KAPITEL 4 / *CHAPTER 4* [4]
INTELLIGENT SYSTEMS OF PREDICATIVE ANALYTICS OF LAW ENFORCEMENT AGENCIES

DOI: 10.30890/2709-2313.2023-17-03-001

Вступ

Зараз у середовищі правоохоронних органів розвинених країн питання переходу від реактивної до проактивної діяльності стоїть на рівні з питанням виживання цивілізації. Запорукою ефективного впровадження такої моделі діяльності є застосування інтелектуальних платформ автоматичного аналізу різнотипних і різноформатних даних. Чому? Тому що, навіть якщо ми на кожному кроці наставимо відеокамер і будемо обробляти відео потоки від них у ручному або навіть, у півавтоматичному режимі, це буде майже марна трата грошей.

Ключовим і самим складним етапом технології предикативної аналітики є Аналіз, в процесі якого здійснюється систематизація і аналітична обробка зібраних на попередніх етапах даних та інформації [1]. Причому на сучасному етапі кількість інформації, яка підлягає обробці і аналізу, досягає настільки великих обсягів, що людина вручну не в змозі їх опрацювати за реальний час. Тому ефективність виконання цього етапу визначається наявністю засобів, які має в своєму розпорядженні аналітик. В першу чергу, наявністю сучасних програмних інструментальних засобів.

Дослідженню питань розробки і впровадження аналітичних систем, а також питанню унормування інформаційно-аналітичної обробки інформації правоохоронними органами, кримінальної аналітики присвячені роботи [1-32].

В загальному випадку під інструментальними засобами аналітика будемо розуміти програмні системи або модулі, методики і методології опрацювання інформації.

Загальну класифікацію інструментальних аналітичних засобів можна представити наступним чином:

1. Методології і методики аналізу.
2. Загально використовувані програмні засоби.
3. Традиційні інформаційно-пошукові системи.
4. Спеціалізовані інформаційно-аналітичні системи і комплекси кримінального аналізу.

До інструментів першої групи можна віднести, зокрема, такі часто використовувані методики як мережний аналіз, ANACAPA, SOCTA, SWOT-аналіз. Вони застосовуються як в ручному так і в автоматизованому режимі.

Мережний аналіз це загальна методологія аналізу, яка передбачає використання математичного апарату теорії графів для дослідження і виявлення зв'язків між об'єктами і подіями.

ANACAPA представляє собою методику розслідування злочинів і аналізу оперативної інформації, яка була розроблена в 1960-ті роки, після вбивства

[4] ***Authors:*** *Uzlov Dmytrij Yurijevich, Strukov Vladymyr Mykhajlovich, Hnusov Yurii Valeriyevych*

президента Кенеді. Методику названо на честь острова на західному узбережжі Америки. Спочатку методика представляла собою систему структурування, візуалізації та аналізу інформації у паперовому виконанні. В подальшому фірмою Anacapa Sciences Inc. (США) були розроблені програмні продукти, які реалізують дану методику. Anacapa Sciences Inc. стояла у витоків розробки спеціальних аналітичних методик для сфери безпеки і ще на початку 1970-тих років почала проведення навчальних курсів з підготовки фахівців-аналітиків. Anacapa Sciences Inc. пропонує наступні 4 базових курси:

1) аналіз інформації в ході проведення розслідувань Criminal Intelligence Analysis (CIA);

2) аналітичні методи розслідування Analytical Investigation Methods (AIM);

3) аналіз фінансових махінацій Financial Manipulation Analysis (FMA);

4) поглиблений аналіз з використанням комп'ютерних технологій Computer-Aided Analysis (CAA).

SOCTA (SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT) є методикою з оцінки ризиків щодо тяжких злочинів та організованої злочинності. SOCTA – ключовий стратегічно-аналітичний документ, присвячений боротьбі зі злочинністю, розроблений Європолом. Останній документ SOCTA опублікований Європолом у 2017 році – SOCTA 2017. Він готувався на протязі 2015-2017 років. В ході його підготовки був проведений безпрецедентний за масштабами аналіз серйозної і організованої злочинності, за результатами якого розроблені відповідні рекомендації.

SWOT-аналіз - це випробуваний часом, відносно простий, але ефективний інструмент підтримки прийняття рішень[1]. Суть SWOT-аналізу - у виявленні сильних і слабких сторін, можливостей і загроз для організацій, установ і т. п. Оцінка чотирьох елементів SWOT-аналізу проводиться шляхом визначення зовнішніх і внутрішніх чинників, які обумовлюють сильні і слабкі сторони, можливості і загрози.

SWOT-аналіз давно і ефективно використовується в розвідувальному співтоваристві, бізнесі, в дослідницьких цілях. У той же час, за даними дослідження Європолу «Інструментальні методу аналізу і прогнозування ОЗ на практиці 2014» в більшості країн ЄС правоохоронці взагалі не використовують SWOT-аналіз. У тих небагатьох країнах, де він все ж застосовується, це роблять не оперативні співробітники, поліцейські на землі, а дослідники в науково-навчальних організаціях правоохоронних структур.

Незважаючи на свою простоту, SWOT-аналіз є ефективним методом, особливо на мікрорівні при вивченні конкретних ОЗУ. У кримінальному SWOT-аналізі, також як в традиційному, визначаються сильні і слабкі сторони ОЗУ, а також можливості і загрози для цих організацій. При цьому сильні і слабкі сторони характеризують внутрішні чинники, а можливості і загрози - зовнішні. Щоб дослідити внутрішні чинники - сильні і слабкі сторони - необхідно оцінити конкретні види переваг, які мають кримінальні організації в порівнянні з їх конкурентами. Те ж вірно і для недоліків, тобто, слабких сторін. Зовнішні фактори, які проявляються через можливості і загрози, характеризують адаптаційні можливості організованого криміналу, його потенціал використання

економічних трансформацій, соціальних зрушень, технологічних змін - з одного боку, і здатність відповідати на виклики з боку правоохоронців - з іншого.

До інструментів другої групи можна віднести комп'ютерні програми і системи загального призначення та проблемно-орієнтовані, які з успіхом використовуються для розв'язання задач кримінального аналізу з відносно невеликим обсягом даних. До числа таких інструментів можна віднести Microsoft Excel, MatCAD, MatLAB, StatGraph, Statistica та ін. Можливість ефективного застосування цих інструментів значною мірою визначається наявністю відповідних методик їх застосування для розв'язання конкретних задач кримінального аналізу, кваліфікацією і практичним досвідом фахівців. До інструментальних засобів цієї групи можна також віднести гео-інформаційні системи (ГІС), призначені для візуалізації об'єктів і подій на географічній мапі. Без застосування ГІС на сучасному етапі неможливо уявити аналітичну роботу як у правоохоронній так і у цивільній сфері. Вони є базовим інструментом візуалізації даних. В останні декілька років відбувся справжній стрибок у розвитку систем візуалізації даних, оскільки саме цей аспект аналітичної обробки даних набуває все більшу актуальність. Це пов'язано з тими чинниками, про які ми вже говорили раніше, зокрема – можливістю наочного обґрунтування рішень і висновків, які генеруються автономними системами, і в подальшому надаються особам, які приймають кінцеві рішення, наприклад, керівникам відповідних департаментів правоохоронних органів, які не є фахівцями у сфері штучного інтелекту або методів Data Science.

Типовими прикладами традиційних інформаційно-пошукових систем можна вважати Ліга-Закон і Google. Принципом роботи таких систем є опрацювання пошукового запиту, сформованого за певним шаблоном. Результатом роботи є перелік даних або документів, які відповідають пошуковому запиту. До систем такого типу належить і відомча інформаційно-пошукова система «Інформаційний портал Національної поліції України». Головною метою систем даного типу є пошук інформації відповідно до запиту, оформленого за певним шаблоном, і видачі в якості результату переліку об'єктів бази даних, які відповідають запиту. Вони, як правило, не мають модулів аналітичної обробки великих і надвеликих обсягів інформації, а тим більше, модулів прогнозування скоєння злочинів.

Найбільш ефективними інструментами кримінальних аналітиків є спеціалізовані інформаційно-аналітичні системи і комплекси кримінального аналізу. Системи цього класу мають потужний набір інструментів аналітика, які дозволяють проводити глибокий всебічний аналіз великих обсягів різнотипних даних і формувати гіпотези щодо аналізуємих подій і об'єктів. На поточний момент у розвинених країнах широко застосовуються такі відомі системи даного класу як I2, Palantir, ePOOLICE, PredPol, HOLMS2, RICAS, Maltego. З перелічених систем особливо варто виділити Palantir та ePOOLICE. Їх головною відмінною рисою є можливість сканувати доступний кіберпростір у режимі 24/7, виявляти в ньому «слабкі сигнали» масштабних злочинів і терактів, що готуються, формувати ці сигнали у комплексну систему індикаторів, які дозволяють з великою ймовірністю прогнозувати час і місце скоєння злочину.

Наявність систем такого типу на наш погляд є головною умовою повноцінної реалізації предикативної моделі діяльності правоохоронних органів.

На поточний момент у світі існує досить невелика кількість високотехнологічних інструментальних аналітичних платформ, які використовують найсучасніші технології обробки даних – Data Mining, Web Mining, штучний інтелект та ін. Накопичений певний досвід їх застосування у прогнозуванні, профілактиці, запобіганні та розслідуванні злочинів. Цей досвід є вкрай цінним, оскільки ці платформи є першопроходьцями в цьому напрямі. Виявлені під час їх експлуатації позитивні моменти, недоліки і проблеми дають можливість узагальнити їх та врахувати при розробці і впровадженні аналогічних платформ.

Аналіз відомих аналітичних платформ свідчить про те, що кожна з них має певний перелік аналітичних інструментів, які визначають, власне, функціональність відповідної платформи, її можливості. Причому набір таких інструментів може бути представлений або у складі комплексної аналітичної системи, яка виконує певні функції і задачі, або у формі набору взаємонезалежних інструментальних засобів для виконання окремих аналітичних функцій, які представляються розробником як певний перелік аналітичних сервісів.

Огляд відомих аналітичних платформ дозволяє виокремити такі аналітичні інструменти, які розглянемо нижче.

4.1. Огляд функціоналу аналітичних інструментів для правоохоронних органів.

Під аналітичним інструментом в контексті даної роботи будемо розуміти методику, технічний засіб або програмний продукт (або модуль), за допомогою яких виконується певна аналітична функція (операція). Прикладами таких аналітичних функцій можуть бути наступні: 1) моніторинг відкритого кіберпростору з метою виявлення і фіксації кримінально-значимих об'єктів і подій, 2) виявлення у доступних масивах даних і відображення (в ідеальному випадку - на географічній мапі) зв'язків між кримінальними особами, 3) виявлення у доступних масивах даних і відображення на географічній мапі осередків концентрації злочинів, 4) формування і відображення хронологічної послідовності певної групи подій і т.п. Інструменти аналітика допомагають організувати, інтегрувати, порівнювати, співвідносити та ілюструвати сукупність необробленої інформації. Жоден з інструментів аналітика не дасть дійового результату самостійно; кожен додає компонент нових знань або, принаймні, нового розуміння про дані, які в сукупності сприяють аналізу або призводять до визначення нових вимог до розвідки недостатніх даних. Фактичний аналіз покладається на навички критичного мислення аналітика, а також на його здатність інтегрувати результати різноманітних методологій та інструментальних засобів у узагальнений, дієвий продукт аналітики. Ці продукти можуть включати частини результатів застосування аналітичних інструментів

для ілюстрації складних взаємозв'язків, таких, наприклад, як діаграма незаконних товарних потоків або діаграма зв'язків, що відображає відносини та ієрархію осіб, причетних до злочинного угрупування.

Аналітику потрібно розуміння призначення та функціональних можливостей різних доступних аналітичних інструментів та типів інформації, яку вони надають. На основі практичного досвіду і опису доступних інтелектуальних платформ кримінального аналізу даних сформуємо наступний (можливо не вичерпний) перелік найпоширеніших аналітичних інструментів, які застосовуються кримінальними аналітиками у своїй діяльності:

- **Аналіз схеми скоєння злочину**. Подібно до технологічної карти (методичних рекомендацій) розслідування злочину, схема скоєння злочину показує послідовні кроки, які використовують злочинці, вказуючи послідовність інцидентів, їх дат та часу скоєння, задіяні державні та комерційні структури, особи, засоби переміщення та інше(Рисунок 1). Інциденти відображаються в вигляді блок-схеми, щоб допомогти зрозуміти розвиток подій.

- **Асоціаційна матриця**. Ця матриця допомагає співвіднести два або більше факторів у злочинній діяльності, фіксуючи частоту, з якою одночасно виникають певні фактори (наприклад, особи, організації, номери телефонів, адреси та подібні змінні), щоб виділити корелюючи фактори, які відіграють важливу роль у діяльності злочинців та усувають фактори, які не мають взаємозв'язку (Рисунок 2). Фактори можуть бути схожими, наприклад, співвідношення серії телефонних номерів. Фактори також можуть бути за своєю суттю незалежними, але дають зрозуміти, коли вони співвідносяться, наприклад, складання схеми подорожей двох цілей спостереження, коли телефонний дзвінок або банківська операція здійснюються перед поїздкою.

- **Товарний трафік / графічний аналіз**. Діаграма, яка ілюструє, схему організації переміщення заборонених товарів, зброї, наркотиків за допомогою елементів злочинного середовища (Рисунок 3). Наприклад, товарний потік афганського героїну відображатиме кожну операцію та спосіб контрабанди, разом із транзакційними витратами, з Афганістану до міста в Україні.

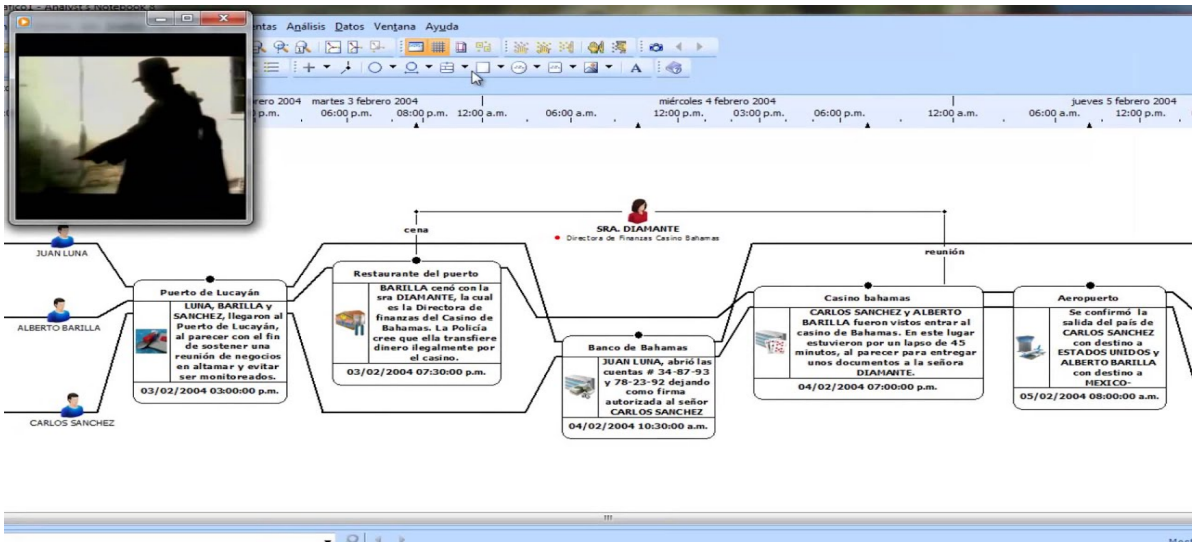

Рисунок 1 - Аналіз схеми скоєння злочину.

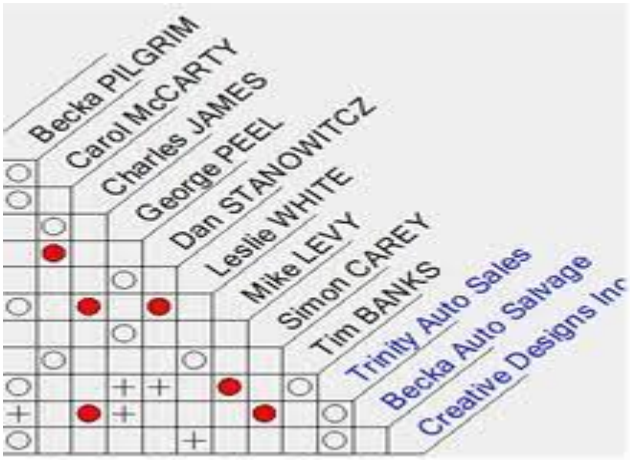

Рисунок 2 - Асоціаційна матриця.

- **Аналіз комунікаційного трафіку**. Важливу інформацію можна отримати в результаті аналізу трафіку телефонів, обміну текстовими повідомленнями та електронною поштою (Рисунок 4). Визначивши, з ким здійснюють зв'язок , частоту зв'язку, їх походження та призначення, тривалість зв'язку та наявність додатків до електронних листів, аналіз може надати значне підтвердження та докази злочинності. Хоча зміст комунікацій, очевидно, буде надавати важливу інформацію, аналіз комунікаційного трафіку також може бути цінним.

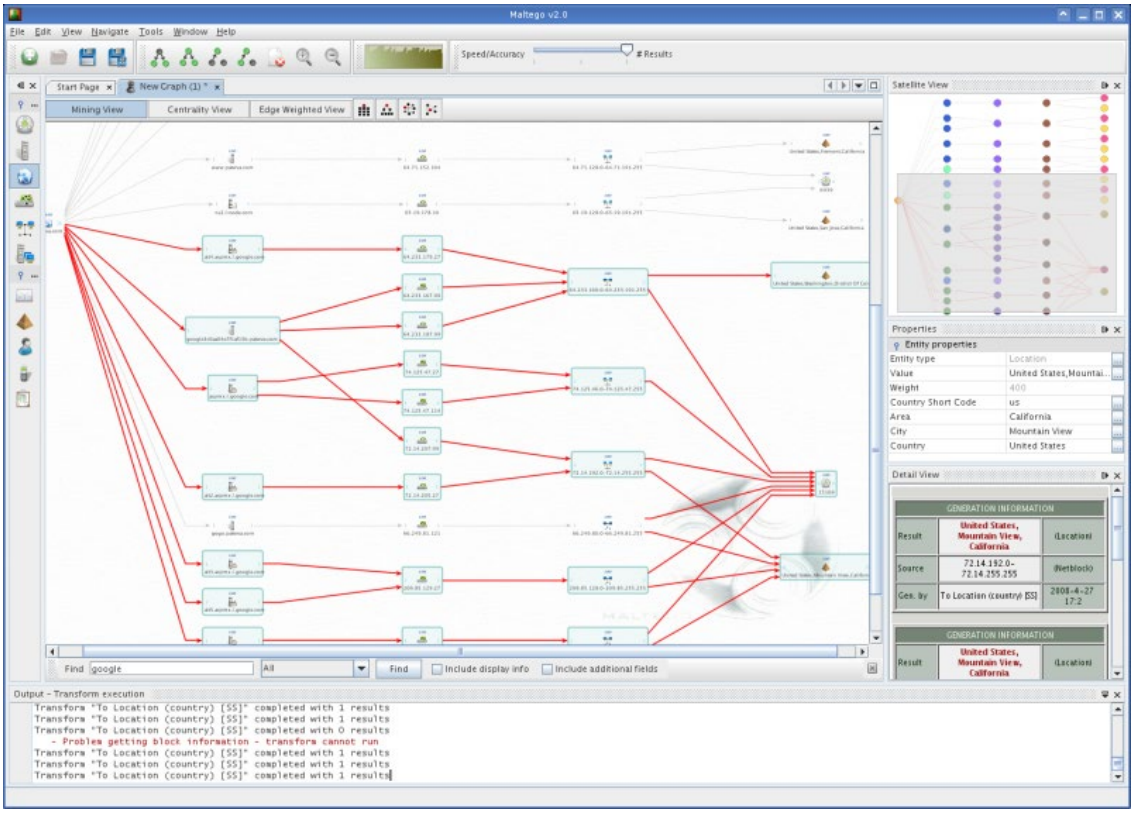

Рисунок 3 - Товарний трафік.

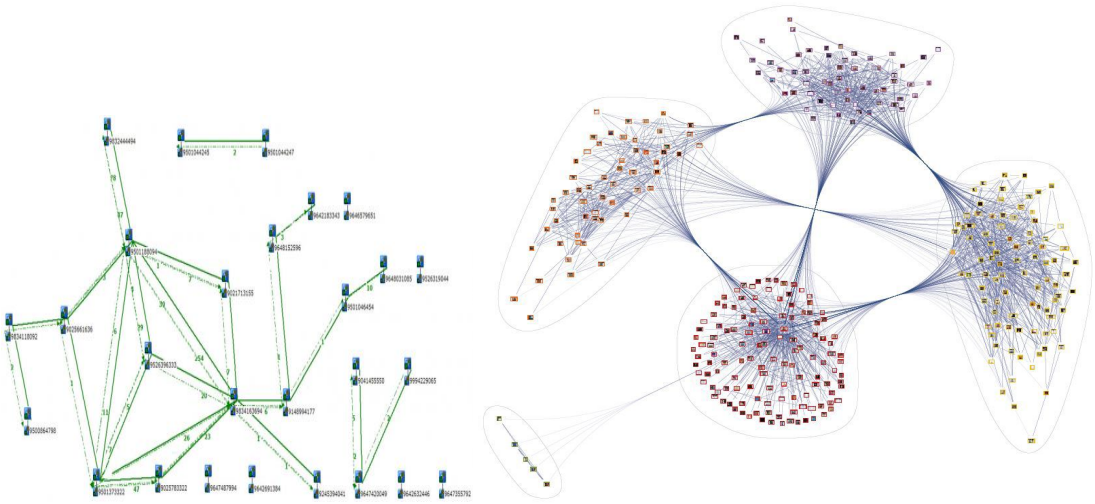

Рисунок 4 - Аналіз комунікаційного трафіку.

- **Аналіз структури злочинності.** Загальний термін для ряду суміжних дисциплін, таких як ідентифікація злочинів або серій інцидентів, аналіз тенденцій злочинності, аналіз гарячих точок та загальний аналіз профілю, і може включати картографування (Рисунок 5).

-

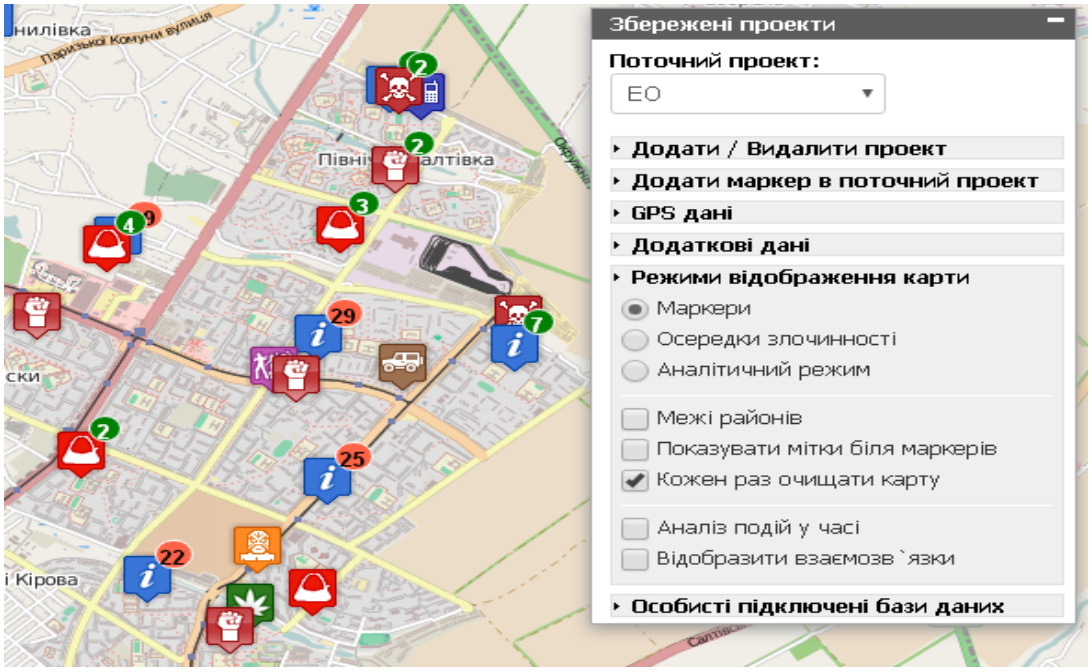

Рисунок 5 - Аналіз структури злочинності.

- **Профайлінг злочинця** – містить детальний аналіз поведінкового профілю злочинця, його кримінальних навичок, загальну інформацію, механізми та характер скоєних злочинів, інше (Рисунок 6). Аналіз, який охоплює цілий ряд аналітичних методів для опису злочинців, їх злочинної діяльності, способу життя, асоціацій, ризику, який вони представляють, та їх сильних і слабких сторін, щоб зосередити увагу на розслідуванні, націленому на них. Профілі також можуть бути зосереджені на жертвах та вразливих особах.

- **Кримінальний профайлінг.** Такі профілі містять детальний аналіз об'єктивної складової злочину, а саме механізму скоєння, специфічні навички, що були використані, методи та інструменти.

- **Демографічний / соціальний аналіз тенденцій**. Аналітичний метод, орієнтований на демографічні зміни та їх вплив на злочинність. Він також аналізує такі соціальні фактори, як безробіття та безпритульність, і розглядає важливість змін населення, ставлення та діяльності, оскільки вони можуть впливати на злочинність.

Рисунок 6 - Профайлінг злочинця.

- **Аналіз потоку подій**. Діаграми, що забезпечують візуальне зображення ряду важливих подій або інцидентів (наприклад, кримінальної операції) та послідовних взаємозв'язків цих подій, таких як подорожі учасника злочину, грошові операції чи інші події, що мають вирішальне значення для скоєння злочину (Рисунок 7).

- **Фінансовий аналіз**. Існує безліч методів фінансового аналізу, які спільно прагнуть спів віднести різноманітні фінансові операції, включаючи характер операцій; залучені сторони; походження, посередництво та призначення транзакцій; та порівняльний аналіз доходів та витрат. Сукупно, метою є документування тенденцій транзакцій (як приватних осіб, так і організацій) та виявлення розбіжностей або підозрілої фінансової діяльності. З огляду на те, що практично всі злочини мають певну форму фінансового елементу, фінансовий аналіз є важливим інструментом.

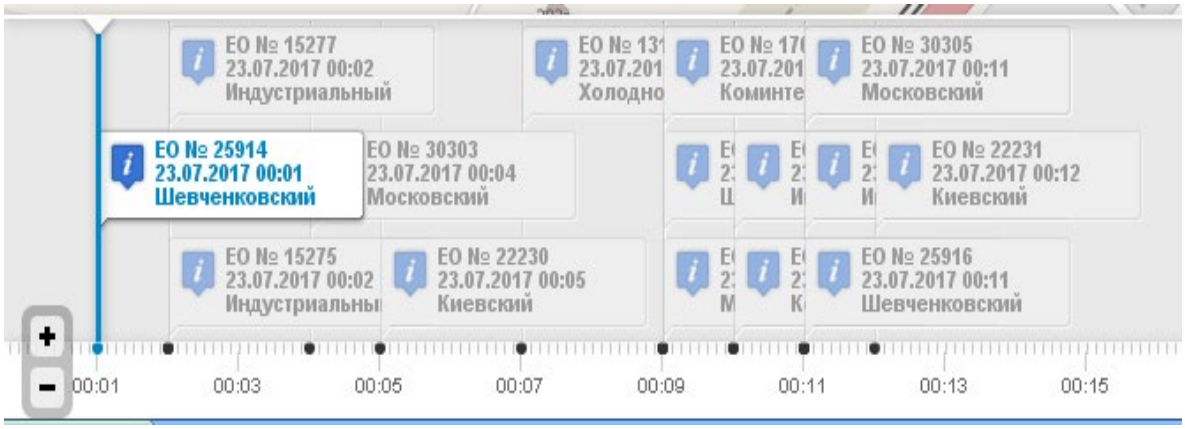

Рисунок 7 - Аналіз потоку подій.

- **Перевірка гіпотез**. Аналітик висловить гіпотезу про зв'язки людей та організацій у злочинному підприємстві, необхідних операціях для функціонування підприємства та важливих товарах або ресурсах, необхідних для успіху підприємства. На відміну від попередніх пунктів у цьому списку, які є візуальними зображеннями різних елементів підприємства, перевірка гіпотез використовує зображення, щоб визначити, чи були визначені всі елементи злочину, які можуть бути використані для запобігання продовженню злочинної діяльності і (в ідеалі) визначення кримінальної відповідальності учасників.
- **Аналіз зв'язків**. Діаграма, яка ідентифікує всіх підтверджених та підозрюваних осіб та організації у злочинному підприємстві та ілюструє їх взаємозв'язок між собою (Рисунок 8).
- **Профілі ринку**. Ці профілі є оцінками, які досліджують кримінальний ринок навколо певного товару в певній місцевості, наприклад, наркотиків чи викрадених транспортних засобів, або такої послуги, як проституція. Вони постійно переглядаються та оновлюються.
- **Мережевий аналіз**. Цей аналіз не лише описує зв'язки між людьми, які утворюють злочинні мережі, але також значення зв'язків, ролі, яку виконують окремі особи, а також сильні та слабкі сторони злочинної організації (Рисунок 9).
- **Оцінка оперативних можливостей**. Такий аналіз оцінює перекриття джерелами інформації, щоб зберегти фокус операції на попередньо узгоджені цілі, особливо у випадку значного плану збору розвідувальних даних або іншої масштабної операції.

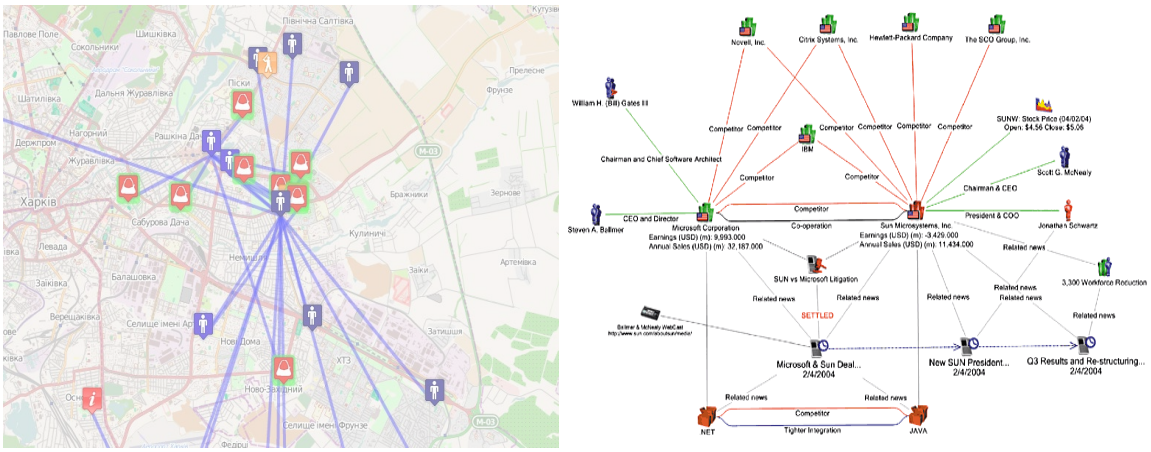

Рисунок 8 - Аналіз зв'язків.

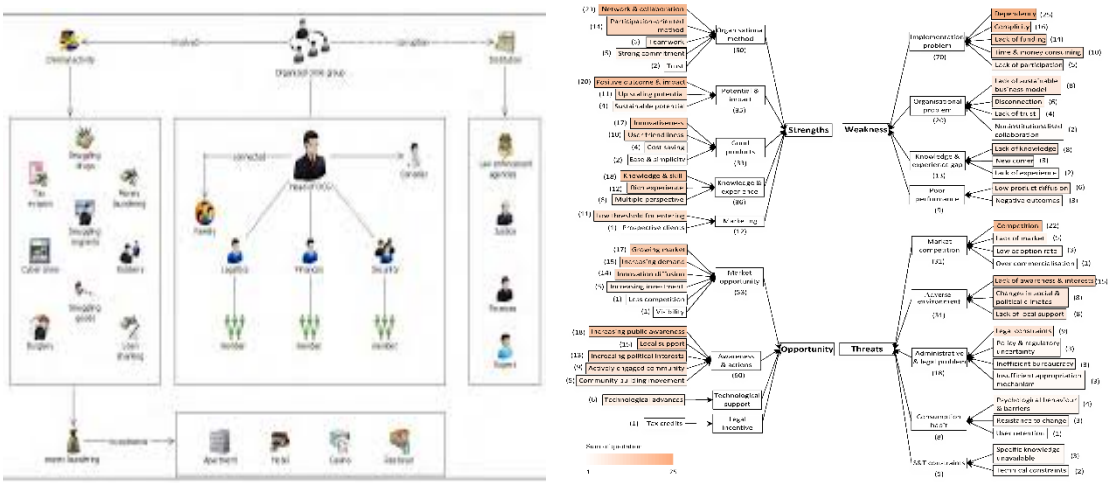

Рисунок 9 - Мережевий аналіз.

- **Аналіз результатів**. Аналіз, що оцінює ефективність правоохоронної діяльності; наприклад, ефективність патрульних стратегій, ініціатив щодо зменшення злочинності або конкретного методу розслідування.

- **Аналіз ризику**. Аналіз, що оцінює масштаби ризиків, які створюють окремі правопорушники чи організації для окремих потенційних жертв, широкої громадськості та правоохоронних органів.

Кожен із цих методів використовується для кращого розуміння необробленої інформації та її взаємозв'язків та для ілюстрування кримінального явища.

- **Моніторинг доступного кіберпростору.** Це у загальному випадку комплексна процедура, яка представляє собою сканування в режимі 24/7 усіх доступних електронних джерел інформації, таких як державні і недержавні інформаційні ресурси у різноманітних форматах: 1) структуровані дані у форматах баз даних, xls, xlsx, csv, csv2, xml та ін.; 2) неструктуровані дані - текстові дані, графічні файли, відео та аудіо файли; дані з соцмереж мессенджерів, IoT та ін. На поточний момент у світі існує дуже обмежена кількість інтелектуальних аналітичних платформ, які мають у своєму складі

модулі з такою функцією. Усі платформи такого типу можна поділити на дві групи: 1) такі, що виявляють явні (прямі) ознаки злочинної активності і 2) такі, що виявляють сховані, непрямі ознаки на основі так званих «слабких сигналів» шляхом побудови системи спеціальних індикаторів [22].

- **Формування системи індикаторів ОЗ на основі виявлення «слабких сигналів» в процесі моніторингу доступного кіберпростору.** Це складна наукомістка процедура, яка має своєю метою виявлення явних або прихованих ознак скоєних або плануємих злочинів на основі побудови ієрархічної системи індикаторів злочинної діяльності, кожний з яких формується шляхом узагальнення певної сукупності «слабких сигналів».

4.2. Особливості і порівняльний огляд існуючих інструментальних систем для вирішення завдань правоохоронних органів щодо кримінальної аналітики.

Інструментальні платформи з програмним забезпеченням правоохоронних органів розроблюється під конкретну систему кримінальних обліків конкретної країни і цілком відповідають структурам інформаційно-пошукових систем, в яких накопичується інформація про протиправні інциденти, осіб, об'єкти та інше. Самі інциденти кваліфікуються згідно чинного кримінального або адміністративного законодавства країни.

Разом з цим, на теперішній час, для забезпечення потреб правоохоронних органів існують міжнародні стандарти та методи інтелектуального аналізу, що застосовуються для розслідування злочинів, виявлення кримінальних подій та різноманітних видів кримінального аналізу, зокрема, в рамках моделі ILP (Intelligence Led Policing) – Поліцейської діяльності, керованою аналітикою[1], та інших моделей предикативної поліцейської діяльності.

Нижче представлено огляд найбільш відомих аналітичних платформ, які використовуються в правоохоронних органах різних країн.

Crime Center (Shotspotter).

Запатентована система датчиків, алгоритмів та штучного інтелекту, яка точно виявляє, знаходить і попереджає поліцію про стрілянину [9]. Є складовою частиною RTCC – Real-time crime center (ситуаційно-аналітичні центри реального часу) поліції США. Основним завданням системи є виявлення та швидке реагування на застосування вогнепальної зброї та вибухівки. Система має ГІС платформу та забезпечує швидке інформування про локацію інциденту зі стрілянниною або вибухом (Рисунок 10). Може інтегруватися в інші ГІС платформи правоохоронних органів.

Maltego.

Пропонується в якості інструмента для графічного аналізу інтернет посилань, пошукового інструменту по відкритим джерелам інтернету у реальному часі та збору інформації, а також представлення цієї інформації візуально на основі графів, завдяки чому шаблони та зв'язки між різними джерелами та відповідною інформацією легко ідентифікуються.

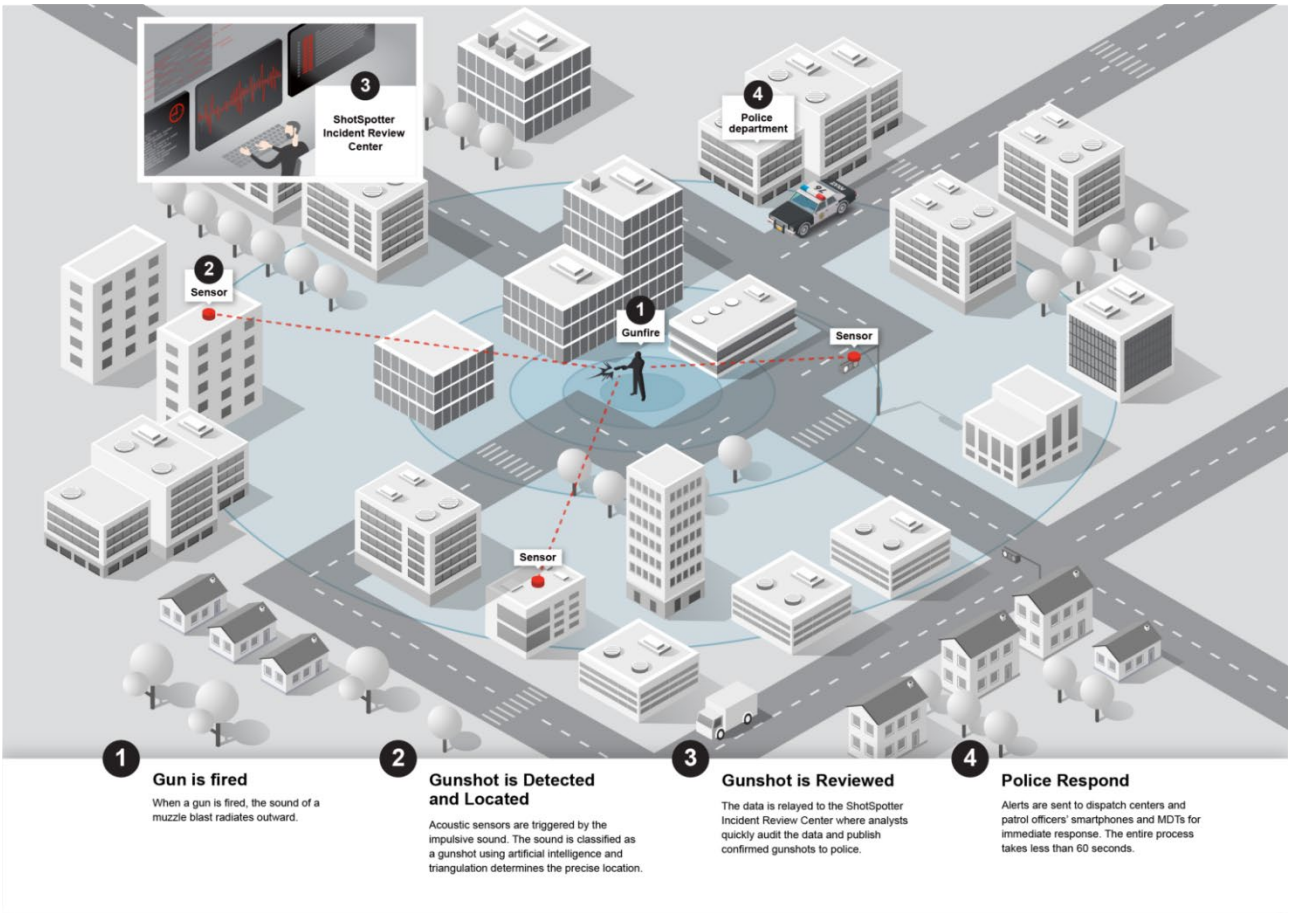

Рисунок 10 - Crime Center (Shotspotter).

За допомогою Maltego ви можете видобувати дані з розподілених джерел, автоматично об'єднувати відповідну інформацію в одному графі та візуально наносити її на карту, щоб дослідити ваш ландшафт даних (Рисунок 11). Maltego пропонує можливість підключати дані та функції з різних джерел, використовуючи Transforms. Через Transform Hub ви можете підключити дані понад 30 партнерів, таких як Recorded Future, DomainTools, Crowdstrike, ThreatConnect та різноманітні загальнодоступні джерела (OSINT), а також власні внутрішні дані. Однак для роботи з власними даними необхідно їх доволі важка конвертація, та розроблення логістичної моделі та моделі асоціативних правил. Застосовується здебільше для OSINT.

IBM i2 Analyst's Notebook.

Це візуальне аналітичне середовище, яке дозволяє максимально ефективно використовувати величезні обсяги інформації, накопичені державними службами та підприємствами. 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 в 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 [19].

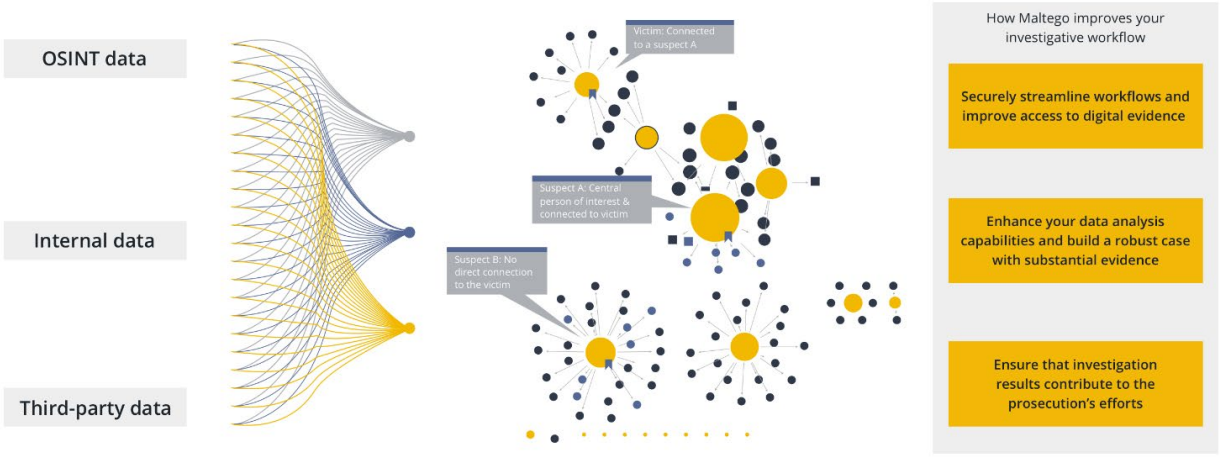

Рисунок 11 - Система Maltego.

IBM i2 Analyst's Notebook допомагає вирішувати такі завдання:

- швидка систематизація розрізнених даних в єдиному узгодженому поданні;
- визначення ключових осіб, подій, зв'язків і закономірностей, які не завжди можна виявити іншими засобами;
- покращене розуміння структури, ієрархії і способів дій злочинних, терористичних і шахрайських організацій;
- спрощення обміну складними даними, що дозволяє приймати своєчасні і точні оперативні рішення;
- можливість отримання вигоди за рахунок швидкого впровадження, яке забезпечує швидке зростання продуктивності, завдяки надійним рішенням для візуальної аналітики.

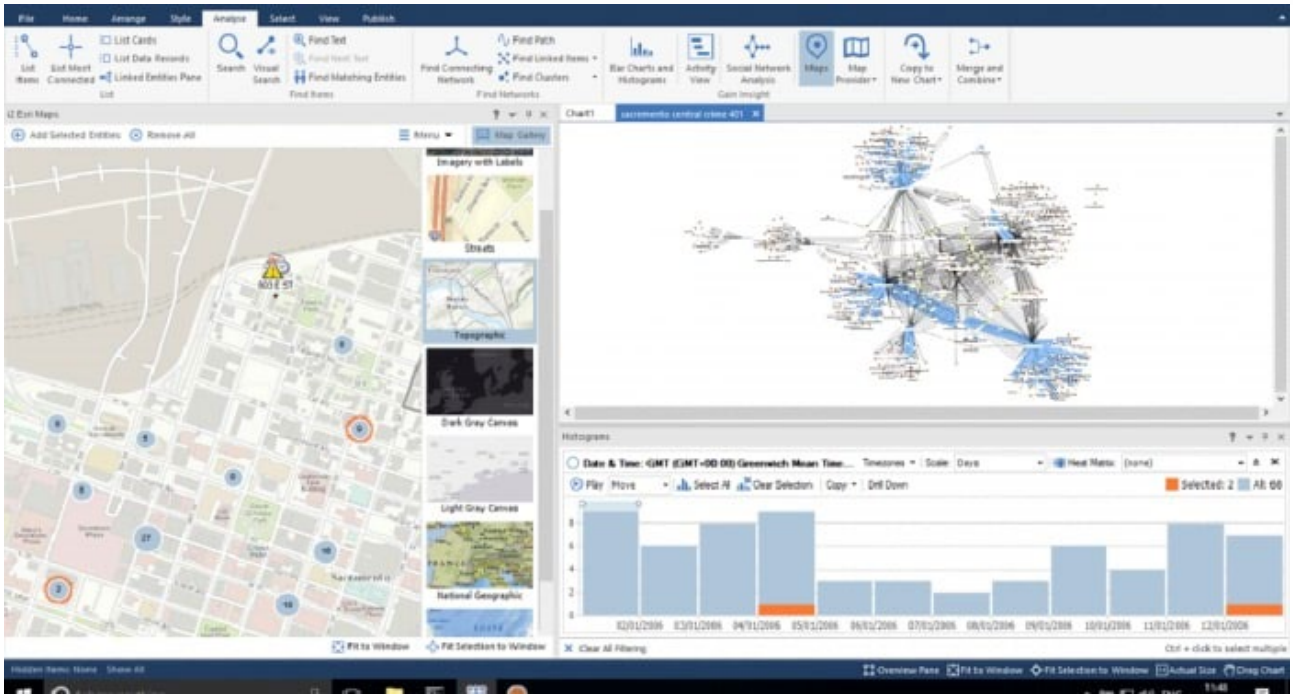

Рисунок 12 - Система IBM i2 Analyst's Notebook.

I2Analyst Notebook максимально розкручена серед аналітиків система, яка започаткована в началі 2000 років, має кілька версій. Система орієнтована на побудову різноманітних схем, але має необхідність великої кількості операцій ручної обробки даних, не дуже пристосована для роботи з Big Data та Big Stream Data, має складну систему конвертації зовнішніх даних, доволі важку систему ГІС, потребує багато ресурсів, коштовна.

Command Central Aware Motorola.

Command Central Aware від Motorola це набір інструментів, який включає ГІС як платформу для відображення всієї інформації та візуального аналізу, інструменти інтелектуальної обробки та керування відео потоками та системами розпізнавання зображень, статистичним аналізом інцидентів, керування нарядами та іншими засобами. Інтегрує, організовує та визначає пріоритети множини потоків інформації, щоб оператор-людина міг швидко зрозуміти їх та прийняти перші управлінські рішення. Рішення розміщує відповідну інформацію на одному дисплеї або групі дисплеїв і переміщує інші джерела у фоновий режим, де це не відволікає увагу від поточного завдання.

Інтелектуальне програмне забезпечення для моніторингу може виявляти контрольовані шаблони або сценарії у відео потоках, що допомагає виявляти протиправні дії. Людина-оператор може не помітити, що рюкзак залишився притуленим до стіни, що прилягає до входу в центр громадського транспорту, але штучний інтелект комп'ютера це зробить. Подібним чином, програмне забезпечення буде «бачити» людей, які рухаються проти потоку руху, або йдуть нехарактерно повільно чи швидко, вказуючи на те, що їх поведінка відмінна від тих, хто їх оточує. Транспортний засіб, що в'їжджає у зону, зарезервовану для пішоходів, негайно буде позначений, а оператор попереджений про його присутність. Потім оператор може зосередитись на відповідній камері або сусідніх камерах та направити ресурси на місце для подальшого дослідження. Застосовується для RTCC, кризових центрів. Використовується Національною гвардією США.

Palantir Gotham.

Palantir Law Enforcement має інтуїтивно зрозумілий, зручний інтерфейс, який дозволяє будь-якому агенту, детективу чи слідчому швидко отримати доступ до всієї доступної інформації в одному місці . Замість того, щоб користуватись різними системами, користувачі можуть здійснити пошук підозрюваного, цільового об'єкта або місця за допомогою єдиного порталу та отримати необхідні дані з усіх відповідних систем. Palantir підключається до національної системи обміну інформацією США (National Information Exchange Model), підтримує існуючі системи управління справами, системи управління доказами, арештами, судовими даними, іншими даними про злочини, даними автоматизованої диспетчеризації (CAD), а також має підключення до федеральних сховищ, оперативних баз, даних з державних сховищ. Вміє обробляти як структуровані, слабо структуровані так і неструктуровані дані, такі як сховища документів та електронні листи. Palantir наймасштабніший продукт з капіталізацією більш ніж 500 млн. доларів США. Розроблювався для потреб федеральних агентств і має багатий арсенал інструментів штучного інтелекту для

роботи з Big Data, Big Stream Data. Працює з гетерогенними даними. Частково використовується Europol [9].

SmartCOP.

Інтелектуальна платформа SmartCOP для відділів поліції має повністю інтегровану лінійку програмних продуктів що включає автоматизовану диспетчеризацію, управління правоохоронними документами, аналітику, програмне забезпечення для мобільних патрулей та AVL, мобільну звітність, міжвідомчу взаємодію та веб-портал для публічних записів.

Система SmartCOP забезпечує безперебійну інтеграцію з інтерактивним відображенням карт в реальному часі для обробки дзвінків, диспетчеризації, мобільних даних, записів та управління інформацією для оптимізації ефективності операцій. SmartCOP пропонує багатофункціональне рішення, яке забезпечує гнучкість і включає інтегровану картографію (використовується ESRI), картки запуску AVL та пов'язані історичні дані. SmartCOP простий у використанні та дуже легко настроюється. Побудована під національну систему обміну інформацією США (National Information Exchange Model). На Європейському ринку не представлена.

Система раннього виявлення загроз організованої злочинності ePOOLICE.

ePOOLICE - це система раннього виявлення загроз з боку організованих злочинних угрупувань (ОЗУ) з використанням методів обчислювального сканування і розвідувальних систем [9, 22]. Проект спільно фінансувався країнами ЄС і Європейським Союзом в рамках Сьомої Рамкової програми досліджень і розробок (FR7). Програма FR7-SEC-2012-1 розробляється в рамках загальноєвропейської програми «Безпека і суспільство», її розділів «Форсайт», «Сценарії» та «Безпека». Мета проекту полягає в створенні ефективної загальноєвропейської системи середовищного сканування для попередження готуючихся до злочинів діючих і виникаючих ОЗУ[9, 22]. Підсумком реалізації проекту ePOOLICE став працездатний прототип ефективної системи раннього попередження виникаючих загроз з боку ОЗ. Згідно з рішенням ЄС, проект передбачає:

• проведення науково-технологічних досліджень з метою розробки ефективних систем сканування, аналізу і прогнозування загроз з боку ОЗУ. При цьому сканування має здійснюватися в загальнодоступному інтернеті, соціальних мережах і медіа, а також в новому інформаційному середовищі, що все більше фрагментується, включаючи комунікаційні мережі месенджерів, інтернет грошей і інтернет речей;

• виявлення ознак, індикаторів або індексів, що описують ранні або «слабкі» сигнали формуючихся загроз з боку ОЗУ;

• формування нормативних вимог до апаратного і програмного забезпечення, а також кваліфікації та компетенції аналітиків, здатних вирішити завдання відстеження та раннього виявлення загроз ОЗУ.

В якості ключових аспектів прототипу системи можна виділити:

• управління інформацією і знаннями в умовах середовищної невизначеності та інформаційної неповноти, що базується на розпізнаванні

патернів, що сигналізують про загрози, а також активності ОЗУ;

• наявність центрального інтегрованого сховища даних з можливістю користувачів в залежності від рангу і статусу працювати з цими даними в інтерактивному режимі з своїх робочих місць;

• створення спеціального середовища програмування і представлення даних користувачам, що робить можливим одночасну роботу з різними типами файлів;

• використання методології динамічної складності і спеціальних методів представлення складних явищ і процесів в простих таблицях і візуальних образах, що дозволяють конденсувати інформацію;

• дотримання міжнародних і країнових правових, етичних і режимних вимог до подібного роду систем.

Хоча ePOOLICE не фіксується на зборі і зберіганні персональних даних, вона, тим не менш, може отримувати такі дані щодо осіб, за якими ведуться справи оперативної розробки, справи оперативного спостереження, і поліцейські розслідування. Крім того, платформа в силу її програмно-апаратної конфігурації може ненавмисно витягувати персональні дані широкого кола осіб в тих випадках, коли ці дані розміщені на загальнодоступних ресурсах або в соціальних мережах, чатах і т. п.

Оскільки отримання достовірних даних про внутрішні процеси в конкретних ОЗУ не тільки вельми скрутне, але і вкрай коштовне, програма здійснює розпізнавання загроз ОЗУ шляхом моніторингу середовища активності ОЗУ. В рамках цього моніторингу не тільки виділяються вразливі точки локації і сфери можливої активності ОЗУ, але і виявляються індикатори, події і т. п. у зовнішньому середовищі, які є діагностичними ознаками підготовки ОЗУ до злочинів[9].

Реалізація аналітичних функцій інтелектуальних систем в аналізі кримінальних подій на базі інструментального комплексу RICAS.

На теперішній час ГУНП в Харківській області проведено апробацію інноваційного програмно-апаратного комплексу аналітичної обробки інформації різноманітних банків даних з відображенням на детальній інтерактивній карті міста як самих об'єктів так і результатів їх аналізу [2]. Комплекс має назву «RICAS». Згідно «Звіту про оцінку потреб щодо впровадження моделі поліцейської діяльності, керованою аналітикою (Intelligence-Led Policing/ILP) в Національній поліції України» від грудня 2016 року проведеного EUAM та UNDP – "систему можна використовувати на державному рівні в якості платформи для аналітичного супроводу та підтримки процесу прийняття рішень". В процесі експлуатації комплексу підтверджується його гнучкість та спроможність інтегрування будь-яких даних з можливістю часового та просторового аналізу їх зв'язків між собою. Комплекс розроблено із застосуванням найновіших технологій в області роботи з геоінформаційними даними, крім того за основу взято всесвітньовідомі картографічні сервіси з відкритим доступом (Open Street Map / OSM) та постійним поповненням силами світового співтовариства, що забезпечує максимальну актуальність відкритої інформації.

Аналітичні можливості комплексу досить значні [2]. Система дозволяє

відшукати приховані зв'язки між заданими об'єктами та відображувати знайдені зв'язки як у вигляді геоінформації, а також у вигляді хронологічної стрічки подій; відображувати на географічній карті місцевості ділянки концентрації всіх злочинів, що реєструються поліцією, із забезпеченням можливості вибору: а) одного або декількох видів злочинів; б) цікавого району (або районів); в) цікавого проміжку часу (за останній день, тиждень, місяць та ін.); г) в реальному часі змінювати границі досліджуваного інтервалу часу і переміщати цей проміжок вздовж вісі часу (Рисунок 13).

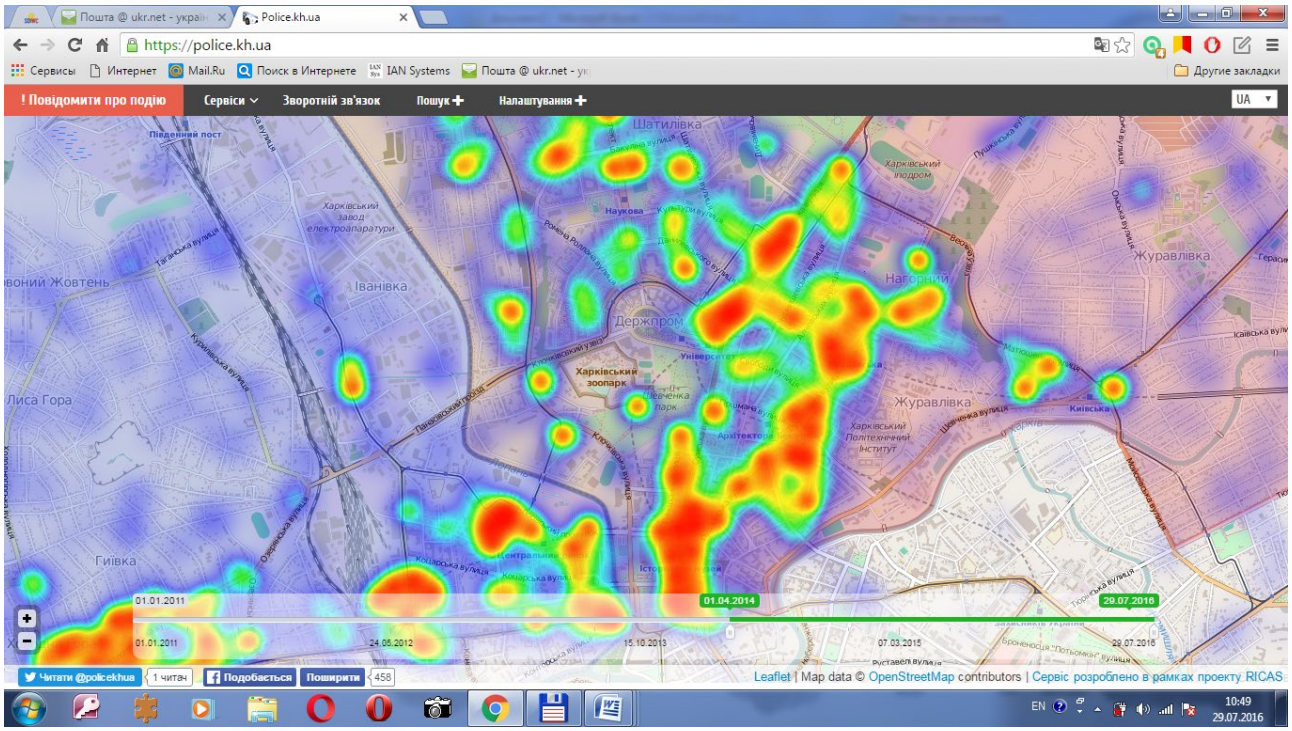

Рисунок 13 - Карта концентрації злочинів.

Також впроваджується модуль аналізу неструктурованої інформації, що дозволяє здійснювати пошук за аналогією або по заданим критеріям в режимі реального часу фактично у будь-яких текстових масивах.

RICAS побудовано на ґрунті наступних припущень:

- будь-яка кримінальна інформації містить дані про час та місце скоєння, що можуть бути відображені не тільки у вигляді текстового опису (населений пункт, вулиця, будинок), а й у формі географічних координат та відмітки часу;
- кожний об'єкт (суб'єкт) події має зв'язок із географічним об'єктом, що може бути описаний (адреса проживання, скоєння, місце роботи та ін.);
- кримінальні події, суб'єкти та об'єкти можуть мати зв'язки, що спостерігаються лише при збільшенні масштабів даних та візуалізації даних в єдиному інформаційному просторі (на мапі) з урахуванням розвитку в часі.

RICAS не є відокремленою системою, а побудована як інтелектуальний інструмент аналізу існуючих баз даних, що дозволяє не тільки виконувати запити та отримувати результати в текстовому вигляді, а й проводити пошук за неочевидними критеріями, аналізувати перетини зв'язків та ступінь близькості

об'єктів, осіб та подій з одночасною наочною візуалізацією результатів аналізу у просторі та часі (Рисунок 14). Система оперує засобами математичного моделювання та інтелектуального семантичного аналізу, наочного темпорального аналізу, аналізу поведінкового профілю та аналізу прихованих зв'язків. Задля уніфікації пошукових функцій та швидкої побудови поведінкового профілю, використовується алгоритм «тегування» (побудови ключових реквізитів), а також антиціпаційний алгоритм (схема передбачення) – коли ціль пошуку відома заздалегідь та потрібно лише встановити зв'язки. Семантичне ядро системи дозволяє виконувати складні запити, що містять статичні та динамічні складові: обмеження в часі, методу скоєння злочину, дислокації об'єктів та інші.

Враховуючи автоматизацію процесу обробки інформації та побудови новітніх реквізитів (зв'язків та перехресть, класифікацію та кластеризацію) в режимі реального часу, завдяки збільшенню обсягів інформаційних джерел, підключенню до хмарного сервісу RICAS не тільки інформаційних систем органів внутрішніх справ, а й інших відкритих державних реєстрів, систем обліку осіб, речей, подій, кримінальний аналіз буде значно точнішим та повним при формуванні доказової бази в конкретних провадженнях, а прогнозування стану криміногенної обстановки дозволить більш ефективно проводити профілактичні заходи та попереджувати злочинні прояви з більшою долею вірогідності.

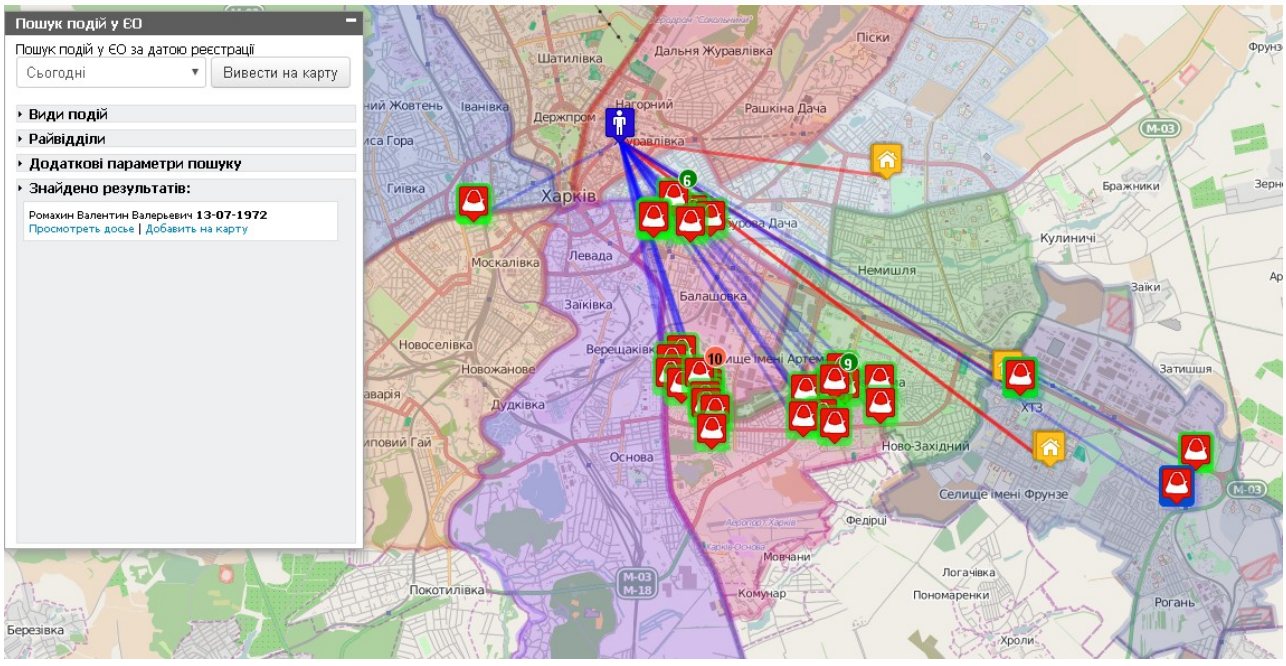

Рисунок 14 - Система RICAS.

Аналітичні можливості розглянутих інтелектуальних платформ відображені в узагальнюючій таблиці 1.

Таблиця 1 - Порівняння аналітичних можливостей інтелектуальних платформ для правоохоронних органів.

	CrimeCenter https://crimecenter.com https://www.shotspotter.com/	**Motorola-Command-Center-Software**	**SmartCOP** smartcop.com/	**Palantir gotham** https://www.palantir.com/palantir-gotham/	**ePOOLICE**	**RICAS** https://ricas.org/	**Maltego** https://www.maltego.com/	**IBM I2**
Аналіз схеми скоєння злочину			+	+	+	+	+	+
Товарний трафік / графічний аналіз	+	+		+	+	+	+	+
Аналіз комунікаційного трафіку		+	+		+	+	+	+
Аналіз структури злочинності	+	+	+	+	+	+		
Кримінальний профайлінг	+	+	+	+	+	+		
Профайлінг злочинця			+	+	+	+		
Семантичний аналіз				+	+	+		
Аналіз звязків Link Analysis			+	+	+	+	+	+
Візуальна аналітика на картографії Crime Mapping		+	+	+	+	+		
Демографічний / соціальний аналіз тенденцій			+	+	+	+		
Мережевий аналіз			+	+	+	+	+	+
Оцінка оперативних можливостей				+	+	+		+
Аналіз результатів				+	+	+		
Моніторинг доступного кіберпростору				+	+			
Формування системи індикаторів ОЗ				+	+			
Необхідність адаптації до ІП НПУ МВС України	Так	Так	Так	Так	Так	Ні	Так	Так

Висновки.

На основі проведеного дослідження можна сформулювати наступні вимоги до функціональних характеристик інтелектуальних систем автоматизованого аналізу для потреб кримінального аналізу: система повинна надавати співробітникам максимально повні результуючі дані для ефективного вирішення завдань предикативної діяльності правоохоронних органів за такими напрямками:

- постійний моніторинг соціально-економічної та криміногенної ситуації на різному рівні відповідальності, в різних сферах життєдіяльності регіонів, негативних процесів та їх вплив на соціально-економічну ситуацію, з встановленням горизонтальних структур кримінальної спрямованості та вертикальних центрів управління цими структурами; як наслідок – надання аналітичних меморандумів про стан соціально-економічної та криміногенної ситуації в регіоні, негативних процесів, прогнозів щодо виникнення можливих конфліктних ситуації, латентних конфліктів, схем відмивання коштів, процесів в кримінальному середовищі – на всіх рівнях відповідальності;

- виявлення латентних схем, механізмів, конфліктів кримінальної спрямованості в соціально-економічній діяльності суб'єктів господарювання; виявлення процесів, що можуть вплинути на дестабілізацію криміногенної ситуації; виявлення системності у виникненні негативних процесів, розуміння базису їх існування на аналізі діючих законів та нормативних актів; виявлення схем відмивання коштів, здобутих незаконнім шляхом, суб'єктів підприємницької діяльності, підприємств державної власності, установ бюджетної сфері, які в них задіяні;

- розкриття та профілактика злочинів; координація підрозділів у розкритті серійних злочинів, або злочинів, вчинених стійкими злочинними групами з ознаками організованості; розробка методичних рекомендацій по розкриттю злочинів;

- своєчасне інформування керівництва про оперативну обстановку в регіоні по напрямках роботи, територіях, стратегічно-важливих об'єктах; надання керівництву своєчасної та об'єктивної інформації про володіння ситуацією у районі чи по напрямку роботи керівниками територіальних та структурних підрозділів; стратегічне прогнозування та підтримка прийняття тактичних рішень керівництвом на всіх рівнях відповідальності, забезпечення оперативного аналізу процесів за наслідками прийнятих рішень.

Визначення використовуваної платформи залежить від повноти виконуючих функцій різноманітних кримінальних аналізів, можливості адаптації до системи обліку даних (ІП НПУ МВС України), до мови, кошторису робіт щодо конвертації та адаптації, кошторису самої платформи.