ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

Збірник наукових статей за матеріалами доповідей учасників Всеукраїнського науково-практичного семінару 23 березня 2018 р.

Львів 2018

УДК 004 : 351.746.2
І-74

Рекомендовано до друку Вченою радою Львівського державного університету внутрішніх справ (протокол № 10 від 30.05.2018 р.)

І-74 Інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичного семінару 23 березня 2018 року / упорядники А.В. Баб'як, В.В. Сеник, Т. В. Магеровська /. – Львів: ЛьвДУВС, 2018. – 209 с.

У збірнику вміщено наукові статті за матеріалами доповідей, підготовлених учасниками Ввеукраїнського науково-практичного семінару конференції «Інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції», що проводився 23 березня 2018 р. у Львівському державному університеті внутрішніх справ.

Опубліковано в авторській редакції

УДК 004
ББК 32.973

ВСТУПНЕ СЛОВО РЕКТОРА ЛЬВІВСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ ВНУТРІШНІХ СПРАВ, ПОЛКОВНИКА ПОЛІЦІЇ, КАНДИДАТА ЮРИДИЧНИХ НАУК, ДОЦЕНТА

БЛАГУТИ РОМАНА ІГОРОВИЧА

Шановні колеги!

Щиро радий привітати вас від імені науково-педагогічного колективу Львівського державного університету внутрішніх справ та від себе особисто з початком роботи науково-практичного семінару «Інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції». Ми покладаємо великі надії на результати його роботи, адже питання, винесені на розгляд семінару, мають велике значення як для закладів вищої освіти МВС, так і для Національної поліції України.

У сьогоднішніх умовах протидії організованій та транснаціональній злочинності інформаційно-аналітичне забезпечення оперативно-розшукової діяльності кримінальної поліції набуває особливого значення. Застосування сучасних інформаційних та телекомунікаційних технологій в ОРД дозволяє інтегрувати й опрацьовувати величезну кількість даних, що містяться у відкритих джерелах інформації та спеціалізованих автоматизованих інформаційних системах, отримуючи при цьому нові знання кримінального та криміногенного характеру.

Разом з тим, стрімкий розвиток інформаційно-телекомунікаційних засобів вимагає нових підходів до організації інформаційно-аналітичного забезпечення ОРД.

Проблеми інформаційно-аналітичного забезпечення підрозділів кримінальної поліції набувають особливої актуальності через низку чинників. Мова йде про демократизацію соціальних

процесів в Україні, запровадження законодавчого регулювання ОРД, набрання чинності новим Кримінальним процесуальним кодексом України, дотримання прав людини в ході ОРД, захист персональних даних. Одним із наслідків цього стало виникнення певних проблем в отриманні оперативно-розшукової інформації та її використанні у кримінальному судочинстві.

Крім того, швидкий розвиток комп'ютерної техніки, інформаційних та телекомунікаційних технологій, які використовуються для отримання, обробки та використання оперативно-розшукової інформації, потребують відповідних організаційних змін у діяльності підрозділів інформаційної підтримки Національної поліції.

Національна поліція України з урахуванням досвіду поліції інших країн планово запроваджує міжнародні стандарти управління інформацією у сфері запобігання правопорушенням та розслідування злочинів. Заходи з упровадження кримінального аналізу проводяться в рамках реалізації відомчої програми одночасно зі створенням системи аналізу ризиків.

Консультативна місія Європейського Союзу в Україні підтримує впровадження в Національній поліції України моделі поліцейської діяльності, керованої аналітикою (Intelligence-Led Policing/ILP).

Зважаючи на розвиток організованих форм злочинності в Україні, наявність корумпованих зв'язків в органах державної влади, значного поширення набула злочинність з міжрегіональними та міжнародними зв'язками, що потребує систематизації великих масивів інформації, здобутої з різноманітних джерел.

Злочинці стають дедалі підготовленими, використовують для вчинення злочинів сучасні 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-аналітичне забезпечення підрозділів кримінальної поліції потребує правового врегулювання на законодавчому та відомчому рівні.

Під час роботи науково-практичного семінару заплановано розглянути актуальні проблеми діяльності підрозділів кримінальної поліції України в сучасних умовах; теоретичні і прикладні аспекти використання сучасних інформаційних технологій у правоохоронній діяльності; кримінальний аналіз та прогнозування у протидії окремим видам злочинів; актуальні правові та організаційно-тактичні проблеми інформаційно-аналітичного забезпечення оперативно-розшукової діяльності підрозділів кримінальної поліції України; науково-методичні та нормативно-правові аспекти забезпечення інформаційної безпеки і боротьби з кіберзлочинністю; проблемні питання підготовки фахівців у галузі інформаційних технологій для органів Національної поліції України; актуальні питання підвищення якості інформаційно-аналітичної підготовки фахівців для підрозділів кримінальної поліції.

У роботі науково-практичного семінару беруть участь наукові та науково-педагогічні працівники вищих навчальних закладів і науково-дослідних установ МВС України, практичні працівники підрозділів Національної поліції.

Упевнений, що науково-практичний семінар «Інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції» стане важливим етапом процесу підготовки кадрів для Національної поліції України.

Бажаю всім плідної роботи та творчого натхнення.

МОЖЛИВОСТІ ВИКОРИСТАННЯ МЕТОДУ РЕКОНСТРУКЦІЇ ПІД ЧАС ВСТАНОВЛЕННЯ СПОСОБУ (МЕХАНІЗМУ) СКОЄННЯ ЗЛОЧИНУ

Афонін Д.С.
старший науковий співробітник Науково-дослідної лабораторії з проблемних питань кримінального аналізу Одеського державного університету внутрішніх справ

Встановлення способу (механізму) скоєння злочину є одним з основних завдань розслідування. Криміналістика має достатньо методів та засобів щодо встановлення картини злочину. Одним з таких методів є реконструкція. Багато вчених приділяло увагу методу реконструкції, в зв'язку з тим що вона дозволяє вивчити минуле та відновити за окремими слідами спосіб (механізм) скоєння злочину. Однак до теперішнього часу не має єдиної концепції щодо технології застосування реконструкції, алгоритмізації цього методу та кола слідчих (розшукових) дій при проведенні яких можливо застосування цього методу.

Розробці питань застосування методу реконструкції під час розслідування злочинів приділяли увагу Л.Є. Ароцкер, Р.С. Бєлкин, А.І. Вінберг, Г.О. Густов, О.О. Ейсман, В.Я. Колдін, В.О. Коновалова, В.В. Куванов, О.О. Леві, І.М. Лузгін, В.К. Лисиченко, М.С. Польовий, М.В. Салтєвський, Я.Г. Ципарський та інші вченні.

Так, А.Р. Ратинів оцінює реконструкцію, як один із видів моделювання. Розглядаючи матеріальне моделювання, він відносить до нього всі випадки відтворення предметів та явищ, пов'язаних з подією минулого. А.Р. Ратінов зазначає: «В принципе тот же характер носит воссоздание обстановки и условий, в которых происходят либо могли произойти те или иные события. Речь идет о следственном действии, которое именуется следственным экспериментом... Такое моделирование иногда именуют реконструкцией места происшествия» [1].

Р.С. Бєлкін розглядав реконструкцію, як один з прийомів розслідування. Він вважає, що цей прийом полягає в підготовці умов для проведення експерименту та інших слідчих (розшукових) дій. Р.С. Бєлкін вказує: «Мы реконструируем обстановку либо в целях ее последующего осмотра, либо для проведения в созданных условиях следственного эксперимента или опознания тех или иных объектов и т.п. Реконструкция выступает при этом как начальный этап или как условие, тактический прием производства того или иного следственного действия» [2].

Значну увагу застосуванню реконструкції під час проведення слідчих (розшукових) дій приділяють зарубіжні криміналісти, зокрема криміналісти США, ФРН та Чехії.

Так, Х. Бек (ФРН) вказує, що реконструкція є одним із багатьох методів, які використовуються з метою розкриття злочину; вона застосовується в ході огляду, при допиті та інших слідчих діях; вона не замінює собою все розслідування, а є саме одним з методів, який використовується у боротьбі зі злочинністю» [3]. Х. Бек розрізняє загальну реконструкцію обстановки на місці події, реконструкцію окремих обставин, або додаткову реконструкцію, яка проводиться з участю підозрюваного або без нього для вирішення окремих завдань розслідування та перевірки доказів.

Е. Штельцер (ФРН) під криміналістичної реконструкцією розуміє один з методів розкриття і запобігання злочинів. Цей метод, на його думку, полягає у відновленні або відтворенні (Nachbildung) деяких обставин або в уявному відтворенні (Wiederholung) деяких релевантних події фактів, які дозволяють встановлювати та перевіряти докази [4].

У. Гері Графф (США) вважає що реконструкція є одним з основних методів розслідування злочинів, який використовується переважно при огляді місця події [5]. Реконструкція, на його думку, базується на ретельному аналізі доказової інформації, її систематизації, встановленню причино-наслідкових та просторо-часових зв’язків. Також, на

його думку, реконструкція дає уявлення про спосіб, місце, час скоєння злочину, особу злочинця тощо.

Чеський криміналіст Мирослав Виходил застосовує поняття слідча реконструкція та розглядає її, як особливий метод верифікації показань та інших джерел доказів. Він вказує, що реконструкція – це слідча дія, яка є комплексним відтворенням обстановки і обставин події... На його думку, вона проводиться на підставі порівняння даних, отриманих в процесі розслідування, з об'єктивною обстановкою з метою перевірки цих даних, а також з метою одержання нових доказів» [6].

Тлумачення реконструкції, як методу що охоплює весь процес розслідування, на нашу думку, можна вважати надмірно широким та таким, що перебільшує сутність цього методу та принижує можливості інших методів та прийомів. Розслідування – це збирання, дослідження, перевірка та оцінка доказів у передбачених законом процесуальних формах для встановлення обставин події. Мета розслідування не відтворення події, а досягнення істини у висновках по справі та підготовка матеріалів для суду або для прийняття інших рішень.

На нашу думку, більш правильним розглядати реконструкцію як різновид моделювання, який є одним з методів пізнання обставин правопорушення та перевірки об'єктивності самого розслідування. В цій якості реконструкція забезпечує відтворення зв'язків між елементами, які у своїй сукупності утворюють систему, що представляє аналог досліджуваного оригіналу (предмета, події, ситуації тощо). Сутність методу реконструкції повністю збігається з сутністю моделювання, тому реконструкцію, на нашу думку, необхідно розглядати як ретроспективний вид моделювання.

Реконструкція, як різновид моделювання, має ряд особливостей. Так, в результаті матеріального, а також знакового моделювання створюється принципово новий об'єкт, подібний оригіналу, але він є в своєї основі іншим: зліпки зі слідів, муляжі, макети, фотографії, аудіо- та відеозаписи, схеми тощо. У реконструкції під час розслідування злочинів, іноді зберігаються елементи

справжньої обстановки, справжнього предмета. Тому слідчий повинен їх обов'язково використовувати та не замінювати їх іншими матеріалами, крім випадків коли справжні об'єкти повністю зруйновані.

Прийоми деяких реконструкцій спрямовані на те, щоб досягти такого відношення між оригіналом (наприклад, первісної обстановки на місці події) та моделлю, яке забезпечувало збереження існуючих елементів оригіналу, включених у реконструкцію. В зв'язку з тим, що реконструкція може включати елементи оригіналу, необхідно встановити їх тотожність, зв'язок з подією, зібрати відомості про відсутні елементи, перевірити, наскільки вірні ці відомості, відтворити відсутні елементи, відновити зв'язки між усіма елементами системи і, нарешті, відтворити ці зв'язки шляхом реконструкції.

Реконструкція використовується як метод, що реалізує одно із завдань слідчої (розшукової) дії – встановлення способу (механізму) скоєння злочину, як одної з обставин, що підлягає доказуванню. Реалізація методу реконструкції відбувається через застосування прийомів залежно від ситуації і конкретних завдань слідчої (розшукової) дії, але успішне застосування цього методу потребує подальшої конкретизації, алгоритмізації та систематизації проведення.

---

1. Ратинов А.Р. Судебная психология для следователей. – М., 1967, – с. 123.
2. Белкин Р.С. Собирание исследование и оценка доказательств. – М., 1966. – с. 257.
3. Beck H. Die Rekonstruktion der Methode der Wiedergabe. – Schriftenrehe der Deutschen Volkspolizei, 1956, H. 4, S. 64.
4. Stelzer. Sozialistische Kriminalistik. – Band 1. Berlin, 1978, – S. 181.
5. Gary W. Graff. Case Management: The Foundation for Crime Scene Reconstruction. – J. Association for Crime Scene Reconstruction. 2016; 20 : – 35-43.
6. Vychodil Miroslav. Rekonstrukce trestneho cino. – Praha, 1972, S.5. – 159.

РОЗРОБКА БАЛІСТИЧНОГО СТАНДАРТУ ПО ГІЛЬЗАМ ЯК ЗАСІБ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, УЧИНЕНИХ ІЗ ЗАСТОСУВАННЯМ ВОГНЕПАЛЬНОЇ ЗБРОЇ

Бондар В.С.
начальник відділу організації наукової роботи
Луганського державного університету внутрішніх справ
імені Е.О. Дідоренка, кандидат юридичних наук, доцент

Одним факторів підвищення ефективності інформаційно-аналітичного забезпечення виявлення та розслідування злочинів, учинених із застосуванням вогнепальної зброї є якісна ідентифікація зброї по слідах бойку, яка пов'язана з перевіркою за великими масивами гільзотек.

Цільову спрямованість на вирішення завдань ідентифікації має балістичний облік Експертної служби МВС України, який функціонує на центральному та обласних рівнях і складається, зокрема з оперативно-пошукових колекцій:

- куль, гільз та патронів зі слідами зброї (формується з куль, гільз, патронів зі слідами зброї, їх копій та зображень, вилучених під час проведення слідчих (розшукових) дій та оперативно-розшукових заходів);
- куль та гільз, експериментально відстріляних з вилученої, знайденої та добровільно зданої зброї;
- куль та гільз, експериментально відстріляних з табельної зброї, що знаходиться на озброєнні правоохоронних органів, уповноважених органів державної влади;
- куль та гільз, експериментально відстріляних зі зброї, зареєстрованої на об'єктах дозвільної системи;
- відомостей про зразки саморобної зброї;

- куль та гільз, експериментально відстріляних зі зброї, яка перебуває у власності громадян;
- гільз утраченої гладкоствольної вогнепальної зброї;
- відомостей про вчинені із застосуванням вогнепальної зброї злочини та факти її вилучення з незаконного обігу.

Зазначений балістичний облік регламентований положеннями наказу МВС України від 10.09.2009 № 390 «Про затвердження Інструкції з організації функціонування криміналістичних обліків експертної служби МВС України». Перевірка здійснюється шляхом порівняння слідів зброї на кулях та гільзах з масиву кулегільзотеки та слідів зброї на контрольних кулях та гільзах.

Для проведення перевірок широко використовуються автоматизовані балістичні ідентифікаційні системи (далі – АБІС) виробництва Чехії, зокрема «BalScan», яка застосовує в своїй основі фотограметричний метод та дозволяє отримувати тривимірні розгортки поверхонь куль та гільз зі слідами зброї калібру від 5 до 11,43 мм та ін.

Вирішення цього завдання гарантує слідчому та оперативному працівнику не лише виявлення конкретної зброї, з якої було зроблено постріли, що стали наслідком скоєного правопорушення за умов попередньої наявності інформації про зброю у автоматизованій базі даних, а й отримання наступних відомостей:

- перелік можливих для визначення фактів застосування її в минулому;
- встановлення конкретної категорії, моделі зброї, її виробника;
- оперативне винайдення можливих каналів надходження зброї на територію міста, регіону, країни та осіб, які супроводжували ці процеси тощо, тобто швидко відслідковувати: модель із номерними позначеннями; власника зброї або ж механізм її реалізації – звідки завезена; якою установою /Ф.О.П. поставлена на загальнодержавний облік; хто є реалізатором; на якому складі військової частини могла перебувати на обліку тощо.

Отриманню такого роду інформації передує ретельна робота з веденням окремої спеціалізованої бази даних із зазначенням необхідних фактичних даних, своєрідного «досьє зброї»:

- серія, номер, індекс;
- марка, модель;
- виробник;
- країна виробника;
- шлях потрапляння в Україну;
- облік МВС чи Збройних сил України, інші правоохоронні органи;
- шлях у руках власників (переоформлення/продаж).

Коли зброя потрапляє в категорію речей, які «важко дістати», працівникам оперативних підрозділів за власною агентурною інформацією набагато легше відслідковувати факти появи такої зброї «поза законом».

Наприклад, за відсутності шуканого об'єкту (зброї, що розшукується) під час судово-експертного дослідження тільки стріляних гільз судовий експерт лише теоретично в змозі надавати певним виявленим слідам від деталей зброї характеру стійкості та індивідуальності, що утворювали б відповідний комплекс ознак, достатній для проведення подальшої ідентифікації вже самої зброї. За наявності шуканого об'єкту, або ж попередньо отриманих експериментально відстріляних гільз/куль із певного зразка зброї, дослідження і виокремлення відповідних ознак базується на принципах повторюваності, простежуваності та стійкості.

Аби судовий експерт мав таку можливість, необхідно забезпечити відповідні підрозділи контрольними відстрілами зброї усіх видів, що перебуває на теренах областей/держави, – магазинної, зброї власників (за дозволами від МВС), табельної зброї правоохоронних органів, табельної зброї військових підрозділів (у тому числі Збройних сил України тощо), нагородної зброї та ін.

До можливих шляхів вирішення окреслених вище проблем, на мій погляд, варто віднести:

1) запровадження світовою спільнотою поширення автоматизованих балістичних ідентифікаційних систем із єдиним реєстром кодування інформації, що дало б можливість отримувати оперативну інформацію під час перевірок вилучених об'єктів за створеним та накопиченим масивом даних із багатьох країн світу у режимі реального часу;
2) впровадження балістичного стандарту по гільзам;
3) маркування зброї мітками будь-якого характеру (криміналістичними або ж літерними/символьними), яке має проводити кожен виробник зброї, що має контролюватися державою.

У теперішній час методики ототожнення нарізної вогнепальної зброї за слідами на стріляних гільзах з використанням АБІС різних систем у цілому розроблені. Однак, індивідуальні ознаки зброї, які відображуються в слідах бойків, мають велику морфологічну різнобічність та високу варіативність, а самі зображення – нерівномірну яскравість. Ці фактори серйозно ускладнюють процес порівняння цифрових зображень слідів бойків у автоматичному режимі балістичними ідентифікаційними системами. Попередні дослідження показали, що розробити єдиний унікальний алгоритм, який би дозволив однаково ефективно виділяти індивідуальні ознаки з різною морфологією не є можливим.

Засобом вирішення даних проблем є впровадження балістичного стандарту (наборів клонів куль та гільз), який дозволить вирішувати наступні завдання:

1) тестування роботи АБІС:
   - якості сканування слідів на гільзах (кулях);
   - режимів автоматичного порівняння слідів;
   - однаковості роботи різних балістичних станцій;
2) тестування кваліфікації експертів-балістів різних балістичних лабораторій.

Досвід запровадження даного стандарту є в США та країнах ЄС. Американські та європейські експерти навчились робити точні копії куль та гільз зі слідами зброї (клони). Вони запропонували

використовувати ідентичні набори клонів куль та гільз зі слідами зброї для тестування якості роботи експертів-балістів. Здійснюють віялову розсилку таких наборів за всіма лабораторіями та через деякий час збирають дані, скільки та які парні сліди, які непарні тощо.

В ці набори були включені гільзи, стріляні в різних моделях зброї. Різні моделі зброї це добре, але ще важливіше, щоб сліди містили різні типи ознак.

Судовий експерт у своєму клопотанні має акцентувати увагу на необхідності надання слідчим для проведення експертного експерименту та отримання порівняльного матеріалу не лише аналогів патронів досліджуваних гільз, а саме ідентичні за типом виробника та спорядження.

Тобто, якщо досліджуваними стріляними гільзами є гільзи патронів калібру 7,62х39 мм, наприклад виробництва «Sellier & Bellot JSC» (Чеська Республіка, клеймо – «S&B»), з практичної точки зору навіть безглуздо сподіватися, що ідентична в усьому слідова картина внаслідок пострілу може залишитися на поверхні патронів виробництва, наприклад, ЗАТ «Барнаульський патронний завод» (РФ, клеймо – «БПЗ»). Адже навіть патрони одного калібру та від єдиного виробника можуть мати різне спорядження кулями/капсулем та пороховим зарядом. Та, і попри це, при проведенні багатооб'єктових експертиз багато часу втрачається на встановлення первинної групової приналежності стріляних гільз певним моделям зброї, а вже потім на проведення лінійних ідентифікаційних досліджень: «екземпляр зброї – досліджувана група об'єктів (гільзи/кулі)».

Отже, в роботі було вирішено послідовно два завдання:

1) проведена класифікація індивідуальних ознак слідів бойку;
2) для індивідуальних ознак морфологічних типів, які часто зустрічаються, розроблені ефективні алгоритми їх виділення та переведення зображень, поданих у градаціях

сірого в бінарний вигляд. Коректність виділення індивідуальних ознак та бінаризації зображень багато в чому визначає ефективність подальшого порівняння слідів.

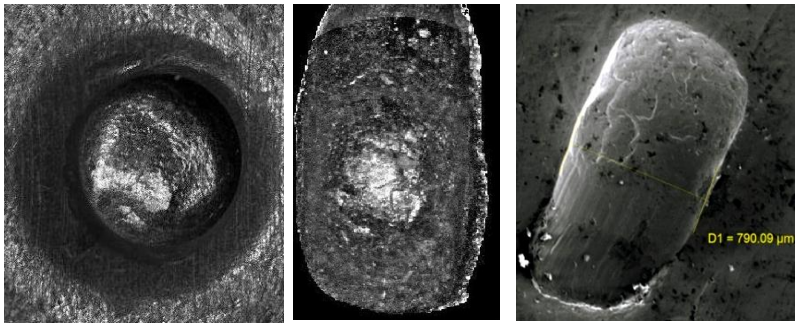
Після відпрацювання методики вирівнювання яскравості зображень була проведена класифікація основних форм (типів) індивідуальних ознак зброї, які відобразилися в сліді бойку. В процесі аналізу слідів бойків більше 30 моделей зброї вдалося виділити 6 основних форм морфологічних типів індивідуальних ознак (без урахування групових ознак, таких як форма, діаметр, глибина сліду тощо), на основі яких можуть бути сформовані ще й додаткові комбіновані типи: а) великі неоднорідності мікрорельєфу з відносно плавними змінами яскравості; б) відносно дрібні топографічні неоднорідності мікрорельєфу; в) ознаки у вигляді контурів та топографічних неоднорідностей з чітко виділеними межами; г) ознаки у вигляді кілець (підгрупові ознаки); ґ) сліди з неоднорідностями мікрорельєфу у вигляді нашарувань; д) – ознаки у вигляді трас, розташованих на дні гільзи та (або) динамічної частини сліду бойку.

Наприклад, на зображенні крім ознак у вигляді кіл можуть бути присутніми ще й окремі ознаки у вигляді плям невизначеної форми.

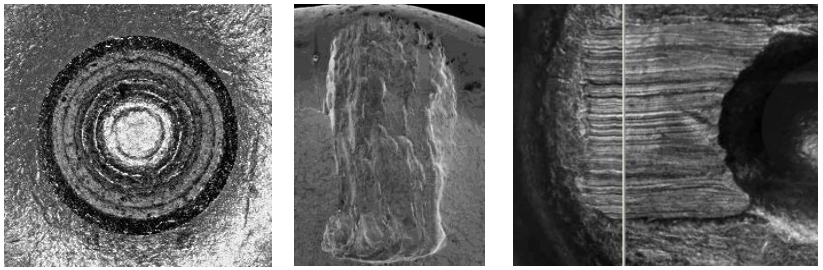
Профіль слідів може бути напівсферичним, трапеціедальним тощо.

Це також слід ураховувати при формуванні наборів для тестування.

Іншим засобом підвищення ефективності інформаційно-аналітичного забезпечення виявлення та розслідування злочинів даної категорії є нанесення прихованого лазерного маркування, так званої «криміналістичної мітки» на гільзах чи кулях, стріляних з ручної стрілецької вогнепальної зброї, що забезпечуються внесенням змісту у слідоутворюючі частини та механізми вогнепальної зброї – канал ствола, патронник ствола, «чашка» затвору тощо, під якою розуміється заздалегідь визначене позначення, зміст, конфігурація та локалізація якого містить інформацію про комплекс ознак зброї.



а) *б)* *в)*



г) *ґ)* *д)*

Рис. 1. Основні морфологічні типи індивідуальних ознак на цифрових зображеннях слідів бойків.

Під поняттям «криміналістичної мітки» автор розуміє заздалегідь визначене позначення, зміст, конфігурація та локалізація якого несе в собі інформацію, що класифікує чи ідентифікує зброю.

Слідчий може додатково ініціювати створення експертом оперативно-розшукових таблиць за виявленими криміналістичними мітками та слідовою інформацією про зброю, з якої досліджувані кулі/гільзи були стріляні.

Потенціал судово-балістичних експертиз, що призначаються в кримінальних провадженнях зазначеної категорії, може бути

реалізований шляхом вирішення таких ідентифікаційних, класифікаційних та діагностичних завдань:

- встановлення ознак лазерного маркування зброї на досліджуваних гільзах/кулях;
- встановлення ознак додаткової обробки (кернування, гравіювання тощо) на складових деталях досліджуваної зброї, що відображуються на стріляних кулях/гільзах;
- встановлення виду, системи, моделі, зразка досліджуваного екземпляра зброї.

Виходячи з положень теорії судової ідентифікації, маркування, які наносяться на деталі зброї з метою їх подальшого ототожнення, мають задовольняти низці вимог:

1) комплекс ознак маркування, який відображується в слідах на стріляних кулях та гільзах, повинен бути індивідуальним, тобто кожному екземпляру зброї повинен відповідати певний комплекс ознак;
2) сліди маркування, які залишаються на ідентифікуючому об’єкті, повинні бути стійкими, тобто незалежно від кількості пострілів комплекс ознак, що індивідуалізує, повинен зберігатись;
3) на різних екземплярах зброї не повинно бути повторень мікрорельєфу маркувальних позначень;
4) складність видалення маркувань.

У спеціальній літературі описані різні способи подібного маркування.

Існуючі в Європі та США методи прихованого маркування та ідентифікації зброї здебільшого відносяться до систем радіочастотного захисту. Тому певний інтерес становить ідея використання радіочастотної технології ідентифікації або RFID (Radio Frequency Identification). Основу цього способу складає використання RFID-міток, які впроваджуються в об’єкт та за своєю конструкцією є антенами, які приминають електромагнітний сигнал, чипом, який обробляє сигнал, що надходить та формує

сигнал у відповідь. Для зняття та запису інформації на мітки використовуються спеціальні прибори зчитувачі.

Використання RFID-міток дозволяє максимально автоматизувати систему обліку, здатну функціонувати в режимі реального часу. Недоліками подібної системи є: можливість знаходження міток – RFID та їх дезактивація; чутливість чипів RFID-системи до інтенсивного нагріву, особливо це стосується механізмів ствольної коробки та стволу. Однак даний спосіб з технічних причин ще не реалізований.

Інші пропоновані передові способи та пристрої для прихованого маркування стволів стрілецької вогнепальної зброї, їх наукова новизна полягають у вирішенні проблем, які полягають у наступному – використовуючи графічну форму зберігання інформації, подібну ASII коду, зменшується розмір кодового елементу, який наділяється здатністю зберігати необхідну кількість знаків інформації. Розроблена технологія електрохімічного маркування полягає у формуванні на поверхні виробу сукупності лунок діаметром 0,5-1,0 мм та глибиною 200-300 мкм. Унікальність маркування полягає в тому, що прихована ідентифікаційна марка у вигляді сукупності розподілених точок малого розміру несе зашифровану інформацію про виробника, дату виготовлення та інші технічні характеристики. Розпізнання такого маркування здійснюється спеціальним сканером, зв’язаним з обчислювальним комплексом. Маркування має високу механічну стійкість, високий оптичний контраст. Підробка маркування даного типу іншими методами (без повторення даної технології) неможлива, тому на даній стадії маркування має високий ступінь захисту від підробок.

Отже, найбільш прийнятним методом є нанесення механічних або лазерних штрихів на деталі зброї, що утворюють сліди.

Цілком прийнятним є вже запроваджений шлях, відповідно до вимог п. 4.14 ДСТУ 78-41-002-97, при надання «криміналістичних міток» стріляним гільзам з переробленої зброї військового призначення у момент проведення заряджання та подальшого

пострілу, що вдало використовується на вітчизняних зброярних підприємствах – виробниках мисливської нарізної вогнепальної зброї на території країни: КНВО «Форт» МВС України; ТОВ «Ерма-Інтер», м. Київ; ПАТ «Завод Маяк», м. Київ; ТОВ «Собр», м. Дергачі, Харківської області. Даний ефект досягнуто за допомогою додаткової канавки у патроннику ствола мисливського карабіна («Сайга»); окремим кернуванням стінки патронника та ствола карабіна («АКМС-МФ», «АКМТ-МФ», «МКМ-072 Сб» тощо) чи додатковим ступінчастим конусом у структурі патронника ствола карабіна («Вулкан», «Вулкан-М», «Вулкан-С») (рис. 2, 3).

Вивчення відповідних слідів на стріляних гільзах надає можливості навіть у «польових умовах» отримувати важливу для розслідування криміналістично значущу інформацію.

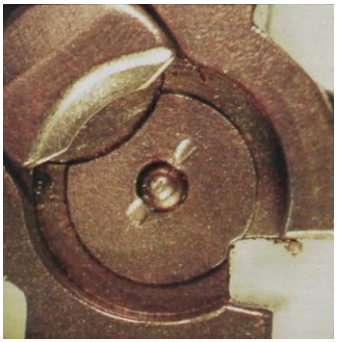


Рис. 2. Зображення слідоутворюючої поверхні затвору мисливського карабіна «АКМ МП УОС» калібру 7,62х39 мм

Рис. 3. Зображення слідів на слідосприймаючий поверхні гільзи, стріляної з мисливського карабіна «АКМ МП УОС» калібру 7,62х39 мм.

Однак слід зазначити, що результати досліджень слідової картини на стріляних кулях, що наводяться в літературі, свідчать про те, що впродовж перших 8-10 пострілів спостерігається висока варіативність слідів, утворених лазерним маркуванням, при подальшій експлуатації зброї сліди від маркування змінюються

повільніше. Таким чином, виходячи з зазначених принципів судової ідентифікації, яким має задовольняти маркування, найбільш слабким місцем є її стійкість від пострілу до пострілу. Одним зі шляхів підвищення вираженості трас є збільшення глибини та ширини полів лазерного маркування.

КАРТОГРАФІЧНИЙ МЕТОД ПРОГНОЗУ ЗЛОЧИННОСТІ

Борець Т. О.
старший науковий співробітник наукової лабораторії з проблем кримінальної поліції Національної академії внутрішніх справ, кандидат юридичних наук

Бурак М. В.
старший науковий співробітник наукової лабораторії з проблем кримінальної поліції Національної академії внутрішніх справ, кандидат юридичних наук

Так, з метою попередження злочинності органи та підрозділи поліції повинні мати повні, достовірні та обґрунтовані відомості, які б дозволили розглянути злочинність за територіальною і часовою ознаками, вивчити взаємозв'язок причин її виникнення та наслідків негативного впливу на суспільство, спрогнозувати подальший розвиток тощо. Інформаційну основу для проведення такого аналізу повинна забезпечувати не тільки чітка організація обліку і звітності у підрозділах поліції, але й відповідна візуалізація такої інформації, що може забезпечити застосування картографічного методу дослідження і пізнання реальності.

Аналіз діяльності правоохоронних органів зарубіжних країн свідчить, що дослідження в області кримінології тісно пов'язані з розвитком тематичного картографування, що підтверджується рядом окремих картографічних творів та сервісів, які надають інформацію про скоєні злочини у вигляді веб-карт, що дуже поширені у Сполучених Штатах Америки. Наприклад, на початку XIX ст. там не було регулярного збору статистичних даних. У США на основі багаторічного досвіду створені ресурси на базі

ГІС-технологій, які надають вільний доступ до інформації про скоєні злочини (їх різновид, місце вчинення, дату і час). Це так звані карти кримінологічної ситуації (карти злочинності), які постійно оновлюються і через Інтернет доступні не тільки для жителів США, а й для усього світу. Поки відомо два такі сайти з інтерактивними картами, на яких способом значків представлена інформація по штатах і великих населених пунктах Америки, а вільне масштабування і детальність цифрової основи дозволяє вивчити ситуацію гранично точно і локалізовано (квартали, вулиці, будинки). Цей ресурс постійно оновлюється, що дає змогу відслідковувати просторово-часову тенденцію кримінологічної ситуації та володіти сучасною і актуальною інформацією [1, с. 95].

В Україні ситуація значно складніша, такого сервісу не існує, і лише іноді в Інтернеті та періодичних виданнях публікуються карти-схеми, де способом картограм чи ареалів подається інформація про злочинність на території України абов окремих її областях. Наприклад, у 2013 році для Києва розроблена онлайн-карта злочинності «Zloch.in.ua», яка відображала дані за січень-серпень 2013 р., однак, їх оперативне оновлення не передбачається.

Отже, основним принципом розробки карт є відповідність картографічних легенд методам і показникам вимірювання злочинності, прийнятих у кримінально-правовій статистиці. Картографічне представлення кількісно-якісних показників злочинності проводиться шляхом відображення основних статистичних показників: рівень злочинності, коефіцієнти злочинності, структура злочинності, динаміка злочинності, відомості про латентність злочинності. Усі перераховані показники мають суто інвентаризаційний чи оцінювальний характер і є підґрунтям для розробки кримінологічного прогнозу в регіоні, який дозволить:

- попередити суспільство і державу про можливі варіанти розвитку кримінологічної ситуації у майбутньому;
- провести обґрунтовану кримінологічну експертизу необхідних законопроектів чи інших нормативно-правових актів;

- здійснити належне планування боротьби зі злочинністю і розробити заходи, спрямовані на її запобігання;
- сприяти розробленню спеціальних програм для вирішення соціально-економічних проблем суспільства;
- вирішити питання про законодавче забезпечення тих чи інших суспільних відносин, внесення змін чи доповнень до чинного законодавства, яке регламентує різноманітні сфери суспільного життя;
- виявити можливі позитивні і негативні наслідки заходів запобігання злочинності, окремих її форм, груп чи видів злочинів.

Карти кримінологічного прогнозу можуть і повинні розроблятися у тісній співпраці картографів і аналітиків-правознавців, бо лише останні в силу своєї професійної кваліфікації можуть об'єктивно оцінити інформацію інвентаризаційних і оцінювальних карт, які відображають показники, що розраховуються за визначеними, відомими алгоритмами.

В контексті формування дієвого механізму попередження злочинності, на нашу думку, важливою складовою при розробці карти кримінологічного прогнозу є отримання думок спеціалістів щодо можливих змін тенденцій і закономірностей злочинності на планований період. Існують суворі процедури збирання думок експертів, їх аналізу і розрахунку експертних оцінок. Найпопулярнішим є так званий дельфійський метод (метод Дельфі), розроблений у США. Згідно з цим методом опитування експертів здійснюють у такий спосіб: запитання експертам ставлять так, щоб вони мали будь-яку кількісну характеристику; опитування здійснюється в кілька турів, під час яких питання і відповіді уточнюються; у разі відхилення прогнозів від думки більшості, експерти обґрунтовують свою думку. До експертизи можуть залучати додаткових експертів. Так формується мережа експертів, яких можна використати для повторної експертизи [2, с. 176].

Також аналіз показників динаміки злочинності та її окремих видів за кілька попередніх років дає змогу виявити тенденцію до зміни цих показників (зменшення чи збільшення коефіцієнта злочин-

ності). На підставі цього за допомогою спеціальних математичних розрахунків можна визначити, як коефіцієнти змінюватимуться в майбутньому.

Тому, цілком логічною потребою є те, що розробці карти повинно передувати детальне вивчення інформації про рівень злочинності на території, що картографується. Для цього, необхідно досліджувати:

- кількість зареєстрованих кримінальних правопорушень (у тому числі кількість особливо тяжких, тяжких, середньої тяжкості та невеликої тяжкості);
- кількість потерпілих від злочинів (з числа яких – жінки, особи похилого віку та інваліди 1 і 2 груп, неповнолітні, діти віком до 14 років)
- види вчинених кримінальних правопорушень тощо.

Важливим, на нашу думку, при розробці карти є побудова прогнозу злочинності на основі демографічного прогнозу змін у чисельності та структурі населення. Дані про соціально-демографічний склад правопорушників накладають на припустиму демографічну структуру, внаслідок чого визначають імовірний рівень злочинності. Найефективнішим цей метод є для короткострокових прогнозів.

Таким чином, детальне вивчення причинно-наслідкових зв'язків здійснення злочинів і соціально-географічних передумов їх виникнення, застосування апарату картографічного моделювання, методів математико-картографічного аналізу, математичної статистики і теорії інформації з широким залученням сучасних геоінформаційних технологій дасть змогу знайти важелі покращення кримінологічної ситуації у криміногенно несприятливих районах області.

Відтак, розроблені кримінологією прогнози про майбутній стан злочинності в тому чи іншому регіоні або у країні загалом є підґрунтям для планування заходів, спрямованих на попередження злочинів.

1. Пересадько В.А. Картографування кримінологічної ситуації (на прикладі Сумської області) / В.А. Пересадько, Є.В. Орлов // Проблеми безперервної географічної освіти і картографії. – 2015. – Вип. 22. – С. 94-98. [Електронний ресурс]. Режим доступу: http://goik.univer.kharkov.ua/wp-content/files/issue_22/22_26.pdf
2. Горбатенко В. Метод «Делфі» та специфіка його застосування у прогнозних розробках / Володимир Горбатенко, Ігор Петренко // Політичний менеджмент. – 2008. – № 6. – С. 174–182. [Електронний ресурс]. Режим доступу: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=PoMe_2008_6_19

ОКРЕМІ АСПЕКТИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ЗЛОЧИННОСТІ В СИСТЕМІ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ

Бесчастний В.М.
ректор Донецького юридичного інституту МВС України,
доктор наук з державного управління, професор

Комплекс заходів, які охоплюються поняттям інформаційне (або в іншій трактовці – інформаційно-аналітичне) забезпечення протидії злочинності, у прикладному плані в аспекті реалізації та вдосконалення включає насамперед розробку управлінських рішень у вказаній сфері.

Майже ні в кого не викликає сумнівів той факт, що існуюча система реєстрації оперативно-розшукової та слідчої інформації, особливо в правоохоронних органах України, фактично мало пристосована і неефективна для використання в розкритті та розслідуванні злочинів. Проте проблема одержання об'єктивної інформації на всіх стадіях протидії злочинності є однією з найбільш значних і актуальних. Її характер і види можуть змінюватися залежно від динаміки розвитку криміногенної ситуації та моделювання обставин вчиненого злочину. Однак

непорушним і беззаперечним при цьому завжди є один із критеріїв її добору – зв'язок із подією злочину.

Урахування організаційних змін у функціонуванні автоматизованих інформаційних систем МВС України [1], які використовуються під час оперативно-розшукового запобігання злочинам, дозволяє зробити висновок щодо необхідності їх подальшого розвитку за такими ключовими напрямами:

- завершення процесу удосконалення нормативно-правового забезпечення функціонування відомчих інформаційних ресурсів;
- забезпечення ефективності та швидкості технічного доступу до віддалених ресурсів;
- розроблення нормативних документів, що стануть правовою основою для спільного використання баз даних оперативними підрозділами різних міністерств та відомств;
- удосконалення інформаційних технологій, систем та інформаційно-аналітичних моделей, які застосовуються у системі прийняття та обробки рішень.

Також потребує вдосконалення обмін інформацією та інші форми співпраці у діяльності правоохоронних органів. Проблема тільки на перший погляд може бути вирішена на рівні угоди про співпрацю. Якщо її розглядати комплексно, то слід оцінювати ситуацію в двох площинах. Перша – зовнішня співпраця підрозділу з іншими службами (відомствами).

На сьогодні проблемою новостворених та реорганізованих служб та підрозділів (підрозділів кіберполіції, Державного бюро розслідувань, Національного антикорупційного бюро України) є налагодження співпраці, в першу чергу, інформаційно-оперативного обміну з представниками правоохоронних органів іноземних держав.

Переважно швидкість отримання відповіді на запит, який оформлюється письмово, за підписом керівника служби, нерідко залежить від комунікативних здібностей працівника та особистих знайомств. Діяльність взаємного обміну інформаційних баз підрозділів, навпаки, ускладнюється виокремленням структурних

підрозділів. Так, виокремлення Державної міграційної служби в окремий департамент відчутно уповільнило процедуру отримання інформації, яка раніше надавалася оперативно в режимі реального часу, а не за схемою письмових запитів.

З огляду на це потрібна на рівні відомств МВС, СБУ, Державної прикордонної служби, Державного бюро розслідувань, Національного антикорупційного бюро України, Національного координаційного центру кібербезпеки та інших відомств розробка та затвердження міжвідомчої Інструкції щодо різних форм обміну даними з інформаційних ресурсів, диференційовано з визначення рівнів оперативності надання інформації та альтернативності способів повідомлення адресату залежно від потреби прийняття рішення.

Інша площина – це внутрішня співпраця між структурними підрозділами поліції та територіальними органами. Стримуючим фактором в об'єднанні зусиль працівників у середині підрозділу і територіальних підрозділів (підрозділу) служби є фактично встановлена система показників розкриття злочинів як оцінки діяльності оперативних працівників. Штучною перепоною досягнення відповідної взаємодії є система показників роботи, що спрямовує на виконання роботи самостійно і відокремлено кожним підрозділом для урахування у статистичній звітності. Відповідна ситуація позначається на якості розкриття злочинів та незадовільному стані оперативного реагування, відсутності навичок співпраці різних оперативних служб щодо спільного оперативного впливу правоохоронних органів.

Без кардинального підходу до зміни в оцінці роботи працівників правоохоронної системи ситуація не зміниться. Отже, наявна проблема породжує питання щодо формування висновків та рекомендацій про стан, динаміку, структуру злочинності, що перебувають у прямій залежності від достовірності статистичних даних та повноти їх збору. З огляду на це є необхідно визначити реальні проблемні ланки як в інформаційно-методичному забезпеченні, так і потреб науково-інформаційних досліджень та розробок. На нашу думку, навіть із запозиченням інших моделей

оцінки діяльності працівників правоохоронної системи у зарубіжних країнах, питання не вирішити. Слід враховувати особливості діяльності різних підрозділів та їх систему звітності. Тому суб'єктивне бачення у вирішенні цієї проблеми, що відобразиться у пропозиціях дослідника, виглядатиме як теорія, непридатна для практичної діяльності. Проблема потребує поступового, комплексного вирішення колегіальним органом (робочою групою) таких питань, як ризики нових моделей оцінки, запровадження пілотних проектів в окремих регіонах щодо зміни системи оцінювання їх діяльності, опитування (використовуючи інтерв'ювання) практичних працівників, особливо керівників підрозділів, враховуючи стаж практичної діяльності та досвід керування відповідним підрозділом щодо питань контрою та стимулювання діяльності працівників підрозділу без щомісячних показників. Невід'ємною складовою є матеріальні затрати та затрати часу, залучення потенціалу наукових установ, практичних працівників різних служб, титанічна робота з узгодження діяльності суб'єктів правоохоронної системи.

Взаємодія працівників правоохоронних органів з населенням та різними формами її самоорганізації містить значний резерв для нарощування потенціалу протидії злочинності. Обумовлено це не тільки необхідністю самої широкої участі громадян у справі профілактики злочинів та інших правопорушень, але також і тим, що всебічна підтримка правоохоронних органів під час забезпечення правопорядку і боротьби зі злочинністю є запорукою досягнення реальних успіхів у цій справі. Зараз досить стрімко впроваджується така форма взаємодії правоохоронних органів з громадськими організаціями і установами, як співпраця з об'єднаннями правників, а також організаціями і фондами, діяльність яких пов'язана з наданням спонсорської, благодійної допомоги у боротьби зі злочинністю [2, с. 292-294].

Впровадження сучасних технічних засобів, комп'ютерної техніки, спеціальних комп'ютерних програм і технологій зумовлює потребу постійного вдосконалення інформаційно-оперативного забезпечення правоохоронної діяльності. Хоча і тут є проблеми.

Варто згадати епопею із запровадженням дактилоскопічних обліків всіх громадян України з 16-річного віку в рамках законопроекту «Про дактилоскопіювання осіб», що зазнало ніщівної критики з боку правозахисних організацій та не призвело до припинення практики повального дактилоскопіювання усіх категорій осіб, затриманих та доставлених до міськрайлінорганів внутрішніх справ [3]. Це болюче питання ще стоїть на порядку денному.

З метою удосконалення інформаційно-оперативного забезпечення працівників правоохоронних органів пропонуємо здійснити:

- широке застосування новітніх технологій в оперативно-розшуковій діяльності, а отже, поліпшення матеріально-технічної бази оперативної роботи;
- розробку та вдосконалення алгоритму дії щодо розкриття злочинів, пов'язаних з інформаційними ресурсами, та процесу їх документування;
- організаційні заходи щодо розробки нових оперативно-довідкових обліків про інформаційні ресурси, що пов'язані з розповсюдженням забороненого контенту в обігу через соцмережі, форуми, через відеохостинги, хостинги зображень у мережі Інтернет, обліки реєстратора та реєстранта доменного імені.

На новий рівень має бути виведено забезпечення практичних працівників методичними рекомендаціями з виконання службових та процесуальних дій, застосування кримінальних, кримінально-процесуальних норм, з урахуванням особливостей та специфіки несення служби. Позитивним прикладом є створенням електронних кейсів, які розсилалися за електронною адресою для працівників підрозділів правоохоронних органів з таким наповненням:

1. «Зміни до законодавства».
2. «Відомчі інструкції», що містять відкриту інформацію без грифа обмеження доступу.
3. «Роз'яснення судової практики» – узагальнення рішень національних судів, практики Рішень Європейського суду

з прав людини проти України, роз'яснення спеціалізованого суду щодо застосування адміністративно-правових, кримінально-правових та кримінально-процесуальних норм.

4. Кейс «методичні рекомендації», що включає роз'яснення щодо застосування кримінальних, кримінально-процесуальних норм, питань криміналістики, судової медицини за різими категоріями злочинів.

Відповідне завдання можливо було доручити Департаменту роботи з персоналом, організації освітньої та наукової діяльності МВС України та Управлінню забезпечення прав людини Національної поліції [4].

Надсилання документів з грифом «Для службового користування» іншим установам у межах України здійснюється рекомендованим поштовим відправленням або кур'єрською службою установи (кур'єрами), підрозділами урядового фельд'єгерського зв'язку, підрозділами органів спеціального зв'язку. Передача службової інформації (надсилання документів з грифом «Для службового користування») телекомунікаційними, інформаційно-телекомунікаційними мережами здійснюється лише з використанням засобів криптографічного захисту інформації, що в установленому порядку допущені до експлуатації, з дотриманням вимог технічного захисту інформації [5].

Паралельно це актуалізує впровадження наукових результатів у практичну діяльність з широким залученням науковців до розробки відомчих нормативно-правових актів, інструкцій, методичних рекомендацій, їх системного тлумачення.

Щодо пропозиції зміни в форматі занять у системі службової підготовки та вивчення питань, практики Рішень Європейського суду з прав людини, в яких громадяни скаржилися на незаконні дії або бездіяльність працівників органів внутрішніх справ, а також рішень відносно інших держав, які стосувалися порушення прав громадян з боку працівників правоохоронних органів, то, на нашу думку, враховуючи формат занять зі службової підготовки

(функціональна, загальнопрофільна, тактична, вогнева, фізична) [6], обсяг нормативно-правових актів, які регламентують діяльність Національної поліції України та брак часу, пов'язаного з виконанням службових обов'язків, рішення Європейського суду з прав людини проти України доречно надсилати серед матеріалів кейса 3. «Роз'яснення судової практики» з виокремленням практики Рішень Європейського суду з прав людини проти України.

Існує також необхідність розробки методичних рекомендацій за участю представників різних відомств. Керуватись при цьому варто принципом залучення до робочої групи вузькопрофільних експертів для створення алгоритму дій з розкриття та розслідування злочинів у певній сфері діяльності (паливно-енергетичній, фінансово-кредитній, банківський, бюджетній, медичній сфері) з урахуванням технічного оснащення, особливостей документування та реальних можливостей співпраці. При цьому змін потребує і система «реагування» відомства на потреби організаційної, технічної, методичної, кадрової допомоги в контексті різних видів забезпечення протидії злочинності.

Враховуючи процес інформатизації суспільства та оцінюючи швидкість передачі інформаційного контенту через ЗМІ, вважаємо актуальним проведення нових кримінологічних досліджень, зокрема повідомлень ЗМІ як джерела кримінологічної інформації; наслідків впливу на свідомість громадян продукту конвергентної журналістики (злиття інформаційних і комунікативних технологій в єдиний інформаційний ресурс). Це наукове завдання для кримінологічної науки, що зумовлює активне використання контент-моніторингу інтернет-ресурсів, в тому числі публікацій ЗМІ та інтернет-ЗМІ як метод інформаційного забезпечення протидії злочинності.

Отже, удосконалення інформаційного забезпечення, в першу чергу, полягає у забезпеченні ефективності та швидкості технічного доступу до віддалених ресурсів та залучення інформаційних ресурсів інших державних органів для протидії злочинності. У межах даного підрозділу запропоновано заходи, спрямовані на усунення недоліків й удосконалення інформаційно-аналітичного,

інформаційно-оперативного та науково-інформаційного забезпечення протидії злочинності, серед яких:

- затвердження на державному рівні програми (стратегії) протидії злочинності як вектора діяльності відповідних суб'єктів;
- удосконалення ресурсу пошукових систем з урахуванням завдань та потреб інформаційного забезпечення всіх структурних підрозділів правоохоронних органів;
- для унормування використання інформаційних баз затвердження міжвідомчої Інструкції щодо різних форм обміну даними з інформаційних ресурсів, диференційовано з визначення рівнів надання інформації та альтернативних способів повідомлення адресату залежно від потреби прийняття рішення;
- доопрацювання форми первинного обліку про кримінальне правопорушення щодо відомостей про потерпілого – освіту, сімейний стан, перебування потерпілого в уразливому стані, стосунки з винним, вчинення злочинів щодо потерпілого в минулому, – що додатково розширить можливість для системного інформування населення про місця та способи пошуку жертв злочинцем, визначення характеристики потерпілих і проявів віктимної поведінки і формування відповідних заходів віктимологічного запобігання;
- розробка механізму апробації наукових здобутків кримінологічних досліджень у практичній площині;
- внесення змін у формат занять в системі службової підготовки з акцентом на удосконалення інформативно-аналітичного та науково-інформаційного забезпечення;
- систематичне забезпечення офіційною статистичною інформацією в розгорнутому форматі науково-дослідних установ, діяльність яких пов'язана з протидією злочинності, та профільних кафедр вищих навчальних закладів;
- проведення нових кримінологічних досліджень впливу на свідомість громадян та наслідки і якість поширення

інформації про злочинність як продукт конвергентної журналістики;

- налагодження співпраці правоохоронних органів і громадських організацій щодо надання альтернативної інформації про злочинність та участь у заходах протидії злочинності [7].

---

1. Цехан Д.М., Луцюк П.С. Інформаційно-аналітичне забезпечення запобігання злочинам у сфері господарської діяльності оперативними підрозділами ОВС. URL: http://www.gp.gov.ua/ua/pd.html?m=publications&_t=rec&id=110522http://criminology.onua.edu.ua/?p=477 (дата звернення: 20.09.2016).
2. Бандурка О.М., Литвинов О.М. Протидія злочинності та профілактика злочинів: монографія. Харків: Вид-во ХНУВС, 2011. 308 с.
3. Рекомендації громадських слухань «Дотримання прав людини в діяльності МВС» (проект) Українська Гельсінська спілка з прав людини. URL: http://helsinki.org.ua/articles/rekomendatsiji-hromadskyh-sluhan dotrym annya- prav-lyudyny-v-diyalnosti-mvs-proekt (дата звернення: 20.09.2016).
4. Повідомлення про оприлюднення проекту наказу МВС «Про затвердження Положення про підрозділи забезпечення прав людини територіальних органів Національної поліції України». URL: https://www.npu.gov.ua/uk/publish/article/1842099 (дата звернення: 20.09.2016).
5. Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію: постанова Кабінету Міністрів України від 19.10.2016 р. № 736. URL: http://zakon2.rada.gov.ua/ laws/show/736-2016-%D0%BF (дата звернення: 20.09.2016).
6. Положення про організацію службової підготовки працівників Національної поліції України: наказ Міністерства внутрішніх справ України 26.01.2016 р. № 50. URL: http://zakon5.rada.gov.ua/laws/show/z0260-16 (дата звернення: 20.09.2016).
7. Бесчастний В.М. Напрями удосконалення інформаційного забезпечення у протидії злочинності. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2016. №1. С.17-22.

ВІРТУАЛЬНІ СПОДІВАННЯ РЕАЛЬНИХ РЕЗУЛЬТАТІВ У ІНФОРМАЦІЙНО-АНАЛІТИЧНОМУ ЗАБЕЗПЕЧЕННІ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Бочковий О.В.
провідний фахівець науково-дослідної лабораторії з проблем попередження, припинення та розслідування злочинів територіальними органами НП України Луганського державного університету внутрішніх справ імені Е.О. Дідоренка, кандидат юридичних наук, старший науковий співробітник

Останнім часом, стала нормою організація різного роду медійних семінарів та нарад для презентації новітніх ідей та перспективних планів. При цьому, якщо раніше такі перформанси були притаманні приватним суб'єктам для популяризації своїх творінь, то сьогодні, це норма для усіх без виключення державних установ з обов'язковим висвітленням на сторінці у Фейсбук.

Але, між першими та другими є одна суттєва різниця. Приватні особи, зазвичай, презентують вже виконаний твір або здійснений винахід для його популяризації. Зокрема, за останні місяці я не зустрічав особу, яка б не знала про успішні запуски ракет Ілона Маска.

У той же час, періодично відвідуючи конференції, семінари та круглі столи з питань інформаційно-аналітичного забезпечення правоохоронної діяльності в Україні на протязі більше 10 років, помітив тільки активну зміну назв підрозділів правоохоронних органів, без суттєвих змін у принципах їх роботи та результатах. Складається враження, що більшість таких презентацій організовується для формального звітування перед інвесторами чергового гранту, єдиною ціллю якого є отримання фінансової вигоди.

Будучи учасником міжнародного семінару з протидії фінансовим злочинам у лютому 2017 року, який проходив у Національній академії внутрішніх справ, від представників іноземних правоохоронних

органів, які виступали як консультанти, почув вражаючу фразу: «ми втрачаємо зацікавленість у консультаціях, адже нічого, з того, що ми даємо, не впроваджується». І тут є над чим задуматись!

Щоб не бути голослівним проаналізуємо світову практику інформаційно-аналітичного забезпечення правоохоронної діяльності. Так, ще у далекому 2001 році в англійському журналі «Police» опублікована стаття про використання сучасних інформаційних технологій у роботі фінансових слідчих. Адже давно відомо, що практично кожна особа залишає за собою електронний слід інформації (наприклад, у Великобританії загальна кількість баз даних, де громадяни можуть залишити електронний слід, у 2001 році становила близько трьохсот, сьогодні ця цифра значно більша). Перед слідчими постає завдання зібрати дані з цих баз відносно конкретної особи, потім відфільтрувати з цих відомостей такі, що відповідають параметрам розслідування, тобто, інакше кажучи, перевірити отриману інформацію стосовно більш широкого контексту розслідування для того, щоб звести воєдино всі відомості і провести аналіз, згідно з яким необхідно діяти далі [1; 2]. Правоохоронні органи зарубіжних країн широко використовують автоматизовані інформаційно-пошукові системи, які дозволяють значно оптимізувати розкриття та розслідування злочинів, учинених членами організованих угруповань [3, С. 57].

Більше того, новітні технології дають змогу активно та продуктивно протидіяти транснаціональній злочинності за рахунок відсутності кордонів у глобальній мережі. Значно полегшується взаємодія та обмін даними між правоохоронними органами різних країн. Приміром, розшукуваний злочинець може бути встановлений шляхом застосування однієї з програм ідентифікації особи по фото чи відео зображенню. Такий досвід вже практикується окремими закордонними державними та приватними відомствами [4; 5; 6].

Донедавна фантастичні уявлення щодо прогнозування злочинності[1] знаходять своє відображення у реальних дослідженнях.

[1] «Особлива думка» (англ. The Minority Report, укр. Звіт меншості) — повнометражний кінофільм режисера Стівена Спілберга. Вийшов на екрани світу 17 червня 2002.

Зокрема, у США та Японії вже почали тестувати програми передбачення злочинів із залученням штучного інтелекту [7; 8].

Сучасне суспільство стрімко розвивається, виникають нові суспільні відносини, які потребують охорони від протиправних посягань. Ми є свідками виникнення нових відносин у сфері комп'ютерних технологій й робототехніки, більшість приватних та державних структур переходять на автоматичне адміністрування, запроваджується технологія блокчейн, тощо.

Цікавлячись та знаючи можливості сучасних наукових розробок у сфері інформаційних технологій та приклади їх використання правоохоронними органами країн Заходу, на думку спадають слова відомого героя з кінофільму «Пригоди Шуріка»: «… и в тот час, когда космические корабли бороздят просторы нашей вселенной…», в Україні більшість зусиль направлені на суперництво між різними правоохоронними структурами.

Ймовірно, на кінець, прийшла пора визнати рівень та стан нашого забезпечення і припинити грати «голого короля», пора розпочати адекватно сприймати реальність.

Адже про яке ефективне інформаційно-аналітичне забезпечення ми ведемо мову, коли в країні відсутній єдиний інформаційний простір. Навіть в рамках підрозділів Національної поліції України бази даних містять інформацію у несумісних форматах. Вдумайтеся: тільки з 2017 року почала діяти єдина база даних патрульної поліції по усій Україні. До 2017 року, колишні бази даних ДАІ були локалізовані у межах області, а запити передавались в ручному режимі.

Передове місце у цій боротьбі, за сучасних умов, займають інформаційні технології. Інформаційно-аналітичні системи як у США так і в більшості інших розвинутих країн є джерелом необхідної інформації для правоохоронних структур та значним ресурсом економії часу. Та навіть за умови отримання оперативно значимої інформації, оперативні підрозділи практично позбавлені можливості ефективного застосування оперативно-розшукового потенціалу через невиправдано ускладнену процедуру отримання

дозволу як на НСРД так і на оперативно-розшукові заходи. Порядок отримання дозволу на проведення ОРЗ та НСРД, займає такий проміжок часу, що часто відпадає сама доцільність такого заходу. До цього ще добавимо буденні, нажаль, проблеми, пов'язані з відсутністю сертифікованої техніки для роздрукування необхідних документів, транспортні проблеми з доставляння документів до слідчого судді апеляційного суду, який на віддаленні 100 або 200 км. від населеного пункту й інші нормативні перепони, яких, нажаль, після останніх змін до КПК України тільки побільшало.

Тут же на противагу наводимо приклад найближчого західного сусіду Польщі, де законодавці, разом з керівництвом поліції працюють над підвищенням ефективності здійснюваних правоохоронних заходів. Зокрема, відповідно до ст. 20 Закону Республіки Польща про Поліцію ще від 6 квітня 1990 року підрозділи поліції мають право отримувати доступ за допомогою телекомунікаційних пристроїв до інформації, накопиченої у реєстрах без необхідності подавати письмові заяви [9]. Тобто підрозділи поліції отримують право здійснювати заходи, що тимчасово обмежують конституційні права громадян без рішення суду, напряму від операторів комунікацій, якщо для цього є відповідні підстави [10].

Звісно, відсутність такої можливості в Україні обурює оперативних працівників. Адже останні, поряд з організаційно-матеріальними складнощами оперативної роботи, вимушені лавірувати поміж численних нормативних перепон у документуванні злочинної діяльності. Навіть за таких умов, правозахисники стверджують про занадто широкі можливості оперативних служб щодо збору інформації про особу, що може становити загрозу порушення прав та свобод громадян у разі її витоку.

Виникає тоді закономірне питання: попередження тяжкого злочину чи затримання зловмисника, що є метою втручання у приватне спілкування зі сторони правоохоронних органів хіба менш важливе за необхідність навчання штучного інтелекту, який розробляє корпорація Google? Адже саме з цією метою Google

записує наші розмови, які здійснюються за допомогою програмних продуктів. Загроза витоку такої інформації чи потрапляння її до рук зловмисників також, нажаль, може мати місце [11].

Темп, з яким сьогодні вчиняються злочини та знищуються його сліди, особливо з застосуванням сучасних інформаційно-телекомунікаційних систем, порівнюється з швидкістю реагування правоохоронних органів в Україні так само, якби у змаганнях серед болідів формули 1 приймав участь поліцейський на велосипеді.

Проте надія є. Одним з прикладів успішного використання інформаційно-технічних досягнень в правоохоронній сфері була інформаційно-аналітична система «Сова», розроблена ще на початку 2000-х в УМВС України в Луганській області. Принциповою особливістю системи була інтеграція в єдиний інформаційний масив усіх наявних в УМВС відомчих інформаційних ресурсів (у тому числі масиви даних оперативно-розшукової діяльності) і бази даних інших відомств[12]. Ефективність використання системи забезпечувалась, перш за все, впровадженням у розробку сучасних інформаційних технологій (зокрема технології візуального аналізу даних, мультимедійних технологій, а також технології геоінформаційних систем). Повною мірою були реалізовані функції багатобазової структури: оператор системи міг підключити для забезпечення багатофакторного аналізу будь-яку базу даних, розташовану в будь-якій географічній точці. Система складала в одне ціле фрагменти інформації, отримані з різних джерел, та перетворювала їх у зрозумілі наочні графічні схеми[13, с. 265]

Завдяки відпрацьованим технологіям, за 9 місяців 2010 року тільки трьома співробітниками одного з підрозділів УІТ УМВС в Луганській області (відділу «ОРІОН») було розкрито 297 тяжких і особливо тяжких злочинів, розслідування яких традиційними методами виявилося невдалим (розслідування було припинено у зв’язку з невстановленням винного). Серед них – вбивства (зокрема подвійні), розбійні напади, грабежі, торгівля зброєю,

тяжкі наркозлочини і т.д. При цьому нерідко первинна інформація про злочинців спочатку взагалі була відсутня в інформаційних масивах – сама система була безпосереднім джерелом нової інформації про осіб [14, 15]. Загалом, тільки до 2009 року, за допомогою баз даних в УМВС Луганської області розкрито 5,3 тис. злочинів, що складає 70% від їх загальної кількості, розшукано 144 злочинці, встановлена особа 13 невпізнаних трупів й встановлена доля 53 безвісти зниклих осіб [16, С. 10].

Єдиним та основним «недоліком» даної системи, який не дозволив їй працювати на загальнодержавному рівні була її невідповідність тодішнім державно-політичним умовам. Адже можливості системи дозволяли в автоматичному режимі виявляти приховані зв'язки осіб, які займали високе положення у злочинній ієрархії й повідомляти про злочинні ризики у осіб, які займали відповідальні державні посади. Такі системи успішно діють у західних країнах та вдало виявляють корупційні правопорушення, але запровадження подібних в Україні тоді було не на часі. Зрештою, систему, під аггравовані лозунги захисту прав та свобод громадян, спочатку значно обмежили в можливостях, а потім, у 2014 році законсервували.

Таким чином, враховуючи сучасний рівень злочинності та наше стремління до євроінтеграції потрібно переглянути підходи до запровадження сучасних інформаційно-аналітичних систем у діяльність правоохоронних органів, зменшивши при цьому бюрократичний вплив на вказані процеси. Більше того, сучасний стан нормативно-правового забезпечення правоохоронної діяльності не дозволяє у повній мірі використовувати інформаційний потенціал згаданих систем оперативними підрозділами НП України, навіть у разі їх активного запровадження та використання, але це тема наступної доповіді.

1. Police. – 2001. – September. – P. 24–27.
2. Выявление преступников с помощью информационных технологий [Текст] // Борьба с преступностью за рубежом. Информбюллетень. – М: ВИНИТИ, 2003. – № 6. – С. 19-23.

3. Гуславский В.С. Информационно-аналитическое обеспечение раскрытия и расследования преступлений: монография [Текст] / В.С. Гуславский, Ю.А. Задорожный, Б.Г. Розовский. – Луганск: Элтон-2, 2008. – 287 с.
4. Поиск человека по фотографи – это реальность [Електронний ресурс] – Режим доступу: http://softopirat.com/main/399-poisk-cheloveka-po-fotografii-yeto-realnost.html. – Назва з екрану.
5. По фото в соцсети можно узнать о человеке все! [Електронний ресурс] – Режим доступу: http://3rm.info/publications/13829-po-foto-v-socseti-mozhno-uznat-o-cheloveke-vse.html. – Назва з екрану.
6. Создана программа для поиска человека в Интернете по фото [Електронний ресурс] – Режим доступу: http://zhzh.info/blog/2011-11-13-3096. – Назва з екрану.
7. Илюхин Олег В США втайне от граждан испытали технологию предсказания преступлений [Електронний ресурс] – Режим доступу:https://hitech.vesti.ru/article/781523/ – Назва з екрану.
8. Японская полиция будет использовать искусственный интеллект для предсказания преступлений [Електронний ресурс] – Режим доступу: http://tass.ru/obschestvo/4910175 – Назва з екрану
9. Ustawa z dnia 6 kwietnia 1990 r. o Policji. [Електронний ресурс] – Режим доступу: http://isap.sejm.gov.pl/DetailsServlet?id= WDU19900300179 – Назва з екрану.
10. Amnesty International. Польша: Новый закон о слежке станет серьёзным ударом по правам человека, AI индекс: EUR 37/3357/2016, 29 января 2016 [Електронний ресурс] – Режим доступу: https://www.amnesty.org/en/documents/eur37/3357/ 2016/en/ – Назва з екрану.
11. Константин Шиян. Google постоянно подслушивает вас через микрофон. Вот как найти эти записи! [Електронний ресурс] – Режим доступу: https://lifter.com.ua/628/Google-postoyanno-podslushivaet-vas-cherez-mikrofon-Vot-kak-nayti-eti-zapisi – Назва з екрану.
12. Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності: монографія [Текст] / [В.А. Буржинський, М.Г. Вербенський, В.С. Гуславський, В.М. та ін.]. – Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2009. – 110 с.
13. Орлов Ю.Ю. Застосування оперативної техніки в оперативно-розшуковій діяльності міліції (теорія і практика): монографія

[Текст] / Ю.Ю. Орлов. — К.: Київський нац. ун-т внутрішніх справ, 2007. – 559 с.
14. Задорожний Ю.А. Информационные технологии в ОРД: опыт и проблемы или проблемы и опыт? [Текст] / Ю.А. Задорожний, Б.Г. Розовский // Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. - 2011. – № 4. – 219-228
15. Бочковий О.В. Роль і місце автоматизованих систем в інформаційно-аналітичному забезпеченні прийняття рішень про проведення оперативно-розшукових заходів, що тимчасово обмежують конституційні права громадян [Текст] / О.В. Бочковий // Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. Спеціальний випуск. - 2011. – № 4. – С. 313-324.
16. Єфіменко В.В. Стислий аналіз оперативної обстановки в Луганській області та проблема підвищення професіонального рівня співробітників карного розшуку [Текст] / В.В. Єфіменко. // 90 років карному розшуку України та проблеми вдосконалення його діяльності в сучасних умовах боротьби зі злочинністю. / Вісник ЛДУВС ім. Е.О. Дідоренка Спец. Випуск № 2 у двох частинах. Частина 1. Луганськ, 2009. – С.10-13.

ОСОБЛИВОСТІ МЕТОДИКИ ОПИТУВАНЬ ІЗ ЗАСТОСУВАННЯМ ПОЛІГРАФА ПІД ЧАС РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ОРГАНАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Гарват Т.В.
курсант 4-го курсу факультету №1 ІПФПНП
Львівського державного університету внутрішніх справ

Серед усіх існуючих методів психофізіологічних досліджень поліграф залишається найбільш ефективним засобом виявлення приховуваної інформації. При цьому визначено, що на сьогоднішній день існує безліч методів психофізіологічних досліджень, а саме: електро- і магнітоенцефалографія; метод викликаних потенціалів; реєстрація електричної активності шкіри; реєстрація показників серцево-судинної системи; реєстрація реакції очей; дослідження нейродинамічних властивостей людини; самооцінка

психофізіологічного стану та, зрештою, поліграфологічні дослідження тощо [1].

Необхідність використання поліграфологічного опитування у правоохоронній діяльності під час розслідування злочинів обґрунтовує Т. Ф. Моїсєєва, визнаючи її одним з ефективних способів отримання ідеальних слідів відображення та орієнтовної інформації про злочинне діяння.

Аргументом, який доводить доцільність застосування поліграфа в практичній діяльності органів Національної поліції є швидкість обробки та аналізу отриманої інформації експертом-поліграфологом, об'єктивність результату психофізіологічного тестування із застосуванням поліграфа, яку досить важко одержати традиційними методами.

Окрім того, застосування поліграфа забезпечує отримання додаткової інформації, яка безпосередньо пов’язана з напрямом або об’єктом розслідування, прискорює його перебіг, забезпечує швидку, повну та об’єктивну оцінку достовірності, повідомленої особою, інформації, сприяє викриттю злочинів, що готуються [2, с. 336].

Поліграф здатен реєструвати такі психофізіологічні показниками, як: ритм дихання, рівень кров’яного тиску, інтенсивність потовиділення, а деякі детектори здатні, також, фіксувати напруженість голосових зв’язок, розширення капілярів, реакцію зіниць очей тощо. Можливість технічного пристрою охопити, проаналізувати та дослідити таку кількість психофізіологічних показників та змін в поведінкових реакціях опитуваної особи мінімізує можливість отримання помилкового результату при проведенні опитувань із застосуванням поліграфа під час розслідування злочинів органами Національної поліції.

Аналізуючи вищенаведене, необхідно звернути увагу на методику поліграфологічного опитування, в діяльності органів Національної поліції, під час розслідування кримінальних правопорушень. Під час вибору методики поліграфологічного опитування, необхідно зауважити, що на інформативність та достовірність отриманих даних можуть впливати безліч чинників. До

них, зокрема, відносяться: стан опитуваної особи, її психофізіологічні та психологічні особливості, прояв внутріщньоособистісних зв’язків, темперамент опитуваної особи тощо.

Під методикою опитування із використанням поліграфа розуміється певна сукупність дій, які визначають правила проведення кожного з етапів тестування та надають можливість встановити зв'язок між проявами фізіологічної активності опитуваного та достовірністю повідомленої ним інформації.

Отже, особливістю методики інструментальної діагностики емоційної напруги людини є процес актуалізації і вилучення ідеального сліду, який відбувається за допомогою технічного засобу – поліграфа, що призначений, зазвичай, для одночасної реєстрації більше ніж десяти психофізіологічних реакцій та процесів, пов’язаних з виникненням емоцій. В основі вищенаведеного методу лежить аналіз та оцінка показників, отриманих в результаті поліграфологічного опитування, під час впливу на емоційний стан опитуваної особи слів-подразників. Ефективність використання даного методу обґрунтовується страхом опитуваної особи перед можливим викриттям, що призводить до змін психофізіологічних функцій, які не піддаються її свідомому контролю, оскільки становлять фізіологічну складову (температура тіла, частота серцебиття, ритм та глибина дихання, ступінь м’язової напруги, біотопи мозку) [3, с. 96]. Саме така неможливість свідомого контролю емоційного та фізіологічного стану особою, під час поліграфологічного опитування, надає змогу полегшити процес збору, оцінки та перевірки інформації під час розслідування злочинів органами Національної поліції.

До найважливіших методик поліграфологічних досліджень, що характеризуються фіксованою сукупністю прийомів щодо спеціальних (нейтральних, значимих або перевірочних і контрольних)запитань, об’єднаних за певним логічним принципом можна віднести:

- методику перевірочних (значимих) і нейтральних запитань – МПНП (relevant and irrelevant question technique),

яка традиційно орієнтована на загальні ознаки певної теми й ґрунтується на спільному використанні значимих і нейтральних запитань. Базовий логічний принцип цієї методики полягає в тому, що у разі правдивих відповідей досліджуваного реакції на значимі і нейтральні запитання носитимуть приблизно однаковий характер, а при обмані значимі запитання викликатимуть більш виражені реакції, ніж нейтральні. Ця методика відрізняється простотою та надійністю результатів;

- методику контрольних запитань – МКП (control question technique), яка, як правило, використовує загальні ознаки тематики, що перевіряється, базуючись на спільному застосуванні нейтральних, значимих а також контрольних запитань. Базовий логічний принцип цієї методики полягає в тому, що в ході перевірки чесний випробовуваний буде більше стурбований контрольними запитаннями, на відміну від значимих, зважаючи на що і реакції на контрольні запитання носитимуть найбільш виражений характер, ніж значимі запитання, а у обманщика буде протилежна ситуація;
- методику (виявлення) приховуваної інформації – МПІ (concealedin form ation technique), яка базується на використанні приватних ознак досліджуваної теми, які мають бути однозначно відомі людині, що має відношення до неї. Базовий логічний принцип цієї методики полягає в тому, що безпосередньо пов'язаний з темою дослідження випробовуваний даватиме більш виражені реакції на істинні ознаки, ніж на неправдиві чи вигадані, а для особи, що не має відношення до теми дослідження і не має в розпорядженні відносно неї ніякої інформації, усі запитання будуть рівнозначні, і реакції на них будуть приблизно однакові [4, с. 336–338].

В свою чергу, методика поліграфологічного опитування об'єднуються у два класи: методика піку напруги і методика питань порівняння [5, с. 23].

Під поняттям методика піку напруги варто розуміти сукупність тестових процедур, що включають в себе тест з відомим рішенням, пошуковий тест, тест на виявлення приховуваної інформації та стимулюючий тест [6].

Методика питань порівняння – це загальна назва для стандартних тестових форматів, що поєднують в собі два ймовірних варіанти (правдивий і неправдивий). Методика питань порівняння складається із тесту Дж. Ріда, модифікованого тесту головних питань, тесту порівняння зон, тесту з позитивним контролем, тесту Юта, Азера, чотирьох-трекового тесту. Попри це, саме питання порівняння – це певний тип запитання, який використовується для виявлення реакцій, що порівнюються з реакціями на релевантні питання. Існує два основних типи запитань-порівняння: з прямою неправдою та з можливою неправдою. Підтипами для запитань-порівняння з прямою неправдою є тривіальне і персональне запитання. Запитання з можливою неправдою поділяються на виключні і невиключні [7, с. 189].

Отже, за наявності в пам'яті опитуваної особи ідеальних слідів відображення події минулого експерт-поліграфолог застосовує спеціальні стимули, які мають виявити інформаційні сліди відображення та дозволять визначити їх походження. Поліграф зафіксує стійкі психофізіологічні реакції в особи, яка проходить поліграфологічне опитування, а кількість повторів одного й того ж запитання експертом-поліграфологом у різних текстових варіаціях зменшить імовірність ознак випадкового збігу даних, отриманих на комп'ютерних поліграмах [8, с. 508–509].

Однак методика, що використовується під час поліграфологічного опитування дозволяють не лише визначити найбільш перспективні напрями виявлення та розслідування кримінального правопорушення, а й сприяють встановленню осіб не причетних до його вчинення. Застосування методики поліграфологічного опитування під час розслідування злочинів органами Національної поліції є надзвичайно важливим і допомагає визначити: достовірність показань опитуваної особи щодо обставин конкретного злочину; коло осіб, причетних до злочину, або тих, які мають

інформацію щодо конкретного кримінального правопорушення; місцеперебування матеріальних доказів на місцевості та в приміщенні; правдивість показань свідків, достовірність інформації, отриманої від потерпілих чи заявників тощо [9].

Підсумовуючи, необхідно зауважити, що задля ефективного використання методики поліграфологічного опитування та отримання достовірних результатів необхідно врахувати певні особливості. А саме той факт, що експерт-поліграфолог, на момент опитування, повинен володіти усією доступною інформацію про подію кримінального правопорушення, у зв'язку з розслідуванням якого проводиться опитування із використанням поліграфа. Зокрема така інформація може стосуватись анкетних даних особи, яка підлягає дослідженню на поліграфі, відомостей щодо проведення окремих слідчих (розшукових) дій. Це допоможе експерту-поліграфологу підготувати запитання для проведення опитування із врахуванням психофізіологічних особливостей опитуваної особи.

1. Методи психофізіологічних досліджень [Електронный ресурс]: Режим доступу: http://pidruchniki.com/10561127/psihologiya/metodi_psihofiziologichnih_doslidzhe
2. Салтевський М. В. Криміналістика (у сучасному викладі) : [навч. посіб.] / М.В. Салтевський. К. : Кондор, 2005. 588 с.
3. Клименко Н. Можливості використання в розслідуванні злочинів деяких нетрадиційних криміналістичних та спеціальних знань і методів / Н. Клименко, О. Клецов // Право України. 1998. № 1. С. 95-103
4. Князев В., Варламов Г. Полиграф и его практическое применение: учеб. пособие / В. Князев, Г. Варламов. М.: «Принт–Центр», 2012. 859 с.
5. Поповичев С.В. Взаимосвязь потребности в безопасности субъекта и вероятности распознавания лжи в опросе с использование мполиграфа: дис. … кандидита психолог. наук: 19.00.01 Сергей Владимирович Поповичев. М., 2011. 184 с.
6. Методологічні основи використання поліграфа для отримання доказової інформації при розслідуванні [Електронный ресурс]: Режим доступу: злочинів http://www.pap.in.ua/1_2014/83.pdf

7. Furgerson R. Polygraph police model for lawen forcement // Polygraph. – 1987. Vol. 16. – № 3. – P. 188-205.
8. Дідик В. Я. Огляд практики використання поліграфа («детектора брехні») / В. Я. Дідик, А. А. Бова // Президенту України, Верховній Раді України, Уряду України, органам центральної та місцевої виконавчої влади. – Київ : Рад. шк., 1999. Т. 12. С. 506–510.
9. Половникова Ж. Ю. Применение полиграфа в системе МВД Украины [Електронный ресурс] / Ж. Ю. Половникова. – Режим доступу: http://www.poligraph.com.ua/crimpol/article2.htm. – Загл. с экрана.

ДЕЯКІ ПИТАННЯ ВИКОРИСТАННЯ АНАЛІТИЧНОЇ РОЗВІДКИ В МЕРЕЖІ ІНТЕРНЕТ ПІД ЧАС ОПЕРАТИВНО-РОЗШУКОВОЇ ПРОТИДІЇ ЗЛОЧИНАМ У СФЕРІ ДЕРЖАВНИХ ЗАКУПІВЕЛЬ КРИМІНАЛЬНОЮ ПОЛІЦІЄЮ

Дараган В.В.
доцент кафедри оперативно-розшукової діяльності та спеціальної техніки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Сучасний світ інформаційних технологій та всеохоплююча інформатизація суспільства інтегрують кожного громадянина у мережу, хоче він того чи ні [1, с. 50]. Крім того, в мережі існує великий масив інформації про підприємства, установи та організації та їх власників, а у зв’язку з політикою відкритості роботи Уряду та державних установ в Україні з кожним роком збільшується об’єм інформації про державні підприємства, установи та організації державної форми власності. Наявність такого масиву інформації про об’єкти оперативного обслуговування зумовлює необхідність в здійсненні її пошуку, накопичення та аналізу з боку правоохоронних органів.

На сьогодні існують різноманітні методи збору інформації, що використовуються комплексно або окремо. Одним з таких є

розвідка відкритих джерел. Розвідка на основі відкритих джерел, яку ще називають Open source intelligence (OSINT) – одна з розвідувальних дисциплін. Включає в себе пошук, вибір і збір інформації, отриманої із загальнодоступних джерел і її аналіз. У розвідувальному співтоваристві термін «відкритий» вказує на загальнодоступність джерела (на відміну від секретних джерел та джерел з обмеженим використанням), він не пов'язаний з поняттям open source (відкрите програмне забезпечення) або public intelligence (громадська розвідка). За твердженнями аналітика ЦРУ Шермана Кента, висловленими у 1947 році, політики отримують до 80 відсотків інформації, необхідної їм для прийняття рішень в мирний час, з відкритих джерел [2]. Пізніше колишній керівник РУМО США (1976-1977), генерал-лейтенант Самуель Вілсон зазначав, що «90 відсотків розвід даних приходить з відкритих та відносно відкритих (конфіденційних) джерел і лише 10 – за рахунок роботи інших видів розвідки».

Специфічна категорія технічних і людських ресурсів, джерела інформації і методи їх збору – все це відрізняє OSINT від інших видів розвідки. До переваг OSINT, на відміну від інших видів розвідки, відносять доступність джерел інформації, обсяг джерел інформації, різносторонність, оперативність отримання, легкість подальшого використання і вартість отримання [3].

Відомо, що аналіз відкритих інформаційних джерел забезпечує одержання цінної інформації для правоохоронної діяльності. Очевидно, інформація, що представляє оперативний інтерес для правоохоронних органів, можу добуватися і шляхом контент-аналізу інформаційних ресурсів глобальних комп’ютерних мереж [4, с. 144].

В процесі протидії злочинам у сфері державних закупівель неабиякого значення для здійснення аналітичної діяльності набуває інформація наявна в мережі Інтернет, зазначене обумовлене наступними чинниками:

- уся інформація про заплановані та проведені торги знаходиться в мережі Інтернет у вільному доступі;

- наявність вільного доступ до значної кількості інформації, необхідної для аналізу законності проведення певного тендеру;
- уся інформація, яка надходить від замовників або учасників тендеру акумулюється на порталі prozorro.gov.ua;
- можливість пошуку необхідної інформації за ключовими словами через пошукові форми;
- можливість спілкування з можливими свідками без розшифрування своєї приналежності до правоохоронних органів;
- можливість отримання інформації про спосіб життя, коло спілкування фігурантів;
- можливість отримання інформації про злочини на інші правопорушення допущені під час проведення державної закупівлі, а також можливих свідків;
- можливість отримання інформації про способи вчинення злочинів у сфері державних закупівель;
- можливість отримання оперативно-значимої інформації анонімно, не викликаючи підозри у зацікавлених осіб;
- можливість швидко та безоплатно отримати довідкову інформацію;
- можливість збору оперативно-значимої інформації щодо діяльності окремих суб'єктів господарювання.

Виходячи з зазначеного, на нашу думку, аналітична розвідка в мережі Інтернет повинна стати однією із пріоритетних складових інформаційно-аналітичної роботи в процесі протидії злочинам у сфері державних закупівель підрозділами захисту економіки Національної поліції України.

З одного боку, очевидним є факт того, що глобальна мережа Інтернет активно заповнює інформаційний простір у всіх державах та на всіх континентах, є активним засобом формування інформаційного суспільства в Україні. Інтернетом користуються для роботи, розваг або спілкування в чатах і форумах [5, с. 3].

Найбільш ефективним напрямком інформаційного пошуку в мережі Інтернет для підрозділів захисту економіки Національної поліції є оперативний моніторинг інформаційних ресурсів, що представляє систему спостереження за станом кримінальних процесів або відомостей про такі процеси, що містяться в мережі Інтернет з використанням засобів і методів оперативно-розшукової діяльності для їх подальшого аналізу з метою протидії криміналітету [6, с. 77].

Як показали результати дослідження І.І. Карташова та С.А. Постолова вказана діяльність може здійснюватися за наступними напрямами:

1. Здійснення пошуку по інформаційних ресурсів глобальних комп'ютерних мереж з використанням пошукових систем.
2. Пошук інформації щодо окремих осіб, що представляють оперативний інтерес, що розміщується ними на своїх сторінках в соціальних мережах.
3. Застосування контент-аналізу.
4. Безпосереднє спостереження за місцями мережевого спілкування, яке передбачається постійне вивчення повідомлень, що публікуються в чатах, форумах, конференціях.

Окрім запропонованих науковцями напрямів здійснення моніторингу в мережі Інтернет, на нашу думку, в процесі здійснення аналітичної розвідки в мережі Інтернет під час оперативно-розшукової протидії злочинам у сфері державних закупівель доцільно здійснювати моніторинг за наступними напрямками:

1. Моніторинг публікацій у засобах масової інформації;
2. Моніторинг інформації щодо проведення державних закупівель (за предметом закупівлі; за розпорядником державних (бюджетних) коштів; за учасником тендеру тощо);
3. Моніторинг змін нормативно-правового регулювання здійснення державних закупівель та бюджетного законодавства;
4. Пошук інформації щодо окремих юридичних осіб, що представляють оперативний інтерес.

У наш час, в умовах стрімкого розвитку інформаційних технологій, постійного збільшення обсягу інформаційних ресурсів, постають задачі швидкого та коректного пошуку потрібної інформації [7].

І.Ф. Хараберюш та О.І. Хараберюш в процесі дослідження питання використання Інтернету як джерела оперативно-значимої інформації пропонують використовувати наступні інформаційні ресурси Інтернету [8, с. 110]:

1. Каталоги – це рубрика тори або класифікатори, які систематизують велику кількість документів, що значно полегшу пошук інформації.
2. Пошукові системи, які здійснюють різне маніпулювання з інформацію: індексування тексту та пошук по одному чи декільком ключовим словам; морфологічний пошук – ототожнювання різних граматичних форм; ранжування щодо відповідності документа запиту.
3. Онлайнові бази даних.
4. Форуми та чати.

Отримана з вказаних джерел інформація слугує основою для здійснення аналітичної роботи. При цьому, в процесі здійснення аналізу, як правило здійснюється співставлення наявної інформації з різних джерел у тому числі й оперативних.

В процесі здійснення аналітичної розвідки в мережі Інтернет під час оперативно-розшукової протидії злочинам у сфері державних закупівель відносно конкретної інформації щодо розпорядника державних (бюджетних) коштів, учасника торгів або окремо взятою фізичної особи в першу чергу доцільно використовувати наявні в мережі пошукові системи.

Пошукова система – це автоматизована інформаційна система (програмно-апаратний комплекс із веб-інтерфейсом), що надає можливість пошуку інформації в Інтернеті у відповідності до запиту користувача [9].

Областю використання пошукових систем є мілліарди сторінок Інтернет. При цьому приблизно мільйон сторінок додається

щодня і стільки ж оновлюється, а всі дані, що на них містяться, представляються різними цифровими форматами. Стрімкий приріст вмісту глобальної мережі Інтернет ставить лідерів пошукових послуг та розробників програмних технологій перед необхідністю знаходити нові механізми, ресурси та алгоритми, які б забезпечували належний рівень швидкості та якості обробки різноманіття користувацьких запитів [10, с. 83].

Згідно з даними gs.statcounter.com станом на листопад 2017 року в Україні майже 90 % користувачі під час пошуку інформації в мережі інтернет використовують пошуковий сервіс компанії Google (www.google.com.ua) [11].

Виходячи з зазначеного, в процесі використання аналітичної розвідки в мережі Інтернет під час оперативно-розшукової протидії злочинам у сфері державних закупівель працівникам підрозділів захисту економіки Національної поліції України, доцільно використовувати пошуковий сервіс компанії Google.

Отже, використання аналітичної розвідки в мережі Інтернет є складовою і невід'ємною частиною оперативно-розшукової протидії злочинам у сфері державних закупівель кримінальною поліцією від ефективності здійснення такої діяльності щодо збирання й аналізу оперативно-значимої інформації багато в чому залежить успіх вирішення тактичних та стратегічних задач протидії злочинам у зазначеній сфері.

1. Бочковий О.В. Можливості та перспективи використання аналітичної розвідки в умовах відкритого суспільства / О. В. Бочковий // Південноукраїнський правничий часопис. - 2016. - № 2. - С. 49-52.
2. Ромачев Н.Р. Конкурентная разведка / Н.Ю. Нежданов. – М. : Ось-89, 2007. – 375 с.
3. Шурат Т.Г. Деякі аспекти розвідки з відкритих джерел інформації (OSINT) / Т.Г. Шурат, А.О. Смук // Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики : матеріали Всеукр. наук.-практ. конф. (Дніпро, 20

жовт. 2017 р.) : у 2-х ч. – Дніпро : Дніпроп. держ. ун-т внутр. справ, 2017. – Ч. 1. – С. 126-128.
4. Хараберюш І.Ф., Мацюк В.Я., Некрасов В.А., Хараберюш О.І. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій: Монографія. – К.: КНТ, 2007. – 196 с.
5. Бабічев Д.О. Інформаційно-аналітичне супроводження протидії злочинам загальнокримінальної спрямованості з використанням інтер-нет-мереж // Співпраця поліції/міліції зі службами безпеки Інтернет-сайтів (аукціонів, соціальних мереж тощо) у боротьбі з інтернет-злочинністю на підставі національного законодавства та законодавства, яке діє у Європейському Союзі: тези доповідей міжнародної науково-практичної конференції (Хмельницький, 16-17 листопада 2010 року) / МВС України, УМВС України в Хмельницькій області. – Хмельницький: УМВС, 2010. – С. 2-6.
6. Карташов И.И. Информационные ресурсы сети Интернет как источник оперативно-розыскной информации о состоянии оперативной обстановки / И.И. Карташов, С.А. Постолов // Вісник Луганського університету внутрішніх справ імені Е.О. Дідоренка. Спеціальний випуск. – № 2. – 2011. Частина 2. – С. 75-81.
7. Полянко А. Особенности поисковой системы Google [Електронний ресурс] / А. Полянко // Site-seo.ru – поисковая оптимизация и интернет-маркетинг – Режим доступу: http://site-seo.ru/info/seostati/GoogleMSNYa/40/.
8. Хараберюш І.Ф. Інтернет та локальні мережі як джерело отримання оперативно-значимої інформації / І. Ф. Хараберюш, О.І. Хараберюш // Вісник Луганського державного університету внутрішніх справ. 2007. Спец. вип. № 1. У 2 ч. Ч. 1: Удосконалення оперативної розробки об'єктів ОРД оперативними підрозділами органів внутрішніх справ у сучасних умовах. - Луганськ : Луган. держ. ун-т внутр. справ / державний університет внутрішніх справ Луганський ; голов. ред. Е. О. Дідоренко, 2007. - С. 108-113.
9. Максимов Н. В. Информационные ресурсы и поисковые системы / Н. В. Максимов, О. Л. Голицына, Г. В. Тихомиров, П. Б. Храмцов, М: МИФИ, 2008. – 400 с.
10. Яшина К.В. Розробка сучасної інформаційно-пошукової системи математичне моделювання / К.В. Яшина, К.М. Ялова, В.В. Завгородній // Науковий журнал «Математичне моделювання», Кам'янське, – № 2 (29), 2013. – С. 83-86.

11. Search Engine Market Share Ukraine [Електронний ресурс]. – Режим доступу: http://gs.statcounter.com/search-engine-market-share/all/ukraine.

НОРМАТИВНО-ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Дідик Н.І
доцент кафедри адміністративного права та адміністративного процесу факультету №3 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Інформаційна безпека відіграє важливу роль у забезпеченні інтересів будь-якої держави. Створення розвиненого і захищеного інформаційного середовища є неодмінною умовою розвитку суспільства та держави. Останнім часом в світі відбуваються якісні зміни у процесах управління, зумовлені інтенсивним впровадженням сучасних інформаційних технологій. Разом з цим посилюється небезпека несанкціонованого втручання в роботу інформаційних систем, і вагомість наслідків такого втручання дуже сильно зросла. Як наслідок, в багатьох країнах все більше уваги приділяється проблемам захисту інформації та пошуків шляхів її вирішення.

Країни, які не можуть забезпечити власну інформаційну безпеку, стають неконкурентоспроможними і, як наслідок, не можуть брати участь у боротьбі за розподіл ринків та ресурсів. Тому, незаперечним є те, що в будь-якій розвиненій країні має існувати система забезпечення інформаційної безпеки, а функції та повноваження відповідних державних органів повинні бути закріплені законодавчо.

Поняття інформаційної безпеки включає в себе з одного боку забезпечення якісного інформування громадян та вільного доступу до різних джерел інформації, а з іншого - контроль за непоширенням таємної інформації, сприяння цілісності суспільства,

захисту від негативних інформаційних впливів тощо. Рішення цієї комплексної проблеми дозволить як захистити інтереси суспільства і держави, так і сприяти реалізації права громадян на отримання всебічної та якісної інформації.

Проблема ефективного забезпечення безпеки інформації в державі передбачає вирішення таких масштабних задач, як: розроблення теоретичних основ забезпечення безпеки інформації; створення системи органів, відповідальних за безпеку інформації; вирішення проблеми керування захистом інформації і її автоматизації; створення нормативно-правової бази, що регламентує рішення всіх завдань забезпечення безпеки інформації; налагодження виробництва засобів захисту інформації; організація підготовки відповідних фахівців та ін [1].

У всіх складових національної безпеки: політичної, економічної, військової та інших, вага інформаційної складової безперервно зросте. Інформаційна безпека відіграє все більш значущу роль в загальній системі забезпечення національної безпеки країни. Це прямо зазначено в Стратегії розвитку інформаційного суспільства в України та закріплено в її принципах.

Метою реалізації Стратегії є формування сприятливих умов для розбудови інформаційного суспільства, соціально-економічного, політичного і культурного розвитку держави з ринковою економікою, що керується європейськими політичними та економічними цінностями, підвищення якості життя громадян, створення широких можливостей для задоволення потреб і вільного розвитку особистості, підвищення конкурентоспроможності України, вдосконалення системи державного управління за допомогою інформаційно-комунікаційних технологій.

Для розвитку інформаційного суспільства необхідно застосовувати принципи:

- рівноправного партнерства державних органів, громадян і бізнесу;
- правомірності одержання, використання, поширення, зберігання та захисту інформації;

- гарантованості права на інформацію, вільного отримання та поширення інформації, крім обмежень, установлених законом;
- прозорості та відкритості діяльності державних органів;
- свободи вираження поглядів і переконань;
- інформаційної безпеки;
- постійного навчання;
- підконтрольності та підзвітності державних органів громадськості;
- сприяння пріоритетному розвитку інформаційно-комунікаційних технологій;
- чіткого розмежування повноважень і скоординованої взаємодії державних органів;
- гарантованості повного ресурсного забезпечення національних програм та проектів розвитку інформаційного суспільств [2].

Інформаційну безпеку слід розглядати як політико-правову категорію, що виражає зв'язок між інтересами особистості, суспільства та держави у сфері інформації і правовим забезпеченням їх захисту. Це стан захищеності особи, суспільства та держави в інформаційному просторі, захист інформації, інформаційних ресурсів і інформаційно-телекомунікаційної інфраструктури від можливих внутрішніх і зовнішніх загроз.

Національна політика розвитку інформаційного суспільства в Україні ґрунтується на засадах: пріоритетності науково-технічного та інноваційного розвитку держави; формування необхідних для цього законодавчих і сприятливих економічних умов; всебічного розвитку загальнодоступної інформаційної інфраструктури, інформаційних ресурсів та забезпечення повсюдного доступу до телекомунікаційних послуг та ІКТ; сприяння збільшенню різноманітності та кількості електронних послуг, забезпеченню створення загальнодоступних електронних інформаційних ресурсів; поліпшення кадрового потенціалу; посилення мотивації щодо використання ІКТ; широкого впровадження ІКТ в науку, освіту, культуру, охорону здоров'я, охорону навколишнього середовища; забезпечення інформаційної безпеки. Така політика передбачає:

- перехід до пріоритетного науково-технічного та інноваційного розвитку;
- законодавче забезпечення розвитку інформаційного суспільства;
- формування сприятливих економічних умов розвитку інформаційного суспільства;
- розвиток загальнодоступної інформаційної інфраструктури;
- забезпечення повсюдного доступу до телекомунікаційних послуг та інформаційних ресурсів;
- сприяння збільшенню різноманітності та кількості електронних послуг;
- забезпечення створення загальнодоступних електронних інформаційних ресурсів;
- підготовка людини для роботи в інформаційному суспільстві;
- створення системи мотивацій щодо впровадження і використання ІКТ;
- наука та культура в інформаційному суспільстві;
- охорона здоров'я в інформаційному суспільстві;
- охорона навколишнього природного середовища;
- інформаційна безпека в інформаційному суспільстві [3].

Законодавство про інформаційну безпеку входить у систему інформаційного законодавства та регулює відносини у вказаній сфері. Розвиток національного законодавства у зазначеній сфері розпочався після прийняття 1994 року Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»[4].

Необхідність адаптації національного законодавства до вимог Європейського Союзу зумовлює інтенсивний розвиток інформаційного законодавства, зокрема про інформаційну безпеку, за різними напрямами (прийняті закони України «Про захист персональних даних»,[5] «Про електронний цифровий підпис»,[6] «Про внесення змін до деяких законодавчих актів України щодо інсайдерської інформації» тощо) [7].

Водночас доцільно зауважити на неврегульованість відносин щодо забезпечення інформаційної безпеки в різних сферах життя суспільства. З огляду на це є доцільним реформування законодавства у сфері забезпечення інформаційної безпеки. Це повинно охоплювати систематизацію чинних законів, законодавче закріплення визначень низки термінів, принципів, засад державної політики в сфері забезпечення інформаційної безпеки, врегулювання проблем, пов'язаних із охороною службової таємниці, протидією інформаційному екстремізму, тощо [8, с. 246].

Деякі зазначені аспекти відображено у Стратегії національної безпеки України [9] та Доктрини інформаційної безпеки України [10]. Водночас реформування можливе на теоретичній основі, що вимагає обґрунтування природи, структури та місця інституту правового забезпечення інформаційної безпеки в системі права.

Для організації взаємодії органів Національної поліції із засобами масової інформації та громадськістю з метою інформування населення про результати роботи поліції у боротьбі зі злочинністю та підтримання публічного порядку і безпеки в державі, профілактику правопорушень, формування позитивного іміджу поліції, популяризацію професії поліцейського в системі поліції було створено Департамент комунікації. Підрозділом напрацьовано сталу систему інформування населення про діяльність Національної поліції. Для представників ЗМІ не рідше одного разу на тиждень організовуються брифінги та прес-конференції за участю керівництва, надається сприяння в отриманні коментарів посадових осіб, іншої актуальної інформації. До послуг журналістів та громадськості – широкий спектр інформації, яка щоденно розміщується на офіційному веб-сайті в мережі Інтернет та розсилається електронними мережами в десятки редакцій ЗМІ [11].

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та

вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави. Для захисту інтересів держави Президент 15 березня 2016 року затвердив Стратегію кібербезпеки України. Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [12].

Щодо завдань Національної поліції Україниу сфері забезпечення інформаційної безпеки у контексті діяльності засобів масової інформації, то вони обумовленні Указами Президента України від 03.05.2014 № 449/2014 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [13] та 26 травня 2015 року № 287/2015 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» [9] та конкретизовано в наказі МВС України від 19.08.2014 № 840 «Про деякі питання інформаційної безпеки України» [14].

---

1. Аналіз головних складових інформаційної безпеки держави / Степко Олександр Михайлович. - [Електронний ресурс]. – Режим доступу: file:///C:/Users/Nataly/Downloads/3214-8602-1-PB.pdf

2. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: розпорядження Кабінету Міністрів України від 15.07.2013 р. №386. - [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/386-2013-р.
3. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007р. // Офіційний вісник України. – 2007. – № 8. – Ст. 345 .
4. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94 // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.
5. Про захист персональних даних: Закон України від 07.07.2010р. // Офіційний вісник України. - № 49. – 2010. - Ст. 199.
6. Про електронний цифровий підпис: Закон України від 04.07.2003 р. // Офіційний вісник України. – № 25. – 2003. - Ст. 111.
7. Про внесення змін до деяких законодавчих актів України щодо інсайдерської інформації: Закон України від 22.04.2011 р. № 3306-VI // Відомості Верховної Ради України. – 2011. – № 44. – Ст. 471.
8. Ярема О.Г., Єсімов С.С. Предмет правового забезпечення інформаційної безпеки в інформаційному праві // О.Г. Ярема, С.С. Єсімов / Науковий вісник ЛьвДУВС. - №2. – 2016. - 244-252 с.
9. Про Стратегію національної безпеки України: Указ Президента України від 26.05.2015 р. № 287/2015. - [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/287/2015
10. Про Доктрину інформаційної безпеки України: Указ Президента України від 29.12.2016 р. 47/2017. - [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents /472017-21374
11. Про затвердження Положення про Департамент комунікації Національної поліції України: Наказ Національної поліції України від 04.12.2015 р. №145. - [Електронний ресурс]. – Режим доступу: http://old.npu.gov.ua/mvs/control/main/uk/publish /article/1854459
12. Стратегія кібербезпеки України: Указ Президента України від 15.03.2016 р. 96/2016. - [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/96/2016
13. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Указ Президента України від 3 травня 2014 р. № 449. - [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/ru/documents/17823.html.

14. Про деякі питання інформаційної безпеки України: Наказ МВС 19.08.2014 р. №840. - [Електронний ресурс]. – Режим доступу: http://consultant.parus.ua/?doc=09K5IACFBB

ІМПЛЕМЕНТАЦІЯ МЕТОДІВ АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ В ДІЯЛЬНІСТЬ ОРГАНІВ ПРАВОПОРЯДКУ УКРАЇНИ В УМОВАХ ІНТЕГРУВАНЯ ДО ЄВРОПЕЙСЬКОГО СПІВТОВАРИСТВА

Заєць О.М.
завідувач кафедри криміналістики, судової медицини та психіатрії Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Рушійною силою світових процесів є інформація, при цьому у сфері боротьби зі злочинністю та її запобігання необхідно приймати рішення на основі точної та актуальної інформації. Це – визначальний чинник, який зумовлює досягнення позитивного результату і дозволяє всім працівникам органів правопорядку, які ведуть боротьбу зі злочинністю, бути на крок попереду злочинців. Тому вже недостатньо мати лише первинну інформацію. Дані необхідно збирати, зіставляти та інтерпретувати, з метою проведення оцінювання, прогнозування, створення рекомендацій та висновків. Іншими словами, відразу після отримання інформації у первинній формі відповідні спеціалісти повинні провести її через аналітичні рівні, щоб створити оперативно-аналітичну інформацію.

Поліцейська аналітична діяльність – це модель аналітичної діяльності, що сконцентрована на допомозі у прийнятті рішень для працівників органів правопорядку, базуючись на процесі аналізу інформації та поширенні даних. [1]

Оперативно-аналітичний цикл є базовою основою поліцейської аналітичної діяльності як результат збирання даних, їх структурування, оцінки та аналізу. Цей процес може бути виконаний з використанням комп'ютерного програмного забезпечення, що

дозволяє спростити збирання даних. Для того, щоб інформація набула статусу оперативно-аналітичної, вона повинна бути аналізована досвідченим аналітиком із застосуванням спеціальних методик. Простіше кажучи, це модель поліцейської діяльності, згідно з якою оперативно-аналітична інформація слугує підставою для проведення операцій або розслідувань, а не навпаки.

Надаючи аналітикам можливість опрацьовувати дані про злочини, працівники органів правопорядку отримують можливість використовувати готовий оперативно-аналітичний продукт, а не первинну інформацію. При цьому вони отримують такі переваги: по-перше, продукт окреслює конкретно тенденції злочинності не лише за географічною ознакою, а й у часових рамках; по-друге, у зв'язку з тим, що продукт надає можливість мати більше інформації щодо місць ймовірного скоєння злочинів, більше часу та зусиль можливо витратити на попередження скоєння злочинів; по-третє, оскільки час витрачається більш продуктивно, співробітники мають більше можливостей у наданні допомоги своїм колегам у разі потреби.

Прикладом впровадження нової інтелектуальної моделі поліцейської діяльності, керованої аналітикою є аналітичний продукт, який запроваджений у м. Харків де була проведена оцінка ІТ-додатку «Інтелектуальна система кримінального аналізу у режимі реального часу» (R.I.C.A.S.).

Система RICAS розроблена для відображення та аналізу даних та інформації, які містяться в системі «АРМОР» та в інших базах даних, і є інструментом, який забезпечує швидке прийняття рішень. Додаток доступний у публічному та обмеженому режимі. Останній доступний лише підрозділам поліції, за допомогою використанням VPN-з'єднання за протоколом шифрування SSL.

Ця система може забезпечити доступ до наступних баз даних та інформації: бази даних поліції про скоєні злочини, інформація кримінального характеру та реєстрації подій, GPS-даних, даних про безвісно зниклих осіб та осіб, що перебувають у розшуку, та осіб, які відбували покарання, державні реєстри тощо. Зазначений

обсяг інформації можна використовувати у поєднанні з різними видами інших даних та інформації, зображеннями, що свідчать про скоєння злочину або порушень громадського порядку, введеними в систему в ручному режимі працівниками правоохоронних органів, а також забезпечений доступ до камер відеоспостереження, встановлених у місті, в режимі реального часу.

Пошук (вибірка) необхідної інформації здійснюється за допомогою декількох опцій шляхом індексації зі всього контенту системи RICAS, що забезпечує швидкий та точний пошук інформації для аналізу.

Система має декілька стандартних аналітичних опцій. Користуючись цією системою, аналітики поліції Харкова можуть проводити базовий аналіз, готувати звіти щодо профілю підозрюваних та рівня злочинності на окремих територіях.

Безумовно, цю систему можна використати на державному рівні в якості платформи для аналітичного супроводу та підтримки процесу прийняття рішень разом з іншими аналітичними ІТ-системами. Однак існує проблема, яка полягає у відсутності процедур та робочих методологій у сфері збирання, оброблення, аналізу та, що не менш важливо, поширення/розповсюдження даних/звітів.

Крім того, невідомо яким чином аналітичні звіти, підготовлені з використанням системи RICAS будуть відповідати стандартам та процедурам, передбаченим моделлю поліцейської діяльності, керованою аналітикою. Необхідно врахувати цей аспект під час розвитку та розбудови або можливого впровадження цього програмного забезпечення на національному рівні.

Ця платформа була розроблена для використання через мережу Інтернет. У зв’язку з чим вбачається, що відсутні чіткі процедури доступу до персональних даних. Також вбачається, що не застосовується принцип «необхідних знань» (принцип службової необхідності) тоді, коли йдеться про доступ до певної категорії даних.

Ще однією проблемою може виявитися сумісність цієї системи з іншими системами. Функція імпорту даних системи RICAS

інтегрована в цю систему і є напівавтоматичною (потребує додаткового програмного забезпечення на етапі зіставлення даних з іншими системами).

Система «ОРІОН» містить всю інформацію з обмеженим доступом (грифом) з агентурних повідомлень та оперативно-розшукових справ. Лише 5 осіб на рівні Центрального апарату мають доступ до цієї системи, і лише ці особи мають право вносити в цю систему та обробляти з її допомогою інформацію, зібрану у паперовій формі. У тому разі, коли у оперативних департаментів виникає необхідність у отриманні даних та інформації щодо об'єктів/фігурантів, внесених у систему «ОРІОН», вони повинні надіслати письмовий запит до Департаменту інформаційної підтримки.

Що стосується робочих процесів та доступу до інформації на регіональному рівні, тут склалася така ж сама ситуація, що й на національному рівні, але доступ до даних та інформації гарантовано надається лише тому регіону, якому вони належать. Якщо підрозділ регіонального рівня бажає отримати дані та інформацію національного рівня, до Департаменту інформаційної підтримки надсилається відповідний письмовий запит.

Система «АРМОР» містить всі дані та інформацію, зібрану всіма підсистемами департаментів: звіти про правопорушення, стислі результати огляду місця події, інформацію про осіб, що перебувають у розшуку, незначні інциденти, ДТП тощо. Адміністрування та супровід системи «АРМОР» також здійснює Департамент інформаційної підтримки, при цьому департаменти мають доступ лише до інформації, зібраної в їхніх підсистемах. Доступ до інших даних та інформації в системі здійснюється через Департаменту інформаційної підтримки.

Відтак, перспективність подальшого розвитку інтелектуальної моделі поліцейської діяльності, керованої аналітикою вбачається в розробці теоретико-методологічних засад його прикладного використання. Успішна реалізація та впровадження нових методів кримінального аналізу дасть можливість у майбутньому її

поширити на всю систему Національної поліції України та активно використовувати аналітичні способи та прийоми, завдяки яким можливо забезпечити виконання завдань органів досудового розслідування щодо ефективного розслідування кримінального провадження, створить передумови для більш ефективного виконання суб'єктами оперативно-розшукової та слідчої діяльності своїх завдань та правоохоронних функцій, що, у свою чергу, сприятиме підвищенню ефективності протидії злочинності.

1. Основи кримінального аналізу : посібник з елементами тренінгу / О.Є. Користін , С.В. Албул, А.В. Холостенко, О.М. Заєць та ін. – Одеса : ОДУВС, 2016 – 112 с.
2. Албул С.В. Кримінальна розвідка як функція оперативно-розшукової діяльності: Європейський досвід та Українські перспективи / С.В. Албул // European Reforms Bulletin: international scientific peer-reviewed journal: Grand Duchy of Luxembourg. – 2015. – № 2. – P. 2-6.
3. Власюк О.В. Роль і місце кримінального аналізу у розкритті та розслідуванні злочинів на державному кордоні України [Текст] / О. В. Власюк // Матеріали постійно діючого науково-практичного семінару – Х. : Інститут підготовки юрид. кадрів для СБУ Нац. юрид. акад. України ім. Я. Мудрого, 2011. – Випуск № 3. – Частина № 1. – С. 82-85.
4. Zaiets O.M. Application software IBM I2 ANALYST'S NOTEBOOK in law enforcement Ukraine for pretrial investigation of criminal offenses / O.M. Zaiets // European Reforms Bulletin. − 2016. − № 1. − P. 82-87.
5. Махнюк, А.В. Теоретичні основи провадження кримінального аналізу у сфері правоохоронної діяльності [Текст] / А. В. Махнюк // Науковий вісник Державної прикордонної служби. – 2011. – № 94. – С. 3-7.
6. Некрасов В.А. Сучасне розуміння кримінальної розвідки як напряму діяльності правоохоронних органів / В.А. Некрасов // Кримінальна розвідка: методологія, законодавство, зарубіжний досвід: матеріали Міжнародної науково-практичної конференції (м. Одеса, 29 квітня 2016 р.). – Одеса: ОДУВС, 2016. – С. 19-20.

ПЕРСПЕКТИВИ РОЗВИТКУ БІОМЕТРИЧНОГО РИНКУ ТА РІЗНИХ ТИПІВ ТЕХНОЛОГІЙ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ ТА ІДЕНТИФІКАЦІЇ

Захаров В.П.
професор кафедри ОРД факультету №2 ІПФПНП
Львівського державного університету внутрішніх справ,
доктор юридичних наук, професор

Захарова О.В.
доцент кафедри криміналістики, судової медицини та
психіатрії факультету №1 ІПФПНП
Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент

Біометрія швидко набуває індустріальних рис. Це промислові масштаби виробництва, багатомільйонні замовлення державних і комерційних структур, формування професійного співтовариства.

На цьому ринку зростає сегментація і диверсифікація; зростають потреби у стандартизації та уніфікації; загострюється конкуренція, активізуються процеси об'єднань і поглинань. Та, незважаючи на існуючі розбіжності перспективної оцінки обсягу світового біометричного ринку, всі дослідницькі та консалтингові фірми вважають – буде збережена загальна тенденція до подальшого зростання біометричного ринку.

Найближчими роками три великі біометрики (технології ідентифікації за відбитками пальців, обличчям, райдужною оболонкою ока) збережуть домінуючі позиції, але загалом їхня сукупна частка знижуватиметься. Однак передбачається, що до 2018 р. популярність райдужної технології поступиться лише популярності ідентифікації за відбитками пальців, а на третє-четверте місце за популярністю можуть вийти методи ідентифікації людину за голосом.

Але ставити питання: яка ж технологія біометричної ідентифікації краща, – не можна. Адже все залежить від конкретної сфери її застосування. Наприклад, ідентифікацію особи у повній темряві (якщо в цьому є необхідність), краще здійснювати за голосом, а застосування методик, що використовують відбитки пальців, 3-D зображення обличчя або унікальний малюнок райдужної оболонки ока найчастіше використовують під час виготовлення документів, які посвідчують особу, в програмах супроводу авіапасажирів, які часто мандрують, під час перетинання кордону та в інших випадках.

Несподіванкою можна вважати зниження оцінки перспектив технологій розпізнавання за обличчям на тлі загальносвітового поширення біометричних документів, які посвідчують особу і де цей ідентифікатор поки що є обов'язковим. Негативний прогноз вочевидь обумовлений труднощами, які виникли під час практичної реалізації привабливої ідеї інтегрувати ідентифікацію за обличчям з системами відеоспостереження. У доповіді Європейської комісії був зроблений висновок, який стосується технології розпізнання за обличчям: Точність знижується, коли реєстрація і подальша ідентифікація виявляються віддалені у часі. Вбачається, що буде потрібна регулярна перереєстрація через певний час.

Але практично всі фахівці з біометрії вважають, що такі системи «прийшли, щоб залишитися». У деяких ситуаціях вони досить ефективно працюють сьогодні, але загалом стрімкий прогрес таких технологій очевидний і він відбувається дуже швидко.

Позитивною новиною є значне зміцнення позицій засобів ідентифікації за малюнком вен у сфері банківських технологій. Але необхідно зазначити, що нині набула поширення ідентифікація за малюнком вен поки що тільки в Японії. Крім того, проблеми може створити і боротьба, що посилюється, між двома конкретними видами імплементації цієї технології (сканування малюнка вен на долоні та на пальці).

Останнім часом позитивні перспективи отримали також засоби ідентифікації за голосом – вони набувають дедалі більшого поширення, особливо у фінансовій сфері (телефонний банкінг тощо) і в складі автоматизованих кол-центрів.

Щодо сегментації галузевого ринку, то фахівці були одностайні в своїх висновках про те, що найпопулярнішими були та залишаються системи, які реалізують технології ідентифікації за відбитками пальців і за обличчям; третє й четверте місця ділять рішення, що засновані на розпізнаванні користувачів за малюнком вен і голосом.

Головними причинами, що перешкоджають подальшому й ще більшому поширенню біометричних систем, учасники опитування вважають їхню досить високу вартість і слабку поінформованість осіб, котрі ухвалюють рішення про переваги біометричних технологій.

Розглянемо деякі особливості розвитку державного та корпоративного секторів біометричного ринку.

Державний сектор у перспективі буде ключовим замовником біометричних компаній і головним рушієм ринку. Але він зумовлює в основному екстенсивний розвиток галузі. Разом із традиційним використанням біометричної ідентифікації в криміналістичних цілях сьогодні біометрія активно запроваджується в прикордонному контролі й у зв'язку з цим завершується масовий перехід до паспортно-візових документів нового покоління; без біометричних технологій неможливо уявити сучасні національні ідентифікаційні картки та інші ідентифікаційні документи (наприклад, посвідчення державних службовців, водійські посвідчення нового типу). У майбутньому в більшості країн держсектор і суспільний сектор повинні збільшити свою частку через реалізації програми так званого електронного урядування.

Корпоративний або комерційний сектор стимулює інтенсифікацію розробок нових продуктів і послуг. Разом зі збереженням традиційного інтересу до біометричних рішень щодо забезпечення інформаційної безпеки, контролю фізичного доступу і ведення обліку робочого часу комерційні структури зараз відчувають нагальну потребу в ефективних системах управління ідентифікацією користувачів фінансових послуг, заохочення купівельної лояльності, обслуговування пасажирів транспорту (насамперед авіаційного).

Як самостійний сегмент можна виокремити так званий «*суспільний»* (тобто в основному некомерційний) *сектор*. Найважливішими споживачами якого є освітянські установи, наукові організації, культурні та медичні установи.

Останнім часом стрімко збільшує свою частку на ринку «*споживчий» сектор* (consumer ID), де засоби біометричної ідентифікації використовують приватні особи для власних потреб. Як ключові сфери застосування біометрії тут можна виокремити захист інформації, що зберігається у ноутбуках, лептопах і смартфонах (для чого здебільшого використовують вбудовані в комп'ютерні пристрої сканери відбитків пальців), ідентифікацію користувачів стільникових телефонів та подібних пристроїв, а також підтвердження транзакцій в системах мобільної комерції (зокрема, які здійснюються за технологією «Near Field Communications» /NFC/).

На ринку біометричних продуктів, разом із відомими лідерами – «Identix», «Digital Persona», «Precise Biometrics», «Visionics», «Ethentica», «BioScript», «Secugen», «AcSys Biometrics», з'являються нові корпорації, які не є спеціалізованими в галузі біометрії, наприклад, «Sony», «LG», «Compaq», «Apple», «Sumsung» та ін. Цей факт засвідчує значне зростання привабливості біометричного ринку і те, що незабаром біометричні пристрої стануть звичним явищем у нашому побуті.

---

1. Митин Владимир. Биометрические технологии, которые мы выбираем / Митин Владимир // PC Week/RE. – 2010. – 09 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...
2. Технологии биометрической идентификации по лицу могут повысить свою эффективность // DGL.RU. – 2013. – 02 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...
3. Биометрический институт опубликовал результаты очередного исследования отраслевого рынка // BIOMETRICS.RU. – 2013. – 06 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

4. Лукашов И. Биометрия становится индустриальной технологией / И. Лукашов // CNews. – 2017. – 21 августа. [Электронный ресурс]. – Режим доступа:http://www.cnews.ru/reviews/free/security2007/articles/biomarket.shtml

ВИКОРИСТАННЯ ОПЕРАТИВНОГО, ТАКТИЧНОГО ТА СТРАТЕГІЧНОГО АНАЛІЗУ У БОРОТЬБІ ЗІ ЗЛОЧИННІСТЮ

Зачек О.І.
доцент кафедри оперативно-розшукової діяльності факультету №2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

Дмитрик Ю.І.
доцент кафедри оперативно-розшукової діяльності факультету №2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Значний рівень злочинності в даний час вимагає застосування у боротьбі проти неї найбільш сучасних та ефективних засобів. Таким засобом на сьогодні є кримінальний аналіз, який на основі збору, оцінки та впорядкування інформації дозволяє отримати її додаткову складову – роз'яснення значення інформації. Це дозволяє опрацьовувати значні масиви даних щодо злочинної діяльності та отримувати результат у графічному вигляді, що значно спрощує аналіз даних та надає можливість зробити висновок про структуру злочинної організації.

Як зазначив тимчасово виконуючий обов'язки начальника Управління кримінального аналізу Національної поліції України Володимир Єрофєєв: «Підрозділ аналітики національної поліції орієнтований на проведення оперативного, тактичного та стратегічного аналізу. Оперативний аналіз необхідний для збирання та обробки даних по резонансних злочинах щоб скоординувати роботу слідчо-оперативної групи. Тактичний аналіз дає можливість оцінити обстановку через нанесення інформації на карти, визначаючи райони з підвищеним ризиком скоєння злочинів.

Нарядам патрульної поліції надаватимуться рекомендації для проведення цільових відпрацювань районів. Стратегічний аналіз спрямований на аналіз діяльності організованих злочинних груп, а відтак – і на перспективу в роботі по боротьбі з ними» [1].

Оперативний аналіз – це робота за кримінальними провадженнями щодо конкретних осіб, злочинних угруповань з метою перевірки гіпотез щодо їх ймовірної злочинної діяльності, встановлення зв'язків, структури злочинних груп, ролі їх окремих учасників, у тому числі їх соціального та економічного статусу, з використанням аналізу телефонних трафіків, трансакцій, потоків та маршрутів переміщення об'єктів тощо [2]. Це процес, коли аналітичні продукти створюються, використовуючи всю наявну інформацію та надаються поліції з метою допомоги у проведенні поточних розслідувань та операцій шляхом досягнення чітко поставлених короткострокових цілей.

Внаслідок здійснення процесу кримінального аналізу створюються супровідні аналітичні продукти:

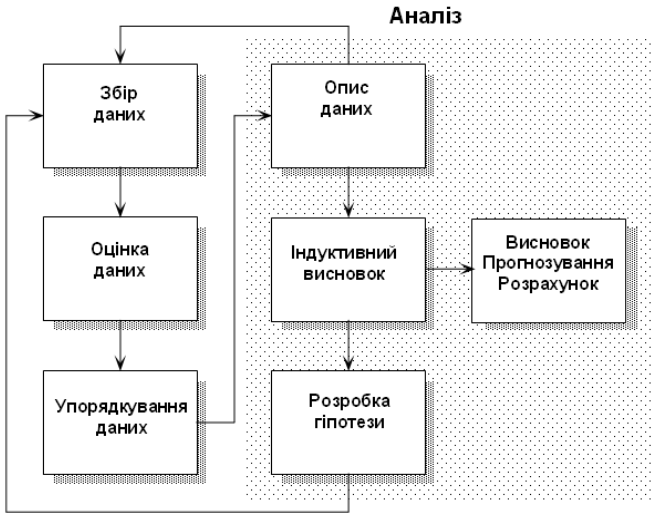


Рис. 1. Складові процесу оперативного кримінального аналізу.

- графіки/схеми (зв'язків, потоку товарів, телефонних з'єднань, діаграма послідовності дій/подій);
- карти (просторовий аналіз діяльності, переміщення, телефонних дзвінків);
- робочі книги Excel, в яких були використані різні аналітичні техніки (зведені таблиці, функції Excel, обчислення);
- інформаційні замітки що синтезують аналітичні результати і рекомендації.

Найбільш важливими інструментами, які використовує поліція для опрацювання інформації, що стосується оперативного аналізу, є:

- Ms Excel. Дозволяє задіяти автоматичні методи, використовуючи Visual Basic для мови програмування додатків або останні розробки такі як Power Query, Power Pivot та Power Map (всі є складовою частиною пакету Office 2016).
- IBM i2 Analyst's Notebook. Є найбільш важливим інструментом для інтеграції даних та їх візуалізації.
- iBase. Інструмент для інтеграції даних великих об'ємів та складних запитів до бази даних.
- GIS. Поліція використовує Geomedia Professional та ArcGis як інструменти для аналізу географічних даних.

Для проведення кримінального аналізу доцільним є використання спеціалізованої аналітичної системи «IBM i2 Analyst's Notebook», яка фактично є міжнародним стандартом для проведення аналітичних досліджень під час розслідування злочинів. Цю систему використовують правоохоронні органи, силові відомства, банки, страхові компанії, телекомунікаційні компанії 70-ти країн, у тому числі: Інтерпол, Європол, ООН, НАТО [3, с. 69].

Тактичний аналіз – це аналіз криміногенної ситуації на конкретній території за невеликий проміжок часу, за певним видом злочину чи протиправної діяльності певної групи [2]. Він проводиться з метою ідентифікації ризиків, тенденцій та найбільш вражених злочинністю зон, на короткострокову та середньострокову

перспективу. Зокрема, визначаються тенденції розвитку злочинності, встановлюються місця концентрації злочинів, визначаються шаблони злочинів, встановлюються профіль підозрюваного та жертви, визначаються напрями діяльності із розслідування та збору оперативної інформації. Тактичний аналіз за типами поділяється на добовий, місячний та той, що виконується на запит.

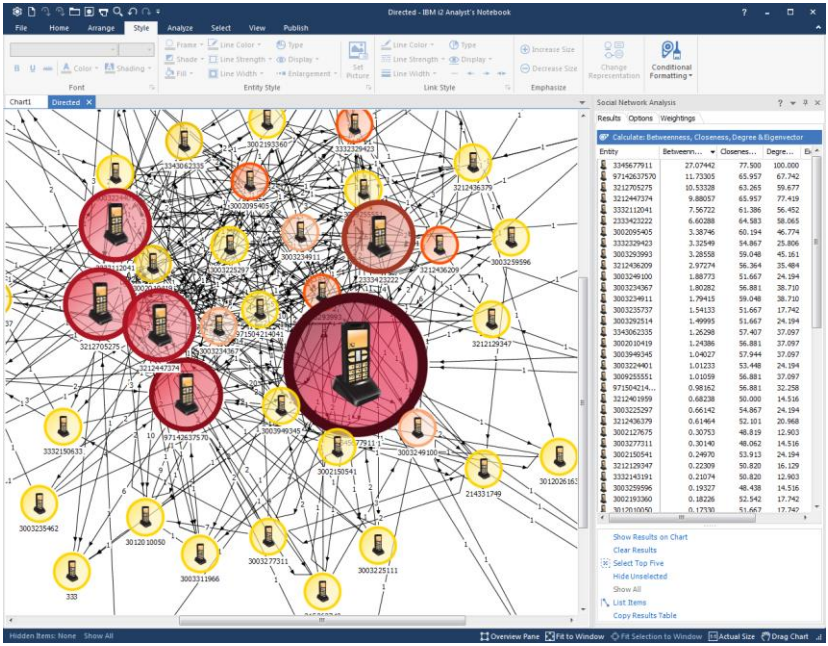


Рис. 2. Схема телефонних дзвінків у програмі IBM i2 Analyst's Notebook

В тактичному аналізі застосовуються наступні аналітичні техніки:

- аналіз проблем;
- геопросторовий аналіз;
- часовий аналіз;
- статистичний аналіз;
- аналіз шаблонів злочинів;

- порівняльний аналіз;
- аналіз ризиків;
- аналіз місць концентрації злочинів.

Геопросторовий або географічний аналіз – це набір методів, прийомів та програм на основі географічного представництва з метою виявлення гарячих точок та географічних моделей.

Географічний аналіз здійснює:

- перетворення адрес в географічні координати та координат в адреси;
- створення KML-файлів та завантаження в Google Earth;
- створення шляхів, полігонів, редагування елементів;
- створення графіків, карт гарячих точок та теплових карт;
- географічне передбачення та створення шаблонів.

Часовий аналіз обробляє наступні дані:

- час повідомлення про злочин;
- час вчинення злочину;
- інтервали часу: години, дні, місяці, роки;
- кримінальна тенденція – константа або стійке зростання чи спадання числа злочинів;
- розгул злочинності: характеризується високою частотою кримінальної злочинності в рамках короткого часу.

Види статистичного аналізу:

- описовий – використовує збір даних і добування даних, що дозволяє заглянути в минуле і відповісти на питання: «Що сталося?»;
- прогностичний – використовує статистичні моделі і техніки прогнозування для розуміння майбутнього і відповіді на питання: «Що може статися?»;
- перспективний – використовує алгоритми оптимізації та симуляції щоб дати поради та відповісти на питання: «Що ми можемо зробити?».

Категорії аналізованих даних:

1. Тип події – злочин, правопорушення, незначне правопорушення, ДТП; у сфері державних інтересів чи у сфері приватних інтересів, тощо.
2. Опис засобів вчинення:
   - з використанням зброї (ножа);
   - використовуючи фізичне насилля;
   - використання транспортного засобу для вчинення злочину чи втечі, тощо.
3. Спосіб вчинення злочину (підготовка, вчинення, втеча).
4. Просторові (географічні) фактори (геопросторові координати чи адреса, тип території, тощо.
5. Тимчасові фактори (збільшення, зменшення, сезонність, тренди).
6. Опис підозрюваного (анатомія, одяг, шрами, тощо).
7. Інформація щодо відомих злочинців.
8. Опис жертви.
9. Профіль товарів чи предметів.

Стратегічний кримінальний аналіз застосовується для більш масштабних довгострокових проблем і цілей, зокрема, для виявлення значних фігур злочинного світу, прогнозування зростання видів злочинної діяльності і встановлення пріоритетів діяльності правоохоронних органів. Стратегічний аналіз широко використовується у різних сферах, у довгостроковій перспективі (від 3 до 10 років), він використовує багато елементів: політичні, економічні, соціальні, технологічні фактори та різні типи даних.

Згідно визначення Інтерполу, стратегічний аналіз призначений для інформування осіб, які приймають рішення на високому рівні, а переваги реалізуються у довгостроковій перспективі. Метою є надання особам, які приймають рішення на високому рівні, попереджень щодо загроз та допомоги у визначенні пріоритетів у підготовці їх організацій до вирішення виникаючих питань кримінального характеру. Це може включати перерозподіл ресурсів за різними напрямами злочинності, чи збільшення тренінгів у конкретних методах боротьби зі злочинністю.

Важливою особливістю є те, що стратегічний аналіз допомагає загалом вищому керівництву організації, чи, іноді, керівництву середньої ланки. Бажано уникати використання стратегічного аналізу на місцевому рівні, оскільки територія є незначною, є неузгодженість даних, інформації та оперативної інформації з прогалинами, які не відповідають потребам стратегічного рівня.

Специфічною та цікавою частиною стратегічного аналізу є відображення аналітиком передбачень та оцінок деяких конкретних аспектів щодо майбутнього для правоохоронних органів, розвитку злочинності, базуючись на даних, які в значній мірі пов'язані з минулим. Тобто інтерпретуються дані з минулого з метою створення деяких рекомендацій, формулювання гіпотез та передбачення, чого очікувати завтра.

Порядок проведення стратегічного кримінального аналізу містить наступні етапи [4, с. 106]:

1. Аналіз середовища (обстановки).
2. Аналіз ресурсів (можливостей) відомства.
3. Формування місії та варіантів стратегії.
4. Аналіз варіантів стратегії з урахуванням обраних критеріїв прийняття управлінського рішення.
5. Вибір (формування) загальної стратегії.

---

1. Кримінальний аналіз – це ефективна робота поліції та безпека громадян [Електронний ресурс] // МВС України: [сайт]. Новини від 11.10.2017. URL: http://mvs.gov.ua/ua/news/10309_Kriminalniy_analiz___ce_efektivna_robota_ policii_ta_bezpeka_ gromadyan_FOTO.htm (дата звернення: 20.03.2018).
2. Концепція впровадження моделі поліцейської діяльності, керованої аналітикою «Intelligence Led Policing» [Електронний ресурс]. URL: https://www.slideshare.net/NationalPolice/ss-75925350 (дата звернення: 20.03.2018).
3. Кіреєва О. Використання альтернативних аналітичних інструментів у кримінальному аналізі // Збірник наукових праць Національної академії державної прикордонної служби України. Серія: військові та технічні науки. 2016. № 4 (70). С. 64-76.

4. Фаріон О.Б. Алгоритм проведення стратегічного кримінального аналізу оперативно-розшуковими підрозділами Державної прикордонної служби України // Сучасні інформаційні технології у сфері безпеки та оборони. 2012. № 3 (15). С. 106-110.

ЗАОХОЧУВАЛЬНІ НОРМИ У ПЕНАЛЬНІЙ ПОЛІТИЦІ УКРАЇНИ

Ковальчук В.П.
головний науковий співробітник відділу організації наукової роботи Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Серед засобів, що застосовуються державою у системному впливі на злочинність, найсуворішим за своїм проявом було і залишається покарання. Тому закон про кримінальну відповідальність не тільки визначає, які суспільно небезпечні діяння варто віднести до злочинів, а й встановлює покарання за кожен із них. Однак запровадження у зв'язку з прийняттям Кримінального кодексу України 2001 року (далі – КК України) нових видів покарань та відповідні зміни у порядку їх виконання не здійснюють ще належного впливу на стан злочинності. Тому сьогодні набувають актуальності дослідження державної реакції на злочин та процесів реформування системи протидії злочинності, а також питання співвідношення заходів державного примусу та заохочення.

Деякі аспекти заохочення в кримінальному праві досліджувались у працях А.Бабенка, Ю. Бауліна, В. Борисова, В. Глушкова, В. Голіни, В. Грищука, Т.Денисової, Л. Іногамової-Хегай, І. Лановенка, М. Мельника, А. Музики, В.Навроцького, О. Наден, П. Рабіновича, М. Селіванова, В. Сташиса, В. Тація, Г.Усатого, Є. Фесенка, П. Фріса, П. Хряпінського, Д. Ягунова, С. Яценка та ін.

Проте дослідження заохочувальних норм у сфері протидії злочинності не отримали свого комплексного вивчення, не визначено їх місце під час призначення покарання, його відбування або звільнення від нього. Тому метою цієї публікації є визначення заохочувальних норм у пенальній політиці держави та їх структури.

Під пенальною політикою слід розуміти самостійний напрям правової політики держави у сфері протидії злочинності, який визначає мету, оптимальні вид і розмір покарання, розробляє положення щодо призначення та звільнення від покарання та його відбування, формує засоби протидіючого впливу на злочинність під час реалізації покарання та знаходить своє відображення в нормах кримінально-правового, кримінально-виконавчого, кримінально-процесуального й кримінологічного законодавства і практиці його застосування [1, с. 15].

Пенальна політика держави охоплює такі галузі: кримінально-правову (базову, системоутворюючу та визначальну стосовно інших), кримінально-виконавчу (забезпечує виконання покарання), кримінально-процесуальну (забезпечує призначення справедливого покарання, встановлення процесуальних гарантій прав засуджених) та кримінологічну (забезпечує запобігання злочинам та протидію злочинності на всіх етапах реалізації покарання).

Саме кримінально-правова галузь пенальної політики держави знаходить свій прояв у формуванні положень КК України, що стосуються визначення видів та розмірів покарання, його призначення, звільнення від покарання та його відбування, особливостей покарання неповнолітніх, оптимізації міри покарання, передбаченої в санкціях Особливої частини КК України. Основними напрямами її формування є пеналізація та депеналізація. Проте поряд із змінами інтенсивності кримінально-правової репресії в теорії кримінального права виділяють ще один засіб досягнення мети покарання – засіб заохочення осіб, яким призначають покарання, які його відбувають або звільняються від нього та його відбування.

Серед науковців та практиків немає єдиного підходу до заохочення у правовій політиці в сфері протидії злочинності, а його визначення є однією з центральних проблем у теорії кримінального права. Від підходів до визначення цього політико-правового явища залежить, які саме норми належать до заохочувальних і яку роль вони відіграють у справі протидії злочинності.

Варто відзначити, що на сьогодні заохочувальні норми в кримінальному законодавстві України досліджує П. Хряпінський та визначає їх як самостійну групу кримінально-правових норм, що складається з правових приписів, які, з одного боку, надають право особі, що вчиняє або вчинила злочин, на соціально-схвальну, позитивну поведінку, а з іншого – породжують право або обов'язок держави усунути чи пом'якшити кримінально-правове обтяження [2, с. 172].

Потрібно наголосити на тому, що норми, які заохочують позитивну посткримінальну (можливо – пенальну) поведінку особи в системі заохочувальних норм, займають значне, але не виняткове становище. Своєю чергою, пенальна поведінка є елементом посткримінальної поведінки. Вона проявляється у процесі призначення покарання, його відбування і звільнення від нього та його відбування. Під час реалізації покарання, коли всі превентивні заходи виявилися неефективними, саме на заохочувальні норми покладається функція стимулювання виправлення особи у справі досягнення мети покарання і саме вони є важливим орієнтиром бажаної та необхідної поведінки засудженого. Тому ми розглядаємо заохочувальні норми не тільки на кримінально-правовому, а й на кримінально-виконавчому рівні, що обумовлено специфічною спрямованістю заохочувальних норм у стимулюванні виправлення засуджених осіб.

Заохочувальні норми, що передбачені нормами кримінально-виконавчого права, ми пропонуємо поділити на дві групи. Перша група містить норми, які значно не впливають на правовий статус засуджених (наприклад ч.1 ст.54; ч.1 ст.67; ч.1 ст.81; ч.2 ст.120; ст.125; ст.127; ч.1 ст.130; ч.2 ст.143; ст.144; ч.6 ст.151 Кримінально-виконавчого кодексу України (далі – КВК України), друга – містить норми, які значно впливають на правовий статус засуджених (наприклад ч.1 ст. 46; ч.1 ст.54; ч.1 ст.67; ч.1 ст.81; ст.100; ч.1 ст.101; ч.2 ст.120; ст.125; ст.127; ч.1 ст.130; ч.2 ст.143; ст.144; ч.6 ст.151 КВК України).

Правовий статус засудженого регламентований главою другою «Правовий статус засудженого» розділу першого КВК України. В теорії кримінально-виконавчого права під правовим статусом

засудженого прийнято розуміти сукупність юридично закріплених прав, свобод та законних інтересів (конституційних, громадянських та інших), якими володіє засуджений в період відбування покарання [3, с. 209; 4, с. 34; 5, с. 47].

Під нормами, що значно впливають на правовий статус засудженого, ми пропонуємо розуміти ті, які передбачають можливість застосування кримінально-правових інститутів звільнення від відбування покарання чи заміни покарання більш м'яким (наприклад, ч.2 ст. 67 КВК України закріплює положення, що засуджені до обмеження волі, які стали на шлях виправлення або сумлінною поведінкою і ставленням до праці довели своє виправлення, можуть бути у встановленому законом порядку представлені до заміни невідбутої частини покарання більш м'яким або до умовно-дострокового звільнення від відбування покарання; ч.2 ст.81 КВК України закріплює положення, що засуджені до покарання у вигляді тримання в дисциплінарному батальйоні військовослужбовці, які сумлінною поведінкою і ставленням до праці та військової служби довели своє виправлення, можуть бути представлені командиром дисциплінарного батальйону в установленому законом порядку до умовно-дострокового звільнення від відбування покарання; ч.1 ст. 151 КВК України закріплює положення, що засудженим до довічного позбавлення волі може бути подано клопотання про його помилування після відбуття ним не менше двадцяти років призначеного покарання).

Під нормами, що значно не впливають на правовий статус засудженого, ми пропонуємо розуміти ті, які безпосередньо не передбачають застосування кримінально-правових інститутів звільнення від відбування покарання чи заміни покарання більш м'яким, а полегшують умови відбування покарання, тобто регламентують кримінально-виконавчий, так би мовити, «внутрішній» статус засуджених (наприклад, ч.2 ст. 143 КВК України закріплює положення, що у виховних колоніях засуджені при сумлінній поведінці і ставленні до праці та навчання після відбуття не менше однієї четвертої частини строку покарання

мають право на поліпшення умов тримання і їм може бути дозволено: додатково витрачати на місяць гроші в сумі шістдесяти відсотків мінімального розміру заробітної плати; додатково одержувати один раз на три місяці короткострокове побачення, яке за постановою начальника виховної колонії може проходити за межами виховної колонії; додатково одержувати протягом року три посилки (передачі) і чотири бандеролі; ч.6 ст. 151 КВК України закріплює положення, що при сумлінній поведінці і ставленні до праці після відбуття десяти років строку покарання засудженому до довічного позбавлення волі може бути дозволено додатково витрачати на місяць гроші в сумі двадцяти відсотків мінімального розміру заробітної плати).

У рамках пенальної політики держави досліджуються заохочувальні норми під час реалізації основного та найсуворішого елементу кримінальної відповідальності – покарання. Тому необхідно зауважити, що важливим є усунення чи пом'якшення не всього кримінально-правового обтяження, а лише одного з його елементів – покарання. Уже від цього результатом соціально-схвальної, позитивної поведінки особи може бути призначення більш м'якої міри покарання, полегшення умов його відбування чи звільнення від покарання та його відбування.

Вважаємо за необхідне надати власне визначення заохочувальних норм у пенальній політиці держави як самостійної групи кримінально-правових та кримінально-виконавчих норм, що складаються з правових приписів, які, з одного боку, надають право особі, що вчинила злочин, на соціально-схвальну, позитивну поведінку, а з іншого – породжують право або обов'язок держави призначити більш м'яку міру покарання, полегшити умови його відбування чи звільнити від нього та його відбування.

На наш погляд, визначення заохочувальних норм у пенальній політиці держави надасть змогу проведення їх системного аналізу, а запропонована нами схема допоможе розробити ряд теоретичних та практичних рекомендацій щодо подальшого вдосконалення діяльності з протидії злочинності.

1. Назимко Є.С. Пенальна політика України: поняття, зміст та тенденції розвитку: [монографія] / Є.С. Назимко, І.Ю. Карпушева / [переднє слово та загальна редакція заслуженого юриста України, професора В.П. Філонова]. – Донецьк: ВІК, 2009. – 212 с.
2. Хряпінський П.В.Заохочувальні норми у кримінальному законодавстві України [навч. пос.] / П.В. Хряпінський. – К.: Центр учбової літератури, 2008. – 192 с.
3. Трубников В.М., Филонов В.П., Фролов А.И. Уголовно-исполнительное право Украины [учебник] / Трубников В.М., Филонов В.П., Фролов А.И. – Донецк, 1999. – 640 с.
4. Степанюк А.Х., Яковець І.С. Кримінально-виконавчий кодекс України: [науково-практичний коментар] / За заг. ред. Степанюка А.Х. – Х.: ТОВ «Одіссей», 2005. – 560 с.
5. Бадира В.А., Денисов С.Ф., Денисова Т.А., Мінаєв М.М., Хашев В.Г. Кримінально-виконавче право [навчальний посібник] / За ред. Т.А. Денисової. – К.: Істина, 2008. – 400 с.

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Крижна В.В.
старший науковий співробітник наукової лабораторії з проблем кримінальної поліції Національної академії внутрішніх справ, кандидат юридичних наук, старший науковий співробітник

Актуальність використання інформаційних технологій зростає й у зв'язку з інтенсивним впровадженням у діяльність правоохоронних органів засобів комп'ютерної техніки. Цей процес впливає на організацію розслідування кримінальних правопорушень, методичне забезпечення працівників Національної поліції України (далі – НП України), а здійснення автоматизованого пошуку відомостей щодо будь-яких об'єктів (осіб, предметів, подій) сприяє науково-організаційної праці, оптимізує збирання, зберігання, систематизацію та аналіз доказової інформації.

Для вирішення розшукових заходів нині накопичений чималий досвід застосування новітніх технологій у процесі попередження,

виявлення та розслідування злочинів, розшуку підозрюваного та обвинуваченого, провадження окремих слідчих (розшукових) дій, здійснення судових експертиз[1].

Очевидно, що однією з важливих умов підвищення рівня протидії злочинності є широке використання сучасних досягнень науково-технічного прогресу, які останніми роками зробили прорив у сфері інформаційних технологій.

Інформаційні технології – це сукупність методів, інформаційних процесів із використанням засобів обчислювальної техніки, що забезпечують високу швидкість оброблення даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця розташування [2].

Для вирішення оперативно-розшукових завдань нині накопичений чималий досвід застосування новітніх технологій у процесі попередження, виявлення та розслідування злочинів, розшуку підозрюваного та обвинуваченого, провадження окремих слідчих (розшукових) дій, зокрема негласних слідчих (розшукових) дій.

Оперативність і ефективність застосування положень Кримінального процесуального кодексу України (далі – КПК України) неможливі без застосування сучасних інформаційних технологій та автоматизованих баз даних.

Технічне забезпечення оперативних підрозділів НП України є актуальним з огляду на новації, що містяться в положеннях КПК України, які закріплюють сучасні інструменти для боротьби зі злочинністю та застосування яких повинно чітко відповідати вимогам чинного законодавства.

Очевидно, що однією з важливих умов підвищення рівня протидії злочинності є широке використання сучасних досягнень науково-технічного прогресу, які останніми роками зробили прорив у сфері інформаційних технологій [3].

Одним з основних завдань функціонування системи інформаційного забезпечення діяльності стала інформатизація підрозділів, що здійснюють оперативно-розшукову діяльність. В України вже

накопичено чималий досвід використання різноманітних інформаційних та інформаційно-телекомунікаційних систем оперативно-розшукового та інформаційно-довідкового призначення.

Наказом НП України від 30 грудня 2015 р. № 228 створено Департамент інформаційної підтримки та координації поліції (далі – ДІПКП) «102» НП України, який організовує та здійснює передбачені законодавством України заходи, спрямовані на інформаційно-аналітичне та інформаційно-пошукове забезпечення правоохоронної діяльності й захист персональних даних під час їх обробки у структурних підрозділах апарату НП України. ДІПКП визначає основні напрями діяльності поліції у сфері інформатизації, здійснює інформаційно-пошукову та інформаційно-аналітичну роботу, бере участь у розроблені проектів нормативно-правових актів МВС із питань, що належать до компетенції поліції та стосуються інформаційно-аналітичного забезпечення, а також оброблення персональних даних в органах і підрозділах поліції.

Завданнями використання інформаційно-комунікаційних технологій у підрозділах НП України є:

- забезпечення можливості оперативного отримання інформації у повному, систематизованому та зручному для користування вигляді співробітниками та підрозділами НП України для розкриття, розслідування, попередження кримінальних правопорушень і розшуку злочинців;
- збирання, оброблення та узагальнення оперативної, оперативно-довідкової, аналітичної, статистичної та контрольної інформації для оцінки ситуації та прийняття обґрунтованих оптимальних рішень на всіх рівнях діяльності підрозділів НП України;
- забезпечення динамічної та ефективної інформаційної взаємодії всіх галузевих служб і підрозділів НП України, інших правоохоронних органів, державних установ, різних груп громадськості, мас-медіа;
- забезпечення захисту інформації [4].

За допомогою комп'ютерної техніки не тільки раціоналізуються інформаційні процеси, але й упроваджуються комп'ютеризовані системи підтримки прийняття слідчими, експертами, оперативними співробітниками, суддями відповідних рішень. За останні роки розроблено кілька десятків систем, які, по суті, моделюють діяльність слідчих-методистів, які допомагають розслідувати найбільш складні злочини, формулюючи за результатами вивчення кримінальних правопорушень конкретні рекомендації [5].

Як свідчить практика, щоб комп'ютеризована інформаційна система була працездатною, необхідно дотримуватися таких правил:

1) вся інформація, що вводиться, повинна записуватися з використанням спеціальної термінології мовою, що виключає різне тлумачення;
2) перероблення інформації має здійснюватися відповідно до алгоритму точно, з певною послідовністю операцій, що дає можливість вирішити будь-яку конкретну задачу з деякого класу однотипних задач, причому вихідні дані можуть у певних межах змінюватися.

Отже, впровадження та використання нових інформаційно-комунікаційних технологій є головною умовою покращення роботи щодо встановлення підозрюваного або його розшуку, а також діяльності підрозділів НП України та функціонування правоохоронної системи загалом. При цьому є проблеми фінансового забезпечення, низький рівень володіння співробітниками відповідними інформаційними ресурсами та навичками роботи з новою технікою або новими системами. У нинішніх умовах швидкого технічного процесу кожен працівник НП України повинен бути прогресивним користувачем інформаційно-комунікаційних технологій. Крім того, оперативним працівникам необхідно проходити курси підвищення кваліфікації з метою отримання нових знань, умінь і навичок під час застосування в повсякденній роботи інформаційних технологій.

1. Рогатюк І.В. Використання інформаційних технологій у досудовому розслідуванні: сучасний стан і перспективи розвитку / І.В. Рогатюк // Науковий вісник Національної академії внутрішніх справ. – 2013. – № 3. – С. 312–320.
2. Інформаційні технології / Вікіпедія [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki.
3. Інформатика : [навч. посібник] / [А.Ю. Гаєвський]. – 2-ге вид., доповн. – К. : «Видавництво А.С.К.», 2007. – 512 с.
4. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України : [монографія] / Б.А. Кормич. – О. : Юридична література. – 2003. – 271 с.
5. Іщенко П.П. Інформаційне забезпечення слідчої діяльності : [науково-практичний посібник] / П.П. Іщенко ; під ред. Є.П. Іщенко. – М.: Юрлитинформ, 2011. – 168 с.

ОКРЕМІ СПОСОБИ ІДЕНТИФІКАЦІЇ IP-АДРЕСИ ЗЛОВМИСНИКА СПІВРОБІТНИКОМ ОПЕРАТИВНОГО ПІДРОЗДІЛУ

Лепеха О.М.
керівник Поліського управління кіберполіції Департаменту кіберполіції Національної поліції України, кандидат юридичних наук

Кондратюк О.В.
професор кафедри оперативно-розшукової діяльності факультету №2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Пізнавальна діяльність оперативника ґрунтується на виявленні (пошуку) і аналізі інформації, плануванні, розробці та перевірці оперативних версій, з'ясуванні причинно-наслідкових зв'язків між окремими елементами злочинної діяльності, встановленні невідомих обставин злочину. Охарактеризуємо алгоритм дій, який допоможе оперативнику самостійно в межах оперативного пошуку визначити IP-адресу потенційного зловмисника. Для цього можна використати прості методи соціальної інженерії і

веб-ресурс, як от iplogger.ru. Завданням оперативника є з робочого комп'ютера із виходом в Інтернет створити обліковий запис у будь-якій соціальній мережі (вибір мережі здійснюється за результатами інформаційного аналітичного пошуку). Далі оперативник заходить на сайт iplogger.ru., де на головній сторінці буде поле, в яке потрібно ввести будь-який URL, наприклад, адресу пошукової системи, після чого натискає на поле «Згенерувати IPLOGGER-посилання». За результатами вказаних дій на екрані з'явиться посилання, яке потрібно відправити потенційному зловмиснику (особі, яка становить оперативний інтерес для підрозділу поліції), чию IP-адресу є намір дізнатися. Очікуємо (сподіваємося), щоб зловмисник не був професійним хакером, якому відомо методи діяльності правоохоронних органів та їх спеціалізованих підрозділів, і натиснув на посилання, адже лише так система зможе передати набір цифр, які і будуть індивідуальною адресою злочинця в мережі. Відправляючи повідомлення, оперативник, використовуючи методи тієї ж соціальної інженерії, повинен сформувати його зміст так, щоб встановити дистанційно психологічний контакт із особою, попередньо викликавши в неї зацікавленість, тобто співробітник підрозділу-ініціатора повинен спонукати злочинця до активних дій (натиснути на посилання-пастку). У процесі оперативного пошуку відпрацьовуються різні особи і, звичайно, серед них є законослухняні. У разі натрапляння на таку особу не потрібно допускати виникнення конфліктних ситуацій – у разі, якщо «потерпілий» вимагатиме пояснення за скоєне (оперативником), свої дії необхідно пояснити, наприклад, помилковою відправкою листа (пошти), супроводжуючи вибаченнями, не загострюючи конфлікт тощо. У разі успішної реалізації задуманої комбінації зловмисник все ж натисне на посилання, то оперативник зможе дізнатися його IP-адресу, увійшовши у поле «перегляд статистики», де в списку повинна з'явитися IP-адреса. Якщо зловмисник не встиг прочитати посилання-пастку, то сторінку потрібно періодично оновлювати, натиснувши клавішу F5.

Одним із простих способів встановити IP є отримання від «зловмисника» листа електронною поштою. IP комп'ютера

користувача завжди відображений в корені листа. На різних поштових серверах корінь листа має різну назву – на Yandex «властивості листа», на mail RFC-заголовок, на Gmail – «Показати оригінал листа» тощо. Відкриється сторінка з HTML-кодом листа, в якому оперативник бачить IP поштового сервера та вихідний фізичний IP. Після встановлення IP оперативний підрозділ спрямовує регіональному провайдеру запит про отримання персональних даних користувача, внаслідок чого можна отримати дані про особу, яка уклала договір з провайдером, його адресу та контактні дані. За допомогою тієї ж команди WHOIS можна визначити в якій країні, регіоні зареєстрований цей веб-ресурс, де знаходиться сервер, яка компанія обслуговує хостинг цього сайту, після чого до неї можна надіслати запит про персональні дані особи, на яку зареєстровано сайт. У разі, якщо сайт є форумом, на якому відбувається реєстрація користувачів, отримавши доступ із правами адміністратора до цього ресурсу, можна отримати повну базу користувачів (потенційних зловмисників) з IP адресами.

Іншим способом є можливості використання email-агента, наприклад, MS Outlook або The Bat, який допоможе дізнатися чужий IP. Для цього оперативнику необхідно отримати лист саме цим поштовим агентом. В процесі перегляду коду листа необхідно відкрити сам лист, натиснути кнопку «Файл» – «Властивості» – «Подробиці», в результаті чого в заголовку листа можна побачити відповідні IP-адреси, нижня – та, яка цікавить оперативника. За допомогою ICQ (вид віртуального спілкування за допомогою текстових повідомлень в спеціальній програмі) також можна дізнатися чужий IP, але для цього потрібен патч (інформація, призначена для автоматизованого внесення певних змін в комп'ютерні файли). Для версії ICQ 2001b потрібно Build 3659, а для ICQ 2002a Beta – Build 3722. Ці патчі додають у вікні властивостей віконце, де і буде відображатися IP-адреса. Простішою дією буде установлення програми «netstat.exe», яку потрібно запускати разом з ICQ, внаслідок чого буде постійний доступ до IP-адрес. У процесі оперативного відпрацювання телекомунікаційної мережі Інтернет оперативник самостійно може визначити

адміністратора чи власника веб-сайту (розділи «контакти/ «про нас», інформація щодо реєстранта доменного імені та веб-серверу з бази даних «whois»/ripe.net/domaintools.net/2ip.com.ua/ robtex.com) для подальшого складання запиту до реєстратора/ провайдера/власника веб-сайту. Визначення даних адміністратора чи власника анонімного веб-сайту можна самостійно реалізувати за допомогою пошуку встановлено рекламного ідентифікатора google (веб-сайт містить рекламне вікно google, переглядаючи інформацію програмного/вихідного коду сторінки з контекстного меню веб-оглядача google-ідентифікатор можливо знайти за префіксом «pub-», наприклад 2ip.com.ua має pub-2871984509315629. Пошуком зазначеного ідентифікатора можливо встановити інші веб-сайти власника, наприклад intech.kiev.ua та katalog.biz.ua).

ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОГО–АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ОРГАНІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ ЩОДО ПРОТИДІЇ НЕЗАКОННОМУ ЗАВОЛОДІННЮ ТРАСПОРТНИМИ ЗАСОБАМИ

Лисий О.В.
здобувач кафедри оперативно-розшукової діяльності
Національної академії внутрішніх справ

Одним з пріоритетних напрямів діяльності Національної поліції України є розроблення інформаційно-аналітичного забезпечення, яке призначене для комплексного використання сил та засобів по попередженню та розскритю злочинів, пов’язанних з незаконним заволодінням транспортних засобів.

Таким чином, розроблення інформаційно-аналітичного забезпечення аналізу стану та динаміки розвитку злочинів, пов’язанних з незаконним заволодінням транспортними засобами є найважливим завданням при створенні систем аналізу кримінологічної обстановки, що склалася, та тенденцій її розвитку. Воно передбачає наявність інформації про стан, динаміку, структуру злочинів,

пов'язанних з незаконним заволодінням транспортними засобами. При цьому необхідно мати в своєму розпорядженні досить повну інформацію, що відображала б реальний стан даного виду злочинів в країні.

Структура інформаційно-аналітичної діяльності повинна включати інформаційне забезпечення, інформаційно-аналітичну роботу, створення баз даних, що включає інформаційний пошук, цілі, мотиви, способи та прийоми їх здійснення.

Стаття 25 «Повноваження поліції у сфері інформаційно-аналітичного забезпечення» Закону України «Про Національну поліцію» передбачає, що поліція в рамках інформаційно-аналітичної діяльності:

- формує бази (банки) даних, у тому числі щодо злочинів пов'язаних з незаконним заволодінням транспортними засобами, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України;
- здійснює інформаційно-пошукову та інформаційно-аналітичну роботу;
- користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади.

Розвиток інформаційно-аналітичного забезпечення органів Національної поліції щодо протидії незаконному заволодінню транспортними засобами зумовив появу інформаційно-аналітичних підрозділів, практично за всіма напрямами діяльності, пов'язаної з інформаційними процесами, зокрема, з обробкою потоків інформації з метою прийняття оптимальних управлінських рішень.

З концептуально-теоретичних позицій доцільно виділити ряд важливих особливостей інформаційно-аналітичної забезпечення органів Національної поліції України, які мають істотне значення для інтеграції у європейські поліцейські структури.

Базовими елементами та засобами реалізації інформаційно-аналітичного забезпечення органів Національної поліції щодо протидії незаконному заволодінню транспортними засобами виступають

інформаційні системи, системи зв'язку та передачі даних, сучасна інформаційно-телекомунікаційна інфраструктура.

З одного боку, інформаційно-аналітична робота дозволяє виявити і пізнати закономірності, у контексті кримінологічних досліджень щодо злочинів пов'язаних з незаконним заволодінням транспортними засобами. З іншого боку, інформаційно-аналітичне забезпечення відображає результати повсякденної діяльності органів Національної України поліції з протидії незаконному заволодінню транспортними засобами. Це охоплює аналіз стану злочинів даного виду за певний проміжок часу, вивчення ефективності та практичної доцільності конкретної форми роботи, її нормативно-правове регулювання, що застосовується у протидії незаконному заволодінню транспортними засобами.

У даний час окремі завдання щодо протидії незаконному заволодінню транспортними засобами вирішується за допомогою Інтегрованої інформаційно-пошукової системи МВС України.

Для ефективної реалізації цих функцій в рамках окремо взятого територіального органу Національної поліції України потрібні об'єктивно встановлені та закріплені критерії збору інформації, встановлений порядок її обробки. Доцільно зауважити, що технологія збору і обробки даних повинна охоплювати усі напрямки діяльності складових елементів системи органів Національної поліції України, визначені Законом України «Про Національну поліцію», та складових системи МВС України (Державної служби України з надзвичайних ситуацій, Державної міграційної служби України, Державної прикордонної служби України, Національної гвардії України.

Оптимізація вирішення завдань пошуку, відбору та систематизації інформації, необхідної в діяльності органів Національної поліції України, базується на єдиному інформаційному просторі системи МВС України, який логічно визначити як сукупність спеціалізованих баз і банків даних, технологій їх ведення та використання, інформаційно-телекомунікаційних систем і мереж, суб'єктів інформаційно-аналітичної діяльності, які функціонують

на основі єдиних принципів і за загальними правилами забезпечують інформаційну взаємодію системи Міністерства внутрішніх справ України і громадян.

Очевидно, що функціонування єдиного інформаційного простору сприяє суттєвому розширенню інформаційної бази, необхідної для інформаційно-аналітичної діяльності, зниженню витрат на процеси пошуку, обробки, зберігання та відбору вихідної інформації, виявлення тих аспектів, у рамках яких слід здійснювати аналітичну обробку інформації, виявлення суті та динаміки просторово-часових і причинно-наслідкових зв'язків між досліджуваними фактами, явищами, процесами. У результаті спочатку наявні дані перетворюються в нову інформацію про стан злочинності пов'язаної з незаконним заволодінням транспортними засобами та результати оперативно-службової діяльності органів Національної поліції, оперативно-довідкову, розшукову, криміналістичну, архівну, науково-технічну і іншу інформацію більш високого порядку, яка дозволяє приймати обґрунтовані оперативні і управлінські рішення, здійснювати координацію та взаємодію всіх підрозділів по розриттю злочинів пов'язанних з незаконним заволодінням транспортними засобами.

Найважливішу роль у цьому плані повинна виконувати аналітична робота в сфері щодо протидії незаконному заволодінню транспортними засобами, що характеризується сукупністю особливих ознак, які виокремлюють її з-поміж інших видів аналізу в діяльності органів Національної поліції, що є одним з основних елементів процесу пізнання, здійснюваного під час вирішення завдань. На базі використання різнопланових відомостей аналітичне забезпечення дає змогу встановлювати індивідуальну або групову належність різних об'єктів кримінологічного впливу, досліджувати їхні властивості та стан, а також результати та співвідношення чинників, що впливають на них; прогнозувати подальший хід кримінальних подій; виявляти приховані взаємозв'язки між об'єктами тощо.

Елементи аналітичної роботи прямо або побічно присутні абсолютно на всіх стадіях кримінологічного моніторингу. Тому її

зміст слід розглядати в набагато ширшому аспекті - не тільки як діяльність спеціалізованих суб'єктів у сфері інформаційно-аналітичного забезпечення правоохоронної діяльності, але і як стрижневу функцію моніторингу протидії злочинності, до реалізації якої причетні всі суб'єкти. З певною мірою умовності між моніторингом протидії злочинності й аналітичною роботою в функціональному контексті можна поставити знак рівності.

Постійне загострення криміногенного стану в Україні висуває вимоги до корінного поліпшення інформаційно-аналітичного забезпечення діяльності органів Національної поліції у боротьбі із злочинами, пов'язанними з незаконним заволодінням транспортними засобами, створення принципово нової системи, яка має поєднувати всі накопичені та наново створювані масиви оперативно-розшукового призначення в єдину інформаційно-обчислювальну мережу МВС України. Ця система дозволяє здійснювати обмін необхідною інформацією на всіх рівнях управління, від МВС до будь-якого підрозділу поліції та іншого відомства.

Інформаційно-аналітичне забезпечення в органах Національної поліції повинно створюватися шляхом вирішення основних задач, а саме:

- інтеграція інформації, що формується правоохоронними органами, для формування єдиних інформаційних банк даних та забезпечення на їх базі повноти інформованості і координації діяльності різних підрозділів МВС;
- статистичне узагальнення накопиченої інформації, яка використовується у вигляді вихідних даних при проведенні аналітичних досліджень, виділення основних якісних і кількісних показників злочинності;
- контроль за виконанням заходів, що вживаються для попередження та боротьби з незаконими заводіннями транспортними заходами, та їх впливом на динаміку розвитку злочинності, як інформаційної основи для прийняття нових рішень на всіх рівнях;
- формування підсумкових інформаційних масивів як основи для оцінки результатів роботи органів Національної поліції.

Єдине інформаційно-аналітичне забезпечення дозволяє на основі більш повного використання всіх даних, що надходять, сучасних методів та засобів створити основу для ефективної роботи органів Національної поліції щодо протидії незаконому заволодінню транспортними засобами.

1. Захарова В. І. Основи інформаційно-аналітичної діяльності / Захарова В. І., Філіпова В. Я. – К.: «Центр учбової літератури», 2013. – 336 с.
2. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради. – 2015. – № 40-41. – Ст. 379.
3. Наказ МВС України від 26.09.2013 № 920 «Про затвердження Порядку організації доступу до інформаційних ресурсів під час інформаційної взаємодії між Міністерством внутрішніх справ України, Державною міграційною службою України та Державною прикордонною службою України». [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/ show/z1771-13.
4. Нормативно-правове забезпечення системи інформаційного забезпечення ОВС України [Електронний ресурс]. – Режим доступу: http://pravo.vuzlib/book_n046_page_40.html.

АКТУАЛЬНІ ПРОБЛЕМИ ПРОТИДІЇ ВТЯГНЕННЮ ПІДЛІТКІВ У ЗЛОЧИННУ ДІЯЛЬНІСТЬ В СУЧАСНИХ УМОВАХ

Лісовий М.А.

доцент кафедри оперативно-розшукової діяльності факультету №2 ІПФПНП Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Втягнення неповнолітніх у злочинну діяльність давно стало однією з основних проблем побудови правової європейської держави України та інших держав, тому що існує «залежність злочинності дорослих від злочинності неповнолітніх, оскільки остання є у певному розумінні джерелом і резервом усієї

злочинності». І щоб не допустити зростання злочинності, необхідно активізувати увагу на злочинності неповнолітніх, її попередженні, і головне – захистити неповнолітніх осіб від негативних явищ, серед яких одним із найнебезпечніших є втягнення дорослими особами неповнолітніх у злочинну діяльність.

Протиправна поведінка підлітків пов'язана насамперед з такими особливостями їхньої психіки, як підвищена навіюваність, не сформованість життєвих орієнтацій, юнацький негативізм, наслідування. Багато підлітків втратили зацікавленість у навчанні, роботі, їх приваблює сфера беззмістовного дозвілля - тусовки у під'їздах, випивки, азартні ігри тощо. Для підлітків групи ризику характерне своєрідне, за визначенням вчених «інформаційно-комунікативне хобі». Прагнення постійно одержувати легку інформацію, що не потребує ніякого критичного інтелектуального осмислення: пусті розмови, сидіння годинами перед телевізором, захоплення популярною музикою, вживання наркотиків тощо.

Для способу життя підлітків групи ризику характерним є: зневажливе ставлення до виконання своєї соціальної функції - вчитися, набувати знань; наявності великої кількості «зайвого часу»; невміння проводити вільний час; відсутність індивідуальних захоплень; вживання наркотичних речовин.

Перебування підлітків у конфлікті з законом у багатьох випадках спричинення їхньою незайнятістю у позаурочний час, що зумовлено відсутністю за місцем проживання достатньої кількості клубів, спортивних гуртків, секцій. Гострою є також проблема працевлаштування неповнолітніх, пов'язана з небажанням підприємців в умовах жорсткої конкуренції легально використовувати малоефективну та достатньо дорогу працю підлітків. Позбавленні можливості працювати та організовано проводити своє дозвілля, неповнолітні потрапляють у сферу інтересів кримінальних осіб, які часто залучають їх до злочинної діяльності.

Як свідчить аналіз практики Національної поліції неповнолітні залучені до значної кількості організованих злочинних груп. Як

правило організовані злочинні групи активно схиляють неповнолітніх до злочинної діяльності. Можна виділити такі основні напрями діяльності організованої злочинності щодо неповнолітніх:

1. Виховання споживачів певних кримінальних послуг
2. Контроль організованої злочинності за деякими формами кримінальної діяльності неповнолітніх
3. Втягнення неповнолітніх в організовані злочинні формування.

Досить часто злочинні угрупування здійснюють колективне залучення неповнолітніх шляхом створення різноманітних спортивних секцій, гуртків, молодіжних політичних партій де їм прищеплюється неповага до суспільства, антигромадські погляди та почуття фізичної переваги над іншими.

Виходячи з вищенаведеного оперативним підрозділам Національної поліції слід зосередити свої сили та засоби на протидію залученню неповнолітніх саме організованими злочинними угрупуваннями та попередженні групової злочинності неповнолітніх.

Оперативні підрозділи Національної поліції повинні вжити всіх необхідних заходів щодо недопущення втягнення неповнолітніх у злочину діяльність. Водночас недопущення досягається двома способами:

1. Загальне попередження. Сспрямоване на усунення самої можливості втягнення неповнолітніх у злочинну та іншу антигромадську діяльність. До такого попередження можна віднести інформування населення через засоби масової інформації про юридичну відповідальність за здійснення на неповнолітніх криміналізуючого впливу, а також за їх втягнення у злочинну діяльність, здійснення правового виховання населення, правової агітації. Проведення віктимологічної профілактики серед неповнолітніх, надання консультативної допомоги неповнолітнім та їх батькам тощо.

2. Індивідуальна профілактика. Застосуванням індивідуального впливу на конкретних учасників організованих злочинних груп з метою недопущення з їх боку можливих втягнень у злочин неповнолітніх та робота із неповнолітніми громадянами так званої «групи ризику» з метою недопущення вчинення ними злочинів.

Індивідуальне попередження втягнення неповнолітніх у злочинну діяльність слід починати з виявлення осіб, які потребують попереджувального впливу. Це здійснюється шляхом систематичного і своєчасного збору та узагальнення інформації. Також необхідно здійснювати оперативне спостереження за місцями можливого перебування неповнолітніх правопорушників; організації контролю за поведінкою осіб, які притягувались до кримінальної відповідальності за втягнення неповнолітніх у злочинну та іншу антигромадську діяльність або за вчинення злочинів спільно з неповнолітніми; встановлення місць збуту викраденого майна, вживання алкогольних напоїв, наркотичних та одурманюючих речовин, місць розпусти і звідництва, які відвідують неповнолітні, а також утримувачів цих місць; проведення бесід з неповнолітніми, які перебувають на обліку в органах внутрішніх справ, на предмет виявлення серед їх найближчого оточення дорослих осіб, які мають певний досвід протиправної діяльності, засуджених за вчинення злочинів до заходів покарання, не пов'язаних з позбавленням волі, або звільнених від кримінальної відповідальності за нереабілітуючими обставинами, а також інших дорослих осіб, які б могли здійснити на неповнолітніх негативний вплив, втягнути у злочинну та іншу антигромадську діяльність; проведення роботи серед неблагополучних сімей на предмет виявлення серед батьків або осіб, що їх замінюють, тих, які справляють на неповнолітніх негативний вплив та існує вірогідність втягнення ними неповнолітніх у злочинну та іншу антигромадську діяльність; здійснення контролю за поведінкою неповнолітніх, які перебувають на обліку в органах внутрішніх справ; перевірки заяв та повідомлень про суспільно небезпечні діяння, вчинені неповнолітніми, які не досягли віку кримінальної відповідальності; перевірки обставин вчинення правопорушень неповнолітніми, доставленими до органів внутрішніх справ; проведення суб'єктами попередження рейдів та інших попереджувальних заходів на території обслуговування.

Відповідно до досліджень особливо в попередженні групової злочинності неповнолітніх потрібно зауважувати на попередженні злочинів на стадії замислу та підготовки, оскільки саме на цих стадіях можливе переростання їх в посягання чи закінчений злочин. Тому необхідно організовувати отримання первинної інформації про замисел або підготовку учасників злочинних груп до вчинення злочину. У разі отримання такої інформації необхідно виконати комплекс заходів, спрямованих на недопущення досягнення злочинного результату. Водночас весь комплекс таких заходів умовно можна розділити на дві великі групи:

- створення умов, які будуть ускладнювати підготовку до реалізації злочинного замислу;
- індивідуальний вплив на кожного неповнолітнього учасника групи з метою схилення його до відмови від вчинення злочину.

Важливим напрямом створення умов, які ускладнюють підготовку або вчинення злочинів, є проведення заходів щодо вилучення неповнолітнього з злочинних груп. Однак вилучити неповнолітнього з групи та переорієнтувати в соціально-позитивні дуже важко. Тому вважається, що передусім важливо організувати виявлення втягнення неповнолітніх у такі групи на ранніх стадіях, коли ще не зміцніли їх зв'язки між учасниками груп та ще не вчинені конкретні злочини.

Отже з метою попередження втягнення неповнолітніх у злочинну діяльність слід здійснювати оперативно-розшукові заходи за такими етапами:

1) виявлення злочинного наміру втягнення неповнолітніх у злочинну діяльність;
2) перевірка первинної інформації про втягнення неповнолітніх у злочинну діяльність з використанням негласних працівників;
3) застосування заходів із недопущення реалізації злочинного наміру, а саме: встановлення неповнолітньої особи відносно якої є намір залучення до злочину; вплив на

неповнолітню особу з метою її відмови від втілення злочину; створення умов, які ускладнюють підготовку та реалізацію злочинного замислу; застосування засобів громадського або адміністративного впливу за різні види правопорушень; демонстрація дій, що створюють переконаність особи в незворотності викриття та покарання, а також в поінформованості органів внутрішніх справ про її поведінку та замисли.

1. Гребельский Д. В. О соотношении криминалистических и оперативно-розыскных характеристик преступлений / Д. В. Гребельский. – М.: ВНИИ МВД СССР, 1981. – 170 с.
2. Горяинов К. К. Общая характеристика преступлений / К. К. Горяинов. – М.: ВНИИ МВД СССР, 1980. – 76 с.
3. Топольська І.О. Боротьба із втягненням неповнолітніх у злочинну діяльність або іншу антигромадську діяльність/монографія/Луганск РВВ ЛАВС 2003 – 192с.
4. Кримінальний кодекс України
5. Гайдар А. І. Оперативно-розшукові заходи органів внутрішніх справ у боротьбі з груповою злочинністю неповнолітніх: дис. к.ю.н. / А. І. Гайдар. – ХНУВС, 2006. – 110–126с.

СПРОЩЕНЕ ЕЛЕКТРОННЕ ПРОВАДЖЕННЯ У ГОСПОДАРСЬКОМУ СУДОЧИНСТВІЇ

Мелех Л.В.

доцент кафедри господарсько-правових дисциплін факультету №6 Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Спрощене електронне провадження є перспективним напрямком адаптації форм електронних проваджень, що існують у багатьох країнах світу стосовно господарського правопорядку України.

Надаючи сторонам можливість користуватися засобами комп'ютерної техніки при подачі позову, відзиву на нього, інших письмових пояснень та заперечень, не можна вважати спрощенним

провадження, оскільки це є тільки зручним технічним супроводом, який став можливим за допомогою розвитку комп'ютерних технологій та створенню і існуванню мережі Інтернет. Вказане можна визначити як підвищення зручності форми викладення матеріалу, що існує в об'єктивній реальності.

У науково-практичних форумах більшістю науковців електронне провадження сприймається як апріорі спрощене, проте, тут слід заперечити, оскільки електронне провадження не завжди є спрощеним, більше того, зазначимо, що воно в переважній більшості не є спрощеним, оскільки у представлених моделях інших країн являє собою електронний супровід позовного провадження та процесуальних дій, що передбачені в його межах, і тільки законодавче встановлення безпосередньо спрощення процесуальної форми дає підстави вважати провадження спрощеним.

Аналізуючи досвід світових правових систем щодо розробки та впровадження порядку реалізації судових проваджень за допомогою комп'ютерних технологій, в цілому можна відмітити тенденцію електроніфікації позовної процедури розгляду, тоді як можливість та порядок розгляду певних категорій спорів, що відповідають встановленим критеріям, виключно за допомогою засобів комп'ютерної техніки та мережі Інтернет, залишена поза увагою.

На сьогоднішній день в Україні вже накопичено певний емпіричний і теоретичний досвід правового забезпечення в інформаційній сфері.

Високу роль електронного судочинства в транспарентності судової системи відзначає Решетняк В.І., який справедливо звертає увагу, що електронне судочинство повинно стати головним інструментом подолання правового нігілізму за допомогою забезпечення відкритого і доступного правосуддя, прискорення строків розгляду спорів і підвищення якості судових актів [1, с. 54].

Крім того, електронне судочинство є чинником, який підвищить прозорість судової системи та певність судової процедури, а також є одним з факторів зниження конфліктності у суспільстві [2, с. 74].

З урахуванням світової інформатизації та комп'ютеризації правове явище електронного судочинства а також порядок його реалізації на практиці потребує детального вивчення вітчизняними науковцями та адаптації до українського законодавства.

В роботах українських вчених, зокрема, С. Пограничного, М. Бондаренко, І.В.Туркіної [3-5], висвітлені деякі аспекти інформаційних технологій у вітчизняному судочинстві. Однак, це лише загальний огляд інформаційних технологій, шляхів їх впровадження в судочинство та спроби визначити основні напрямки політики судової влади в галузі інформаційних технологій [5, с. 200].

Позитивне висловлювання вказаних авторів про електроніфікацію судової системи граничить з об'єктивним побоюванням готовності юридичної спільноти країни та судової системи в цілому до впровадження інформаційних комп'ютерних технологій в українське судочинство, у зв'язку з низьким рівнем розвитку інформаційних технологій в судочинстві, в тому числі і в матеріальному аспекті.

Проаналізувавши існуючі в науці критерії спрощення судочинства, можна зробити висновок, що модель спрощеного електронного судочинства, має встановлювати не тільки електронний супровід розгляду певних категорій спорів в порядку позовного провадження, але й відрізнятись від позовного провадження скороченням певних стадій процесу, як-то безпосередній судовий розгляд з судовими засіданнями за участю представників сторін (на його зміну приходить розгляд та змагальність поданих сторонами в електронному вигляді документів), а також скороченням строків розгляду позову з підстав його базування на вимогах, що були раніше розглянуті судом в іншій справі.

На відміну від існуючих світових моделей спрощених проваджень, що в структурі спрощеного електронного провадження розгляд справи буде здійснюватись безпосередньо у призначені судом дні для подання витребуваних доказів, без стандартного судового засідання. Зазначене, на відміну від повної відмови від судових засідань буде більш дисциплінувати суддів, а також

давати змогу сторонам процесу та іншим його учасникам орієнтуватись на певні дати для підготовки та надання суду витребуваних матеріалів.

Крім того, в моделі спрощеного електронного провадження, зазнає змін процес подання доказів, вивчення судом матеріалів, поданих в електронному вигляді, що не потребують паперового дублювання з огляду на їх джерела отримання.

Для з'ясування поняття та суті спрощеного електронного провадження слід окреслити його ознаки. Їх можна визначити за критерієм явної відмінності від інших форм провадження.

Так, першою ознакою є безпаперова форма позову, підписаного єдиним електронним підписом, доступ до якого буде у керівника юридичної особи або особи, ним уповноваженої, та доданих до нього документів в якості доказів, відповідно до Закону України "Про електронний цифровий підпис" [6].

Дана форма існування доказів в об'єктивній реальності може бути запроваджена за допомогою спеціальних технічних засобів, які унеможливлять підробку письмових доказів.

При застосуванні в Україні процедури електронного спрощеного провадження в практичному аспекті, електронний цифровий підпис відіграє важливу роль в автентичності оригіналу паперового документу його електронній копії або достовірності електронного документу, та є його невід'ємним атрибутом.

Другою ознакою є те, що спрощене електронне провадження характеризується як провадження без фізичної участі сторін.

Водночас, до третьої ознаки можна віднести здійснення спрощеного електронного провадження за допомогою засобів комп'ютерної техніки та мережі Інтернет.

Таке можливо за умови наявності відповідного технічного устаткування та програмного забезпечення, при чіткому нормативному супроводі та впровадженню нових технологій в нині існуючий господарський процес.

Четвертою ознакою є розгляд в порядку спрощеного електронного провадження чітко визначених категорій, а саме: 1) стягнення штрафних санкцій, 3 % річних, втрат від інфляції, нарахованих на заборгованість, що була предметом розгляду господарського суду та стягнута за його рішенням; 2) стягнення боргу та похідних від нього вимог за мировими угодами, що були затверджені господарським судом за результатами розгляду іншої господарської справи.

Отже, підсумовуючи, зазначимо, що спрощене електронне провадження являє собою процес розгляду спору без участі сторін, виключно на підставі поданих до суду за допомогою засобів комп'ютерної техніки та отриманих судом в електронному вигляді документів на підтвердження певних обставин справи, встановлення яких необхідно для вирішення її по суті. Це є принциповою відмінністю даного виду провадженні від нині існуючих.

1. Решетняк В. И. Электронное правосудие и транспарентность судебной системы [Електронний ресурс] / В.И. Решетняк // Электронное приложение к юридическому журналу. – 2011. – № 3. – С. 51-55.
2. Чуча С. Ю. Электронное судопроизводство как фактор снижения конфликтности в обществе / С. Ю. Чуча, И. В. Сорокина, Е. А. Кулагина // Закон. – 2011. – № 2. - С. 73 – 76.
3. Пограничный С. Виртуальный суд: опыт и перспективы / С. Пограничный // Судебно-юридическая газета. – 2009. – № 03 (003). – С.4.
4. Бондаренко М. Судочинство он-лайн: мрія чи реальність / М. Бондаренко // Правовий тиждень. – 2009. – № 48 (147). – С.5
5. Туркіна І .Є. Інформаційні технології в судовій системі / І.Є. Туркіна // Публічне управління: теорія та практика: збірник наукових праць Асоціації докторів наук з державного управління. – Х.: Вид-во «ДокНаукДержУпр», 2011. – № 3(7) – С. 199-202.
6. Закон України "Про електронний цифровий підпис" від 22.05.2003 № 852-IV // Офіційний сайт Верховної ради України [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/852-15.

КРИМІНАЛЬНИЙ АНАЛІЗ ПОКАЗНИКІВ ЗЛОЧИННОСТІ В УКРАЇНІ

Михайлов Р.І.
начальник факультету №1 Донецького юридичного інституту МВС України, кандидат юридичних наук

Політова А.С.
доцент кафедри кримінально-правових дисциплін та судових експертиз факультету №1 Донецького юридичного інституту МВС України, кандидат юридичних наук

Дослідження особливостей того чи іншого виду злочинів, їх наукове осмислення, дозволяє не лише отримати повні і точні дані про дійсний стан злочинності в країні, виявити вплив тих чи інших факторів на злочинність, але й спрогнозувати ймовірні зміни її стану, отже, визначити пріоритетні напрямки, найбільш ефективні засоби та методи діяльності правоохоронних органів щодо протидії злочинності та її окремим проявам.

Кримінальна ситуація в Україні протягом останнього десятиліття продовжує невпинно загострюватися, про що говорить збільшення кількості вчинених злочинів, а також підвищення їх суспільної небезпеки. Для формування ефективної системи протидії злочинності необхідно вивчити та провести кримінологічний аналіз стану злочинності на сучасному етапі розвитку українського суспільства.

У підручниках з кримінології зазначено, що кримінологічний аналіз стану злочинності полягає у дослідженні процесів і явищ, які входять до предмету кримінології і характеризують злочинність або певним чином впливають на неї [1, с.57]. Виходячи із наведеного визначення, предметом кримінологічний аналіз стану злочинності є:

- характеристика окремих видів злочинів, виділення за певними кримінально-правовими та кримінологічними ознаками;

- злочинність, її стан, рівень, структура, динаміка та географія поширеності;
- особа злочинця;
- жертви злочинних посягань, їх характеристика за соціально-демографічними та кримінологічними ознаками;
- причини та умови економічного, соціального, демографічного, політико-правового, соціально-психологічного характеру, що зумовлюють вчинення злочину;
- прогноз злочинності в цілому та окремих видів злочинів [2, с. 14-15].

Одним із основних і найважливіших елементів кримінологічної характеристики стану злочинності є її рівень. При цьому значний інтерес викликає рівень розкриття злочинів. Саме аналіз рівня розкриття окремих видів злочинів дає уявлення про ефективність протидії злочинності з боку правоохоронних органів та залежність зміна структури злочинності від діяльності останніх. На наш погляд, доречно проаналізувати стан злочинності України з 90-хроків XX століття.

О.Г. Кулик умовно період з 1992 до 2012 рр. можна поділити на два періоди, який витікає із динаміки зареєстрованих злочинів [2, с. 37].

Перший період – це 1992-1996 рр. У зазначений період кількість зареєстрованих злочинів в Україні постійно зростала в середньому на 10% за рік. Так, наприклад, у 1995 р. було зареєстровано 641860 злочинів, а коефіцієнт злочинності в розрахунку на 10 тис. населення України склав 124,1. Разом з тим, за даними 1996 р. зафіксована істотна зміна тенденції. Кількість зареєстрованих злочинів знизилась на 3,8% і склала 617535. Відповідно знизився до 120,2 і коефіцієнт злочинності [3, с. 14]. Проте, О. Литвак відзначає, що згідно з опублікованими розрахунками, коефіцієнти інтенсивності злочинів в України за роки її незалежності на 100 тис. населення були: у 1992 р. – 921, 1993 р. – 1033, 1994 р. – 1096, 1995 р. – 1241, 1996 р. – 1202. Зростання за 5 років – на 30,5%, у середньому – 6% щорічно [4, с. 14].

Другий період (1996-2009 рр.) вирізняється тенденцією для переважного зниження кількості зареєстрованих злочинів, що

відбувалося нерівномірно. До 2002 р. їх число постійно скорочувалося в середньому на 4,8% за рік і склало 450661 (-29,8%), а коефіцієнт злочинності дорівнював 939. У 2003 р. мав місце сплеск кількості зареєстрованих злочинів до 556331 (+23,5% порівняно з показником минулого року), а коефіцієнта злочинності – до 1168, що майже на чверть більше, ніж у 2002 р. У наступні чотири роки відновилася тенденція до зниження зареєстрованої злочинності, в результаті якої у 2008 р. було зареєстровано 384424 злочини,а коефіцієнт злочинності скоротився до 833 [2, с. 39]. У 2009 р. було зареєстровано 434679 злочинів (+13 порівняно з показником 2008 р.), а коефіцієнт злочинності склав 946.

Продовжуючи аналіз стану злочинності, ми вважаємо за необхідне, виділити і третій період – з 2012 р. і дотепер.

У зв'язку з набуттям чинності 20 листопада 2012 року нового Кримінального процесуального кодексу України, змінився порядок реєстрації заяв та повідомлень про злочин. Так, станом на 20.11.2012 у МВС України зареєстровано 443700 злочинів, що на 6,6% менше порівняно з аналогічним періодом 2011 р. У цей період спостерігається незначне зменшення кількості зареєстрованих злочинів середньої тяжкості – 231200, що на 4,8% менше ніж минулого року, тяжких злочинів – 145700, що на 7,1% менше ніж минулого року. Разом з тим, збільшилась питома вага злочинів середньої тяжкості та становила 52,1% (у 2011 р. – 51,1% від загальної кількості зареєстрованих злочинів), питома вага тяжких злочинів зменшилась у 2012 р. на 32,8% (у 2011 р. відповідно на 33%). Істотно зменшилась (на 11,3 %) кількість зареєстрованих особливо тяжких злочинів – 9300, злочинів невеликої тяжкості – 57400 (на 11,5%).

Що ж стосується аналізу злочинності останніх років, то абсолютний приріст 2016 р. (показники за 11 місяців) по відношенню до 2010 р. становить 270,5 тис. злочинів. Середньорічний абсолютний приріст за 2010-2016 рр. становить 45 тис. злочинів, середній темп зростання – 1,093, середній темп приросту – 9,3%.

За січень-вересень 2017 року правоохоронними органами було зареєстровано 446158 тис. кримінальних правопорушень, з яких 355208 тис. – це ті кримінальні правопорушення, щодо яких судом було винесене рішення. Тобто, фактично 90950 тис. злочинів залишаються поза межами правосуддя. Максимальний відсоток розкриття злочинів за період 2010-2016 рр. був забезпечений у 2010 р. та становив 72,1%. Мінімальний – у 2016 р. – 25,2%.

Структура сучасної злочинності в Україні характеризується значною часткою тяжких та особливо тяжких злочинів, загальна кількість яких у першому півріччі 2017 р. сягнув 168632 тис Залежно від об'єкта посягання традиційно лідирують злочини проти власності, частка яких у січні-вересня 2017 р. сягнула 284852 тис. Серед зареєстрованих злочинів проти власності превалюють крадіжки – 220501 тис. (77,4% від всіх злочинів проти власності). Грабежі та розбої становлять 5,0% (14475 злочинів) та 0,8% (2315 злочинів) відповідно шахрайства – 11,6% (33152 злочинів), 5,2% – інші. Таке співвідношення загально-кримінальних корисливих злочинів є традиційним для структури злочинності в Україні та не вирізняється специфічними змінами протягом останніх п'яти – шести років.

Рис 1. Стан злочинності в Україні у 1991-2017 рр. [5]

Отже, проведений нами аналіз динаміки злочинності показав, що вона характеризується хвилеподібними коливаннями, при якому, найвище значення амплітуди припадає на 1995 р. та 2016 р., а найнижче – на 2008 р. Тим не менш, вираженою є загальна тенденція до зростання рівня злочинності.

Українським реаліям властивий вплив практично всіх детермінант, які обумовлюють злочинність в державах перехідного типу та деяких країнах «третього світу». У цьому сенсі в Україні діють ті ж криміногенні детермінанти, що і в більшості пострадянських країн та державах Центрально-Східної Європи з урахуванням вітчизняних економічних, політичних та соціокультурних реалій. Водночас видається можливим виділення особливостей дії цих причин, а також деяких специфічних криміногенних факторів в Україні.

Глибинні причини злочинності в нашій державі полягають в особливостях процесів, які відбуваються в усіх сферах українського суспільства і, в першу чергу, в ціннісно-нормативній. Йдеться передусім про девальвацію моралі, заснованої на загальнолюдських цінностях, крах колективістських соціалістичних цінностей радянської епохи, разюча відмінність між проголошеними владою деклараціями та повсякденною реальністю кризового суспільства, яка надзвичайно далека від високих етичних ідеалів (цинізм, аморалізм, гонитва за прибутками за будь-яку ціну, фантастичне збагачення нуворишів, безкарність зловживань політичної еліти та чиновників тощо). Криміногенне значення має також панування примітивних зразків «масової культури» (передусім на телебаченні), основними цінностями яких є крайній індивідуалізм, культ «розкішного життя», жорстокість, розпущена сексуальна поведінка, всеохоплююче споживацтво. Надзвичайно негативний вплив має і кримінальна субкультура (особливо молодіжна), якій належить виключна роль у відтворенні злочинності.

Отже, маємо констатувати усталення стійкого негативного тренду до погіршення кримінологічної ситуації в нашій державі. Не останню роль у цьому відіграє істотна дисфункція

правоохоронної та судової системи, про що можна зробити висновок, виходячи з рівня та динаміки розкриття злочинів і практики судочинства у кримінальних провадженнях.

1. Закалюк А.П. Курс сучасної української кримінології: теорія і практика: у 3 кн. / А.П. Закалюк. – К.: Видавничий Дім «Ін Юре», 2007. – Кн. 3: Практична кримінологія. – 320 с.
2. Кулик О.Г. Злочинність в Україні: тенденції, закономірності, методи пізнання : монографія / О.Г. Кулик. – К.: Юрінком Інтер, 2011. – 288 с.
3. Криміногенна ситуація в Україні: оцінка, тенденції, проблеми / Інформаційне бюро; Штаб МВС України; Науковий центр Національної академії внутрішніх справ. – К., 1997. – 96 с.
4. Литвак О. Злочинність, її причини та профілактика / О. Литвак. – К. : Україна, 1997. – 167 с.
5. Злочинність в Україні: статистика за минулий рік : [Електронний ресурс]. – Режим доступу: https://www.slovoidilo.ua/2018/02/16/infografika/suspilstvo/zlochynnist-ukrayini-statystyka-mynulyj-rik

ОКРЕМІ АСПЕКТИ ВИКОРИСТАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ В ОРГАНАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Мовчан А.В.

професор кафедри оперативно-розшукової діяльності факультету №2 ІПФПНП Львівського державного університету внутрішніх справ, доктор юридичних наук, старший науковий співробітник

У країнах Європейського Союзу, США та інших розвинених країнах світу використання можливостей кримінального аналізу є обов’язковим для всіх правоохоронних органів. Його зміст, правила та процедури чітко визначено й урегульовано в нормативно-правових актах. Це, зокрема, стосується ведення оперативно-розшукової діяльності, досудового розслідування та розгляду кримінальних проваджень у суді.

У ході кримінального аналізу забезпечується цілеспрямований пошук, виявлення, фіксація, отримання, систематизація, аналіз та оцінка кримінальної інформації, її представлення (візуалізація), передача та реалізація.

Зокрема, в аналітичній роботі використовується:

- оперативний аналіз;
- тактичний аналіз;
- стратегічний аналіз;
- аналіз даних з відкритих джерел (OSINT);
- аналіз даних з багатьох джерел (Multi-Source Analysis).

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

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

Водночас зазначимо, що у нинішніх умовах правоохоронні органи України фактично не протидіють системним злочинам. У нас поки що діє організація поліцейської діяльності, яка не орієнтована на проведення системного аналізу ризиків, можливих збитків, вразливостей, суб'єктів щодо їх причетності до скоєння злочинів.

Консультативна місія Європейського Союзу в Україні (КМЄС) підтримує впровадження в Національній поліції України моделі поліцейської діяльності, керованої аналітикою (Intelligence-Led Policing/ILP) [1].

ILP є моделлю поліцейської діяльності, згідно з якою оперативно-аналітична інформація/intelligence слугує підставою для проведення операцій/розслідувань, а не навпаки.

Ця модель дозволяє зменшити матеріальні витрати, знизити рівень злочинності, забезпечити більш високий рівень безпеки

особового складу. Надаючи аналітикам можливість опрацьовувати дані про злочини, оперативні працівники та слідчі отримують можливість використовувати готовий оперативно-аналітичний продукт, а не первинну інформацію.

При цьому вони отримують такі переваги:

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

по-друге, продукт надає можливість мати більше інформації щодо місць ймовірного скоєння злочинів, що дозволяє покращити попередження правопорушень;

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

Майже всі департаменти кримінального блоку Національної поліції України у своїй структурі мають аналітичні відділи, або працівників, які виконують завдання у сфері аналізу. Водночас жоден з аналітичних підрозділів не створює аналітичні продукти відповідно до європейських стандартів. Крім того, відсутня належна взаємодія між департаментами щодо обміну аналітичною інформацією.

У системі Національної поліції існує багато джерел розрізненої інформації, яка аналізується співробітниками різних служб автономно. Наприклад, у Департаменті протидії наркозлочинності аналізується інформація, пов'язана з наркозлочинами, у Департаменті карного розшуку – інформація щодо загальнокримінальної злочинності тощо.

Крім того, кожний оперативний працівник накопичує і зберігає власну оперативну інформацію, яка після його звільнення або переміщення по службі стає практично недоступною для інших оперативних працівників.

Держава витрачає кошти на отримання інформації, а в результаті ця інформація втрачається. При цьому порушується європейський принцип про те, що інформація не належить конкретному поліцейському, інформація належить державі як один із продуктів діяльності поліції. Тому постає задача консолідації всієї

оперативної інформації, її подальшого аналізу, що має сприяти розкриттю насамперед тяжких та особливо тяжких злочинів.

Більшість департаментів в оперативно-службовій діяльності використовує такі джерела інформації, як Інтегровану інформаційно-пошукову систему Національної поліції та статистичну інформацію, надану Департаментом інформаційно-аналітичної підтримки.

Можливості здійснення аналізу інформації з відкритих джерел (OSINT) в кожному підрозділі є різними, хоча мережа Інтернет є одним із найбільш повних джерел даних.

Найбільш поширеним аналітичним інструментом, що використовується у повсякденній роботі органів Національної поліції, є Microsoft Office (Word та Excel), хоча в деяких департаментах застосовується аналітичне програмне забезпечення (зокрема, i2 Analyst's Notebook, E-Gis maps, ArcGIS тощо).

У 2017 році в структурі центрального апарату Національної поліції України створено Управління кримінального аналізу, яке має виконувати функцію координації діяльності у сфері аналізу і впровадження та розвитку моделі поліцейської діяльності, керованої аналітикою.

Суттєвим аспектом аналітичної діяльності є аналіз географічних даних. У нинішніх умовах географічні дані є джерелом цінної інформації на кожному рівні роботи правоохоронних органів. Розвиток цього напрямку аналізу передбачає наявність спеціалістів-аналітиків, які зможуть здійснити оцінку даних на базі географічних інформаційних систем (GIS) для оперативних підрозділів.

Зокрема, з метою профілактики і оперативного реагування на злочини аналітики Управління кримінального аналізу запроваджують географічну прив'язку до кожного житлового будинку, з можливістю нанесення інформації на карту. Це дасть можливість здійснювати якісний аналіз скоєних правопорушень, визначати зони вчинення злочинів, скеровувати в такі місця додаткові наряди патрульної поліції та ставити завдання дільничному офіцеру поліції щодо повторного відпрацювання місць проживання осіб, які перебувають під адміністративним наглядом.

З усіх існуючих методик аналізу оперативної інформації, прийнятих на озброєння правоохоронними органами більшості розвинених країн світу, найбільш часто використовуються програмні продукти і2 і ANACAPA. Такі програмні рішення візуального аналізу даних і отримання нових знань призначені для оперативних підрозділів і слідчих, чия діяльність пов'язана з необхідністю аналітичної обробки інформаційних потоків і даних, представлених в різних форматах.

Зокрема, програмний продукт і2 являє собою комп'ютерне програмне забезпечення на базі SQL-server, покликане узагальнювати, аналізувати, висувати ймовірнісні зв'язки, а також візуалізувати в реальному часі обмін інформацією. Це програмне забезпечення є набором сумісних між собою різних програм, що виконують відповідні специфічні функції на всіх етапах розкриття і розслідування злочинів. У сфері кримінального аналізу і2, як правило, застосовується із програмними продуктами iBase, iBridge, iGlass, Analyst's Workstation.

Серед користувачів даної операційної аналітичної системи можна виділити правоохоронні органи США та Канади (ФБР, ЦРУ, DEA, NSA, RCMP), правоохоронні органи країн Євросоюзу, Інтерпол та Європол [2].

Програмний продукт компанії «Anacapa Sciences Inc.» являє собою передову методику розслідування злочинів і аналізу оперативної інформації. ANACAPA стояла біля витоків розробки спеціальних аналітичних методик для сфери безпеки і ще в 1971 році почала проведення навчальних курсів з підготовки фахівців-аналітиків.

Національна поліція України з урахуванням досвіду поліції інших країн планово запроваджує міжнародні стандарти управління інформацією у сфері запобігання правопорушенням та розслідування злочинів. Заходи з упровадження кримінального аналізу проводяться в рамках реалізації відомчої програми одночасно зі створенням системи аналізу ризиків.

Доповнювати аналітичну діяльність повинна кримінальна розвідка, що надасть можливість отримати доступ до джерел інформації

та слідів злочину, до яких немає вільного доступу або відсутня можливість отримати такий доступ у гласний спосіб.

При цьому шляхом кримінального аналізу здійснюється:

- визначення учасників кримінальних схем, зв'язків, кількості та характеру контактів;
- визначення джерел та напрямів фінансових потоків, інших матеріальних об'єктів;
- визначення механізму організації злочинної діяльності, підґрунтя функціонування кримінального явища;
- оцінка ризиків, загроз, можливих збитків, вразливостей для прийняття управлінських рішень.

Водночас кримінальна розвідка сприяє:

- визначенню джерел інформації та слідів злочину, до яких немає вільного доступу або відсутня можливість отримати такий доступ у гласний спосіб;
- отриманню ґрунтовної інформації про: об'єкт, відносно якого є обґрунтовані підозри щодо причетності до злочину; ієрархічну побудову ОЗУ, специфіку та характер їх діяльності, розгалужену кримінальну інфраструктуру;
- нейтралізації діяльності окремих ОЗУ, руйнування кримінальних технологій [3].

Головною метою кримінального аналізу є зміцнення механізмів попередження, виявлення, документування та розслідування кримінальних правопорушень, а також налагодження механізмів моніторингу криміногенної ситуації, обміну інформацією на державному, регіональному та міжнародному рівнях стосовно тенденцій та ризиків у цій сфері.

Крім того, потребують нагального вирішення наступні проблеми:

1) забезпечення аналітиків доступом до спеціального аналітичного програмного забезпечення;
2) створення захищеної мережі для організації обміну інформацією в електронній формі;

3) створення ІТ-системи збирання та обробки оперативно-аналітичної інформації.

Успішна реалізація та впровадження нових методів кримінального аналізу дасть можливість у майбутньому поширити їх на всю систему Національної поліції та активно використовувати сучасні аналітичні методи і прийоми, завдяки яким можливо створити передумови для більш ефективного виконання оперативними і слідчими підрозділами своїх завдань, що, у свою чергу, сприятиме підвищенню ефективності протидії злочинності в цілому.

Отже, впровадження кримінального аналізу в діяльність правоохоронних органів доводить свою ефективність і в даний час може бути успішно використано в роботі оперативних і слідчих підрозділів Національної поліції.

---

1. Правоохоронна діяльність, керована аналітикою: передова методика сучасної правоохоронної діяльності [Електронний ресурс]. – Режим доступу: http://euam.php7.postbox.kiev.ua/ua/news/opinion/intelligence-led-policing-the-cutting-edge-of-modern-law-enforcement/.
2. Возможности использования аналитических программ в борьбе с организованной преступностью [Электронный ресурс]. – Режим доступа: https://articlekz.com/article/11838.
3. Мельник В., Некрасов В. Як подолати ворога, багатшого за транснаціональні корпорації? [Електронний ресурс]. – Режим доступу: http://n-v.com.ua/yak-podolaty-voroga-bagatshogo-za-korporatsyi/.

АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Мовчан М.А.

начальник відділу Державного науково-дослідного інституту МВС України, кандидат юридичних наук

Інформаційна безпека у сучасному постіндустріальному світі, в якому основним товаром є інформація, яка впливає на прийняття державою тактичних та стратегічних рішень, є основою

національної безпеки. Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни.

Відповідно до статті 17 Конституції України захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [1].

Інформаційна безпека відіграє важливу роль у забезпеченні інтересів будь-якої держави. Створення розвиненого і захищеного інформаційного середовища є неодмінною умовою розвитку суспільства та держави.

Необхідність гарантування інформаційної безпеки зумовлюється, по-перше, потребою забезпечення національної безпеки в цілому; по-друге, існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам; по-третє, врахуванням того, що за допомогою інформації можна впливати на зміну свідомості і поведінку людей.

Країни, які не можуть забезпечити власну інформаційну безпеку, стають неконкурентоспроможними і, як наслідок, не можуть брати участь у боротьбі за розподіл ринків та ресурсів. Деякі науковці припускають, що зникнення великих держав відбувалося не в останню чергу через неспроможність ефективного управління на власній території та невідповідність інформаційної структури новим умовам існування [2, с. 90].

Отже, незаперечним є те, що в будь-якій розвиненій країні має існувати система забезпечення інформаційної безпеки.

Інформаційна безпека, як стан захищеності суспільства, держави, особистості, стан захищеності інформаційних ресурсів, забезпечує прогресивний розвиток життєво важливих сфер для суспільства.

Завдання інформаційної безпеки – це створення системи протидії інформаційним загрозам та захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави. При виникненні криз, загостренні конфліктів

інформаційна боротьба може перерости в інформаційну війну, яка здійснюється за допомогою інформаційної зброї. Показниками виступають цілеспрямованість, масштабність та комплексність дій тощо [3, с. 69].

Головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їх поведінкою і розвитком у бажаному для іншої сторони напрямку. Власне, це є загрозою суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізовується на інформаційному рівні [4, с. 27].

Стратегічне інформаційне протистояння є самостійним і принципово новим видом протистояння. Застосування технологій гібридної війни перетворило інформаційну сферу на ключову арену протиборства. Використання найновіших інформаційних технологій впливу на свідомість громадян спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом та порушення суверенітету і територіальної цілісності [5].

Для вивчення закономірностей інформаційного протистояння та аналізу його кількісних характеристик необхідно формалізувати рівні інформаційної озброєності держави і механізм еволюції в залежності від ресурсного потенціалу та впливу зовнішнього оточення.

Так, країна з високим рівнем інформаційної озброєності має змогу керувати країною з нижчим її рівнем, спрямовуючи розвиток цієї країни в своїх інтересах під постійним інформаційним контролем. Менш розвинена в інформаційному відношенні країна відстає у виробництві нових знань (технологій) і вимушена використовувати готові рішення, які їх нав'язують ззовні, внаслідок чого вона потрапляє в залежність від зовнішніх інформаційних ресурсів і технологій [6, с. 72].

З огляду на зазначене, кожна держава, що є частиною світового інформаційного простору, має виробити комплекс заходів для свого сталого інформаційного розвитку в умовах жорсткої конкуренції з урахуванням чинників інформаційної безпеки.

Як зазначає І. Р. Боднар, для цього необхідно:

- розуміння інформаційного протистояння як феномену, що має певну логіку розвитку;
- створення математичних моделей та на їх базі – сценаріїв ведення інформаційної війни;
- вироблення кількісних і якісних показників інформаційних загроз з метою вдосконалення механізмів прийняття рішень в системах державного і військового управління;
- розроблення програмного продукту на базі національного науково-виробничого потенціалу для забезпечення максимального захисту від зовнішніх впливів на комп'ютерні комунікації;
- аналіз стану і технічний аудит всіх засобів інформаційної війни з урахуванням їх відповідності сучасним вимогам;
- консолідація діяльності органів державної влади, політичних партій та ЗМІ у сфері політичного інформування суспільства для нейтралізації негативного психологічного впливу на соціум [4, с. 28].

У процесі забезпечення інформаційної безпеки важливо розуміти характер, природу, сутність і зміст загроз та небезпек, вміти своєчасно ідентифікувати джерело загрози.

Дії, пов'язані із забезпечення інформаційної безпеки, мають включати:

- спостереження, аналіз, оцінку та прогноз загроз та небезпек, критичної інфраструктури, ступеню національної уразливості;
- відпрацювання стратегії і тактики, планування попередження нападу, укріплення потенційних зв'язків, вирівнювання ресурсів забезпечення інформаційної безпеки;
- дії по забезпеченню інформаційної безпеки;

- відбір сил і засобів протидії, нейтралізації, недопущення нападу, мінімізації шкоди від нападу;
- управління наслідками інциденту (кібератаки, інформаційні операції, інформаційні війни).

Удосконалення забезпечення інформаційної безпеки потребує цілеспрямованого вивчення зарубіжного досвіду організації і проведення інформаційних операцій, методів, засобів здійснення кібератак, а також моделювання інформаційних нападів.

Система забезпечення інформаційної безпеки має бути міжвідомчою та ієрархічно організованою. Її структура й організація має відповідати структурі державного управління з чіткою координацією дій окремих сегментів. Організація ефективної системи забезпечення інформаційної безпеки передбачає централізоване управління із конкретними відомчо- розпорядницькими функціями, які забезпечують моніторинг і контроль за усіма компонентами національного інформаційного простору. Система забезпечення інформаційної безпеки має у будь-яких ситуаціях скоординованої багаторічної і багатоаспектної інформаційної операції володіти здатністю зберігати важливі параметри свого функціонування [7, с. 175-176].

На сьогодні, на державному рівні здійснюються перші кроки інформаційного розвитку, спрямовані на підвищення обороноздатності та зміцнення національної безпеки. Так, починає впроваджуватись цілісна державна політика у сфері інформаційної безпеки. Зокрема, ухвалено та уведено в дію Стратегію кібербезпеки України [8] та Доктрину інформаційної безпеки України [5], якими впроваджуються основні принципи діяльності держави із забезпечення інформаційної безпеки, визначені національні інтереси в інформаційній сфері, актуальні загрози національним інтересам та національній безпеці України та пріоритети державної політики в інформаційній сфері.

З огляду на зазначене, основні акценти державної інформаційної політики повинні базуватись на забезпеченні інформаційної безпеки, що закріплені у згаданих правових актах, з урахуванням права на достовірну, повну та своєчасну інформацію, свободу

слова та інформаційну діяльність, недопущення втручання в зміст та внутрішню організацію інформаційних процесів, крім випадків, визначених законодавством відповідно до Конституції України; збереженні та вдосконаленні вітчизняного національного інформаційного продукту та технологій, забезпеченні інформаційної та національно-культурної ідентифікації України у світовому інформаційному просторі; гарантуванні державної підтримки та розвитку ресурсів науково-технічної продукції та інформаційних технологій.

1. Конституція України : Закон від 28.06.1996 № 254к/96-ВР / Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.
2. Степко О. М. Аналіз головних складових інформаційної безпеки держави / О. М. Степко // Науковий вісник Інституту міжнародних відносин НАУ. Серія: економіка, право, політологія, туризм –Том 1. – № 3. – 2011. – С. 90-99.
3. Боднар І. Р. Інформаційна безпека як основа національної безпеки / І. Р. Боднар // Механізм регулювання економіки – № 1. – 2014. – С. 68-75.
4. Боднар І. Р. Пріоритетні напрями держави в сфері інформаційної безпеки / І. Р. Боднар // Економіка та держава – № 2. – 2012. – С. 27-29.
5. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лютого 2017 року № 47/2017 [Електронний ресурс] – Режим доступу до ресурсу : http://www.president.gov.ua/documents/472017-21374.
6. Гуцалюк М. Інформаційна безпека в сучасному суспільстві / М. Гуцалюк // Право України. – 2005. – № 7. – С. 71–74.
7. Ліпакін В. А. Інформаційна безпека України в умовах євроінтеграції : Навчальний посібник / В. А. Ліпакін, Ю. Є. Максименко, В. М. Желіховський // Серія : Національна і міжнародна безпека – К.: КНТ. – 2006. – 280 с.
8. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 березня 2016 року № 96/2016 [Електронний ресурс] – Режим доступу до ресурсу : http://www.president.gov.ua/documents/962016-19836.

ПРОБЛЕМНІ АСПЕКТИ ДІЯЛЬНОСТІ КРИМІНАЛЬНОЇ ПОЛІЦІЇ ПО РОЗКРИТТЮ ЗЛОЧИНІВ

Орлов В.А.
декан факультету № 2 Донецького юридичного інституту МВС України, кандидат юридичних наук

Вкрай негативні тенденції злочинності, що супроводжуються наростанням фактичного відставання можливостей правоохоронної системи від розвитку злочинності відбувається через недоліки та прорахунки систем забезпечення діяльності правоохоронних органів, що обумовлює високий рівень латентності злочинності, безкарність винних у вчиненні злочинів та в цілому неспроможність правоохоронних органів у сучасних умовах ефективно протидіяти злочинності [1, с. 17]. Наше суспільство відчуває стан захищеності життєво важливих інтересів особи від злочинних посягань та оцінює діяльність органів правопорядку по належному рівню виявлення та попередження конкретних кримінальних правопорушень в містах, селищах та селах.

Тому метою зусиль науковців та практичних працівників є з'ясування проблем пов'язаних з діяльністю кримінальної поліції по розкриттю злочинів та моделювання перспектив у вирішенні актуальних проблем у цій сфері.

Виявленням кримінальних правопорушень, припиненням виявлених кримінальних правопорушень, розшуком осіб, які переховуються від органів досудового розслідування, суду, тих що пропали без вісті в Національній поліції України займаються підрозділи кримінальної поліції. Дієвим інструментом для попередження, своєчасного виявлення і припинення злочинів, а також встановлення фактичних даних по кримінальному правопорушенню є оперативно-розшукова та інформаційно-аналітична (інформаційно-пошукова) діяльність цих підрозділів.

Так, стаття 2 Закону України «Про оперативно-розшукову діяльність» закріпила: «оперативно-розшукова діяльність – це система

гласних і негласних пошукових, розвідувальних та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів».

Але не треба забувати, що сам Закон України «Про оперативно-розшукову діяльність» (далі «Про ОРД») був прийнятий у 1992 році, після чого в нього вносилися численні зміни та доповнення. Після прийняття концептуально нового Кримінального процесуального кодексу України (далі КПК України), внесення відповідних змін до тексту Закону, сам нормативний акт вже є досить недосконалим і взагалі інститут ОРД в тому радянському вигляді не витримує жодної конкуренції. Основним аспектом суттєвих змін в інституті ОРД є виключення можливості заводити оперативно-розшукові справи (далі ОРС) умовної категорії «Злочин» (по злочинам скоєним невстановленими особами), відповідно й проводити *самостійно* оперативно-розшукові заходи з метою встановлення осіб, що скоїли кримінальне правопорушення.

За умови того, що без заведення ОРС проведення оперативно-розшукових заходів забороняється, то співробітнику кримінальної поліції при розкритті злочину скоєного в умовах неочевидності, згідно із Законом України «Про ОРД», залишаються тільки повноваження: 1) опитувати осіб за їх згодою, використовувати їх добровільну допомогу; 2) мати гласних і негласних штатних та позаштатних працівників; 4) отримувати від юридичних чи фізичних осіб безкоштовно або за винагороду інформацію про злочини, що готуються або вчинені; 4) створювати і застосовувати автоматизовані інформаційні системи.

Всі інші можливі оперативні заходи передбачають заведення ОРС «Захист» та ОРС «Розшук» (за наявності підстав) або отримання письмового доручення слідчого, прокурора на проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій у кримінальному провадженні.

КПК України у статті 41 зазначив, що під час виконання доручень слідчого, прокурора співробітник підрозділу кримінальної поліції користується повноваженнями слідчого. Вони не мають права

здійснювати процесуальні дії у кримінальному провадженні *за власною ініціативою* або звертатися з клопотаннями до слідчого судді чи прокурора.

Треба відзначити, що на сьогодні в територіальних підрозділах поліції склалась ситуація, коли співробітники підрозділів кримінальної поліції *припинили будь-яку активну діяльність* в очікуванні письмових доручень слідчого. А слідчі, через надмірне навантаження зареєстрованих кримінальних проваджень (200-300 на одного слідчого), фактично не в змозі аналізувати кожне з них та визначати завдання оперативно-пошукового характеру. При чому слідчі в окремих випадках зловживають своїми повноваженнями і доручають виконання таких процесуальних дій, які вони в змозі виконати самостійно.

Щодо повноважень по використанню гласних і негласних штатних та позаштатних працівників в територіальних підрозділах кримінальної поліції, можемо констатувати, що «агентурна» діяльність знаходиться на вкрай низькому рівні, і відсоток розкриття «неочевидних» злочинів по інформації «негласного апарату» вкрай малий. Чинний Закон України «Про ОРД» не вирішує питання чіткого розмежування негласних слідчих (розшукових) дій та оперативно-розшукових заходів, на сьогодні відсутня деталізація переліку оперативно-розшукових заходів, таким чином потребує вдосконалення правове регулювання ОРД. Отже перед законодавцем постає актуальна задача щодо прийняття нового законодавства в сфері ОРД, яке зможе істотно підвищити ефективність виявлення та попередження злочинів органами правопорядку, якщо дані про ці злочини не внесені до Єдиного реєстру досудових розслідувань[2].

Відносно інформаційно-аналітичної діяльності кримінальної поліції зазначимо, що Закон України «Про Національну поліцію» (ст. 25) надає можливість поліції: 1) формувати бази (банки) даних, що входять до єдиної інформаційної системи МВС України; 2) користуватися базами (банками) даних МВС України та інших органів державної влади; 3) здійснювати інформаційно-пошукову та інформаційно-аналітичну роботу; 4) здійснювати

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

Стаття 26 того ж Закону визначає, що поліція наповнює та підтримує в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи МВС України, стосовно 18 блоків даних, необхідних для виконання повноважень. Зокрема бази даних, що формуються в процесі здійснення оперативно-розшукової діяльності («Антарес»). Але задіяння цих АБД та ІІПС (інтегрована інформаційно-пошукова система) не завжди можливо: *по-перше* це відсутність достатньої ІТ-підготовки співробітників кримінальної поліції територіальних підрозділів, їх необізнаність в можливостях баз даних для встановлення осіб, причетних до вчинення злочину; *по-друге* – створені в територіальних підрозділах сектори інформаційних технологій займаються внесенням в бази даних статистичної звітності, а допомогу співробітникам кримінальної поліції та слідчим у інформаційно-пошуковій та аналітичній роботі не надають.

З цього питання пропонується під час навчального процесу для підготовки працівників для підрозділів кримінальної поліції ЗВО із специфічними умовами навчання впровадити спеціалізований навчальний курс «*Використання інформаційних технологій та автоматизованих баз даних у* діяльності *кримінальної поліції*». В програмі курсу передбачити вивчення: можливостей АБД та ІІПС для пошуку інформації, методів «комп'ютерної розвідки» та відпрацювання практичних навиків їх використання в діяльності кримінальної поліції.

Заходи по окресленим проблемним питанням розроблялись та планувались ще з початку створення Національної поліції України (далі НПУ), а практичний етап цих перетворень був розпочатий нещодавно. В січні 2017 року у Головному слідчому управлінні НПУ та 7 відділеннях поліції було створено так звані відділи «детективів», метою яких було налагодження ефективності розкриття злочинів та розслідування кримінальних проваджень. Вже в січні 2018 року у всіх територіальних органах НПУ було створено «служби детективів» – відділи розслідування

особливо тяжких злочинів слідчого управління [3]. Штат який складається із 75 відсотків оперативних працівників (які приймаються на посади слідчих) та на 25 відсотків – із слідчих. «Детективний» підрозділ здійснює діяльність за напрямками: загальнокримінальні злочини, наркозлочинність, кібербезпека, економічні злочини та злочини в сфері службової діяльності.

Таким чином, об'єднання в одному підрозділі співробітників органу досудового розслідування та кримінальної поліції на місцевому рівні призведе до подолання складнощів у розкритті злочинів. А впровадження інституту детективів в Національній поліції України з підготовкою відповідних законодавчих актів є прогресивним напрямком розвитку кримінальної поліції в Україні.

1. Бесчастний В.М. Теорія та практика кримінологічного забезпечення протидії злочинності в Україні: дис. … д-ра юрид. наук. Харків, 2018. 396 с.
2. Про оперативно-розшукову діяльність: проект закону № 6284 від 04.04.2017. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=61497 (дата звернення 16.03.2018);
3. Голова Нацполіції Сергій Князєв повідомив про завершення конкурсу на посади керівників детективних підрозділів. URL: https://www.npu.gov.ua/news/Informacziya/article-2223304 (дата звернення 16.03.2018).

ДЕЯКІ ПИТАННЯ ПЕРВИННОЇ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

Пекарський С. П.

заступник декана факультету № 2 Донецького юридичного інституту МВС України, кандидат юридичних наук

Протягом 2015-2017 років ми стали свідками формування підрозділів кримінальної поліції, зокрема міжрегіональних територіальних органів у складі кримінальної поліції, а саме Департаментів: внутрішньої безпеки, кіберполіції, захисту економіки. Окрім того

структурні зміни відбуваються в територіальних підрозділах Національної поліції, до складу яких входять підрозділи: карного розшуку, протидії наркозлочинності, кримінальної розвідки, боротьби зі злочинами, пов'язаними з торгівлею людьми тощо. Безпосередньо до структури Національної поліції у складі кримінальної поліції також входять: Департамент оперативної служби, Департамент оперативно-розшукових заходів, Департамент забезпечення діяльності, пов'язаної з небезпечними матеріалами [1]. У 2018 році постало питання про формування Департаменту стратегічних розробок та аналізу, а також про створення нового підрозділу у складі кримінальної поліції - боротьби з організованою злочинністю [2].

Окрім того, сучасний розвиток українського суспільства характерний впровадженням інформаційних технологій у різні сфери життя. Це відкриває перспективи для використання інформаційних технологій в практичній діяльності працівників підрозділів кримінальної поліції та освітній діяльності, пов'язаної з підготовкою фахівців для підрозділів кримінальної поліції. Тому виникає необхідність здійснювати підготовку фахівців-інтелектуалів, які вже на початковому етапі пошуку інформації могли б передбачити результати судового розгляду кримінального провадження, розпочатого на підставі наданої оперативним працівником інформації про факт підготовки або вчинення неочевидного або латентного злочину. У цьому плані система відомчої освіти покликана відображати не тільки якісні перетворення, що відбуваються в підрозділах кримінальної поліції, але й випереджати їх: готувати фахівців до сприймання нових ідей, підходів до здійснення кримінально-правової та оперативно-розшукової функції. Тому, одним із способів підвищення ефективності протидії злочинністю є поєднання всіх досягнень оперативно-розшукової науки із сучасними досягненнями наук не лише кримінально-правового спрямування (кримінальне право, кримінальний процес, криміналогія, криміналістика тощо), а і інших наук – інформатики, кібернетики, філософії, соціології, психології та ін.

Окрім того, існує необхідність постійного оновлення теорії та практики ОРД щодо виявлення ознак підготовки та вчинення зло-

чинів за напрямами діяльності відповідних підрозділів кримінальної поліції, зокрема – латентних злочинів у сфері інформаційної безпеки дітей та молоді, кіберзлочинності, шахрайства тощо.

Отже, зазначаємо, що професійна підготовка фахівців для підрозділів кримінальної поліції відповідно до положень ст. 72 Закону України «Про Національну поліцію» складається з:

- первинної професійної підготовки;
- підготовки у вищих навчальних закладах із специфічними умовами навчання;
- післядипломної освіти;
- службової підготовки – системи заходів, спрямованих на закріплення та оновлення необхідних знань, умінь та навичок працівника поліції з урахуванням оперативної обстановки, специфіки та профілю його оперативно-службової діяльності [3, ст. 72].

Підготовка у вищих навчальних закладах із специфічними умовами навчання повинна відповідати вимогам Закону України «Про вищу освіту» [4]. Своєю чергою, наказом МВС України від 16.02.2016 № 105 затверджено «Положення про організацію первинної професійної підготовки поліцейських, яких вперше прийнято на службу в поліцію» [5]. Первинна підготовка майбутніх оперуповноважених здійснюється за тематичним планом і Професійною програмою первинної професійної підготовки поліцейських, яких вперше прийнято на службу в поліцію на посади оперуповноважених карного розшуку, яка розроблена фахівцями Національної академії внутрішніх справ. Нормативна частина Професійної програми аналогічна нормативній частині професійній підготовки поліцейських за іншими напрямами підготовки (превентивна діяльність, органи досудового розслідування, патрульна поліція).

Проведений нами аналіз тематичного плану та Професійної програми первинної професійної підготовки свідчить, що на навчальну дисципліну «Інформаційні технології в поліцейській діяльності. Безпека роботи з інформацією» виділено лише 8 годин, з яких на лекційні та практичні заняття виділено по 4

години [5]. На нашу думку, такий стан справ не сприяє ефективній первинній професійній підготовці працівників кримінальної поліції, оскільки на даний час, зокрема в Головному управлінні Національної поліції в Донецькій області впроваджений у практичну діяльність Єдиний аналітичний сервісний центр поліції Донецької області (UASC), який дозволяє ідентифікувати автомобіль за маркою, моделлю та навіть кольором, розпізнати обличчя людини. Камери дозволяють оперативно обробляти фото та відео інформацію, допомагають розкривати злочини по «гарячим» слідам, оперативно затримувати розшукуваних осіб, виявляти викрадені автомобілі тощо. Досвід м. Маріуполя впроваджується і в інші міста Донецької області.

Саме тому приходимо до висновку, що варіативна частина, яка містить блок дисциплін професійно-теоретичної підготовки, професійно-практичної підготовки, а також контрольні заходи на нашу думку потребує доопрацювань. Отже, зазначені нами аспекти мають за мету виробку заходів, спрямованих на підвищення ефективності підготовки фахівці для підрозділів кримінальної поліції.

---

1. Структура Національної поліції [Електронний ресурс]. – Режим доступу: http://www.npu.gov.ua/uk/publish/article/1795723
2. Нацполіція вирішила відроди УБОЗ [Електронний ресурс]. – Режим доступу: http://ipress.ua/news/natspolitsiya_vyrishyla_vidrodyty_uboz_243556.html
3. Про Національну поліцію : Закон України від 02 липня 2015 р. № 580-VIII // Відомості Верховної Ради України. – 2015. – № 40-41. – Ст. 379.
4. Про вищу освіту: Закон України від 1 липня 2014 року № 1556-VII [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1556-18/page7;
5. Положення про організацію первинної професійної підготовки поліцейських, яких вперше прийнято на службу в поліцію: затверджено наказом МВС України від 16.02.2016 № 105 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/z0576-16/paran14#n14

ЩОДО ДЕЯКИХ АСПЕКТІВ ВИКОРИСТАННЯ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ РОЗВІДКИ В ІНФОРМАЦІЙНО-АНАЛІТИЧНОМУ ЗАБЕЗПЕЧЕНІ ДІЯЛЬНОСТІ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

Пічкуренко С. І.
доцент кафедри оперативно-розшукової діяльності
Національної академії внутрішніх справ,
кандидат юридичних наук, доцент

Кацан Л.О.
ст. викладач кафедри оперативно-розшукової діяльності
Національної академії внутрішніх справ,
кандидат юридичних наук, доцент

Ефективність протидії злочинності, попередження, виявлення та припинення злочинів, в тому числі, скоєних членами організованих злочинних груп та злочинних організацій в першу чергу залежить від належного інформаційно-аналітичному забезпечення діяльності оперативних підрозділів кримінальної поліції.

До блоку кримінальної поліції входить підрозділи карного розшуку, кримінальної розвідки, боротьби зі злочинами, пов'язаними з торгівлею людьми, оперативної служби, оперативно-технічних заходів, виявлення небезпечних матеріалів та екологічних злочинів, протидії наркозлочинності (межрігіональний підрозділ). внутрішньої безпеки (межрігіональний підрозділ), кіберполіції (межрігіональний підрозділ), захисту економіки (межрігіональний підрозділ) [1,2].

Аналіз відомчих законодавчих актів, щодо оперативно-службової діяльності вказаних підрозділів свідчить, що кожен з них організовує протидію правопорушенням в різних сферах життєдіяльності нашої держави, головними з яких є:

- надання поліцейських послуг у сферах охорони прав і свобод людини, інтересів суспільства і держави, протидії

злочинності, виявлення і розкриття злочинів загальнокримінальної спрямованості, розшук осіб, які їх учинили, документування протиправної діяльності учасників та членів ОГ і ЗО[3].

- забезпечення реалізації державної політики щодо захисту економіки та об’єктів права власності, виявлення, запобігання та припинення злочинів у сфері економіки, у тому числі вчинених суспільно – небезпечними організованими групами та злочинними організаціями, які впливають на соціально-економічну і криміногенну ситуацію в державі та в окремих її регіонах, боротьба з корупцією й хабарництвом у сферах, які мають стратегічне значення для економіки держави, та серед посадових осіб органів державної влади і самоврядування; протидія корупційним правопорушенням і правопорушенням, пов'язаним з корупцією[4].
- забезпечення реалізації державної політики щодо попередження та протидії кримінальним правопорушенням у сфері протидії кіберзлочинності)[5], торгівлею людьми, нелегальною міграцією, правопорушеннями у сфері суспільної моралі [6], незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та запобігання поширенню наркоманії, насамперед учинених злочинними групами осіб, які мають міжрегіональні та міждержавні зв’язки, особливо в їх організованих формах[7], а також виявлення, попередження та припинення кримінальних правопорушень та корупційних діянь, що готуються або вчинені працівниками органів та підрозділів Національної поліції України [8].

Ми підтримуємо думку окремих науковців та практичних працівників Національної поліції України, що підрозділи кримінальної розвідки в змозі на професіональному рівні забезпечити збір необхідної інформації для належного інформаційно-аналітичного забезпечення оперативних підрозділів кримінальної поліції про криміногенну ситуацію у державі, зокрема у сфері протидії організованій злочинності та корупції використовуючи сили,

форми і методи оперативно-розшукової діяльності, передбачені спеціальними нормативно-правовими актами [9,10].

З метою належного використання можливостей кримінальної розвідки та підготовки професіональних фахівців оперативних підрозділів кримінальної поліції слід впровадити у навчальний процес дисципліни з спецкурсу, щодо використання підрозділів кримінальної розвідки у сфері протидії організованої злочинності, впровадження форм, методів та сил ОРД передбачених Законами України «Про оперативно-розшукову діяльність», «Про організаційно-правові основи боротьби з організованою злочинністю», «Про боротьбу з терроризмом», «Про запобігання корупції».

1. Закон України «Про Національну поліцію» // Документи Верховної Ради України : [сайт] – Режим доступу: http://zakon.rada.gov.ua.
2. Структура апарату Національної поліції України: [сайт] – Режим доступу: https://www.npu.gov.ua/uk/publish/article/1795723
3. Положення про Департамент карного розшуку Національної поліції України [Електронний ресурс] : наказ Голови Національної поліції України від14 листоп. 2015 року № 90. – Режим доступу: http://www.npu.gov.ua/uk/. – Назва з екрана.
4. Положення про Департамент захисту економіки Національної поліції України [Електронний ресурс] : наказ Голови Національної поліції України від 7 листоп. 2015 р. № 81. – Режим доступу: http://www.npu.gov.ua/uk/. – Назва з екрана.
5. Положення про Департамент кіберполіції Національної поліції України [Електронний ресурс] : наказ Голови Національної поліції України від 10 листоп. 2015 р. № 85. – Режим доступу: http://www.npu.gov.ua/uk/. – Назва з екрана.
6. Положення про Департамент боротьби зі злочинами, пов'язаними з торгівлею людьми [Електронний ресурс] : наказ Голови Національної поліції України від 29 листоп. 2013 р. N 1167 – Режим доступу: http://www.npu.gov.ua/uk/. – Назва з екрана.
7. Положення про Департамент протидії наркозлочинності [Електронний ресурс] : наказ Голови Національної поліції

України від 17 листоп. 2015 р. N 95 – Режим доступу: http://www.npu.gov.ua/uk/. – Назва з екрана.
8. Положення про Департамент внутрішньої безпеки Національної поліції України [Електронний ресурс] : наказ Голови Національної поліції України від 09 листоп. 2015 р. N 83 – Режим доступу: http://www.npu.gov.ua/uk/. – Назва з екрана.
9. У МВС з'явиться департамент кримінальної розвідки: [сайт] — Режим доступу : http://www.unn.com.ua/uk/news/1452676-u-mvs-zyavitsya-departament-kriminalnoyi-rozvidki
10. Кримінальна розвідка: методологія, законодавство, зарубіжний досвід : матеріали Міжнар. наук.-практ. конференції (29 квітня 2016 р., м. Одеса). – Одеса: ОДУВС, 2016. – 184 с.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРАКТИЧНІЙ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Поливанюк В.Д.
старший викладач кафедри тактико-спеціальної підготовки факультету ПФППД Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, доцент

На сучасному етапі розвитку нашої держави простежується тенденція до активного використання інформаційних технологій у діяльності Національної поліції України. Розглядаючи даний аспект, важко не погодитися з тим, що досягнення науково-технічного прогресу зробили величезний прорив в інформаційному просторі. Саме такі досягнення сприяють підвищенню рівня протидії злочинності.

Актуальністю даної теми є інтенсивне впровадження у практичну діяльність правоохоронних органів комп'ютерної техніки.

Ця тема не є новою для розгляду, що знайшла своє відображення у дисертаціях, колективних монографіях, а також статтях у таких вчених як І.В. Арістова, О.М. Бандурка, А.Й. Берлач, Р.С. Бєлкін, В.В. Бірюков, М.С. Вертузаєв, В.Г. Гончаренко, І.Б. Денисова,

О.М. Джужа, В.Ю. Журавльов, А.В. Іщенко, Р.А. Калюжний, Н.І. Клименко, В.П. Кувалдін, В.С. Кузьмічов, Є.Д. Лук'янчиков, В.А. Минаєв, Ю.Ю. Орлов, І.М. Паршин, М.А. Погорецький, О.В. Рибальський, М.В. Салтевський, В.Г. Хахановський, В.В. Шендрик, В.Ю. Шепітько та інші.

Роботи вищезазначених правників дійсно зробили неабиякий внесок спрямований на дослідження даної тематики, проте проблема інформатизації працівників правоохоронних органів не була розглянута повно та всебічно. Тому до неї неодноразово продовжують звертатися сучасні вчені.

Варто почати з того, що сьогодні важко уявити сучасну картину світу без інформаційного простору. Будь-яка сфера діяльності людини супроводжується комп'ютерною технікою, що пов'язано, перш за все, з досягненням науково-технічного прогресу, а також переходу суспільства на новий етап розвитку.

Важко не погодитися з тим, що починаючи з навчального процесу простежується ефективне використання комп'ютерів та іншої техніки, що пов'язане з покращенням засвоєння матеріалу, а також за допомогою чого заздалегідь розробляється програма.

Теж саме можемо сказати про практичну діяльність працівників органів внутрішніх справ.

На сьогодні важко уявити роботу будь-якого з підрозділів Національної поліції України без інформаційної підтримки та інформаційного забезпечення, накопичення та систематизації інформації в базах даних. Це є наочним підтвердженням загальновідомої тези «хто володіє інформацією, той володіє світом» [1, 202].

Звертаючись до вирішення завдань пов'язаних з оперативно-розшуковою діяльністю на сучасному етапі накопичений неабиякий досвід щодо застосування інформаційних технологій у таких процесах як попередження, виявлення, а також розслідування злочинів, особливо при провадженні негласних слідчих(розшукових) дій, та ін.

Сутність інформаційного забезпечення оперативно-розшукової діяльності можна визначити як доцільну діяльність людини, спрямовану на вихідні фактичні дані з тим, щоб, використовуючи відповідні технічні засоби, перетворити їх форму, придатну для вирішення управлінських або конкретних завдань виявлення, попередження, припинення і розкриття злочинів, розшуку зниклих злочинців, безвісти зниклих громадян [2].

На важливість і необхідність сучасних інформаційних технологій вказує також положення Кримінально процесуального кодексу України, у якому зазначається неможливість оперативності і ефективності процесу без бази даних, яка створена за допомогою інформаційного простору.

Основними тенденціями розвитку інформаційних технологій у правоохоронній сфері є:

1) удосконалення форм та методів управління системами інформаційного забезпечення;
2) централізація та інтеграція комп'ютерних банків даних;
3) впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних та криміналістичних обліків;
4) розбудова та широке використання ефективних та потужних комп'ютерних мереж;
5) застосування спеціалізованих засобів захисту інформації;
6) налагодження ефективного взаємообміну кримінологічною інформацією на міждержавному рівні. Все це забезпечує суттєве підвищення рівня боротьби зі злочинністю [3, 12].

Отже підсумовуючи вищенаведене, можна дійти висновку, що використання сучасних інформаційних технологій покращує ефективність діяльності підрозділів Національної поліції України.

На сучасному етапі технічного процесу кожен працівник повинен якісно оволодівати знаннями у галузі інформаційно-комунікаційних технологій. Більше того, працівники мають проходити підвищення кваліфікації з метою отримання нових якісних знань, навичок, а також умінь при застосуванні інформаційних технологій у практичній діяльності.

Отже, інформаційні технології виступають налагодженим механізмом, який забезпечує якісне функціонування органів внутрішніх справ, які необхідні для виконання їх службових завдань. З розвитком комп'ютерних технологій створюються нові методи роботи, що здатні підвисити професіональні якості працівників.

1. Танкушина Т. Ю. Автоматизовані інформаційні системи в структурі реєстраційної діяльності міліції: становлення, розвиток, сучасність // Вісник Запорізького національного університету: збірник наукових праць. Юридичні науки: [у 2 ч.]. – Запоріжжя: Запорізький національний університет, 2011. – Ч. І. – 224 с.
2. Голубовский В. Ю. Теория и практика информационного обеспечения оперативно-розыскной деятельности подразделений криминальной милиции : авто- реф. дис.д-ра юрид. наук : спец. 12.00.09 / Владимир Юрьевич Голубовский ; С.- Петерб. ун-т МВД РФ. – СПб., 2001. – 50 с. – ББК: Х629.372,0.
3. Інформаційні технології в правоохоронній діяльності : Посібник / В.А Кудінов., В.М.Смаглюк, Ю.І. Ігнатушко, Іщенко В.А. – К.: НАВСУ, 2013. – 82с.

ПРОБЛЕМНІ ПИТАННЯ ВЗАЄМОДІЇ ПІДРОЗДІЛІВ КАРНОГО РОЗШУКУ З ІНШИМИ СУБЄКТАМИ В ПРОЦЕСІ ПРОТИДІЇ ВТЯГНЕННЮ НЕПОВНОЛІТНІХ У З ЛОЧИННУ ДІЯЛЬНІСТЬ

Поляк С.П.

ад'юнкт кафедри оперативно-розшукової діяльності факультету №2 ІПФПНП Львівського державного університету внутрішніх справ

Результати практики вказують, що ефективність протидії злочинам та їх розслідування залежить також від злагодженості в діях суб'єктів, органів та підрозділів, що покликані виявляти та знешкоджувати протиправні явища та діяльність у суспільстві. Такий успіх може бути досягнутий лише через усвідомленість

спільної мети, спільного результату діяльності щодо протидії злочинним проявам. Належна правова регламентація, чітке відокремлення повноважень одного правоохоронного суб'єкта від іншого, а також визначення способів взаємодії та координації всіх суб'єктів у разі необхідності протидії як системним так і окремим протиправним фактам є ключовими та водночас болючими питаннями якісної взаємної.

Питаннями взаємодії в правоохоронній діяльності, зокрема аспектами взаємодії оперативних підрозділів з іншими суб'єктами, займалося багато знаних науковців такі як: А.В. Баб'як, О.М. Бандурка, А.Ф. Волобуєв, Д.В. Гребельський, В.П. Захаров, І.П. Козаченко, А.Г. Лєкарь, Є.Д. Лук'янчиков, Д.Й. Никифорчук, А.М. Подоляк, В.Д. Пчолкін, В.Л. Регульський, та інші.

Забезпечення узгодженості та єдності функціонування окремих елементів правоохоронної системи та інших суб'єктів в процесі досягнення спільних цілей і є підвалиною функціонування та управління суспільними процесами щодо гарантування безпеки самого суспільства та його членів.

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 [1, с. 125].

Аналізуючи взаємодію в процесі протидії втягненню неповнолітніх у злочинну діяльність між підрозділами карного розшуку як суб'єктом оперативно-розшукової діяльності з іншими підрозділами Національної поліції, а також суміжними правоохоронними структурами та державними органами, бачимо об'єктивно існуючий взаємозв'язок між цими суб'єктами, що виникає в силу реалізації та виконання покладених на них повноважень, який багато дослідників називає також координацією діяльності правоохоронної системи з іншими органами.

Необхідно відзначити, що ґрунтуючись на тлумаченні термінів «координація» та «взаємодія» у значенні узгодженості, багато авторів вживають їх як синоніми [2, с. 74]. Окремі науковці у своїх дослідженнях послуговуються терміном «координація»

взагалі не вживаючи терміна «взаємодія» [3, с. 112]. Інші дослідники вважають, що координація – це діяльність щодо організації взаємодії, що поняттям організації охоплюється поняття взаємодії [4, с. 142].

На думку А.В. Баб'яка, між поняттям координація і взаємодія існують істотні відмінності, що не дозволяють розглядати їх як тотожні. Координація здійснюється спеціально для цього утвореним структурним підрозділом координаційним органом з метою підвищення ефективності реагування системи запобігання у вигляді профілактичних заходів. Взаємодія налагоджується самими суб'єктами запобігання повсякденно у випадку, коли немає потреби залучати до цієї справи можливостей координаційного органу [5, с. 9-10].

В.Д. Пчолкін, проаналізувавши сукупність низки ознак, які розкривають сутність процесу взаємодії, уточнює і визначає поняття взаємодії як засновану на спільності цілей і завдань, погоджену за часом, місцем і змістом, визначену законодавством діяльність компетентних суб'єктів щодо раціонального застосування наявних сил, засобів і методів для своєчасного виявлення, попередження та розкриття злочинів [6].

Зазначимо, що основна взаємодія підрозділів карного розшуку щодо документування злочинів пов'язаних із втягненням в них неповнолітніх як і багатьох інших, відбувається на стадії досудового розслідуванні або до його початку. Тому, окремі автори розглядають взаємодію як правильне (або раціональне) поєднання та ефективне використання повноважень, методів і форм діяльності слідчого й оперативних підрозділів [7, с. 12].

Правильною і такою, що відповідає етимології та змісту самого терміна, що аналізується є позиція, яка полягає в розумінні взаємодії як погодженої діяльності слідчого та оперативних підрозділів [8, с. 385].

Проте, те, з чим стикаються на практиці працівники карного розшуку інколи важко назвати погодженою діяльністю.

Колізії у внутрішній взаємодії часто виникають через зловживання слідчими правом надавати доручення на проведення низки процесуальних дій оперативним підрозділам, в тому числі карному розшуку. Подекуди таке право дозволяє розвантажити слідчого окремими організаційними питаннями та оперативним супроводом, враховуючи обсяг кримінальних проваджень на одного слідчого. Однак, така практика скорочує і продуктивність та якість роботи оперативного працівника, виникає вибір виконання ним більш нагального чи менш складнішого завдання, втрачається інтерес до пошуку оперативної інформації за окремими видами злочинів, в тому числі і за категорією, яку ми досліджуємо.

Проте, з іншої сторони, вирізняється чіткий психологічний момент супротиву такої форми взаємодії, оскільки досвідчені оперативні працівники не вбачають необхідності виконувати окремі доручення, мають упереджене ставлення до слідчих і головне акцентують на тому, що не перебувають в адміністративній чи службовій залежності від такої категорії як «слідчі», а є рівнозначними працівниками. Тому, окремі доручення хоча і візуються начальниками відповідних відділень та відділів поліції проте мають можливість бути не виконаними в силу перерахованих обставин, а також у випадку не бачення між цими двома суб'єктами спільної мети та зацікавленості.

У межах внутрішньої взаємодії підрозділи карного розшуку щодо протидії втягненню неповнолітніх у злочинну діяльність та документування таких фактів вступають також у співпрацю з іншими службами та підрозділами Національної поліції. Варто зазначити, що в межах такої взаємодії виділяються кілька суттєвих проблем в основному організаційно-правового характеру, яскравими з яких є:

- відсутність зобов'язуючих норм щодо регулювання взаємодії підрозділів карного розшуку з іншими оперативними та не оперативними підрозділами поліції, унаслідок чого має місце незацікавленість працівників карного розшуку у виявленні злочинів пов'язаних із втягненням в них

неповнолітніх, на відміну від інших злочинів загально-кримінальної спрямованості;

- необізнаність працівників підрозділів слідства та ювенальної превенції з організацією оперативно-розшукової діяльності карного розшуку щодо протидії втягненню дітей у злочинну діяльність.

Будь-який орган чи працівник поліції так чи інакше взаємодіє як з іншими структурними підрозділами, так і з органами публічного управління, тому налагодження більш тісних зв'язків між зазначеними суб'єктами може надати значну допомогу в процесі реалізації інформаційної взаємодії [9, с. 52]. Так, в ст. 11 Закону України «Про оперативно-розшукову діяльність» вказано, що органи державної влади, підприємства, установи, організації незалежно від форми власності зобов'язані сприяти оперативним підрозділам у вирішенні завдань оперативно-розшукової діяльності [10].

Однак, незважаючи на законодавчо визначену необхідність взаємодії щодо протидії втягненню неповнолітніх у злочинну діяльність, існує ряд проблем, які негативно впливають на якісний показник взаємодії підрозділів карного розшуку та зазначених суб'єктів, серед яких:

- ліквідація підрозділу кримінальної міліції у справах дітей, організація діяльності якого та співпраці з державними органами у справах дітей була сталою та визначеною, хоча не завжди досконалою;
- відсутність норм регулювання взаємодії підрозділів карного розшуку з органами і службами у справах дітей, іншими державними органами та ОМС, що стосується безпосереднього отримання інформації для частини негласної роботи щодо документування фактів втягнення неповнолітніх у злочинну діяльність;
- не обізнаність таких недержавних органів щодо засад та специфіки діяльності різних підрозділів поліції, в тому числі карного розшуку, що породжує стереотип «універсального поліцейського» і не важливим стає факт

надання оперативної інформації дільничному інспектору поліції, патрульному чи працівнику ювенальної превенції, які лише публічною профілактикою не можуть досягнути високого результату у цьому напрямі;

- низький рівень організації діяльності соціальних служб та органів у справах дітей щодо протидії втягненню неповнолітніх у злочинну діяльність і відповідно взаємодії у цьому напрямі з оперативними підрозділами, а сам такий процес зводиться до показниково-звітувального.

Отже, що стосується взаємодії підрозділів карного розшуку з іншими суб'єктами щодо протидії втягненню неповнолітніх у злочинну діяльність, слід визначити наявність проблем теоретичного, нормативно-правового, організаційно-управлінського і тактичного характеру. Так, відсутній єдиний підхід до формування теорії взаємодії між правоохоронними та іншими суб'єктами загалом, а також визначення змісту і суті такої взаємодії щодо протидії залучення дітей до різних форм злочинної діяльності зокрема; відсутнє нормативне закріплення поняття взаємодії у галузевому законодавстві поліції, не визначено відповідальність за недобросовісну взаємодію, а також не розроблені інструкції з організації взаємодії підрозділів карного розшуку з іншими суб'єктами у протидії втягненню неповнолітніх у злочинну діяльність; відсутнє методичне забезпечення організації взаємодії підрозділів карного розшуку з іншими суб'єктами щодо протидії досліджуваному злочину та тактичних прийомів її реалізації.

1. Великий тлумачний словник сучасної української мови (з дод., допов. та CD) / Уклад. і голов. ред. В. Т. Бусел. – К.; Ірпінь: ВТФ «Перун», 2009. – 1736 с.
2. Керженцев П.М. Принципы организации. Избраные произведения / Креженцев П.М. – М.: Экономика, 1968. – 339 с.
3. Мангутов И.С. Организатор и организаторская деятельность / Мангутов И.С., Уманский Л.И. – Л.: ЛГУ, 1975. – 185 с.
4. Научная организация управления в аппаратах милиции / под. ред. Ю.М. Козлова. – М.: Юрид. лит., 1975. – 243 с.

5. Баб'як А.В. Координація діяльності оперативних підрозділів ОВС під час запобігання створенню та функціонуванню кримінальних ринків / Діяльність підрозділів кримінальної міліції: сучасний стан та перспективи вдосконалення: тези доповідей та повідомлень учасників Міжнародної науково-практичної конференції (м. Львів, 12 квітня 2013 р.). – Львів: Львівський державний університет внутрішніх справ, 2013. – 632 с.
6. Пчолкін В. Д. Шляхи удосконалення взаємодії оперативних підрозділів органів внутрішніх справ у боротьбі зі злочинами в економічній сфері / В. Д. Пчолкін // Удосконалення взаємодії оперативних підрозділів ОВС і транспортної міліції при розкритті та розслідуванні злочинів : матеріали наук.-практ. конф. – Л. : ЛІВС при НАВС України, 2003.
7. Душейко Г.О. Організаційно-тактичні основи реалізації оперативно-розшукової інформації в стадії порушення кримінальної справи : автореф. дис. на здобуття наук. ступеня канд. юрид. наук / Г.О. Душейко. – Х., 2001. – 19 с.
8. Матусовський Г.А. Основи взаємодії та інформаційного забезпечення в методиці розслідування злочинів / Криміналістика: підручник / кол. авторів: В.М. Глібко, А.Л Дудніков., В.А. Журавель та ін. ; за ред. В.Ю. Шепітька. – К. : Видавничий Дім «Ін Юре», 2001. – 684 с.
9. Процких О. Ю. Інформаційна взаємодія національної поліції України з органами публічної влади та громадськістю / О. Ю. Процких // Право і Безпека. – 2015. – № 4. – С. 50-55. – Режим доступу: http://nbuv.gov.ua/UJRN/Pib_2015_4_12.
10. Про оперативно-розшукову діяльність: закон України від 18.02.1992 р., № 2135–XII // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/2135-12/page (дата звернення: 08.03.2018).

ВПЛИВ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА НА ПРИНЦИПИ ЗАСЕКРЕЧУВАННЯ ІНФОРМАЦІЇ

Романюков М.Г.
науковий співробітник науково-дослідної лабораторії з проблемних питань кримінального аналізу Одеського державного університету внутрішніх справ

Ісмайлов К.Ю.
завідувач кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ, кандидат юридичних наук

Вступ. «Однією з основних реальних потенційних загроз національній безпеці України у інформаційній сфері, є розголошення інформації, що становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів держави та суспільства» [1].

На сьогодні можна спостерігати наступний перехідний період функціонування людства в соціумі до інформаційного суспільства та суспільства високих технологій. Інформаційні технології, виходячи на промисловий рівень, наділяють інформацію новими функціями засобів виробництва, сировинної бази, видами продуктів та товарів повсякденного вжитку. Дані зміни несуть за собою втручання в усі сфери державної життєдіяльності (економічні, політичні та ін.) навіть змінюючи соціум, як інститут. Змінюється образ кожного індивида, його особистості та світогляду. Разом з глобальним оцифровуванням змінюється звична парадигма соціальної реальності пов'язаної з доставкою, обробкою, реагуванням та контролем інфорсвційних потоків [1].

Виникає нова інформаційна зброя, така як вміння маніпулювати інформацією та дезінформацією. Як пише The Times:"Планету чекає зміна парадигми, на стільки ж радикальна, як зміна

кавалерії на танки. Застосування дезінформації для зриву демократичних дебатів, кібератаки, економічна політика з метою тиску, розгортання не декларованих військ, які стають поштовхом до більш стандартного військового втручання. Ситуація, коли на війні зброєю стає що завгодно [2].”

Виникають наступні проблеми, що стосуються насмперед забезпечення безпечного впливу глобальних змін на трансформацію сфери інформаційної безпеки та засекречування інформації. Нову еру вразливостей починають формувати нематеріальні цінності та модифікована структура активів, що вимагає нових ідей при вирішенні питань технології захисту [4].

Історичні етапи технології засекречування. Відповідно до А. Денисова основною технологією влади, що вимагає захисту, належить управління поведінкою вибору. Даний вибір є притаманним людству, суть якого і є влада. На цілі засекречування мали вплив різні історичні епохи. У зв’язку з цим є доцільним розглянути чотири історичні періоди, у яких новий етап технологічної революції супроводжувався приходом до влади нового правлячого класу [3]:

- епоха 1, феодальне або кріпосне (до індустріальне) суспільство;
- епоха 2, індустріальне буржуазне (або соціалістичне) суспільство;
- епоха 3, постіндустріальне, перехідне до інформаційного суспільства, (інвестиційна фаза);
- епоха 4, суспільство високих технологій, винайдених у інноваційній фазі.
- Оскільки від трансформації технологій поведінки вибору залежать об’єкти, цілі та принципи засекречування, виникає необхідність їх розглянути:
- епоха 1, робота в умовах ручної праці, що є примусовою. За А. Денисовим вона характеризується як управління міжособистісних комунікацій думок і роботи.
- епоха 2, має прерогативу «стимул- реакція», в умовах вільного продажу праці на ринку праці. Важка фізична

праця починає механізуватися, а на пізніших етапах автоматизуватися. Розглядаючи дану епоху в рамках сучасних теорій, можна зробити висновок що на сьогодні вона знаходить відображення у кібернетиці 1-го порядку.

- епоха 3 являє собою рефлексію управління на рефлексії свідомості, що супроводжується дотриманням прав людини, роботизацією важкої, небезпечної для здоровя праці. На поглибленому етапі починає автоматизуватися розумова праця. Відбувається зародження технократичного способу мислення [4]. За А. Денисовим, дане управління має на меті використання концепції єдиної індивідуальної свідомості. В сучасних теоріях дана епоха знайшла відображення у рефлексивному управлінні за принципом кібернетики 2-го порядку та вищих аналогів з описом систем із самосвідомістю.
- епоха 4 рефлексивне управління поведінкою вибору за моделлю рефлексії свідомості з використовуванням, по А. Денисову, концепції множинності шарів індивідуальної свідомості. Епоха характеризується як назріваюча інтелектуально-гуманітарна революція.

Оскільки зі зміною залежності об'єктів, цілей та принципів засекречування від технологій поведінки відбувається трансформація предмету та засобів управління вибором, то виникають наступні предмети і засоби управління за епохами:

1. Управління змістом між особистого інформаційного обміну за допомогою сили;
2. Управління каналами, характером і трафіком між особистого інформаційного обміну за допомогою законодавчих, організаційних, технічних а також соціально-психологічних засобів;
3. Рефлексивне управління усвідомленням поведінки вибору, заснованому на математичних моделях морального вибору, за допомогою маніпулювання здатністю до міжособистного інформаційного обміну;
4. Рефлексивне управління усвідомлення вибору за допомогою маніпулювання здатністю до між особистого (не

відомого спостерігачеві) інформаційного обміну за допомогою технологій психоінжинирінгу [3].

Ієрархічна модель системи засекречування. Системи захисту інформації, а далі системи інформаційної безпеки розвивались так, що базові принципи, методи і засоби, напрацьовані на попередніх етапах, не відкидаються, а залишаються, розширюються або удосконалюються, знаходячи собі свою нішу у нових комплексних системах інформаційної безпеки. Більше того набувають подальшого розвитку та вдосконалення, що можна спостерігати при побудові комплексних систем захисту інформації. При цьому має місце принцип повноти та неперервності захисту, як окремої комплексної системи захисту, так і засекречування вцілому. Розглядаючи ієрархічну систему засекречування, можна спостерігати наступну можливість – секрет верхнього рівня може розділятись на нижньому рівні. Цим можна понизити рівень захищеності кожного з розподілених секретів, полегшивши задачу оптимізації всієї системи засекречування.

Цілі засекречування за А. Денисовим розподіляється за рівнем системи засекречування:

1. Засекречування інформаційних потоків
2. Засекречування трафіку та каналів обміну інформаційними пакетами, засекречування моделей та технологій обміну;
3. Засекречування матриць цінностей;
4. Засекречування картин бачення світу.

Систему засекречування можна відобразити у чотирьох рівневій ієрархічній структурі (рис. 1). Розгладаючи дану модель можна сформувати систему чотиритсупеневої системи захисту державної таємниці. На першому рівні необхідно захищати відомості, що закріплені в ЗВДТ. На другому рівні відбувається захист трафіку, моделей та обміну пакетими. Третій рівнень відповідає за захист матриць цінностей. Метод даного захисту полягає у маніпулюванні здатністю до між особистого інформаційного обміну. Четвертий рівень потребує глибоких

досліджень, та буде побудований на принципі систем інтерпретації даних (зокрема віртуальних), що сприймаються органами почуттів людини.

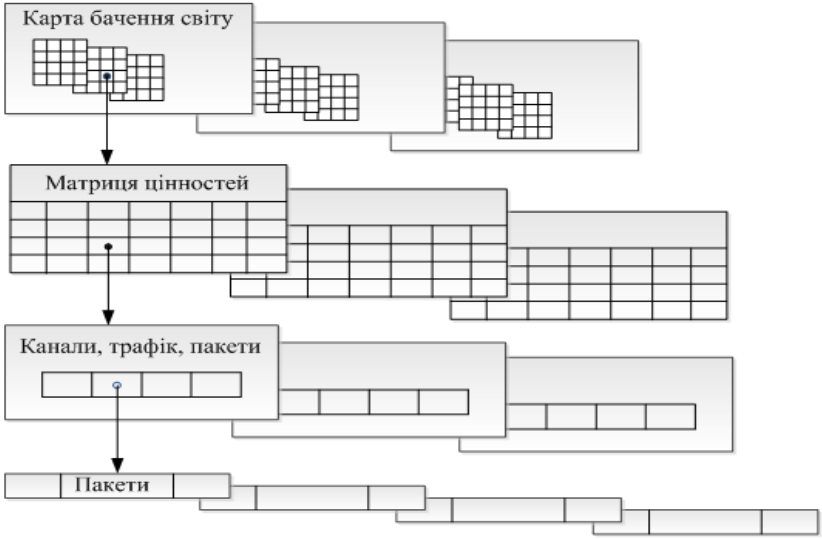


Рис. 1. Характеристика ієрархічної чотириступеневої моделі засекречування.

Висновки. Проаналізувавши модель розвитку суспільства, запропоновано принципи моделі ієрархічної системи засекречування. Дана модель має чотири рівні: на першому рівні засекречуються інформаційні потоки, на другому – моделі та технології обміну інформаційними пакетами, на третьому – має місце засекречування матриць цінностей, на четвертому – відбувається засекречування картин бачення світу. Запропонована модель розкриває можливості до створення більш детальних та обґрунтованих засобів засекречування. Отримані результати дають можливість вдосконалити засоби національної та інформаційної безпеки та відкривають нові напрямки досліджень по створенню ефективних систем захисту правоохоронної діяльності.

1. Корченко О.Г. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці : Монографія / О.Г. Корченко, О.С. Архипов, Ю.О. Дрейс. – К.: наук.-вид. центр НА СБ України, 2014. – 332 с.
2. Путин использует бойню в Украине, чтобы репетировать войну с Западом / The Times, 10 августа 2016. [Электронный ресурс] – Режим доступа: http://glavnoe.ua/news/n279723.
3. Денисов А.А. Нетократия и рефлексия: Засекречивание в постиндустриальном обществе / А.А Денисов // Рефлексивные процессы и управление. – Том 7, № 1, 2007. – С. 33-50.
4. Агеев А.И. Вектор перемен / А.И. Агеев, С.В. Авдеев, Рыжов В.Н. и др. // Экономические стратегии. – № 4, 2016. – С. 84-106.

ДО ПИТАННЯ ЗАХИСТУ СПЕЦІАЛІЗОВАНИХ КОРПОРАТИВНИХ МЕРЕЖ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Рудий А.Т.
військовослужбовець

Щур Є.Л.
інспектор відділу професійного навчання управління кадрового забезпечення ГУ НП у Волинській області

Бойчук Т.Я.
слідчий СВ Рожнятівського відділення поліції ГУ НП у Івано-Франківській області

Заєць Я.В.
здобувач освітнього ступеня магістр Львівського державного університету внутрішніх справ

Актуальність проблеми. З огляду на вимоги сучасного підходу до побудови надійної системи захисту інформаційних активів спеціалізованих корпоративних мереж (СКМ) Національної поліції України актуальним залишається розроблення ефективних механізмів захисту. Ефективність системи захисту СКМ залежить від прийняття виважених рішень які підтримують і

адаптують систему захисту інформації до постійно змінюваних умов функціонування мережевого оточення.

Під поняттям спеціалізованої корпоративної мережі у межах даної публікації будемо розуміти частину інформаційної системи у якій забезпечується взаємодія між значною кількістю достатньо незалежних компонент, які, у свою чергу, можуть розглядатися як окремі локальні комп'ютерні мережі. СКМ притаманні такі характеристики: територіальна роззосередженість; високий ступінь гетерогенності; використання глобальних зв'язків [1].

Зважаючи на те, що СКМ за колом розв'язуваних задач, складу, архітектурі є системою неоднорідною, тому і система захисту інформації (ЗІ) повинна бути неоднорідною. Неоднорідність системи ЗІ полягає у наявності різних об'єктів захисту і, як наслідок, різних вимог до ЗІ у кожній незалежній складовій. Це є наслідком того, що окремій незалежній складовій СКМ притаманні тільки її критичні інформаційні активи, програмно-апаратні засоби оброблення інформації, моделі загроз і різні політики інформаційної безпеки (ПІБ).

Беручи за основу таке розуміння СКМ забезпечення ЗІ є особливою проблемою. Це обумовлено такими чинниками:

- рівень необхідного захисту від несанкціонованого доступу (НСД) для різних користувачів у різних компонентах СКМ може змінюватися у широкому діапазоні;
- наявність механізмів і засобів ЗІ потенційно вплине на продуктивність функціонування усієї ІС.

Аналіз літературних джерел надає широкий спектр різноманітних методів захисту інформаційних систем (ІС), які знижують ризики втрати інформаційних активів. Тому, важливим етапом реалізування захисту ІС є вибір ефективного методу захисту конкретної системи. Для побудови захищеної СКМ потрібні засоби, які не лише виявляють і блокують атаки, але і попереджують останні.

Автори пропонують використати адаптивний підхід до захисту інформаційних активів СКМ, який дає можливість контролювати

практично усі загрози і своєчасно реагувати на них високоефективним способом, що дозволяє не лише усунути уразливості, які можуть призвести до реалізування загрози, але і аналізувати умови, які призводять до їх виникнення.

Метою даної публікації є обґрунтування ефективності систем ЗІ на основі оцінювання рівня загроз із врахуванням цілей дій зловмисників та аналізу ризиків загроз безпеці інформаційних активів, що забезпечується за допомогою засобів адаптивного управління безпекою СКМ на основі випереджуючої реакції системи ЗІ на реалізування імовірних атак.

Виклад основного матеріалу. При розгляді питань ЗІ в СКМ завжди говорять про наявність деяких бажаних станів усієї ІС. Ці бажані стани описують захищеність ІС. Особливістю поняття захищеність є його тісний зв'язок з поняттям загроза (те, що може бути причиною виведення ІС із захищеного стану).

Отже, виокремимо три компоненти, які безпосередньо пов'язані з порушенням безпеки СКМ:

- загроза – зовнішнє, відносно СКМ, джерело порушення властивості захищеності;
- об'єкт атаки – частина СКМ, на яку спрямована загроза;
- канал дії – середовище перенесення зловмисної дії.

Інтегральною характеристикою, яка об'єднує усі компоненти, є політика інформаційної безпеки – якісний (або якісно-кількісний) вираз властивостей захищеності СКМ [2]. Опис ПІБ повинен включати або враховувати властивості загроз, об'єкта атаки та каналу реалізування атаки.

Для СКМ існує своя типова архітектура, структурні компоненти якої розв’язують свої специфічні задачі. У загальному випадку архітектура СКМ включає чотири рівні:

- рівень прикладного програмного забезпечення (ППЗ) – рівень взаємодії з користувачем;
- рівень системи управління базами даних (СУБД) та Web-сервери – рівень збереження і оброблення даних у СКМ;

- рівень операційної системи (ОС) – рівень обслуговування СУБД і ППЗ;
- мережевий рівень – рівень взаємодії вузлів СКМ.

Зловмисник має у своєму розпорядженні широкий спектр можливостей порушення безпеки СКМ. Ці можливості можуть бути реалізовані на всіх чотирьох перерахованих вище рівнях СКМ. Найбільш видовищним проявом порушення безпеки СКМ та ІС державної установи є блокування або модифікування вмісту Web-порталу цієї установи.

Розглянемо етапи здійснення атаки на СКМ (рис. 1).

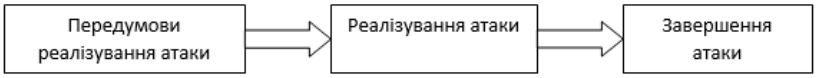


Рис. 1. Етапи реалізування атаки на СКМ

Атакою на СКМ вважається довільна дія, виконувана зловмисником для спроби реалізування загрози шляхом використовування уразливостей. Під уразливістю СКМ розуміється нездатність системи захисту протистояти реалізуванню певної загрози або сукупності загроз.

Уразливими є практично всі компоненти СКМ. Серед них відзначимо:

- мережеві протоколи і пристрої, які формують мережеве оточення;
- операційні системи;
- СУБД і Web-сервери.

Отже, саме забезпечення відсутності уразливостей повинно бути покладено в основу формалізування вимог щодо засобів ЗІ.

Перший, підготовчий етап полягає у пошуку зловмисником передумов для здійснення тієї або іншої атаки. На даному етапі зловмисник шукає уразливості в системі захисту. Використовування цих уразливостей здійснюється на другому, основному етапі реалізування атаки. На третій, завершальній стадії, зловмисник

завершує атаку і прагне приховати сліди вторгнення. У принципі, перший і третій етапи можуть бути атаками.

Слід відзначити, що існуючі механізми захисту, реалізовані у міжмережевих екранах (МЕ), серверах автентифікування, системах розмежування доступу, працюють тільки на етапі реалізування атаки. Властиво, ці механізми захищають від атак, які уже перебувають у процесі реалізування. Ефективнішим було б попередити атаки, запобігти передумовам реалізування атаки. Адаптивна система забезпечення ЗІ афективно працює на всіх трьох етапах реалізування атаки.

У більшості випадків для розв'язання існуючих проблем у системі ЗІ використовуються часткові підходи. Зазвичай вони обумовлені, перш за все, поточним рівнем доступних ресурсів. До того ж адміністратори безпеки схильні адекватно реагувати тільки на ті ризики безпеки, які їм зрозумілі. Фактично таких ризиків може бути істотно більше. Тільки суворий поточний контроль захищеності СКМ і адаптивний підхід, який забезпечує єдину політику інформаційної безпеки (ПІБ) стосовно усієї інформаційної системи, дозволяють істотно знизити ризики безпеки.

Такий підхід до системи ЗІ у СКМ прийнято називати моделлю адаптивної мережевої безпеки (Adaptive Network Security Model, ANSM), який здатний контролювати практично усі загрози і своєчасно реагувати на них високоефективним способом, що забезпечує не тільки усунення уразливостей, які можуть привести до реалізування загрози, але і виявлення умов, які обумовлюють появу уразливостей. Модель адаптивної безпеки СКМ дозволяє зменшити зловживання у мережі, підвищити обізнаність користувачів, адміністраторів і керівництво про події безпеки у СКМ.

Адаптивна компонента моделі ANSM відповідає за модифікування процесу аналізу захищеності, надаючи йому найновішу інформацію про нові уразливості. Також він модифікує компоненту виявлення атак, доповнюючи її останньою інформацією про атаки. Як приклад адаптивної компоненти можна відзначити механізм оновлення баз даних антивірусних програм для

виявлення нових вірусів. Механізм взаємодії систем аналізу захищеності і виявлення атак моделі ANSM подано на рис. 2.

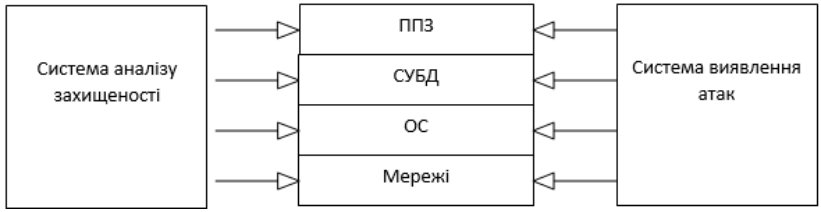


Рис. 2. Взаємодія систем аналізу захищеності і виявлення атак моделі ANSM

Слід відзначити, що пропонована модель не відкидає уже використовувані механізми захисту (розмежування доступу, автентифікування тощо). Вона розширює їх функціональність за рахунок нових інформаційних технологій (ІТ). Для того, щоб привести систему забезпечення ЗІ у відповідність до сучасних вимог, необхідно доповнити наявні рішення трьома новими компонентами, які відповідають за аналіз захищеності, виявлення атак і управління ризиками.

Адаптивний підхід до ЗІ дозволяє виявляти, контролювати ризики безпеки і реагувати на них у режимі реального часу, використовуючи правильно спроектовані і добре керовані процеси і засоби. Адаптивні системи захисту орієнтовані на активне протистояння загрозам безпеці. Реалізування такого підходу потребує проведення аналізу ризиків, розроблення ПІБ, використання традиційних засобів ЗІ, постійного аудиту безпеки та моніторингу стану системи, що має дозволити оперативно реагувати на ризики безпеки [3]. Основними засобами, які використовуються при реалізування адаптивних систем захисту, є пасивні – фільтри, міжмережеві екрани, і активні – давачі виявлення вторгнень, алгоритми розпізнавання аномальної поведінки, адаптивні алгоритми відновлення.

Адаптивна система ЗІ складається з трьох основних елементів:

- технології аналізу захищеності;

- технології виявлення атак;
- технології управління ризиками.

Технології аналізу захищеності – це технології пошуку вразливих місць у мережевому оточенні. СКМ складається із з'єднань, вузлів, хостів, робочих станцій (WS), ОС, СУБД і ППЗ. Усі вони потребують як оцінки ефективності їх захисту, так і виявлення невідомих уразливостей. Технології аналізу захищеності є дійовим методом, який дозволяє реалізувати ПІБ у СКМ перш, ніж здійсниться спроба її порушення ззовні або з середини.

Технології аналізу захищеності, за технічним реалізуванням, полягають у виконанні серії тестів з виявлення уразливостей. Ці тести є аналогічними до тих, що використовуються зловмисниками при здійсненні атак на СКМ.

У СКМ доводиться регулярно перевіряти, наскільки реалізовані або використовувані механізми ЗІ відповідають положенням прийнятої ПІБ. Така задача періодично виникає при зміні і оновленні компонент мережевого оточення, зміні конфігурації ОС тощо. Проте адміністратори безпеки не мають досить часу на проведення подібних перевірок для всіх вузлів СКМ. Тому використання сканерів безпеки значно полегшить аналіз захищеності використовуваних механізмів забезпечення ЗІ у СКМ.

Засоби аналізу захищеності працюють на першому етапі здійснення атаки. Виявляючи і своєчасно усуваючи уразливості, вони, таким чином, запобігають самій можливості реалізування атаки, що дозволяє знизити витрати на експлуатування засобів ЗІ. Найбільшого поширення набули засоби аналізу захищеності мережевих сервісів і протоколів, ОС, СУБД і Web-додатків, ППЗ.

Технології виявлення атак є процесом оцінювання підозрілих дій, які відбуваються в СКМ. Виявлення атак реалізується за допомогою аналізу журналів реєстрації ОС і додатків, а також мережевого трафіку у реальному часі. Компоненти виявлення атак, які розміщені на вузлах або сегментах СКМ оцінюють різні події та уразливості.

Технології управління інформаційними ризиками – процес виявлення, аналізу та зменшення ризиків інформаційної безпеки. Завдання управління ризиками включає в себе створення набору заходів (засобів контролю), які дозволяють знизити рівень ризиків до допустимої величини.

Організація процесу управління ризиками (рис. 3) дозволить виявити і мінімізувати інформаційні ризики, а також: гарантувати ЗІ в агресивному динамічному середовищі ризиків; оптимізувати витрати на реалізування системи ЗІ; забезпечить визначеність у тому, наскільки потрібно захищати інформаційні активи; забезпечить визначеність у тому, як краще досягти прийнятного рівня інформаційної безпеки, і який рівень можна вважати прийнятним; керівництво зможе приймати правильні стратегічні рішення, беручи до уваги інформацію про актуальні ризики; інтегрування функцій безпеки в усі аспекти управління ІС [4].

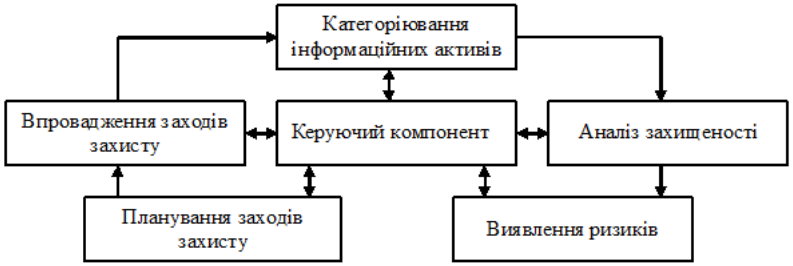


Рис. 3. Організація процесу управління ризиками

Оцінювання ризиків полягає у виявленні і ранжуванні уразливостей СКМ за ступенем небезпеки потенційних дій та збитку, за ступенем критичності загроз з урахуванням вірогідності їх реалізування тощо. Оскільки конфігурація СКМ постійно змінюється, тому і процес оцінювання ризиків повинен проводитися постійно. Це надасть можливість визначитися з пріоритетами реакції на події безпеки, які на сьогодні задаються статично і не дозволяють адаптивно керувати системою ЗІ у КСМ та проводити випереджувальні дії. З оцінювання ризиків необхідно розпочинати побудову системи ЗІ усієї ІС.

Висновки. Розв'язання проблем безпеки СКМ вимагає застосування адаптивного механізму, що працює у режимі реального часу і володіє високою чутливістю до змін в інформаційній інфраструктурі. Ефективність функціонування СКМ залежить від прийняття обґрунтованих рішень з захисту, які адаптовуються до постійно змінюваних умов мережевого оточення.

Адаптивний підхід до безпеки СКМ дає можливість пристосовуватися до зовнішніх змін середовища функціонування компенсовуючи небажані впливи, дозволяючи системі оптимізувати свою роботу відповідно до встановлених критеріїв, і, навіть, змінити ціль функціонування, якщо цього вимагають нові умови.

1. Рудий Т.В. Принципи організації системи захисту інформаційних систем підрозділів МВС / Т.В. Рудий, О.В. Захарова, О.І. Зачек, А.Т. Рудий / Науковий вісник ЛьвДУВС. Серія юридична / головний редактор М.М. Цимбалюк – Львів: ЛьвДУВС. 2012. – Вип. 2 (2). – С. 309-316.
2. Рудий Т.В. Політика інформаційної безпеки в інформаційних системах спеціального призначення / Т.В. Рудий, О.В. Захарова, А.Т. Рудий / Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі: збірник наукових статей за матеріалами доповідей науково-практичної конференції 27 грудня 2013 року. Львів: ЛьвДУВС, 2014. – С. 21-26.
3. Герасимчук О.І. Комплексні системи санкціонованого доступу: навч. посіб. / О.І. Герасимчук, В.Б. Дудикевич, В.А. Ромака. – Львів: Видавництво Львівської політехніки, 2010. -212 с.
4. Рудий Т.В. Організаційні принципи управління інформаційною безпекою інформаційних систем спеціального призначення / Т.В. Рудий, Я.Ф. Кулешник / Збірник наукових праць Таврійського державного агротехнологічного університету (економічні науки) /За ред. М.Ф. Кропивка. – Мелітополь: Вид-во Мелітопольська типографія ″Люкс″, 2012. - №2 (18), том 2. – С. 347-354.

СУЧАСНІ ТЕХНОЛОГІЇ АНАЛІЗУ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Сеник В.В.
завідувач кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент,

Шишко В.Й.
викладач кафедри інформатики
Львівського державного університету внутрішніх справ

Магеровська Т.В.
доцент кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат фізико-математичних наук, доцент

У повсякденній діяльності підрозділів Національної поліції України для прийняття ефективних, обґрунтованих рішень у питаннях протидії злочинності необхідно, насамперед, володіти достовірними і повними даними про її стан, структуру та динаміку, загальні та часткові причини, зрештою, умови вчинення злочинних посягань. А це вимагає критичного дослідження організації, засобів і методів проведення аналізу даних, який до цього часу застосовувався, його ефективності та достатності для протидії злочинності. На даний час вивчення злочинності полягає в отриманні достовірної інформації про її стан, рівень, динаміку, причини і умови, структуру, ефективність заходів щодо протидії їй. Важливо, щоб дана інформація відображала стан та інші характеристики злочинності. Тому необхідно, що вона відповідала, щонайменше, трьом основним вимогам: повноті, своєчасності та достовірності. Очевидно, що зробити правильний висновок про стан злочинності можна лише у тому випадку, якщо отримано достатній обсяг інформації про це явище.

Під час вивчення злочинності практично неможливо отримувати достатньо повну про неї інформацію відразу під час виникнення відповідних фактів чи подій. Для трактування стану злочинності

необхідно накопичувати і сумувати дані про злочини за певний, відносно тривалий період часу. Тому важливою та своєчасною буде і така кримінологічна інформація, яка отримана із звітних даних за певний минулий період часу або отримана в результаті дослідження попередньої практики боротьби зі злочинністю.

Раніше нами зауважувалося, що сьогоднішні дослідження злочинності, на жаль, не охоплюють усієї сукупності взаємодіючих соціально-економічних факторів, які впливають на злочинність. Усі дослідження спрямовані на встановлення зв'язку між окремими факторами і злочинністю, а це обмежує практичну цінність планування заходів для попередження злочинності та вироблення стратегії і тактики боротьби з нею [1].

Аналіз практики діяльності правоохоронних органів закордонних держав свідчить про використання ними різноманітних методів та підходів для проведення кримінального аналізу, від яких залежать як результати досліджень, так і глибина вникнення у закономірності злочинності. Не дивлячись на те, що на даний час цими підрозділами накопичено значний досвід проведення кримінального аналізу, слід констатувати його обмежене застосування підрозділами Національної поліції України у зв'язку з інтенсивним розвитком змін як в економічних, соціальних і правових умов життя нашого суспільства, через окремі бюрократичні перепони, так і через стрімкий розвиток науково-технічного прогресу, який, зокрема, вимагає постійного використання оновлених методів і технологій для проведення таких досліджень.

Сьогодні розрізняють три підходи до проведення кримінального аналізу:

1) ймовірнісний – зазвичай з припущенням, що величини, які досліджуються, підлягають розподілу Гауса;
2) геометричний – вважається, що дані не підлягають ймовірнісній природі і утворюють у багатовимірному просторі структури з певними властивостями;
3) змістовний – припускає можливість досягнення результатів за допомогою методів моделювання [1].

Перші два підходи передбачають використання методів прикладної статистики і використовують саме ймовірнісний та геометричний методи. Ці підходи передбачають, що під час аналізу має місце певна модель, найчастіше лінійна, і метою проведення аналізу є пошук параметрів, які б дану модель задовольняли.

Основою третього підходу є методи інтелектуального аналізу з використанням алгоритмів штучного інтелекту. При цьому, підбирається модель, яка певним чином найкраще описує вихідні дані. Ці методи ефективно використовують в технологіях *Data Mining*, *Big Data* та аналітичних технологіях Maltego, *IBM i2*.

Суть і мета технології Data Mining, її можливості щодо використання у інформаційно-аналітичній діяльності Національної поліції України та кримінальному аналізі розглядалася нами раніше [1, 2]. Можливості технології будуть розкриті в наступних дослідженнях. У зв'язку із цим та у зв'язку із обмеженим обсягом даної статті це питання нами додаткове не розглядатиметься. Ця робота присвячена можливостям технології *IBM i2* [3, 4, 5].

Аналітичні технології *IBM i2* є комплексним інтелектуальним інструментарієм для багатовимірного аналізу. В залежності від глобальності та сфери застосування можуть використовуватися його складові:

1. *IBM i2 Analyst's Workstation* – це інтегрований комплект інструментів для багатовимірного аналізу і візуалізації результатів, що забезпечує аналітикам безпосередній доступ до даних і надає потужні засоби інтерпретації цієї інформації. Функціонально він забезпечує: ефективне зберігання даних і управління ними; об'єднання збереженої інформації у централізованому сховищі та автоматизації типових завдань; швидкий перехід від аналізу тенденцій до аналізу шаблонів даних, просторових шаблонів або зв'язків між даними тощо.

2. *IBM i2 Analyze* – це корпоративне аналітичне середовище, що спрощує обмін інформацією і виконання аналітики з високою гнучкістю, яка забезпечується за рахунок використання веб-клієнтів і розширених клієнтів на настільних ПК. Продукт

прискорює аналіз великих обсягів даних завдяки використанню сервіс-орієнтованої середовища, створеного з метою інтеграції з існуючою корпоративною інфраструктурою відповідного підрозділу, підтримує оперативний аналіз і підвищує обізнаність про поточну ситуацію так як дозволяє швидше приймати обґрунтовані рішення всередині як окремого підрозділу, так і в рамках взаємодії між різними підрозділами. Іншими словами, IBM i2 Analyze – це інтелектуальний аналіз в спеціалізованому середовищі для об'єднання даних у спільній роботі.

IBM i2 Analyze допомагає керівникам підрозділів: приймати обґрунтовані рішення завдяки централізованому і агрегованому поданню інформації з різних джерел; підвищувати ефективність і результативність роботи підрозділів за рахунок загального середовища, що сприяє використанню результатів, отриманих з різних джерел; отримувати додаткову інформацію про ситуації в підрозділах завдяки інтуїтивно зрозумілим засобам аналізу і візуалізації; дотримуватись принципів «необхідно знати» і «необхідно поділитися» за допомогою стійкої, широко поширеної архітектури з надійним захистом; здійснювати інтеграцію з наявними інфраструктурами за допомогою масштабованої та розширюваної сервіс-орієнтованої аналітичної платформи. Таким чином, IBM i2 Analyze можна розглядати як програмний засіб аналізу і візуалізації даних для проведення ефективної аналітичної роботи.

3. *IBM i2 Analyst's Notebook* – візуальне аналітичне середовище, яке дозволяє максимально ефективно використовувати величезні обсяги інформації, накопичені державними органами та установами. Завдяки інтуїтивно зрозумілому інтерфейсу з урахуванням контексту дозволяє аналітикам швидко зіставляти, аналізувати і наочно представляти дані з різних джерел, скорочуючи час на пошук важливої інформації у складних даних. IBM i2 Analyst's Notebook надає актуальні і дієві аналітичні засоби, що допомагають виявляти, передбачати, запобігати і припиняти злочинну, терористичну і шахрайську діяльність.

i2 Analyst's Notebook допомагає підрозділам вирішувати наступні завдання: швидко систематизувати розрізнені дані в єдиному узгодженому поданні; визначати ключових осіб, події, зв'язки і закономірності, які не завжди можна виявити іншими засобами; покращувати розуміння структури, ієрархії і способів дій злочинних, терористичних і шахрайських організацій; спрощувати обмін складними даними, що дозволяє приймати своєчасні та точні оперативні рішення; надає можливість здійснювати продуктивну аналітичну роботу, завдяки надійним рішенням для візуальної аналітичних результатів. Таким чином i2 Analyst's Notebook можна представити як програмне забезпечення для поліції, що дозволяє здійснювати ефективний збір, обробку та використання аналітичної інформації.

4. *IBM i2 COPLINK* – це програмне забезпечення, що дозволяє об'єднувати дані з різних джерел, спільно з іншими підрозділами розробляти тактичні версії. Воно дає можливість співробітникам правоохоронних органів підбирати фотографії підозрюваних осіб для впізнання, зберігати хронологію пошуку зловмисників та впорядковувати розслідування. i2 COPLINK – це модульне програмне забезпечення, яке може бути пристосоване для роботи з додатковими правоохоронними засобами відповідно до визначених потреб користувача, для удосконалення можливостей розкриття злочинів.

IBM i2 COPLINK може допомогти правоохоронцям виконувати такі завдання: виявляти ключі до розкриття справ шляхом упорядкування та надання тактичного, стратегічного доступу до великих обсягів даних, які здаються, на перший погляд, непов'язаними між собою; візуалізувати і аналізувати дані на схемах за допомогою відтворення у часовій послідовності; централізувати кілька сховищ даних в єдиній системі і виявляти приховану цінність в існуючих сховищах інформації; спільно використовувати і захищати дані за допомогою таких безпекових функцій як захист паролями і шифруванням даних. IBM i2 COPLINK є сучасним програмним засобом виявлення і розслідування злочинних схем.

5. *IBM i2 Fraud Intelligence Analysis* – потужний програмний засіб попередження та розслідування шахрайських схем. Він допомагає: майже миттєво виявляти можливі шахрайства та відправляти попередження відповідним фахівцям; аналізувати і візуалізувати складні багатоканальні атаки; своєчасно розсилати оперативну інформацію посадовим особам відповідно до обов'язків.

6. *IBM i2 iBase* – це інтуїтивно зрозуміли аналітичний додаток баз даних, який дозволяє аналітикам збирати, контролювати і аналізувати дані з декількох джерел в захищених середовищах. Цей продукт дозволяє вирішувати повсякденну проблему аналітиків, яка полягає у виявленні і розкритті особливостей взаємозв'язків, шаблонів і тенденцій в сучасних умовах, що характеризуються стрімким зростанням обсягів складних структурованих і неструктурованих даних. i2 iBase надає багатокористувацьке середовище обміну даними, ефективність роботи в якому забезпечується широким набором функцій аналізу і візуалізації.

i2 iBase ефективно забезпечує: гнучке накопичення і управління даними, які пов'язують і перетворюють інформацію з метою візуалізації і подальшого аналізу; автоматизований аналіз на основі завдань для прискорення розкриття прихованих зв'язків, який допомагає аналітикам своєчасно надавати практично застосовні результати; підтримка керованої спільної роботи і потоків операцій, яка спрощує колективну роботу. Таким чином, i2 iBase можна розглядати як додаток для збору, контролю і аналізу даних з декількох джерел у захищених робочих групах.

7. *IBM i2 Pattern Tracer* – це програмне забезпечення, що оперативно аналізує великі обсяги телефонних записів, групує їх за спільними ознаками і виявляє ключових учасників подій. Додаток також дозволяє виявляти потенційних абонентів і запобігати певним подіям в майбутньому. IBM i2 Pattern Tracer може використовуватися разом з IBM i2 Analyst's Notebook.

IBM i2 Pattern Tracer дозволяє: усувати ручний аналіз телефонних записів, чим істотно підвищує ефективність аналітичної роботи щодо телефонних зв'язків; швидко виділяти основну суть

телефонного дзвінка, знаходити серед великого обсягу інформації групи дзвінків зі схожими ознаками і наочно їх відображати; ефективно управляти цільовими ресурсами, допомагати приймати обґрунтовані рішення і опрацьовувати найбільш потрібні ресурси.

8. *IBM i2 iBridge* – це розширене рішення для зв'язку та аналітичного пошуку, яке з'єднує користувачів IBM i2 Analyst's Notebook безпосередньо з базами даних організації. Ефективні інструменти пошуку та виконання запитів повертають результати у вигляді готових до аналізу даних з візуалізацією зв'язків між записами для прискорення створення аналітичних даних.

Навіть такого поверхневого аналізу, обмеженого рамками даної публікації, достатньо для висновку, що діяльність зарубіжних правоохоронних органів на сучасному етапі щодо попередження та розкриття злочинів забезпечується потужними аналітичними засобами на основі алгоритмів штучного інтелекту.

На тлі всезростаючого інтелектуального рівня підготовки та здійснення протиправних намірів злочинними угрупуваннями в Україні надзвичайно актуальним видається впровадження у практику діяльності підрозділів Національної поліції України саме інтелектуальних засобів аналітичної підтримки.

Навчальні заклади системи МВС мають бути промоутерами щодо вивчення та впровадження новітніх технологій з метою перебудови оперативно-розшукової та слідчої ланки в діяльності підрозділів Національної поліції України на основі апробованих засобів глибокої аналітичної обробки інформації, що успішно використовуються в розвинутих країнах світу.

---

1. Сеник В.В. Шишко В.Й., Братичак О.В. Впровадження нових підходів щодо автоматизації кримінального аналізу у практичній діяльності національної поліції України / Використання сучасних інформаційних технологій діяльності національної поліції України: матеріали всеукраїнського наук.-

практ. семінару, м. Дніпро, 24 листопада 2017 року – Дніпро: ДДУВС, 2018. – С. 79-82.
2. Сеник В.В. Перспективи використання технології Data Mining для аналізу та прогнозування стану злочинності / Теорія та практика протидії злочинності у сучасних умовах: збірник тез Міжнародної науково-практичної конференції (10 листопада 2017 року) / упор. О.В. Авраменко, С.С. Гнатюк, І.В. Красницький. – Львів: ЛьвДУВС. – с. 214-215.
3. Выявление скрытых связей на основе анализа текстов с помощью i2. Центр компетенции по технологии IBM BigData. – М., 2014. – 66 с.
4. Peterson Marilyn B. Applications in Criminal Analysis: A Sourcebook. Praeger Publishers, 88 Post Road West, Westport, CT 06881. Library of Congress. Catalog Card Number: 94-11219.
5. IBM-IBM i2 Analyst's Notebook. http://www.i2group.com/us/products/analysis-product-line/analysts-notebook [Електронний ресурс]. – Режим доступу : [27.05.2012]

ЗАСТОСУВАННЯ ОКРЕМИХ ПОЛОЖЕНЬ ЗАКОНОДАВСТВА УКРАЇНИ В СФЕРІ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ ТА ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Сеник С.В.
науковий співробітник ВОНР
Львівського державного університету внутрішніх справ,
здобувач кафедри адміністративно-правових дисциплін
ЛьвДУВС

Сьогодні, у часі реформування діяльності підрозділів Національної поліції в Україні інформаційна та інформаційно-аналітична діяльність безсумнівно має основоположне значення, оскільки спрямована на забезпечення громадського порядку та безпеки, є визначальною у виборі стратегії боротьби зі злочинністю, охорони прав і свобод громадян, власності і «є системоутворюючим елементом будь-якої управлінської діяльності» [1, С. 187].

Однак, на даному етапі реформування і розвитку Національної поліції України виникає питання системного наповнення, підтримання та розширення практики використання інформаційних ресурсів, створення нових інформаційно-аналітичних систем на основі «штучного інтелекту», систематизації інформації, що надходить з різних джерел. Вирішення даного питання не можливо здійснити без наявності відповідної нормативно-правової бази її удосконалення та розвитку.

Перед розглядом нашого питання слід зазначити, що під нормативно-правовим регулюванням науковці розуміють форму регулювання суспільних відносин у певній галузі у відповідності до вимог і дозволів, що містяться в нормах права, тобто здійснюваний за допомогою юридичних засобів процес упорядкування суспільних відносин з метою забезпечення певної сукупності соціальних інтересів, які вимагають правового регулювання [2, с. 207–208]. У нашому випадку такими нормами права є, насамперед, Конституція та конституційні закони, зокрема, такі як: закони України: «Про Національну поліцію» [3], «Про інформацію» [4], «Про державну таємницю» [5], «Про захист інформації в інформаційно-телекомунікаційних системах» [6], «Про оперативно-розшукову діяльність» [7], «Про доступ до публічної інформації» [8], «Захист персональних даних» [9], «Про телекомунікації» [10] та інші. Перелічені закони не обов'язково повністю за своїм змістом призначенні для регулювання інформаційної чи інформаційно-аналітичної діяльності Національної поліції, однак саме вони містять основні положення щодо збору, накопичення інформації, порядку внесення її до банків даних, збереження, особливості використання тощо.

Очолює ієрархію правових актів, які регулюють суспільні відносини у вищезгаданій сфері, звичайно ж Конституція України. Оскільки детальний розгляд застосування її положень щодо питання, яке нами розглядається, було проаналізовано в [11], а також враховуючи обмеженість обсягу даної публікації, зупинимося лише на аналізі вище приведених законів, які, безумовно, враховують усі конституційні норми.

Основоположне значення у нормативному регулюванні інформаційної та інформаційно-аналітичної діяльності поліції України, насамперед, відіграє Закон України «Про Національну поліцію», оскільки саме цим законодавчим актом передбачено надання їй повноважень у сфері обігу інформації, інформаційно-аналітичного забезпечення, формуванню та використанню інформаційних ресурсів. Зокрема, у ст. 25 даного Закону зазначено, що поліція в рамках інформаційно-аналітичної діяльності: формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; користується базами (банками) даних Міністерства внутрішніх справ 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. Окрім цього, поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень. Що ж стосується повноважень поліції у галузі формування інформаційних ресурсів, то вони визначені ст. 26 даного Закону.

Надавши відповідні повноваження Національній поліції у галузі інформаційної та інформаційно-аналітичної діяльності, законодавець у ст. 28 встановив і певні обмеження щодо роботи з інформаційними ресурсами, відповідальність за їх протиправне використання.

Наступним слід розглянути Закон України «Про інформацію», який є основним нормативно-правовим актом у галузі регулювання інформаційних відносин в Україні і у якому встановлено основні правові засади одержання, використання, поширення та зберігання інформації, а також систему інформації, її джерела, доступ до інформації та її охорону.

Згідно зі ст. 2 даного Закону основними аспектами інформаційних відносин у діяльності підрозділів Національної поліції України мають стати правомірність одержання, використання, поширення, зберігання та захисту інформації; її достовірність і повнота; захищеність особи від втручання в її особисте та сімейне життя. Враховуючи конституційні принципи Закон України «Про інформацію» водночас допускає (ст. 6 п. 1) обмеження прав на інформацію в інтересах нацбезпеки, територіальної цілісності чи громадського порядку з метою запобігання заворушенням чи злочинам, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету й неупередженості правосуддя.

Закон України «Про інформацію» у ст. 9 встановлює вичерпний список основних видів інформаційної діяльності, до яких відноситься створення, збирання, одержання, зберігання, використання, поширення, охорона і захист інформації, та розділяє інформацію за доступом на дві групи: 1) відкриту; 2) з обмеженим доступом.

Для регулювання нормативно-правових відносин у суспільстві, які пов'язані з опрацюванням інформації, що віднесена до державної таємниці, засекречуванням, розсекречуванням її носіїв та охороною державної таємниці, вступають в силу положення Закону України «Про державну таємницю». Згідно зі ст. 6 даного Закону Національна поліція України, як виконавець оперативно-розшукових повноважень реалізує свої права з «урахуванням обмежень, установлених в інтересах національної безпеки України». Закон (розділ III) також визначає порядок засекречування інформації. Крім цього слід зазначити, що цим законом регулюються основні організаційно-правові заходи щодо охорони державної таємниці (ст. 18).

Важливе значення у сучасних умовах розвитку науково-технічного прогресу в діяльності підрозділів Національної поліції відведено Закону України «Про захист інформації в інформаційно-телекомунікаційних системах». Даним нормативним актом встановлено основні засади регулювання правових відносин

щодо захисту інформації в автоматизованих системах з урахуванням умов дотримання прав власності громадян України та юридичних осіб на інформацію та права доступу до неї. Цей закон цікавий тим, що його дія поширюється на будь-яку інформацію, що обробляється в інформаційно-телекомунікаційних системах.

Наступним нормативно-правовим актом, який регулює інформаційну діяльність у Національній поліції, є Закон України «Про оперативно-розшукову діяльність». У норми даного закону закладена інформація, яка визначає безпосередній зміст оперативно-розшукових заходів і є у регулятором діяльності, спрямованої на отримання й ефективне використання оперативно-розшукової інформації для протидії злочинності.

Цікавим у даному Законі є те, що для отримання інформації законодавець наділяє підрозділи, які здійснюють оперативно-розшукові заходи, виключними правами (ст. 8), до яких, зокрема, відносять отримання інформації за допомогою спеціальних технічних засобів оперативного призначення, автоматизованих інформаційних систем тощо.

Також важливим нормативно-правовим актом у галузі інформаційної діяльності Національної поліції є Закон України «Про доступ до публічної інформації», у ст. 5 якого передбачено, що доступ до інформації забезпечується шляхом систематичного та оперативного оприлюднення інформації в офіційних друкованих виданнях; на офіційних веб-сайтах в мережі Інтернет; на єдиному державному веб-порталі відкритих даних; на інформаційних стендах; будь-яким іншим способом; надання інформації за запитами на інформацію. Реалізацію цього положення Національною поліцією можна побачити на офіційних веб-сайтах, де висвітлюються резонансні події, злочини тощо.

Не менш важливу роль у діяльності Національної поліції відіграє Закон України про «Захист персональних даних», оскільки відповідно до ст. 4 даного Закону Національна поліція, у зв'язку із специфікою своєї діяльності є володільцем і розпорядником персональних даних, а це зобов'язує її виконувати визначені ст. 6 та

ст. 7 загальні та особливі вимоги до обробки персональних даних. Однак слід зазначити, що ч. 1 ст. 25 надає Національній поліції право обмежити дії статей 6 і 7 даного закону у «випадках передбачених законом, наскільки це необхідно у демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб».

Розглянутий та проаналізований нами перелік законодавчих актів (Законів України) не є остаточним і вичерпним. У діяльності підрозділів Національної поліції, які здійснюють інформаційну та інформаційно-аналітичну роботу, застосовуються норми і інших законів України. Однак, саме вищезазначені нормативно-правові акти становлять основу для адміністративно-правового регулювання її діяльності у сфері обігу інформаційних ресурсів.

---

1. Єсімов С. С. Інформаційно-аналітична діяльність МВС України як об'єкт правового регулювання / С. С. Єсімов // Науковий Вісник Львівського державного університету. – 2017. – С. 184–195. – (Серія юридична ; № 1).
2. Загальна теорія держави і права / [М. Цвік, О. Петришин, Л. Авраменко та ін.] ; за ред. М. Цвіка, О. Петришина. – Харків : Право, 2009. – 684 с.
3. Про національну поліцію : Закону України від 2 липня 2015 р. [Електронний ресурс] // База даних «Законодавство України» ВР України. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/580-19/.
4. Про інформацію : Закон України від 02 жовтня 1992 р. [Електронний ресурс] // База даних «Законодавство України» ВР України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12/.
5. Про державну таємницю : Закон України від 21 січня 1994 р. [Електронний ресурс] // База даних «Законодавство України» ВР України. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/3855-12/.
6. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України [Електронний ресурс] // База даних «Законодавство України» ВР України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/.

7. З Про оперативно-розшукову діяльність : Закон України від 18 лютого 1992 р. [Електронний ресурс] // База даних «Законодавство України» ВР України. - Режим доступу : http://zakon3.rada.gov.ua/laws/show/2135-12/.
8. Про доступ до публічної інформації : Закон України [Електронний ресурс] // База даних «Законодавство України» ВР України. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/2939-17.
9. Про захист пересональних даних : Закон України [Електронний ресурс] // База даних «Законодавство України» ВР України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2297-17.
10. Про телекомунікації : Закон України [Електронний ресурс] // База даних «Законодавство України» ВР України. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/1280-15.
11. Сеник С. В. Конституційні права і свободи як умова інформаційної безпеки людини / С. В. Сеник. В. В. Сеник // Сучасний конституціоналізм: проблеми теорії та практики (до 20-ї річниці Конституції України) : матеріали наукового семінару (24 червня 2016 р.) / упор. М. В. Ковалів. – Львів : ЛьвДУВС, 2017. – С. 243–247.

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ: ОКРЕМИЙ АСПЕКТ

Сіротченков Д.Ю.
викладач кафедри тактико-спеціальної підготовки факультету ПФППД Дніпропетровського державного університету внутрішніх справ, старший лейтенант поліції

Вибір даної тематики зумовлений, перш за все, тим, що на сьогодні набуває все більшого значення інформаційно-аналітичне забезпечення працівників підрозділу оперативно-розшукової діяльності.

Більшість науковців притримуються позиції стосовно того, що удосконалюючи інформаційно-аналітичне забезпечення підвищується результат підрозділів у боротьбі зі злочинністю, а особливо економічною.

Державна інформаційна політика забезпечується, перш за все, підрозділами інформаційно-аналітичного забезпечення, а також оперативного реагування. Вони існують нещодавно, тим самим замінив старі штабні підрозділи.

Дана тема не є новою для обговорення, а тому до неї неодноразово звертались правники, серед яких найбільшої популярності дістали праці таких вчених як Є.А. Антонова, К.К. Горяїнова, Д.В. Гребельський, О.Ф. Долженкова, В.П. Захарова, А.М. Лисенко, В. А. Лукашова, С.С. Овчинський, В.Л. Ординський, В.І. Рудешко.

Не дивлячись на таку кількість вчених, які розглядали даний аспект проблеми, вона була розглянута ними не повністю, що і зумовлює подальші дослідження сучасних вчених, задля всебічного розгляду тематики.

У складі апарату Національної поліції працює Департамент організаційно-аналітичного забезпечення та оперативного реагування (далі-ДОАЗОР). Його діяльність регламентується наказом Національної поліції України (далі-НПУ) «Про затвердження Положення про Департамент організаційно-аналітичного забезпечення та оперативного реагування НПУ» №126 від 27.11.2015 р. Відповідно до Положень ДОАЗОР забезпечує і здійснює у межах своєї компетенції функції НПУ щодо координації, аналізу, планування, контролю та узгодження дій територіальних (міжрегіональних) органів, структурних (відокремлених) підрозділів поліції з реалізації державної політики у сфері забезпечення публічної безпеки і порядку, охорони та захисту прав і свобод людини, інтересів суспільства і держави протидії злочинності[1].

Розглядаючи оперативно-розшукову діяльність, можна помітити, аби встановити істину здійснюється аналітична робота. Під аналітичною роботою слід вважати таку творчу діяльність, яка пов’язана з оцінкою певної інформації, та на основі якої приймаються оптимальні рішення.

Основними завданнями УОАЗОР є:

- моніторинг оперативної обстановки на території обслуговування та організація реагування на її зміни;

- діяльності на території обслуговування, виявлення причин та умов, що сприяють учиненню кримінальних та адміністративних правопорушень, організація ужиття в межах компетенції заходів щодо їх усунення;
- організація діяльності чергових частин підрозділів ГУ;
- здійснення організаційного та методичного забезпечення аналітичної роботи підрозділів ГУ, організація комплексного аналізу стану забезпечення публічної безпеки і порядку, охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, а також надання поліцейських послуг на території обслуговування, аналіз відповідних результатів роботи підрозділів ГУ;
- здійснення контролю за виконанням підрозділами ГУ Конституції України та інших законів України, указів Президента України та постанов Верховної Ради України, прийнятих відповідно до Конституції та законів України, актів Кабінету Міністрів України, нормативно-правових актів МВС, інших актів законодавства України;
- забезпечення в межах повноважень, передбачених законом, виконання завдань з мобілізаційної підготовки та мобілізаційної готовності, територіальної оборони, організація та проведення заходів щодо рятування людей, забезпечення їх безпеки, охорони майна в разі стихійного лиха, аварій, пожеж, катастроф та ліквідації їх наслідків (далі – цивільний захист) в підрозділах ГУ, у тому числі в особливий період, їх координація та методичне забезпечення;
- здійснення в підрозділах ГУ систематичного аналізу та перевірок стану обліково-реєстраційної дисципліни [1].

Отже підсумовуючи вищенаведене, можна дійти висновку, що беручи до уваги реформування МВС Україні, існує нагальна потреба удосконалити практичну діяльність працівників підрозділу кримінальної поліції.

Щоб реалізувати найкращу підготовку фахівців кримінальної поліції необхідно, перш за все, дотримуватися вимог режиму секретності. Та нарешті, необхідно звернути увагу на застосування сучасного інформаційного простору, комунікативних технологій.

Отже, інформаційно-аналітичне забезпечення підрозділів кримінальної поліції – це система заходів, що врегульована нормативно-правовими актами, спрямована, в першу чергу, на аналіз, узагальнення, оброблення, зберігання інформації, навіть з обмеженим доступом, яка впливає на подальші рішення у діяльності ОРД, для забезпечення охорони громадян та держави тощо.

---

1. Про затвердження Положення про Департамент організаційно-аналітичного забезпечення та оперативного реагування Національної поліції України: наказ національної поліції України №126 від 27.11.2015 р.

ОРГАНІЗАЦІЙНО-ТАКТИЧНІ ОСОБЛИВОСТІ ПРЕД'ЯВЛЕННЯ ДЛЯ ВПІЗНАННЯ ЗА ФОНОГРАМОЮ

Христов О.Л.
доцент кафедри криміналістики, судової медицини та психіатрії Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук

Лонська Є.В.
курсант 4 курсу факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ

Аналіз положень чинного законодавства свідчить про неповну процесуальну урегульованість окремих слідчих (розшукових) дій (далі – СРД), зокрема пред'явлення для впізнання, яке в Кримінальному процесуальному кодексі України закріплено в ст.ст. 228–232. Поряд з цим, практика застосування цієї СРД є досить розповсюдженою та затребуваною під час досудового розслідування [1, с. 164].

Одночасно, окремі аспекти деяких видів пред'явлення для впізнання залишаються не врегульованими не тільки на законодавчому рівні, але і не знайшли гідного висвітлення у науковій

літературі в частині розробки організаційно-тактичних особливостей їх проведення.

Слід зазначити, що особливим видом впізнання за комплексом ознак, що упізнаються є пред'явлення для впізнання за голосом та особливостями мови чи за фонограмою.

Такі особливості, на наш погляд, в першу чергу, полягають у тактично грамотному виборі форми пред'явлення ознак об'єкта, тобто голос, який буде звучати в натурі чи пред'являтися за допомогою фонограми.

Необхідність впізнання фонограм голосу або мови особи, що впізнається виникає у наступних випадках:

- коли немає можливості організувати впізнання в «натурі» [2]. Наприклад, за фонограмою впізнання проводиться коли суб'єкт впізнання заявляє на допиті, що зможе впізнати підозрюваних (обвинувачених) за зовнішнім виглядом і голосом, але пред'явити цих осіб для впізнання не є можливим, оскільки вони приховуються від слідства та суду, перебувають у довгостроковому відрядженні, померли або фізично ліквідовані, знаходяться у розшуку або місце перебування їх невідоме, однак є фонограми із записом їх голосу [3, с. 56];
- коли необхідно встановити особу померлого, чий голос було зафіксовано на фонограмі;
- за наявності обґрунтованого припущення, що особа, яку будуть впізнавати, перешкоджатиме його проведенню навмисним викривленням своєї мови;
- коли фонограма голосу та мови є речовим доказом і необхідно встановити особу, голос або мову якої на ній зафіксовано [2].
- коли особа, яку необхідно пред'явити для впізнання за голосом, відмовляється від участі у даній слідчій дії, однак є фонограма із записом її голосу;
- коли особа, яка підозрюється у вчиненні злочину, відмовляється визнати, що саме її голос записаний на магнітну плівку;

- щоб запобігти негативному впливу на свідків та потерпілих, забезпечити безпеку осіб, які беруть участь у кримінальному судочинстві та ін. [3, с. 56].

Крім того, певні особливості виникають і при визначенні процедури отримання зразків запису голосу підозрюваного, а також інших порівняльних зразків, які необхідно представляти у певній кількості.

К. О. Чаплинський зазначає, що для проведення такого виду впізнання використовується спеціально виготовлена фонограма [3, с. 56], проте сама процедура не визначена у правовому полі, тому, можна сказати, що уповноважена особа приймає рішення про процедуру отримання зразків голосу за власним переконанням, враховуючи чинники зручності, ефективності і швидкості.

Поряд з цим, теорія криміналістики містить наукові рекомендації стосовно такої процедури. Так, Є. Д. Лук'янчиков та О. М. Моїсєєв визначаючи порядок пред'явлення для впізнання за фонограмою, пропонують з фонограми усної мови особи, яку пред'являють для впізнання, виділяти частину з декількома чітко проголошеним фразами і найменшою кількістю завад; зміст цих фраз передбачається викладати письмово[4, с. 71]. Порівняльні зразки фонограм пропонується отримувати від двох осіб з голосами схожими з голосом особи, яку пред'являють, шляхом промовляння зазначених фраз для запису на магнітну стрічку [4, с. 71].

Однак, слід зауважити, що процедура отримання фонограми голосу особи, яку впізнають вченими не запропонована.

На наш погляд, можна запропонувати кілька порядків отримання зразків фонограми голосу особи, яку впізнають:

- добровільно надані особою, яку впізнають;
- отримані за результатами проведення слідчих (розшукових) дій, наприклад, допиту;
- отримані за результатами проведення НСРД (ст. 263 КПК України) чи ОРЗ.

У зв’язку з цим, під час документування злочинних дій розроблюваних осіб за оперативно-розшуковою справою, а також під час реалізації матеріалів ОРД підрозділам кримінальної поліції слід передбачати можливість використання в подальшому фонограм, отриманих у ході ОРЗ.

1. Колесник В.А. Деякі проблемні питання пред’явлення особи та речей для впізнання за чинним КПК України / В.А. Колесник // Вісник Академії адвокатури України. - № 1(26), 2013. – С. 163-168.
2. Марченко А. Б. Особливості тактики пред’явлення для впізнання особи за мовою та голосом / А. Б. Марченко // Часопис Академії адвокатури України, 2010. № 9 (4). URL: http://e-pub.aau.edu.ua/index.php/chasopys/article/viewFile/541/561.
3. Тактика пред’явлення для впізнання при розслідуванні злочинів проти життя, здоров’я, волі та статевої недоторканості особи: Навчально-практичний посібник / К.О. Чаплинський. Днапропетроавьск: УМВС України в Дніпропетровській області; Дніпропетровський державний університет внутрішніх справ, Свідлер, 2007. 92 с.
4. Пред’явлення для впізнання : Навчальний посібник / Є. Д. Лук’янчиков, О. М. Моїсєєв. Макіївка: Графіті, 1998. 104 с.

СТАН ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Чистоклетов Л.Г.
професор кафедри адміністративного та інформаційного права Навчально-наукового інституту права та психології НУ «Львівська політехніка»,
доктор юридичних наук, професор

Хитра О.Л.
доцент кафедри адміністративного права та адміністративного процесу факультету №3 ІПФПНП Львівського державного університету внутрішніх справ,
кандидат юридичних наук

На сучасному етапі соціально-політичного розвитку суспільства, в умовах ведення гібридно-месіанської війни [1, с. 16; 2] проти України путінською Росією з використанням найсучаснішої інформаційної технології, спрямованої на зміну конституційного ладу, розпалювання національної і релігійної ворожнечі, захисту інформаційної безпеки стає одним із найважливіших завдань Національної безпеки, діяльність якої спрямована на захисту територіальної цілісності та суверенітету України.

Значне зростання ролі інформаційної безпеки в процесі налагодження суспільних відносин, а також активізація використання сучасних інформаційних технологій істотно впливають як на діяльність державного апарату загалом, так і на роботу системи Національної поліції зокрема. Адже інформатизація може не тільки завдати прямих збитків конкретній особі в разі несанкціонованого доступу до її даних, їхнього використання, модифікації або знищення, а й перетворитися на джерело серйозних загроз розвитку держави [3].

Нині є необхідність у формуванні нової, цілісної, науково обґрунтованої системи гарантування інформаційної безпеки,

котра має діяти не тільки на загальнодержавному рівні, а й забезпечувати функціонування корпоративних організацій, окремих юридичних осіб та правоохоронних органів. Протягом останніх років в Україні мали місце неодноразові спроби реалізації комплексу заходів, спрямованих на вдосконалення механізмів гарантування інформаційної безпеки. Однак, як свідчать статистичні дані, їхнє впровадження не ліквідувало загроз інформаційній безпеці (зокрема, й на рівні правоохоронних органів), тому її система потребує нагального перегляду та вдосконалення. Ці процеси безпосередньо пов'язані з переглядом чинної політики держави щодо гарантування інформаційної безпеки і, відтак, з докорінним реформуванням її системи. [3].

На думку О. Красікова, забезпечення інформаційної безпеки правоохоронних органів України (Національної поліції) здійснюють за двома формами:

- організаційною (організація роботи правоохоронних органів, роботи, пов'язаної з обігом, збиранням, обробкою, зберіганням та використанням інформації, взаємодія працівників правоохоронних органів щодо забезпечення інформаційної безпеки);
- правовою (видання наказів та розпоряджень, розроблення положень, інструкцій, складання планів тощо) [4, с. 11–15].

До аналізу правового змісту інформаційної безпеки спонукає поточний стан суспільно-політичного життя держави. Наявні в інформаційній сфері України суспільні відносини підпадають під дію положень понад чотирьох тисяч нормативно-правових актів різної юридичної сили, що актуалізує проблему узгодження регулятивних та охоронних норм, якими визначаються правові основи інформаційної діяльності, наслідки порушення встановлених щодо неї обмежень, заборон [5].

Основними нормативно-правовими актами, які спрямовані на правове забезпечення належного стану інформаційної безпеки в Національній поліції є закони України «Про доступ до публічної інформації» [6], «Про основні засади розвитку інформаційного

суспільства в Україні на 2007- 2015 роки» від 09.01.2007 № 537-V [7], «Про телекомунікації» від 18.11. 2003 № 1280-IV [8], «Про захист інформації в інформаційно- телекомунікаційних системах» [9], «Про основи національної безпеки України» [10], «Про Національну поліцію» [11], Указ Президента України від 25 лютого 2017 року № 47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про доктрину інформаційної безпеки України», та деякі інші нормативно-правові акти [12]. Проте, як показує аналіз основних положення Доктрини інформаційної безпеки України, сумнівними у її змісті виступають форми реалізації, а саме, які положення повинні виконуватись і хто конкретно буде відповідати за їх невиконання.

Важлива роль у виконанні національної інформаційної безпеки органами Національної поліції надана МВС України. Так, відповідно до покладених на нього завдань, МВС… «забезпечує в межах повноважень, передбачених законом, захист інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом» [13].

Особливо небезпечним злочином у сфері інформаційної безпеки виступає кіберзлочинність, яка на сьогодні є найпотужнішою загрозою у інформаційному просторі. З метою убезпечення цього злочину було прийнято Закон України 5 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України» [14]. Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Поява терміну «кіберзлочини» пов'язують з розширенням технічної бази інформатизації. Зокрема, Т.Л. Тропина пропонує визначати кіберзлочини як «винне досконале суспільно небезпечне

кримінально каране втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціоноване модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, вчинені за допомогою або за допомогою комп'ютерів, комп'ютерних мереж і програм, а також за допомогою або за допомогою інших пристроїв доступу до модельованого за допомогою комп'ютера інформаційного простору» [15, с. 38.].

Важливим в усвідомленні сутності кібертероризму, боротьбі з ним є підготовка в системі навчальних закладів МВС України відповідного кадрового потенціалу, з фаховою профілізацією «інформаційні технології». Також вказуючи на недостатній рівень професійної підготовки працівників поліції у протидії кібертероризму, повчальним для їх діяльності буде зарубіжної досвід поліцейської практики, який вимагає активізації роботи з уніфікації національних законодавств на підставі норм міжнародних договорів на прикладі діяльність Євроюсту, Європолу (англ. Europol Liaison Officer, ELO) та поліцейської служби Європейського Союзу [16].

Так, основними завданнями поліцейської служби є координація роботи національних служб у боротьбі з міжнародною організованою злочинністю і поліпшення інформаційного обміну між національними поліцейськими службами. Серед основних напрямів:

- протидія фінансуванню тероризму, включаючи використання в цих цілях некомерційних організацій; надання технічного сприяння третім країнам;
- розроблення системи взаємного визнання судових рішень, а також рішень інших компетентних правоохоронних органів, зокрема імплементація положень про європейський ордер про арешт;
- підвищення доступності інформації.

Таким чином, ми вважаємо, що інформаційна безпека в діяльності Національної поліції повинна віддзеркалювати стан захищеності прав та інтересів громадян, держави, суспільства та не допускати

свавілля держаних чиновників в процесі реалізації нормативно-правових актів в інформаційній сфері.

Слід також констатувати, що важливою проблемою у правовому забезпеченні інформаційної безпеки Національної поліції залишається невиразне та непослідовне ухвалення інформаційних нормативно-правових актів, у більшості з яких інформаційні відносин регулюється підзаконними, а подекуди й відомчими нормативними актами. Відсутність законодавчого визначення режимів доступу до інформації не рідко приводить до порушення законності. Значна частина норм інформаційного законодавства носить декларативний характер, з певною розмитістю формулювань, без врахування тактичних та стратегічних інтересів національної безпеки, що суперечать правовій політиці в інформаційній сфері, вказуючи на її неоглядність. Прикладом цього є думка, експертів проекту «ArmyUA» Григорія Любовець та Валерія Король, з якою ми цілком погоджуємося, які, характеризуючи гібрідно-месіанську війну, розв'язаної з вини путінської Росії, досить аргументовано стверджують, що насправді ми вже давно зіткнулися з повномасштабним вторгненням, але, на жаль, відмовляємось зафіксувати це на офіційному рівні. Це вторгнення характеризується економічною, фінансовою, культурною, освітньою, ідеологічною та інформаційною експансією, яка проводилась протягом всього періоду незалежності і мала на меті ментальне поневолення українського народу. Офіційне дослідження глибини такого повномасштабного вторгнення… дало б не лише відповіді щодо стану сучасного державотворення української держави, але й суттєво допомогло б у виробленні "вакцини" протидії імперській політиці путінської Росії [17].

---

1. Березовець Т.В. Анексія: острів Крим. Хроніки «гібридної війни» / Т.В. Березовець. – Брайт Букс, 2015. – 584 с.
2. Шелудченко О. Месіанські ідеї в монотеїстичних релігіях Електронний ресурс]. – Режим доступу: http://dspace.nbuv.gov.ua/bitstream/ handle/123456789/14779/3-Sheludchenko.pdf? seqence=3.

3. Субот А. Інформаційна безпека діяльності працівників правоохоронних органів Електронний ресурс]. – Режим доступу: http://veche.kiev.ua/journal/4459/.
4. Красіков Д. О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України: автореф. дис. ... канд. юрид. наук: 12.00.07 / Д. О. Красіков. – К., 2012. – 20 с.
5. Заярний О.А. Правові та організаційні основи удосконалення матеріального адміністративно-деліктного законодавства в інформаційній сфері на шляху євроінтеграції Електронний ресурс]. – Режим доступу: http:// applaw.knu.ua/index.php/arkhiv-nomeriv/3-9-2014-jubilee/item/387-pravovi-ta-orhanizatsiyni-osnovy-udosko-nalennya-materialnoho-administratyvno-deliktnoho-zakono davstva-v-informatsiyniy-sferi-na-shlyakhu-yevrointehratsiyi-zaiarnyi-o-a.
6. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2939-17/print.
7. Про основні засади розвитку інформаційного суспільства в Україні на 2007- 2015 роки: Закон України від 09.01.2007 № 537-V [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/537-16.
8. Про телекомунікації: Закон України від 18.11.2003 № 1280-IV [Електронний ресурс]. – Режим доступу: http://zakon2. rada. gov. ua/laws/ show/1280-15.
9. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/80/94-вр.
10. Про основи національної безпеки України: Закон України від 19.06.2003 № 964-IV [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/964-15.
11. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради. – 2015. – № 40–41. – Ст. 379.
12. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про доктрину інформаційної безпеки України», та деякі інші нормативно-правові акти: Указ Президента України від 25 лютого 2017 року № 47/2017 [Електронний ресурс]. – Режим доступу: http://www.president. gov.ua/documents/472017-21374.
13. Про затвердження Положення про Міністерство внутрішніх справ України: постанова Кабінету Міністрів України від

28.10.2015 № 878 [Електронний ресурс]. – Режим доступу: http://zakon5. rada.gov.ua/ laws/ show/ 878-2015-п.
14. Про основні засади забезпечення кібербезпеки України: Закон України 5 жовтня 2017 року № 2163-VIII // Відомості Верховної Ради (ВВР), 2017, № 45, ст.403.
15. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : Дис. ... канд. юрид. наук : 12.00.08. Владивосток, 2005. – 235 с
16. Європол [Електронний ресурс]. – Режим доступу: https://www. europol. europa. eu/.
17. Любовець Г., Король В. Уроки гібридно-месіанських агресій кремля [Електронний ресурс]. – Режим доступу: https://defence-ua.com/ index. php/statti/1293-uroky-hibrydno-mesianskykh-ahresiy-kremlya.

КРИМІНАЛЬНИЙ АНАЛІЗ ЯК ЗАСІБ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

Шинкаренко І.Р.
професор кафедри ОРД та СТ Дніпропетровського державного університету внутрішніх справ,
кандидат юридичних наук, професор

Основним викликом сьогодення до кримінальної поліції є перебудова моделі діяльності кримінальної поліції з реактивної на проактивну. Означене в умовах існування інформаційного суспільства визначає здійснення постійного аналітичного пошуку та аналітичної діяльності на підставі реструктуризації та оптимізації потоків інформації. Підґрунтям означеного може стати кримінальний аналіз.

Революційним у використанні кримінального аналізу у діяльності кримінальної поліції світу став період 90-х років коли відповідно до наукової революції стало формуватися інформаційне суспільство та змінилися підходи до діяльнгості поліції у бік створення системи протидії всім видам злочинності. Це сприяло створенню Міжнародної асоціації кримінальних аналітиків (IACA), яка

формує стратегію та напрями діяльності кримінальних аналітиків у всьому світі [1].

Таким чином кримінальний аналіз сформувався в окремий напрямок професійної діяльності притаманний всім кримінальним поліціям більшості розвинених держав світу. Як наслідок до структури Генерального секретаріату Інтерполу входить підрозділ кримінального аналізу. Європол будує свою діяльність на підставі технологій та результатів кримінального аналізу.

На сьогодні можемо виокремити основні риси та складові кримінального аналізу кримінальної поліції:

- сукупність систематичних аналітичних процесів;
- вивчення певних характеристик та тенденцій;
- визначення та розуміння (осмислення) зв'язків між кримінальною інформацією (інформацією про злочин) та іншою;
- систематичну специфічну інформаційно-аналітичну діяльність;
- полягає у опрацювання інформації, яка є суттєвою для управління або прийняття рішення;
- здійснюється з метою попередження, припинення, розкриття та розслідування злочинів або приймати управлінські рішення

В умовах сьогодення деякі науковці виокремлюють два вида кримінального аналізу – аналітичний пошук та аналітичне дослідження Основним змістом аналітичного пошуку є організація інформації таким чином, щоб полегшити завдання з вилучення сенсу із зібраних даних. Аналітичне дослідження полягає у встановленні взаємозв'язків між особами, подіями та предметами [2, с. 133].

На наш погляд складовими кримінального аналізу є також діяльність з отримання, обробки, реструктуризації інформації та прогнозування розвитку ситуації.

Слід відзначити, що спроби використання у системі МВС – Національної поліції кримінального аналізу у вигляді аналізу

загально-державної оперативної обстановки та напрямками протидії окремим видам злочинності (стратегічний кримінальний аналіз) використовується декілька десятиліть. Підґрунтям означеного є моніторинг оперативної обстановки, який не обмежується постійним контролем (діагностуванням) ситуації. До його складу входять аналіз та прогнозування оперативної обстановки, планування заходів впливу на стабілізацію оперативної обстановки [3, с. 175-186.].

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

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

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

- прогнозування імовірної ситуації, що може скластися в період проведення оперативно-профілактичних заходів, для визначення варіантів-моделі використання оперативно-розшукових сил та засобів та вибору тактики протидії злочинності (організаційно-управлінське прогнозування);
- прогнозування імовірної поведінки об`єктів оперативно-профілактичного впливу з метою визначення тактичних прийомів здійснення оперативно-розшукових заходів щодо протидії злочинності;
- прогнозування імовірної поведінки негласних співробітників у визначених умовах під час виконання завдань оперативних працівників, що необхідно для визначення моделі їх навчання та інформаційно-тактичного забезпечення їхньої діяльності.

- короткострокове – квартал, півріччя, рік;
- середньострокове – п`ять-десять років;
- довгострокове – п`ятнадцять та більше років.

Таким чином, оперативно-розшукове прогнозування повинно розглядатися як невід'ємна частина процесу оперативно-розшукового моніторингу у складі кримінального аналізу та бути його результативною частиною. Логіка сьогодення та враховуючі закон криміналістичної трансформації Є.Ф. Буринського – О.І. Винберга, означені види кримінального аналізуґґ повинні бути засновані на сучасному програмному забезпеченні та відповідному рівні комп'ютерної техніки.

З означеного можемо констатувати, що:

- *кримінальний аналіз є* діяльністю співробітників правоохоронних органів на ґрунті використання інтелектуального програмного забезпечення та системного підходу щодо збору відповідної інформації, аналітичного вивчення певних характеристик, тенденцій з метою встановлення взаємозв'язків між фактами, подіями, явищами, суб'єктами та об'єктами, оптимізації управління правоохоронними органами на державному, територіальному рівні та під час вирішення конкретних задач протидії злочинності (профілактика –попередження – виявлення – припинення – розслідування кримінальних правопорушень – виконання покарань – ресоціалізації засуджених);
- кримінальний аналіз можливо поділити на три рівня: тактичний, оперативний та стратегічний;
- стримує активне використання кримінального аналізу відсутність відповідних експертних програм та організаційних структур.

До проблем впровадження системи кримінального аналізу в діяльність НП України підґрунтя формування моделі поліцейської діяльності керованої аналітикою ILP слід віднести:

- відсутністґь єдиного централізованого аналітичного підрозділу;

- відсутня концепція впровадження концепції кримінального аналізу в діяльність Національної поліції України;
- відсутність сучасної нормативно-правової бази у сфері формування та використання моделі поліцейської діяльності керованої аналітикою ILP (кримінального аналізу) в органах Національної поліції України;
- ґненалежний рівня використання можливостей кримінального аналізу в структурних департаментах Національної поліції України;
- недостатнє забезпечення оперативних підрозділів Національної поліції України сучасною оргтехнікою, комп'ютерним програмним забезпеченням;
- відсутність системи навчання, підготовки та перепідготовки працівників відповідних аналітичних підрозділів відповідно до світової моделі поліцейськґої діяльності керованої аналітикою ILP;
- відсутністьґ ґсучасної методики щодо збору та обробки інформації з «вулиці» відповідно до стандартів ЄС 4*4/ 5*5; за формування відповідних інформаційних банків даних тощо.

Шляхами подолання означених проблем повинні бути:

- розробка та впровадження програмного забезпечення з метою проведення тактичного аналізу у межах конкретних кримінальних проваджень, а також забезпечення формування слідчих версій. Означені програми необхідно внести до стандарту підготовки слідчих органів досудового розслідування.
- створення на базі одного з ВНЗ факультету підготовки фахівців для аналітичних підрозділів та введення окремих дисциплін за тематикою «Використання інформаційних технологій длч виявлення та розслідування злочинів» для факультетів підготовки фахівців для підрозділів кримінальної поліції та органів досудового розслідування.

1. Problem-oriented policing [Electronic resourse] Wikipedia. — URL : http://en.wikipedia.org/ wiki/Problem-oriented_policing.8. Regional Crime Analysis GIS.
2. Узлов Д. Ю. Применение интеллектуальной системы криминального анализа в реальном времени (RICAS) для аналитического сопровождения оперативно-розыскной деятельности и досудебного расследования / Д. Ю. Узлов, В. М. Струков [та ін.] // Право і безпека: Юриспруденція. Юридична психологія (психологічні науки). - Харків, 2015. - № 2. - С. гтт132-139.
3. Шинкаренко І.Р. Моніторинг оперативної обстановки: теоретичні підвалини/ І.Р. Шинкаренко// Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. - Спеціальний випуск № 4. – 2010. - С. 175-186.

НОРМАТИВНО-ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ ЗБУТУ І РОЗПОВСЮДЖЕННЯ ПОРНОГРАФІЇ У МЕРЕЖІ ІНТЕРНЕТ

Шраго А.О.
ад'юнкт кафедри оперативно-розшукової діяльності та спеціальної техніки ФПФПКП Дніпропетровського державного університету внутрішніх справ, старший лейтенант поліції

Широкий розголос численних фактів розпусних дій, скоєних при використанні мережі Інтернет, великий суспільний резонанс і підвищена увага міжнародної спільноти змусили державу визнати існування проблеми web-порнографії. Розповсюдження порнографії, що здійснюється мережею Інтернет, гарантує розповсюджувачу та споживачеві анонімність, відносну доступність способів її оприлюднення та отримання. Широкий попит на злочинну продукцію ускладнює пошук розповсюджувачів та реалізаторів такої продукції, особливо іноземців, які використовують Інтернет для збуту та розповсюдження порнографічних творів.

Об'єктом нашого дослідження є злочинність в мережі Інтернет, предметом – порнографія в Інтернет та нормативно-правові аспекти боротьби з її розповсюдженням. Мета: аналіз окремих

положень законодавства з проблем протидії кіберзлочинності та порнографії. Методологічним підґрунтям нашого дослідження є праці провідних вітчизняних і зарубіжних вчених у галузі кримінального права та процесу, криміналістики, ОРД, зокрема: Ю. Аленіна, І. Воронова, С. Денисова, Р. Джинджолії, О. Козленка, Д. Паляничка, С. Сафронова, А. Старушкевича, І. Сугакова, С. Хільченка, В. Шендрика та багатьох інших.

Криміналістична особливість кіберзлочинів у тому, що їх припинення та розслідування неможливе без використання комп'ютерних технологій. Це пов'язано з необхідністю пошуку, фіксації, вилучення та збирання доказів в електронній формі, а також для проведення ОРЗ та НСРД. Суб'єктами такого оперативного пошуку можуть бути лише особи, уповноважені на здійснення ОРД, які вправі збирати конфіденційну інформацію про особу без її згоди.

Враховуючи, що оперативний пошук має включати низку заходів, які фактично є оперативно-розшуковими (оперативно-пошукові заходи з забезпечення оперативної закупівлі та (або) контрольованого постачання товарів, заборонених для відкритого обігу; оперативне впровадження у віртуальні соціальні групи, що мають деструктивні цілі, з метою отримання інформації про їх персональний склад, місця зустрічей, плани та засоби, що використовуються в деструктивній діяльності; оперативно-аналітичні заходи, спрямовані на прогноз розвитку ситуації, розробки заходів з утримання її під контролем, заходи оперативно-технічного характеру), його потрібно зарахувати до компетенції лише тих правоохоронних органів, підрозділи яких уповноважені проводити ОРД та (або) НСРД.

Верховною Радою України прийнято спеціальні законодавчі акти, що становлять правову основу ОРД. Так, Закон України «Про ОРД» передбачає проведення ОРЗ, спрямованих на виявлення осіб, які готують або вчиняють злочин, а також пошук і фіксацію фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена КК України, кінцевою метою яких виступає припинення правопорушень.

У статті 8 Закону України «Про ОРД» для оперативних підрозділів визначені права, що можуть бути реалізовані і в кіберпросторі. На практиці оперативні працівники використовують кіберпростір при проведенні ОРД, але ці дії вони виконують, спираючись переважно, на свій особистий досвід, а не на розроблені наукові рекомендації. Своєчасне і комплексне застосування сил, засобів та методів ОРД оперативними підрозділами НП України сприятиме убезпеченню від учинення злочинів зазначеної категорії.

Технології вчинення злочину охоплюють певний метод, порядок, послідовність операцій, прийомів, що застосовуються особою для здійснення суспільно небезпечного діяння. Дії, спрямовані на ввезення, виготовлення, збут і розповсюдження порнографічних предметів, створення або утримання місць розпусти і звідництва, сутенерства або втягнення особи в заняття проституцією, торгівлі людьми з метою сексуальної експлуатації або використання у порнобізнесі, розбещення неповнолітніх відрізняються. Проте, технології їх вчинення в частині зв'язку окремих етапів, обставин, факторів підготовки, вчинення та приховування слідів злочинів є загальними, спільними, деколи взаємообумовленими.

Відповідно, є доцільним не розвивати тенденцію дублювання методик, а узагальнювати наявні, аналізувати практичну діяльність щодо виявлення ознак злочинів та їх розслідування, знаходити загальні типові ситуації та алгоритми дій оперуповноваженого та слідчого, форми їх взаємодії з іншими службами НП України, відпрацьовувати тактику проведення слідчих (розшукових) дій, у т.ч. й негласних, та формувати базові узагальнені методики для використання під час розслідування різних видів злочинів за різними розділами КК, у т.ч. вчинених у специфічних умовах, певними особами тощо [1, с. 197].

Проте, у практичній діяльності науково-методичні розробки не завжди схвально сприймаються. Так, у межах проведеного нами опитування працівників Кіберполіції НП України, 23 % респондентів вказали на те, що вони взагалі не звертаються до

наукових рекомендацій у протидії порнографії, 43 % не використовують їх, бо вважають їх застарілими, 15 % – не ознайомлені з такими рекомендаціями, 19 % – звикли покладатися на власний досвід, з них 7 % вказали, що такі рекомендації обмежують творчий підхід до розслідування.

Однією із причин низької ефективності припинення і розслідування незаконного збуту та розповсюдження у мережі Інтернет є те, що працівники слідчих та оперативних підрозділів досі не готові до ефективного виявлення та розслідування подібних злочинів, недостатньо використовують спеціальні знання, не точно визначають предмет злочину та обставини, що підлягають доказуванню.

Серед причин високої латентності злочинів, передбачених ст. 301 КК України, можна виділяємо такі: 1) недостатня розробка понятійного апарату, що використовується в текстах відповідних статей, зокрема, відсутність чіткого визначення предмета злочинів; 2) особливий стан громадської думки, який в сучасних умовах характеризується неприйняттям названих діянь як злочинів; 3) прихований характер злочинної діяльності, відсутність очевидних її наслідків; 4) недостатня професійна підготовка працівників правоохоронних органів по виявленню і розслідуванню цих злочинів; 5) відсутність зорієнтованості правоохоронних органів на виявлення цих злочинів, які на фоні складної криміногенної ситуації (вбивства, бандитизм, розбій, згвалтування тощо) розглядаються як другорядні і їм не приділяється належної уваги.

Закон України «Про ОРД» надає можливість використовувати права лише для виконання завдань ОРД. На законодавчому рівні не передбачено у переліку завдань профілактики злочинів, попередження та запобігання злочинам, зазначено лише припинення, про що свідчить ст. 1 Закону. Тобто, у Законі України «Про ОРД» наводяться два поняття, які містять суперечності, створюючи колізію правових норм: з одного боку – обов'язок оперативного підрозділу здійснювати профілактику правопорушень (п. 1 ч. 1 ст. 7 Закону), з іншого – перспектива користуватися своїми

правами лише для виконання завдань оперативно-розшукової діяльності (ч. 1 ст. 8 Закону), у змісті яких не має профілактики, попередження, запобігання. Враховуючи наведене вважаємо, що нормативно-правова регламентація профілактичної та попереджувальної діяльності оперативних підрозділів НП України має декларативний характер.

Стрімко розвивається використання Інтернету, як для вербування жертви, так і для реклами послуг. Зустрічі між жертвами та клієнтами організовуються за допомогою спеціальних веб-сайтів. Жертви швидко змінюються, залишаючись в одному місті не більше ніж на 1-2 дні. Ілюзія анонімності і масова кількість онлайн-послуг збільшує і обережність, і рентабельність цих послуг, що робить надскладною ідентифікацію злочинців із використанням лише традиційних методів поліції [2, с. 179].

Правоохоронним органам часто доводиться здійснювати первинний пошук інформації про певні об'єкти в мережі. Найбільш проблемним питанням залишається встановлення особи та визначення її місцезнаходження за тими обліковими даними, що особа лишила в мережі. Як правило, такими ідентифікаторами є адреса електронної пошти, нікнейм у форумі, профіль соціальної мережі тощо. Вказана проблема часто обумовлена підвищеним рівнем анонімності, що реалізується за допомогою різного роду розподілених ресурсів (проксі-сервери, шели) та використанням спеціалізованих захищених мереж (TOR, I2P) [3, с. 256].

Важливими правовими основами діяльності оперативних та слідчих підрозділів НП України є також норми кримінального процесуального кодексу, які, на нашу думку, сьогодні ускладнюють ефективність роботи оперативних підрозділів НП України. Так, положення ст. 41 КПК України забороняють співробітникам оперативних підрозділів (крім підрозділу детективів, підрозділу внутрішнього контролю НАБУ) здійснювати процесуальні дії у кримінальному провадженні за власною ініціативою або звертатися з клопотаннями до слідчого судді чи прокурора.

Пошукові заходи можуть здійснюватися і гласно, і негласно. Виходячи з того, що ефективність правоохоронного моніторингу соціальних мереж буде вищою за умови непоінформованості про нього суб'єктів деструктивних діянь, особливого значення набувають саме негласні заходи. Такі заходи в тому числі можуть здійснюватися оперативними підрозділами НП України.

З одного боку КПК містить прямі вказівки на необхідність проведення відповідних гласних та негласних слідчих (розшукових) дій, а з іншого – забороняє співробітникам оперативних підрозділів здійснювати процесуальні дії за власною ініціативою та звертатись з клопотанням до слідчого судді або прокурора, що, в свою чергу, знижує ефективність боротьби зі злочинами у сфері суспільної моралі, яким властива висока латентність. А тому, виникає сумнів щодо ефективності процесуалізації деяких ОРЗ у НСРД. Фактично, майже весь процес досудового розслідування сьогодні побудовано не лише на законодавчій базі, а більшою мірою на особистих стосунках, що ставить під сумнів ефективність роботи загалом.

Із введенням в дію КПК України значно ускладнилася процедура отримання інформації від провайдерів телекомунікаційних послуг. Якщо раніше отримання такої інформації здійснювалося на підставі положень про «Конвенцію про кіберзлочинність» і Закону України «Про міліцію», то зараз така інформація віднесена до категорії документів, що містять охоронювану законом таємницю. А в розумінні статті 505 Цивільного кодексу України така інформація становить комерційну таємницю, яка є одним із об'єктів інтелектуальної власності. Тому, суб'єкти протидії позбавлені можливості оперативно і своєчасно отримувати необхідну інформацію через запити правоохоронних органів. Сьогодні рівень і темпи зростання кіберзлочинності вимагають адекватного реагування, у тому числі і на законодавчому рівні. А тому, потребують змін положення законодавства про порядок і підстави виконання запитів, отриманих від правоохоронних органів у рамках виконання зобов'язань України, узятих у зв'язку з ратифікацією «Конвенції про кіберзлочинність». Як наслідок,

одним із пріоритетних напрямків є організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Сьогодні жодна держава не може ефективно протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері.

В умовах сьогодення постає необхідність в налагодженні на відповідній правовій основі ефективної взаємодії з міжбанківськими інституціями, телекомунікаційними компаніями, зацікавленими центральними державними органами та правоохоронними органами інших країн з метою документування злочинних груп з міжнародними зв'язками.

Інформаційно-аналітичне забезпечення є важливим і необхідним елементом організації оперативного пошуку ознак злочинів, пов'язаних з незаконним контентом, оскільки воно сприяє прийняттю найбільш доцільних управлінських рішень на всіх рівнях, що є однією з головних умов підвищення ефективності діяльності оперативних підрозділів НП України.

Отже, сьогодні для суб'єктів ОРД необхідною є розробка організаційно-тактичних основ проведення оперативно-розшукової діяльності у кіберпросторі та введення в дію відповідних правових механізмів їх здійснення. Окрім того, у контексті проведеного дослідження, необхідним є: 1) створення сучасної бібліотеки навчально-методичної та наукової літератури за даною спеціалізацією; 2) удосконалення механізмів обробки електронних доказів за цією категорією кримінальних проваджень; 3) зобов'язання компаній зберігати резервні копії електронних даних для підвищення ефективності розслідування таких злочинів; 4) полегшення доступу правоохоронних органів до електронних банків даних; 5) удосконалення системи оперативного супроводження підприємств, установ та організацій, основна діяльність яких пов'язана з використанням комп'ютерних технологій або наданням інформаційних послуг; 6) забезпечення заходів безпеки на об'єктах, що призначені для передачі інформації; 7) підвищення рівня обізнаності щодо торгівлі дітьми

(дитячою порнографією тощо) серед батьків та осіб, які їх замінюють, осіб, які постійно контактують з дітьми у сферах освіти, охорони здоров'я, культури, фізичної культури та спорту, судовій та правоохоронній сферах; 8) підвищення ефективності правоохоронних заходів щодо профілактики злочинів та переслідування осіб, які вчиняють цей злочин або сприяють його вчиненню; 9) створення та координування «гарячих ліній», призначених для повідомлення про факти сексуального насильства та експлуатації дітей в Інтернеті.

Провівши дане дослідження, ми дійшли висновку, що вирішення, зокрема й окреслених проблемних питань, сприятиме підвищенню ефективності діяльності оперативних та слідчих підрозділів НП України, спрямованої на протидію злочинам у сфері суспільної моралі, а відтак, окреслені питання вимагають подальшого поглибленого науково-практичного дослідження.

1. Ищенко Е. П. Криминалистика: Краткий курс / Е. П. Ищенко. – М. : Инфра-М, 2004. – 302 с.
2. Справочное руководство ОБСЕ по обучению полиции: Торговля людьми / серия публикаций ДТУ/ОВСВПД. Том 12. 2013. – 210 с.
3. Бандурка О.М. Оперативно-розшукова компаративістика: монографія / О.М. Бандурка, М.М. Перепелиця, О.В. Манжай та ін. – Х.: Золота миля, 2013. – 352 с.

ПРАКТИКА КРИМІНАЛЬНОГО АНАЛІЗУ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Рудий Т.В.,
професор кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент

Кулешник Я.Ф.,
доцент кафедри інформатики
Львівського державного університету внутрішніх справ,
кандидат технічних наук, доцент

Яровaн С.В.,
начальник відділу професійної підготовки ГУ НП
у Волинській області.

Сучасні виклики і загрози, перш за все гібридні, які обумовлені впливом комплексу політичних, соціально-демографічних, економічних, правових, соціоінженерних, технологічних чинників вимагають системного реагування, адекватної трансформації як усього сектору безпеки, так і інформаційної та кібербезпеки зокрема, а також включення цієї системи у сферу політичних пріоритетів держави [1].

Під впливом сучасних глобалізаційних процесів, розвитку інформаційних технологій (ІТ), телекомунікаційних сервісів, цифрової економіки інформаційна та кібербезпека набувають самостійного, трансдержавного характеру.

Розвиток та безпека інформаційного і кіберпростору, запровадження цифровізації процесів урядування, гарантування безпеки й сталого функціонування інформаційно-комунікаційних систем, державних інформаційних ресурсів мають бути складовими державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні.

Інформаційні відносини уже давно стали об’єктом правового регулювання, але розвиток ІТ та апаратних засобів, систем

телекомунікацій відбувається швидше, ніж приймаються нормативно-правові акти, якими вони регулюються, що є причиною відповідної правової колізії [2, 3].

Однак, останнім часом відбувся певний вимушений (зовнішній політичний вплив) поступ у сфері забезпечення інформаційної та кібербезпеки, зокрема, на інституційно-організаційному рівнях:

- у червні 2016 р. Президент України підписав Указ про створення Національного координаційного центру кібербезпеки (першим етапом його роботи є здійснення аналізу та розроблення галузевих індикаторів стану кібербезпеки):
- Указ Президента України №47/2017 про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»;
- 5 жовтня 2017 р. Верховна Рада України приймає Закон України «Про основні засади забезпечення кібербезпеки України»;
- 17 січня 2018 року Кабінет Міністрів України затвердив урядову концепцію розвитку цифрової економіки в державі на 2018-2020 роки.

Такий стан справ зумовлює глибинні зміни у ставленні нашої держави до безпеки власного інформаційного та кіберпростору, а отже, і до посиленого захисту інформації, засобів її оброблення та кіберсередовища, в якому ця інформація циркулює, визначення об'єктів впливу (рис. 1), тобто до вжиття заходів із забезпечення інформаційної та кібербезпеки [4].

Невизначеними у нормативно-правовому забезпеченні залишаються питання стосовно методології підходів до проблематики забезпечення інформаційної безпеки. На перше місце слід поставити співвідношення понять «інформаційна безпека» та «кібербезпека». Українська наука чітко обґрунтувала необхідність розгляду національного сегменту кіберпростору як складової частини інформаційного простору держави [5]. З цього

випливає і логічність розгляду питань кібербезпеки у контексті інформаційної безпеки (рис. 2) [4].

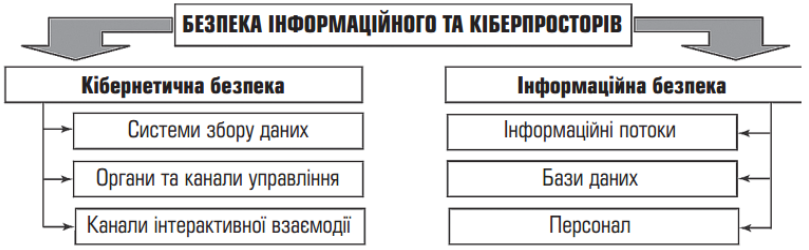


Рис. 1. Об'єкти впливу в інформаційному та кіберпросторі.

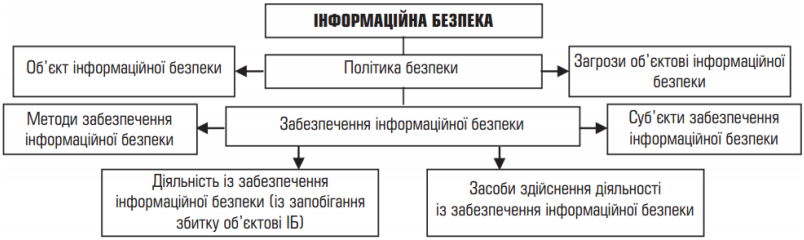


Рис. 2. Структура поняття інформаційна безпека

Сталі режими функціонування підрозділів Національної поліції України (НПУ) з протидії кіберзлочинності не тільки зумовили збільшення обсягів інформації, які доводиться збирати, накопичувати, обробляти за визначеними алгоритмами, аналізувати і зберігати, а й необхідність забезпечення віддаленого доступу до масивів структурованої інформації та стратегічних інформаційних ресурсів. Застосування технологій інформаційно-аналітичної діяльності (ІАД) та відповідних інформаційно-аналітичних систем (ІАС) дозволить структурувати наявні інформаційні ресурси і використовувати їх як моделі консолідованої інформації.

За даними [6] аналітичну роботу ототожнюють з поняттям аналізу, визначаючи його як дослідницьку функцію в управлінні підрозділами, без якої науково організувати їхню діяльність

неможливо. Проте дане твердження є не зовсім правильним. Аналітична робота є діяльністю з дослідження інформації, у той час як аналізом є метод теорії пізнання, коли шляхом розумової діяльності ціле ділиться на частини. Таким чином, аналіз є одним з методів аналітичної роботи, тобто способом дослідження інформації, зокрема, у сфері організаційно-аналітичної роботи у підрозділах НПУ.

Аналітик, спираючись на інформаційні моделі (відбитки в інформаційному просторі подій, фактів, дій, ідей, думок, почуттів людей, природних, політичних, соціальних, соціоінженерних, фінансових, економічних процесів тощо), виявляє об'єктивні закономірності і тенденції, визначає рушійні механізми та, що найголовніше, причинно-наслідкові зв'язки. У цьому змісті аналітик створює нове знання про той фрагмент реальності, який знаходиться в полі його професійного інтересу, виступаючи дослідником своєї предметної області.

Тому, від того, якою мірою аналітичні підрозділи НПУ спроможні якісно аналізувати наявну інформацію і, як результат, надавати аналітичні продукти, які є підтримкою для прийняття адекватних кіберзагрозам управлінських рішень, залежить успіх виконання поставлених завдань.

З огляду на викладене виникла нагальна необхідність у реорганізації та вдосконаленні методів протидії кіберзлочинності. Одним із засадничих підходів стосовно застосування сучасних технологій у сфері протидії кіберзлочинності на якісно новому рівні та прийняття при цьому оптимальних рішень є кримінальний аналіз.

Даючи кримінологічну характеристику кіберзлочинів треба визнати, що більшість виявлених кіберзлочинів розпорошені у звітності різних підрозділів НПУ і це не дає можливості провести комплексний аналіз та характеристику кіберзлочинності. Нещодавно створено Управління кримінального аналізу Національної поліції для консолідації усіх розрізнених джерел оперативної інформації з подальшим глибоким аналізом, що повинно стати вагомим чинником у протидії кіберзлочинності.

Отже, за визначенням керівника Управління кримінального аналізу НПУ кримінальний аналіз – це мисленнєво-аналітична діяльність працівників правоохоронних органів, що полягає у перевірці та оцінці інформації, її інтерпретації, встановленні зв'язків між даними, що отримуються у процесі розслідування та мають значення для кримінального провадження, з метою їх використання правоохоронними органами та судом, подальшого проведення оперативного і стратегічного аналізу (на думку авторів ця дефініція кримінального аналізу притаманна особисто п. В. Єрофеєву).

На основі [7] подамо своє розуміння терміну кримінальний аналіз. Кримінальний аналіз є специфічним видом ІАД, яка полягає в ідентифікуванні та точному визначенні внутрішніх зв'язків між інформаціями (відомостями, даними), що стосуються злочину, і довільними іншими даними, отриманими з різних джерел, їх використанням в інтересах ведення оперативно-розшукової та слідчої діяльності, прийняття адекватних управлінських рішень на основі їх аналітичної підтримки.

Розрізняють такі види кримінального аналізу: стратегічний; тактичний; оперативний [8].

Оперативний аналіз – робота за кримінальними провадженнями відносно конкретних осіб, організованих злочинних груп (ОЗГ) з метою перевірки гіпотез щодо їх імовірної злочинної діяльності, встановлення зв'язків, структури ОЗГ, ролі окремих учасників з урахуванням їх соціального та економічного статусу, використанням аналізу телефонних трафіків, транзакцій, потоків та маршрутів географічного переміщення об'єктів тощо.

Тактичний аналіз – аналіз криміногенної ситуації на конкретній території за невеликий проміжок часу, за певним видом злочину або протиправної діяльності певної групи тощо. Встановлення тенденцій злочинності, встановлення місць концентрації вчинення злочинів, встановлення профілю підозрюваного та потерпілого. Прийняття оптимальних управлінських рішень щодо розподілу сил і засобів, проведення оперативного аналізу.

Стратегічний аналіз – аналіз інформації, спрямований на виявлення тенденцій, закономірностей, прогнозування розвитку злочинності за тривалий період часу

Технології кримінального аналізу передбачають впровадження моделі поліцейської діяльності керованої аналітикою ″Intelligence Led Policing″ (ILP) [8], як моделі діяльності, яка спрямована на підтримку, супровід інституційного управління та рішень посадових осіб на основі процесу аналізу інформації і даних.

Основні складові частини розвитку моделі ILP є такими:

- нормативно-правова база для врегулювання;
- інформаційні ресурси;
- система наповнення інформаційних ресурсів;
- система оцінювання джерел та достовірності інформації;
- спеціальне програмне забезпечення;
- інтегрування спеціалізованого програмного забезпечення з інформаційними ресурсами МВС та інших джерел інформації;
- тренінги для аналітиків практичних підрозділів НПУ;
- стандартизовані форми аналітичних продуктів;

Поліцейська діяльність керована аналітикою спрямована на ідентифікування і точне визначення взаємозв’язків між відомостями, які стосуються кіберзлочинів, осіб, пов'язаних з ними, та даними, що походять з різних джерел і їх використання кримінальними підрозділами НПУ

У відповідності до моделі ILP функції підрозділів кримінального аналізу полягають у наступному:

1. Координування діяльності.
2. Адміністрування доступу до інформаційних ресурсів ІАС.
3. Формування аналітичних продуктів.
4. Надання інформації за запитами.
5. Супроводження банків (баз) даних.
6. Адміністрування за територіальним розміщенням підрозділів з вертикальною підпорядкованістю.

7. Взаємодія з підрозділами кримінального аналізу ІПКП «102» регіональних органів НП [8].

Кримінальний аналіз передбачає, що результат ІАД повинен гарантувати достатній і сталий рівень забезпеченості аналітичними продуктами ініціаторів, що стосується кожного аспекту діяльності підрозділів кримінальної поліції у режимі реального часу. Також враховуються рамки всіх значущих напрямків і весь реалізований комплекс заходів, здійснюваних у сфері протидії кіберзлочинності.

Базовими елементами та засобами реалізації ІАД виступають ІАС – системи зв'язку та трансмісії даних, інформаційно-телекомунікаційна інфраструктура, бази даних правової інформації, технічні, програмні, лінгвістичні, правові, організаційні засоби. Згадані аспекти відтворені у статтях 25, 26, 27 Закону України «Про Національну поліцію» [9]. У сою чергу технологічна платформа ІАС дозволяє здійснювати інтегрування та координування дій між різними підрозділами НПУ.

У практиці кримінального аналізу розрізняють наступні типи аналітичних продуктів:

1. Аналітичний звіт:
   - сепарована інформація з внутрішніх і зовнішніх джерел;
   - висновки;
   - рекомендації, прогнози, настанови;
   - додаткові матеріали (графіки, схеми, дані геолокації).
2. Профіль (досьє) особи, об’єкта ОЗГ:
   - максимальний обсяг інформації на об’єкт аналізу у відповідності до запиту ініціатора.
3. Інформаційне зведення:
   - оброблені табличні дані шляхом вибірки з баз даних за критеріями ініціатора.
4. Витяг інформації:
   - вибірка інформації з баз даних за критеріями ініціатора.

На останок, як висновок, на думку авторів успішне реалізування та впровадження технологій кримінального аналізу дасть можливість активно використовувати ІАД, що сприятиме підвищенню ефективності протидії кіберзлочинності.

4. Стратегія розвитку системи Міністерства внутрішніх справ України до 2020 року. Електронний ресурс. Шлях доступу: https://www.cyberpolice.gov.ua/strategy-2020/.
5. Рудий Т.В. Принципи організації системи захисту інформаційних систем підрозділів МВС / Т.В. Рудий, О.В. Захарова, О.І. Зачек, А.Т. Рудий / Науковий вісник ЛьвДУВС. Серія юридична / головний редактор М.М. Цимбалюк – Львів: ЛьвДУВС. 2012. – Вип. 2 (2). – С. 309-316.
6. Рудий Т. В. Організаційно-правовий супровід захисту інформаційних систем підрозділів національної поліції України на основі міжнародних стандартів / Т.В. Рудий, О. В. Захарова, В. В. Сеник, С. В. Сеник, М. І. Ізьо // Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична / головний редактор Р. І. Благута. – Львів: ЛьвДУВС, 2017. – Вип. 2. – С. 213-225.
7. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.– К.: ДУТ, 2015. – 288 с.
8. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби з кіберзлочинністю: основні напрями реформування. Аналітична записка. Національний інститут стратегічних досліджень. Електронний ресурс. Шлях доступу: http://www.niss.gov.ua/articles/454/.
9. Єсімов С.С. Юридична природа інформаційно-аналітичної діяльності Національної поліції / Електронний ресурс. Шлях доступу: http://aphd.ua/publication-151/.
10. Заєць О.М. Інститут аналітичного супроводження досудового розслідування кримінального провадження в Україні: сучасний стан і перспективи розвитку / О.М. Заєць // Вісник кримінального судочинства, ТОВ "Правова Єдність". – К: 2016. № 4. – С. 17-25.

11. Кримінальний аналіз у діяльності НПУ / Концепції впровадження в Національній поліції України моделі поліцейської діяльності, керованої аналітикою «Intelligence Led Policing» // Електронний ресурс. Шлях доступу: www.slideshare.net/NationalPolice/ss-75925350.
12. Закон України «Про Національну поліцію» / Відомості Верховної Ради України, 2015, №40-41. – С. 379 // Електронний ресурс. Шлях доступу: http://zakon3.rada.gov.ua/laws/show/580-19.

АНАЛІЗ ЯК ДЖЕРЕЛО НОВОГО ЗНАЧЕННЯ

Ященко В.
професор кафедри теорії та історії держави і права, конституційного та міжнародного права Львівського державного університету внутрішніх справ, доктор юридичних наук, професор

У кримінально-правовій, оперативно-розшуковій та й інших сферах правоохоронної діяльності традиційно склалась така ситуація, що аналіз розглядається дещо спрощено, як допоміжний прийом осягнення тих чи інших сторін правового явища, події, факту.

Зокрема, у Законі України «про ОРД» передбачені заходи пошуку, здобування, виявлення даних про протиправну діяльність, а аналіз як аналогічний цим засобам спосіб отримання нової інформації навіть не згадується.

Це негативно відбивається і на діяльності аналітичних підрозділів які наче відносять не до основних, а до допоміжних.

Між тим, дійсність переконує і особливо оперативно-розшукова сфера, що аналіз є не менш важливим способом отримання інформації, скажімо, оперативний пошук, оскільки в силу своєї евристичності проявляє здатність до здобування нового знання.

Ця евристичність випливає, по-перше з сутності самого цього методу: на буттєвому рівні, як відомо, аналіз розглядається як розкладання цілого на окремі частини.

Уже в такому розумінні прихована неточність, пов'язана з тим, що частина може не відображати природи цілого, правильніше буде говорити не про частину і ціле, а про загальне і одиничне. При цьому аналіз – це не розклад предмету на частини, а виокремлення одиничного, як окремого що входить в загальне. І вивчення цього одиничного якраз і є те нове, що було раніше невідоме. Наприклад, є загальна теорія права і є теорія окремих галузей права, де останні не є частинами загальної теорії, а її цпецифічними проявами зі своїми власними закономірностями.

По-друге еврестичність аналізу полягає в тому, що він є одним з чи не найрозповсюдженіших методів, прийомів, способів, пізнання та діяльності. Особлива ця істина важлива у правозастосуванні, у тлумаченні норм права, у правотворчій діяльності, за кожен крок пов'язаний з аналізом. Тобто аналіз виступає одним із логічних методів науки і разом з тим, способом практичного осягання дійсності, що свідчить про певну його універсальність. Водночас використання цього методу у різних сферах має свою специфіку. Скажімо політичний аналіз і правовий аналіз здійснюється за різними закономірностями, в різних понятійно-категоріальних вимірах. Ось чому є нагальною потреба здобуття умінь та навичок, аналізу конкретної сфери діяльності, що потребує відповідної навчальної підготовки фахівців.

І, нарешті, третє, чи не найважливіше свідчення еврестичності аналізу – його органічний взаємозв'язок з синтезом, тобто об'єднання отриманого в ході аналізу знання.

Отже, синтез без аналізу практично не можливий, бо поєднувати в нове знання властивості предметів та відношення між ними можна лише, ті які вивчені в ході аналізу.

Однак, ця своєрідна не самостійність синтезу не говорить про його другорядність як методу. Навпаки, особливість синтезу, що він дає лише нове синтетичне значення. Це значення за змістом є висновковим, отриманим шляхом узагальнення аналітичних як посилкових даних. Складність узагальнення. Випливає з самої його процедури: побачити в одиничному загальне (за деревами

бачити ліс), і сформулювати це загальне у відповідному понятійно-категоріальному визначенні, що і буде новим знанням.

Нажаль сьогодні службові аналітичні документи, обмежуються, аналітичною стороною пізнання, яка нічого плідного, конструктивного в собі не містить. Прогнозування, передбачення, можливі, лише на основі синтезу.

Тому говорячи про аналіз ми повинні органічно пов’язувати його з синтезом і використовувати його як єдиний аналітико-синтетичний метод який фактично і дає можливість досягнення нового знання.

Зміст

НАУКОВЕ ВИДАННЯ

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

Збірник наукових статей за матеріалами доповідей
учасників Всеукраїнського науково-практичного семінару
23 березня 2018 р.

Упорядники А.В. Баб'як, В.В. Сеник, Т.В. Магеровська
Комп'ютерна верстка Т.В. Магеровська

Опубліковано в авторській редакції

Підписано до друку 06.06.2018 р.
Формат 60х84/16. Папір офсетний.
Гарнітура Times. Умов.друк.арк. 18,2
Тираж 100 прим.

Львівський державний університет внутрішніх справ
79007, м. Львів, вул. Городоцька, 26

Свідотство про внесення суб'єкта видавничої справи до державного
реєстру видавців, виготівників і розповсюджувачів видавничої продукції
ДК № 2541 від 26 червня 2006 р.