МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ МВС УКРАЇНИ

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

«ІМПЛЕМЕНТАЦІЯ ILP МОДЕЛІ В УКРАЇНІ»

Матеріали
КРУГЛОГО СТОЛУ

15 березня 2023 року

м. Одеса
ОДУВС
2023

УДК 351.74:341.171(477)

Статті друкуються в авторському варіанті.
Оргкомітет дозволив собі лише скорочення
статей, які суттєво перевищували пропоновані обсяги.

І154 **Імплементація ILP моделі в Україні:** матеріали круглого столу, м. Одеса, 15 березня 2023 р. – Одеса : ОДУВС, 2023. – 133 с.

УДК 351.74:341.171(477)

покращить рівень відповідної внутрішньої та зовнішньої взаємодії. Найбільш актуальним є питання удосконалення механізму міжнародної взаємодії, адже більшість злочинів мають транснаціональний характер, наприклад, кіберзлочинність, торгівля людьми;

- створення та розробка дієвої системи інформаційної безпеки ОВС, яка б визначила загальні положення, основні поняття, цілі, принципи й напрями запровадження та підтримку надійної системи інформаційної безпеки правоохоронних органів України, вжиття комплексних заходів для захисту власного інформаційного простору [3, 55].

Вважаємо, що для вирішення проблеми вдосконалення інформаційного забезпечення, необхідно передбачити певні зміни, уточнення та доповнення у основні завдання системи інформаційного забезпечення правоохоронних органів України що є запорукою підвищення ефективності діяльності ОВС щодо забезпечення правопорядку та прав і свобод громадянина.

Таким чином, вдосконалення інформаційного забезпечення діяльності правоохоронних органів України є багатогранною та потребує комплексного підходу до її вирішення: від нормативно-правових аспектів до матеріально-технічного та кадрового забезпечення.

Список використаних джерел:

1. Швець М.Я Системна інформатизація законотворчої та правоохоронної діяльності К.: Навч. Книга. 2005. 639 с.
2. Системна інформатизація правоохоронної діяльності: Монографія / М. Швець, В. Буржинський, Б. Раціборинський та ін.; НДЦПІ АПрН України. К.: Вид-во ТОВ "ПанТот".2006. 287 с.
3. Бойченко О.В. Герасименко К.С. Концепція інформаційної безпеки в системі інформаційного забезпечення ОВС України. Вісник Запорізького юридичного інституту. 2010.№ 2 С. 54-62.

Форос Г.В.
к.ю.н., доцент
(Одеський державний університет внутрішніх справ)

ЗАГАЛЬНІ ПІДХОДИ ЩОДО ОТРИМАННЯ ІНФОРМАЦІЇ ПІД ЧАС КРИМІНАЛЬНОГО АНАЛІЗУ

Одним із пріоритетних завдань для органів та підрозділів Національної поліції є перебудова моделі її діяльності з урахуванням сучасних провідних тактик і стратегій, розроблених та успішно запроваджених у правоохоронну діяльність США, Канади, Великої

Британії, країн Європейського Союзу, котрі, керуючись викликами інформаційного суспільства, суттєво вдосконалили процеси аналітичного пошуку й аналітичної діяльності.

Батьком сучасної системи організації діяльності поліції та використання кримінального аналізу вважається А. Фольмер начальник поліції м. Берклі (США), який ще у 1906 році запровадив картографічний метод для визначення місць концентрації злочинних угруповань. Підґрунтям цього було вивчення результатів діяльності поліції за минулий рік. Сучасною мовою науки та практики протидії злочинності, це був аналіз оперативної обстановки. Наслідком стало запровадження систем нейтралізації злочинності в її осередках за рахунок оптимізації використання сил поліції [1].

На сьогодні кримінальні аналітики мають у своєму розпорядженні певні інформаційні ресурси, відомості з яких потрібно використовувати під час підготовки аналітичних продуктів. Так, створена інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» (система ІПНП) призначена для інформаційно-аналітичного забезпечення діяльності Національної поліції України, наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних, що входять до єдиної інформаційної системи МВС (ЄІС МВС), забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу та електронної взаємодії з МВС, іншими органами державної влади [2].

Крім цього, підрозділи інформаційно-аналітичної підтримки Національної поліції України здійснюють формування, супроводження та використання у службовій діяльності інформаційних ресурсів (обліки), держателем (власником) яких є Міністерство внутрішніх справ України, зокрема: персонально-довідковий облік - систематизований банк (база) даних ІП «Оперативно-довідкова картотека»; автоматизована дактилоскопічна ідентифікаційна система «Дакто-2000»; ІП «Пізнання»; ІП «Затримані і доставлені».

Слід враховувати, що обмеження в джерелах, що використовуються для збору інформації, не застосовуються, тому можна йти за принципом «здорового максималізму», використовуючи будь-які реєстри та бази даних Національної поліції України, МВС, інших міністерств та відомств. Не є винятком Всесвітня мережа «Інтернет», яка нині видається потужним інформаційний масивом.

Саме в соціальних мережах (Facebook, Linkedin, Instagram тощо) простежується найбільша кількість фотографій та зв’язків між особами. У відкритому доступі знаходяться такі ресурси, як декларації про доходи, учасники тендерних процедур тощо.

Використовуючи такі програми, як Viber, WhatsApp та інші, можна отримати фотографії осіб, знаючи номер їх телефону.

Також потрібно пам’ятати, що сьогодні дуже велика кількість торговельних мереж утворюють свої бази даних, наприклад: мережі автомобільних заправних станцій; мережі медичних лабораторій та приватних медичних установ; супермаркети; інші фінансові установи й торгові представництва; бази кур’єрських служб, служб доставки; бази АЗС, заклади охорони здоров’я.

Зупинимось більш детально на аналізі соціальних мереж. Так, під час проведення аналізу взаємозв'язків досліджують структуру соціальної мережі, під якою розуміють схему об'єктів, котрі поєднані між собою зв’язками.

Аналіз соціальних мереж (з англ. Social Networks Analysis, SNA) - методологія аналізу соціальних мереж. Предметом розвідки в SNA, на відміну від більшості традиційних соціологічних досліджень, не є атрибути окремих осіб, а структура їхніх взаємозв’язків у межах того або іншого співтовариства (робочої групи). В рамках аналізу соціальних мереж розглядаються соціальні відносини з точки зору теорії мереж, що складаються з осередків осіб, учасників мережі і зв’язків - відносин між ними.

Застосування аналізу соціальних мереж як інструменту може бути надзвичайно ефективним, якщо його використовувати як вказівник для аналітичних суджень; однак слід бути обачними, оскільки дані можуть бути неповними.

Такий аналіз проводиться у спеціалізованому програмному забезпеченні Analysts Notebook. Аналітичні функції цієї програми дають змогу досліджувати групові структури та потоки інформації на схемі, фокусуючись на взаємозв’язках, які існують між об’єктами (саме цей тип аналізу називається аналізом соціальних мереж).

Організаційні теорії поєднуються з математичними моделями, щоб допомогти аналітику зрозуміти динаміку груп і організацій, функціонування яких підлягає аналізу.

Аналіз соціальної мережі є методом, який спрямований на розуміння структури соціальної мережі шляхом «вимірювання» відносин між суб’єктами мережі.

Методи аналізу соціальних мереж дають деякі корисні інструменти для вирішення одного з найважливіших (але важких) аспектів соціальної структури: джерел та розподілу влади. Мережева перспектива свідчить про те, що влада окремих суб'єктів не є індивідуальним атрибутом, а виникає внаслідок їх відносин з іншими.

Незаконні мережі відрізняються від юридичних мереж тим, що вони повинні приховувати свою діяльність. Таємна спільнота спрямовує зусилля

на те, щоби функціонувати приховано, а в разі виявлення вживає заходів, які ускладнюють ідентифікацію задіяних осіб.

Необхідність таємності змушує організаторів та активних учасників приховувати свою діяльність, створюючи розріджені мережі.

Окремо необхідно вказати на аналіз інформації з відкритих джерел або як ми всі звикли Open source intelligence (OSINT) і яка включає в себе пошук, вибір і збір інформації, отриманої зі загальнодоступних джерел, та її аналіз. Термін «відкритий» вказує на загальнодоступність джерела (на відміну від секретних джерел і джерел з обмеженим використанням).

Відкриті джерела інформації можна розподілити на 4 категорії: широко розповсюджені дані та інформація; цільові комерційні дані; експертні оцінки; «сіра» література.

Важливим напрямом удосконалення роботи розвідувальних органів є створення ефективної системи отримання інформації з відкритих джерел (подібні системи запроваджені у розвідках провідних країн світу). Водночас в умовах відкритого інформаційного простору та вільного доступу до інформації організація такої роботи є надзвичайно складною і потребує значних фінансових видатків, застосування новітніх технологій та підходів. Разом з тим, як свідчить досвід розвідок провідних країн світу, ефективне функціонування такої системи є для вищих посадових осіб держави видимою якісною характеристикою щоденної роботи розвідувальних служб і певною мірою показовим чинником їх затребуваності. З іншого боку, системна робота з відкритими джерелами інформації суттєво доповнює інформаційні можливості самих розвідувальних органів.

Специфічна категорія технічних і людських ресурсів, джерела інформації і методи їх збору - все це відрізняє OSINT від інших видів розвідки. До переваг OSINT відносять доступність джерел інформації, їх обсяг, різносторонність, оперативність і вартість отримання, легкість подальшого використання. Відомості з відкритих джерел, зокрема засобів масової інформації (газет, журналів, радіо та телебачення, всесвітньої мережі Інтернет), використовуються оперативними підрозділами правоохоронних органів як доповнення до розвідувальної інформації, що надходить іншими каналами.

Список використаних джерел:

1. Козлов Д. В. Використання в оперативно-розшуковій діяльності можливостей кримінального аналізу на морській ділянці відповідальності. Бюлетень Департаменту оперативної діяльності Адміністрації Державної прикордонної служби України. 2011. № 5. С. 48-53.

2. Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України», затверджене наказом МВС України від 03 серпня 2017 р. № 676, зареєстрованого в

Міністерстві юстиції України 28 серпня 2017 р. № 1059/30927. URL::https://zakon.rada.gov.ua/laws/show/z1059-17

3. Балтовський О.А., Ісмайлов К.Ю., Сіфоров О.І., Форос Г.В., Заєць О.М. Теорія систем і системний аналіз: навч. посібник. ОДУВС. 2020. 156 с.

4. Основи кримінального аналізу: підручник / Бабенко А.М., Заєць О.М., Некрасов В.А., Ісмайлов К.Ю., Пефтієв Д.О. та ін.; за заг. ред. Користіна О.Є.. 2019. 270 с.

Форос Г.В.
к.ю.н., доцент
(Одеський державний університет внутрішніх справ)

Колун Д.В.
(Одеський державний університет внутрішніх справ)

ОКРЕМІ АСПЕКТИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Сучасний стан застосування новітніх інформаційно-комунікаційних технологій у всіх галузях потребує розширення їх впровадження у діяльність правоохоронних органів. Важливе значення для розробки заходів протидії злочинності має інформаційно-аналітичне забезпечення. Воно передбачає наявність інформації про стан, динаміку, структуру злочинів, вплив на злочинність соціально-економічного стану держави, діяльність суб'єктів запобігання злочинності. Необхідно мати в своєму розпорядженні досить повну інформацію, що відображала б реальний стан злочинності в країні та фактори, які призводять до її виникнення. Але отримання такої інформації та її аналіз пов'язані з певними проблемами. Зокрема, проблемою є розосередженість обліку злочинів за окремими відомствами. Наявна система збирання показників кримінально-правової статистики про злочинність через відомчий підхід до неї не сприяє формуванню об'єктивної і достовірної картини про стан злочинності в країні та про результати роботи правоохоронної системи. Ситуація, що склалася, негативно впливає і на використання статистичних даних для визначення тенденцій, стратегії і тактики протидії злочинності та іншим правопорушенням [1, с. 49].

До поняття інформаційно-аналітичного забезпечення віднесений організаційний аспект, який вказує на головні напрямки правового регулювання інформаційно-аналітичного забезпечення. Таке значення зазначеного терміну може бути співвіднесене з діяльністю, що пов'язана із

4. Запропоновано відновлення співпраці у 2023 році Консультативної місії Європейського союзу (EUAM) та закладів вищої освіти МВС України в частині проведення тренінгів щодо розвитку теорії та практики ILP та напрацювання понятійного апарату задля формування освітньо-наукового базису імплементації ILP, які були (тренінги) заплановані ще наприкінці 2021 року, але у зв'язку зі відкритою зовнішньою агресією РФ у 2022 році – не проводилися.

5. Констатовано, що формування відповідної національної політики, стратегії та імплементація ILP загалом залежить від ключових факторів успіху: чіткої нормативно-правової бази, яка відповідає міжнародним стандартам щодо прав людини та захисту даних, і включає чітко визначені повноваження та процеси в правоохоронних органах щодо збору, аналізу та поширення відповідних аналітичних даних; організаційної структури, яка сприяє чіткому стратегічному керівництву та оперативному співробітництву, а також процесам прийняття рішень у міжвідомчому середовищі та належному нагляді; технології для полегшення обміну інформацією через сумісність систем; знання та навички всього відповідного персоналу; колективна культура поширення розвідувальної аналітики для підтримки прийняття рішень у всіх операційних напрямках.

6. Розвивається процес адаптації до українських реалій методології Європолу щодо Оцінки загроз серйозних злочинів та організованої злочинності (SOCTA – Serious and Organised Crime Threat Assessment) реалій згідно нормативно-правової бази та специфіки правоохоронних органів, а саме ключовою стала ініціатива Консультативної місії Європейського Союзу в Україні (EUAM), на платформі якої було створено міжвідомчу робочу групу з вивчення методології та впровадження SOCTA в Україні. Представники робочої групи брали участь у навчальних візитах до Європолу та в семінарах, що проводились представниками Європолу в Україні.

7. Зазначено, що впровадження методології Європолу SOCTA в Україні – це еволюційний шлях у становленні системи та формування відповідних компетентностей. З метою подальшого впровадження та адаптації методології Європолу SOCTA в Україні запропоновано: проводити цей процес спільно з імплементацією моделі ILP: філософського підґрунтя, понятійного апарату, мети, завдань, принципів тощо; неформалізоване та небюрократизоване упровадження SOCTA у контексті формування Стратегії боротьби з організованою злочинністю та набуття подальшого її розвитку у плануванні оперативного характеру; розробка та впровадження новітніх підходів до моніторингу виконання і оцінювання результатів, як виконання планів заходів, так і діяльності окремих практичних підрозділів, та відхід від застарілого індикатору ефективності поліцейської діяльності, який зараз базується на статистичних звітах щодо ОГ та ЗО; впровадження SOCTA повинно бути сумісною діяльністю як науковців так і практичних працівників правоохоронних органів; активна просвітницька, освітня та тренінгова діяльності.

ЗМІСТ