сайт Кабінету Міністрів України [Електронний ресурс]. – Режим доступу: http://www.kmu.gov.ua/.
4. Офіційний веб-сайт Міністерства внутрішніх справ України [Електронний ресурс]. – Режим доступу: http://www.mvs.gov.ua/.
5. Офіційний веб-сайт Національної поліції України [Електронний ресурс]. – Режим доступу: http://www.npu.gov.ua/uk/.
6. Офіційний веб-сайт Генеральної прокуратури України [Електронний ресурс]. – Режим доступу: http://www.gp.gov.ua/.
7. Офіційний веб-сайт Міністерства освіти і науки України [Електронний ресурс]. – Режим доступу: http:// www.mon.gov.ua/.
8. Офіційний веб-сайт Львівського державного університету внутрішніх справ [Електронний ресурс]. – Режим доступу: http://www.lvduvs.edu.ua/.
9. Офіційний веб-сайт Національної академії внутрішніх справ [Електронний ресурс]. – Режим доступу: http://www.naiau.kiev.ua/.

НАВЧАЛЬНЕ ВИДАННЯ

Мовчан Анатолій Васильович
доктор юридичних наук,
старший науковий співробітник, професор

Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції

Навчальний посібник

Редагування *І. Б. Попик*
Макетування *Г. Я. Шушняк*
Друк *А. М. Радченко*

Підписано до друку 14.07.2017
Формат 60×84/16. Папір офсетний. Умовн. друк. арк. 14,18
Тираж 100 прим. Зам № 42-17

Львівський державний університет внутрішніх справ
Україна, 79007, м. Львів, вул. Городоцька, 26.

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції
ДК № 2541 від 26 червня 2006 р.