УДК 343.1:[351.74:161.111](100) DOI: https://doi.org/10.32631/pb.2021.4.07

ВОЛОДИМИР МИХАЙЛОВИЧ СТРУКОВ,
кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ,
кафедра кібербезпеки та DATA-технологій;
https://orcid.org/0000-0003-4722-3159,
e-mail: struk_vm@ukr.net;

ДМИТРО ЮРІЙОВИЧ УЗЛОВ,
кандидат технічних наук,
Харківський національний університет радіоелектроніки,
кафедра штучного інтелекту;
https://orcid.org/0000-0003-3308-424X,
e-mail: dmytro.uzlov@nure.ua;

ЮРІЙ ВАЛЕРІЙОВИЧ ГНУСОВ,
кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ,
кафедра кібербезпеки та DATA-технологій;
https://orcid.org/0000-0002-9017-9635,
e-mail: duke6969@i.ua

ІНСТРУМЕНТАЛЬНІ ІНТЕЛЕКТУАЛЬНІ ПЛАТФОРМИ ДЛЯ КРИМІНАЛЬНОГО АНАЛІЗУ

Метою цієї роботи є порівняльний аналіз найбільш відомих зарубіжних і вітчизняних платформ інтелектуального аналізу даних для кримінального аналізу. На основі огляду діючих платформ кримінального аналізу і практичного досвіду сформульовано перелік функціональних складових аналітичних інструментів кримінального аналітика, які наразі застосовуються в різноманітних інтелектуальних платформах кримінального аналізу та у практичній діяльності правоохоронних органів. Виокремлено типові особливості інтелектуального програмного забезпечення правоохоронних органів у цілому та кримінального аналізу зокрема. Зроблено порівняльний огляд функціоналу аналітичних інструментів інтелектуального програмного забезпечення правоохоронних органів зарубіжних країн та вітчизняних розробок, на підставі якого сформульовано вимоги до функціональних характеристик інтелектуальних систем автоматизованого аналізу для потреб кримінального аналізу.

Ключові слова: *кримінальний аналіз, аналітичний інструмент, інтелектуальна платформа, функціональна складова, профайлінг, аналіз зав'язків.*

Оглядова стаття

ВСТУП. Найбільш характерною і впливовою особливістю сучасності є епоха Четвертої промислової революції, яку зазнає людство. У контексті досліджуваної теми найважливішими її особливостями є такі.

1. Обговорюваний останніми роками фахівцями «інформаційний вибух» не спадає, а навпаки, набирає обертів; генератором і водночас інфраструктурою цього явища на сучасному етапі є інтернет речей – IoT (Internet of Thingths), середовище «розумних» пристроїв, які постійно генерують телеметричну інформацію і взаємодіють між собою. У загальному випадку терміналами мереж IoT можна вважати і різноманітні гаджети – смартфони, планшети, відеокамери, розумні годинники тощо. Водночас із усього океану інформації, за оцінками фахівців, менше 1 % піддається аналізу. Чому так відбувається? По-перше, як зазначалося, лавиноподібно зростає обсяг доступної інформації. По-друге, змінюється структура даних, які обробляються автоматизованими інформаційними системами у правоохоронних органах: якщо раніше це були зазвичай регулярні структуровані дані (в більшості випадків – реляційні бази даних), то зараз частка таких даних стрімко зменшується, а високими темпами зростає частка неструктурованих даних, які містять текстовий і відео контент. По-третє, зараз в арсеналі правоохоронних органів украй мало інструментальних систем, функціонал яких дає змогу

ефективно обробляти дані такого типу й у відповідних обсягах.

2. Темпи розвитку технологій, які є драйверами Четвертої промислової революції, характеризується зростаючою швидкістю; це означає, що завтра можливості, які сьогодні вважаються фантастикою, будуть буденним явищем, як це сталося, наприклад, із смартфонами.

3. Вартість високотехнологічних інструментів стрімко зменшується, і вони стають доступними не лише фінансово потужним державним і комерційним структурам, але й пересічним громадянам. Так, на розроблення технології автоматичної обробки (виявлення і розпізнавання) облич у реальному часі у 2017 році ФБР виділило близько 2 мільярдів доларів, а в 2020 році в Інтернеті вже можна було замовити квартирний пристрій, який використовує таку технологію, за 120 доларів. Замовити в Інтернеті спори смертоносної хвороби (наприклад віспи, як це зробили журналісти відомого прес агентства Guardian) і завантажити її в сільськогосподарський дрон замість хімікатів з метою «обробки» якогось мегаполіса наразі є цілком доступною можливістю для пересічного громадянина. Застосування таких потужних високотехнологічних інструментів кримінальними елементами у злочинних цілях здатне завдати непоправної шкоди суспільству. Водночас вартість розроблення високоефективних інструментальних систем протидії високотехнологічним злочинам, їх упровадження та супроводу зростає.

Унаслідок цих обставин правоохоронні структури вимушені переходити від реактивної до предикативної моделі діяльності, коли успіхом уважається не успішне розслідування скоєних злочинів, а їх виявлення та розкриття на етапі підготовки. Зараз у середовищі правоохоронних органів розвинених країн це питання стоїть поряд із 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 оброблятимемо відеопотоки від них у ручному або навіть у півавтоматичному режимі, це буде майже марнуванням грошей.

Зараз у світі існує досить невелика кількість високотехнологічних інструментальних аналітичних платформ, які використовують найсучасніші технології обробки даних – Data Mining, Web Mining, штучний інтелект тощо. Накопичено певний досвід їх застосування у прогнозуванні, профілактиці, запобіганні та розслідуванні злочинів. Цей досвід є вкрай цінним, оскільки ці платформи є першопрохідниками в цьому напрямі. Виявлені під час їх експлуатації позитивні моменти, недоліки і проблеми дають можливість узагальнити їх та врахувати під час розроблення і впровадження аналогічних платформ.

Перелічені вище обставини обумовлюють актуальність проведення досліджень ефективного застосування такого типу платформ у діяльності правоохоронних органів у контексті реалізації предикативної моделі.

ОГЛЯД ЛІТЕРАТУРИ. У зарубіжних країнах вивчення досліджуваного питання було здійснено в роботах Дж. Мена, К. Вестфаля (2009), Р. Боба (2001). Крім того, питання внормування інформаційно-аналітичної обробки інформації правоохоронними органами та кримінальної аналітики неодноразово порушувалося в роботах М. Баззеля, Р. Кларка, К. Козери, В. Мітчела, Дж. Ретклiфа, С. Стренга та ін. Серед вітчизняних фахівців досліджуване питання опрацьовували С. Албул (2016), О. Богінський, О. Бочковий, М. Грібов, Є. Жицький, В. Захаров, К. Ісмайлов (2019), О. Користін (2016), О. Манжай, В. Некрасов (2019), Д. Никифорчук, Ю. Орлов, В. Струков (2020), Д. Узлов (2018), А. Ханькевич, В. Школьніков (2020), працівники профільних департаментів Національної поліції України та інші автори.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. *Метою* цієї статті є порівняльний аналіз найбільш відомих зарубіжних і вітчизняних платформ інтелектуального аналізу даних для кримінального аналізу. *Завданнями* статті є формування переліку функціональних компонентів автоматизованих платформ інтелектуального аналізу даних, виокремлення з них типових компонентів та окреслення напрямів їх ефективного застосування у практичній діяльності правоохоронних органів.

Наукова новизна дослідження полягає в тому, що у статті здійснено порівняльний аналіз найбільш відомих зарубіжних і вітчизняних автоматизованих платформ інтелектуального аналізу даних для кримінального аналізу, сформовано перелік функціональних компонентів таких платформ, виокремлено з них типові компоненти й окреслено напрями їх ефективного застосування у практичній діяльності правоохоронних органів.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. У процесі виконання роботи з урахуванням її оглядового характеру було застосовано певні методологічні інструментарії. За допомогою наукового методу системного аналізу було

виокремлено та проаналізовано складові компоненти досліджених аналітичних платформ. Використання порівняльно-правового методу дало змогу порівняти можливості оглянутих систем і платформ, а також дослідити досвід застосування інтелектуальних платформ кримінальної аналітики у зарубіжних країнах. Із застосуванням індуктивного методу (синтезу) було розроблено рекомендації щодо вибору інтелектуальних платформ кримінального аналізу.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ

1. Огляд функціоналу аналітичних інструментів для правоохоронних органів

Під аналітичним інструментом у контексті цієї роботи будемо розуміти методику, технічний засіб або програмний продукт (чи модуль), за допомогою яких виконується певна аналітична функція (операція). Прикладами таких аналітичних функцій можуть бути: 1) моніторинг відкритого кіберпростору з метою виявлення і фіксації кримінально-значущих 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 тощо. Інструменти аналітика допомагають організувати, інтегрувати, порівнювати, співвідносити та ілюструвати сукупність необробленої інформації. Жоден з інструментів аналітика не дасть дієвого результату самостійно; кожен додає компонент нових знань або принаймні нового розуміння про дані, які в сукупності сприяють аналізу, визначенню нових вимог до розвідки недостатніх даних. Фактичний аналіз спирається на навички критичного мислення аналітика, а також на його здатність інтегрувати результати різноманітних методологій та інструментальних засобів в узагальнений дієвий продукт аналітики. Ці продукти можуть містити 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 угруповання.

Аналітику треба розуміти призначення та функціональні можливості різних доступних аналітичних інструментів і типів інформації, яку вони надають. На підставі практичного досвіду й опису доступних інтелектуальних платформ кримінального аналізу даних сформуємо такий (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 і часу скоєння, задіяні державні та комерційні структури, особи, засоби переміщення тощо; інциденти відображаються у вигляді блок-схеми, щоб допомогти зрозуміти розвиток подій (рис. 1);

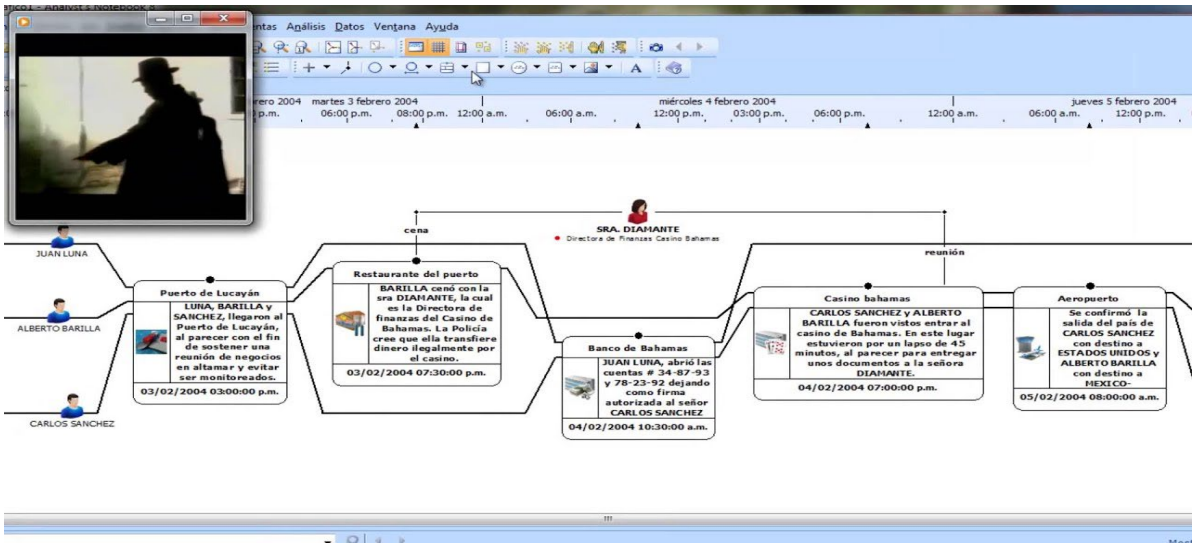

Рис. 1

– ***асоціаційна матриця*** – ця матриця допомагає зіставляти два або більше факторів у злочинній діяльності, фіксуючи частоту, з якою одночасно виникають певні фактори (наприклад особи, організації, номери телефонів, адреси та подібні до них змінні), щоб виділити корелюючі фактори, які відіграють важливу роль у діяльності злочинців та усувають фактори, які не мають взаємозв'язку; ці фактори можуть бути схожими, наприклад співвідношення серії телефонних номерів, а 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 (рис. 2);

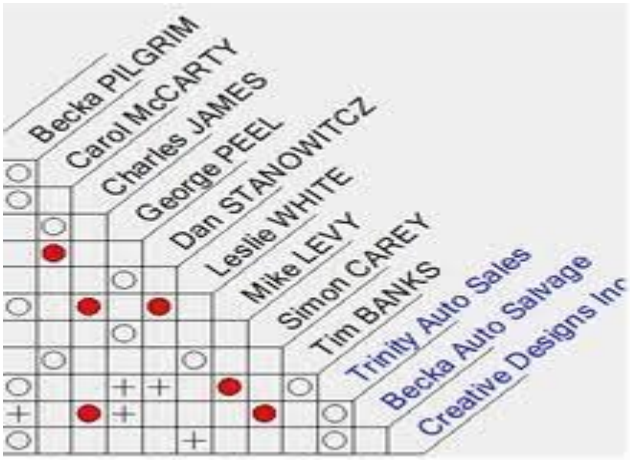

Рис. 2

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

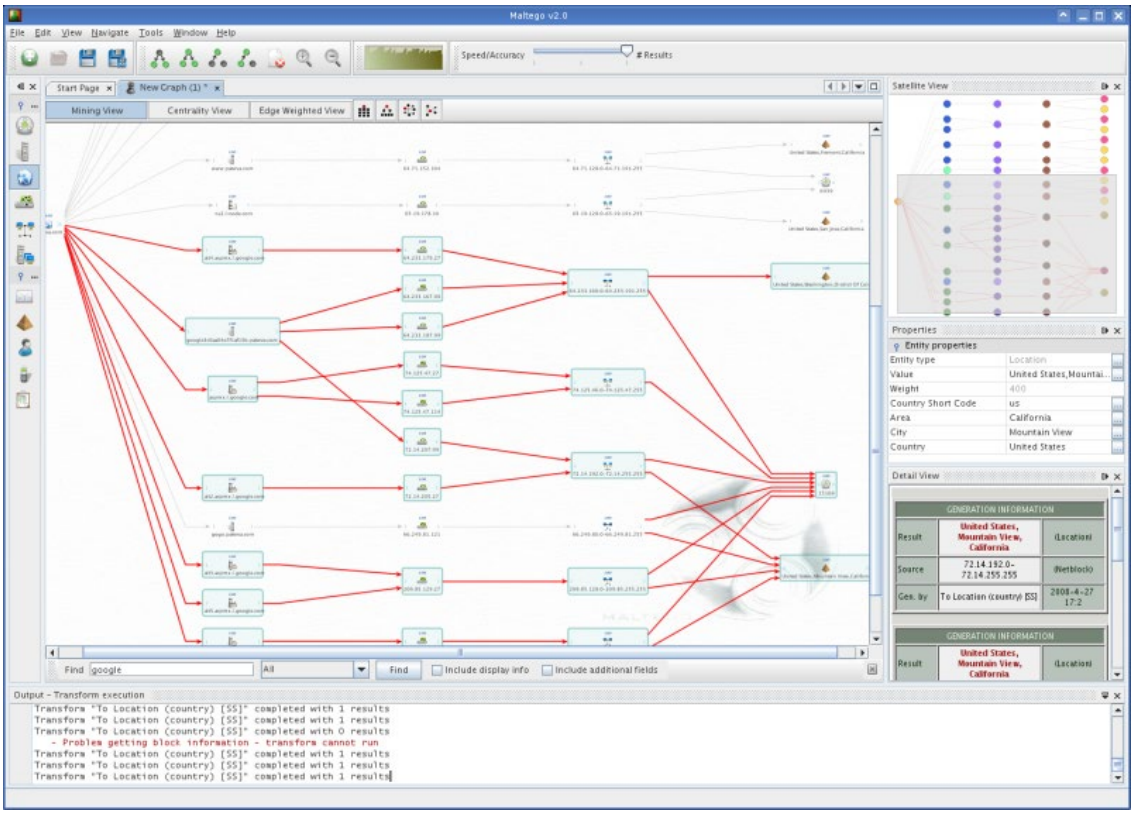

Рис. 3

– ***аналіз комунікаційного трафіку*** – важливу інформацію можна отримати в результаті аналізу трафіку телефонів, обміну текстовими повідомленнями та електронною поштою; визначивши, з ким здійснюють зв'язок, частоту зв'язку, їх походження і призначення, тривалість зв'язку та наявність додатків до електронних листів, аналіз може надати значне підтвердження і докази злочинності; хоча зміст комунікацій, очевидно, надаватиме важливу інформацію, аналіз комунікаційного трафіку також може бути цінним (рис. 4);

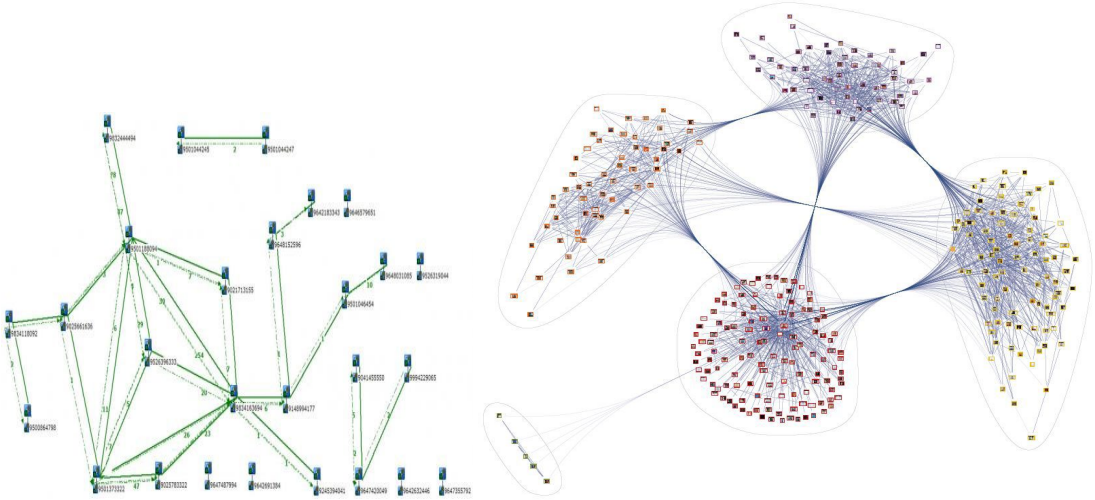

Рис. 4

– ***аналіз структури злочинності*** – загальний термін для низки суміжних дисциплін, таких як ідентифікація злочинів або серій інцидентів, аналіз тенденцій злочинності, аналіз гарячих точок та загальний аналіз профілю, і може включати картографування (рис. 5);

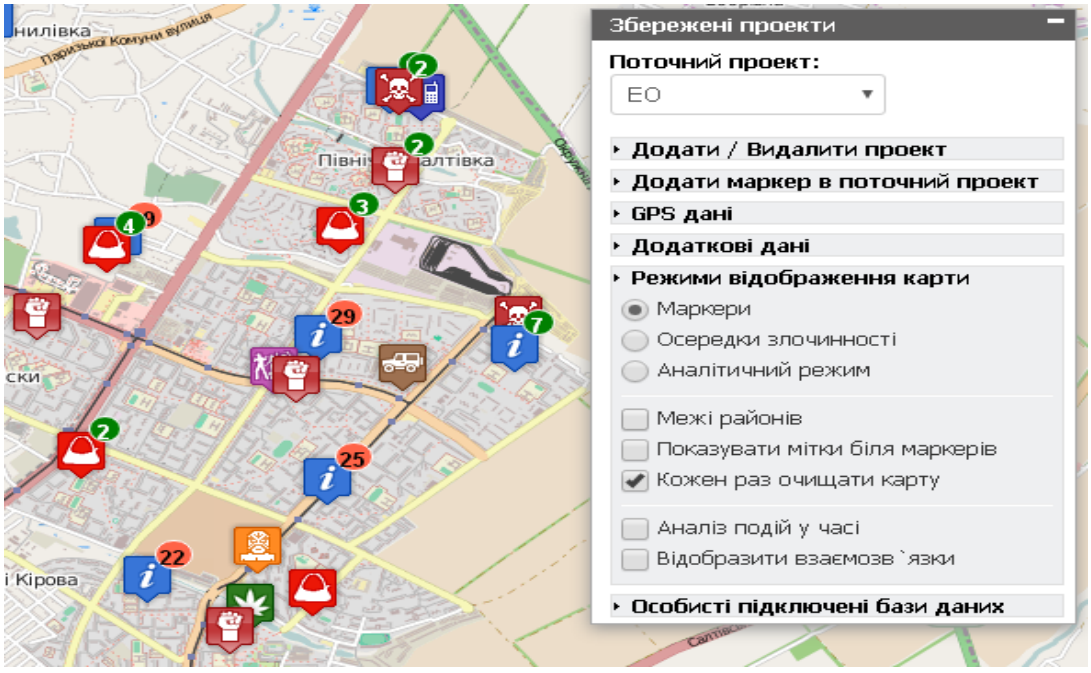

Рис. 5

– ***профайлінг злочинця*** – містить детальний аналіз поведінкового профілю злочинця, його кримінальних навичок, загальну інформацію, механізми та характер скоєних злочинів тощо; аналіз, який охоплює цілу низку аналітичних методів для опису злочинців, їх злочинної діяльності, способу життя, асоціацій, ризику, який вони становлять, та їх сильних і

слабких сторін, щоб зосередити увагу на розслідуванні, націленому на них; профілі також можуть зосереджуватися на жертвах та уразливих особах (рис. 6);

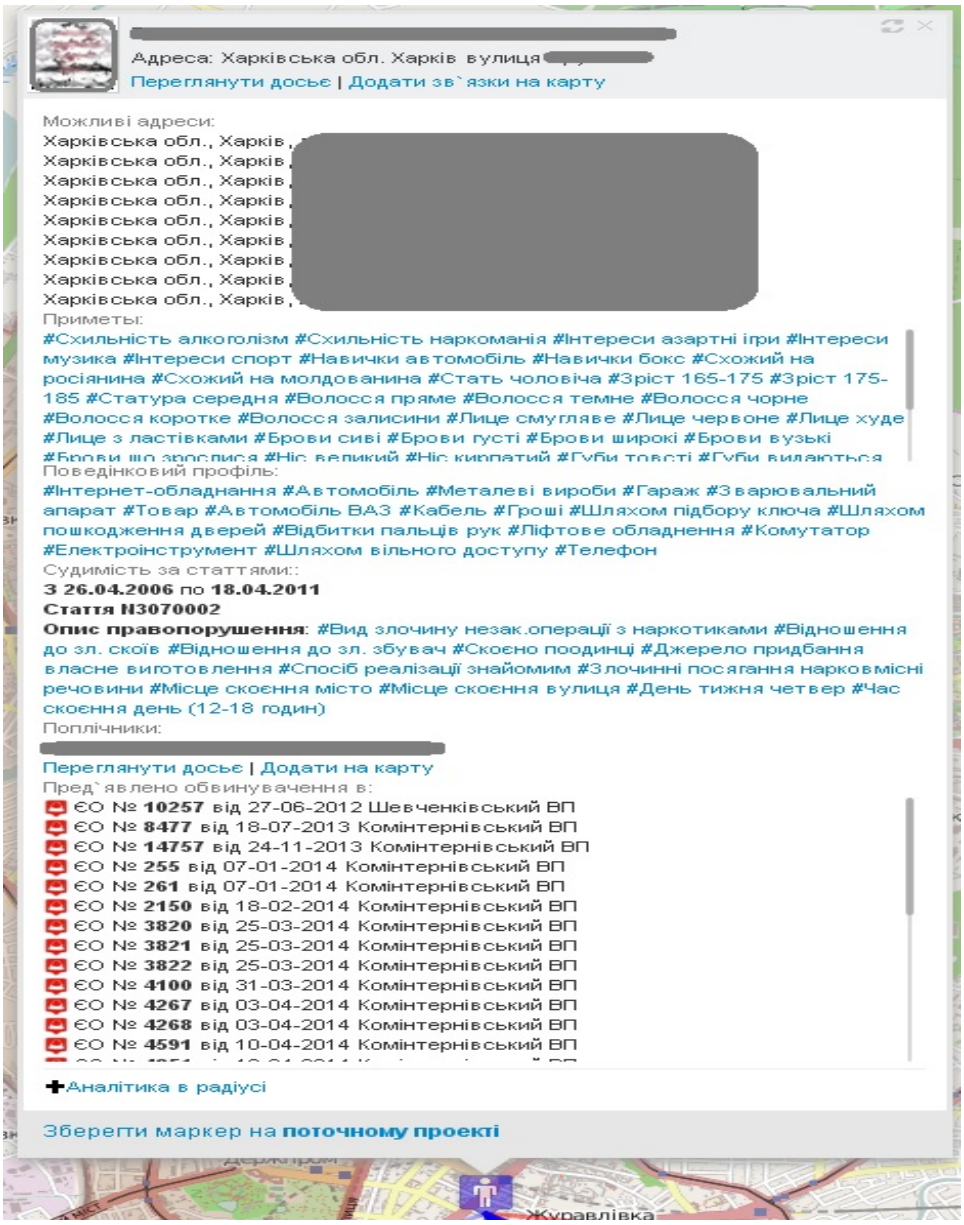

Рис. 6

– ***кримінальний профайлінг*** – такі профілі містять детальний аналіз об'єктивної складової злочину, а саме механізму скоєння, специфічні навички, що були використані, методи й 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, відносин і діяльності, оскільки вони можуть впливати на злочинність;

– ***аналіз потоку подій*** – діаграми, що забезпечують візуальне зображення низки 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 (рис. 7);

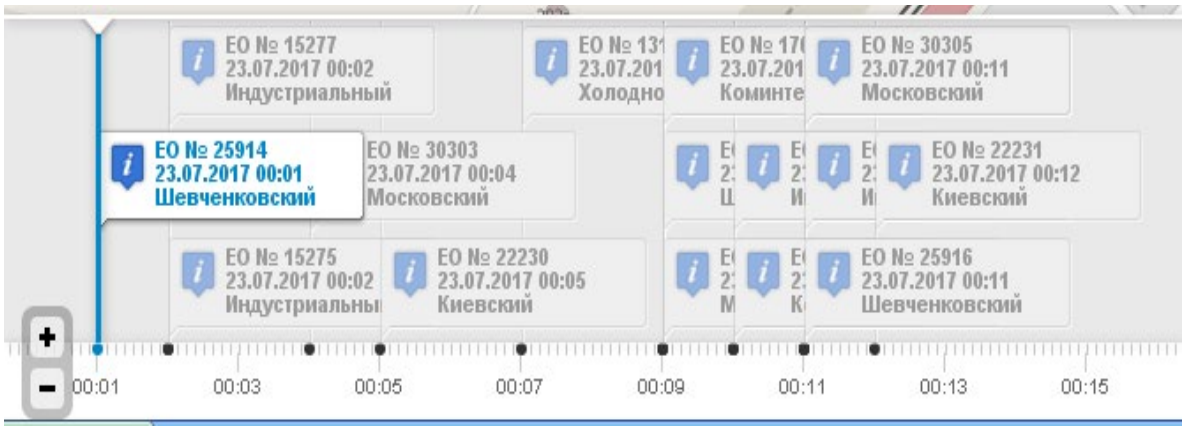

Рис. 7

– ***фінансовий аналіз*** – існує безліч методів фінансового аналізу, які спільно прагнуть зіставити різноманітні фінансові операції, включно з характером операцій, залучені сторони, походження, посередництво і призначення транзакцій та порівняльний аналіз доходів і витрат; спільною 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;

– ***перевірка гіпотез*** – аналітик висловлює гіпотезу про зв'язки людей та організацій у злочинному утворенні, необхідні операції для функціонування утворення та важливі товари або ресурси, потрібні для успіху утворення; 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 та (в ідеалі) визначення кримінальної відповідальності учасників;

– ***аналіз зв'язків*** – діаграма, яка ідентифікує всіх підтверджених і підозрюваних осіб та організації у злочинному утворенні та ілюструє їх взаємозв'язок між собою (рис. 8);

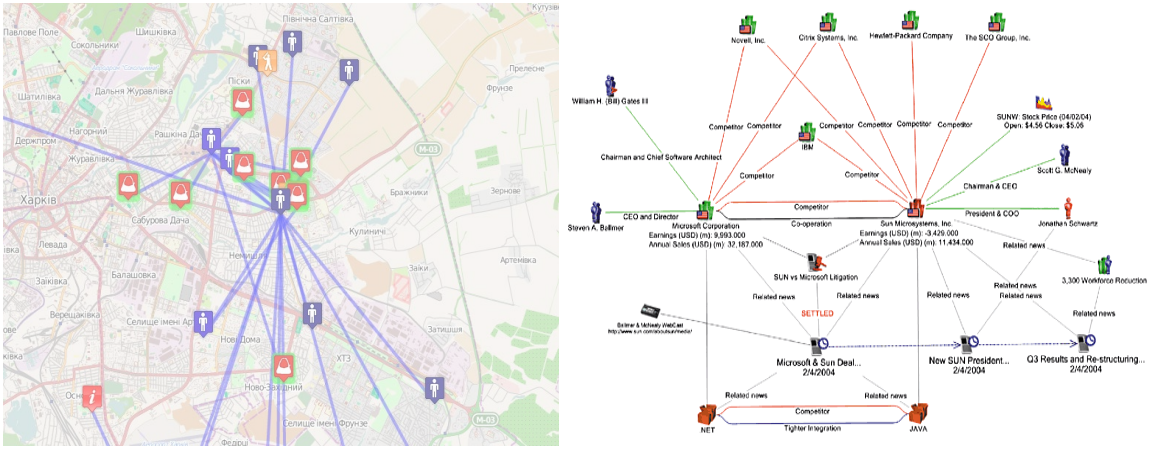

Рис. 8

– ***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 описує не лише зв'язки між людьми, які утворюють злочинні мережі, але й значення зв'язків і ролі, яку виконують окремі особи, а також сильні та слабкі сторони злочинної організації (рис. 9);

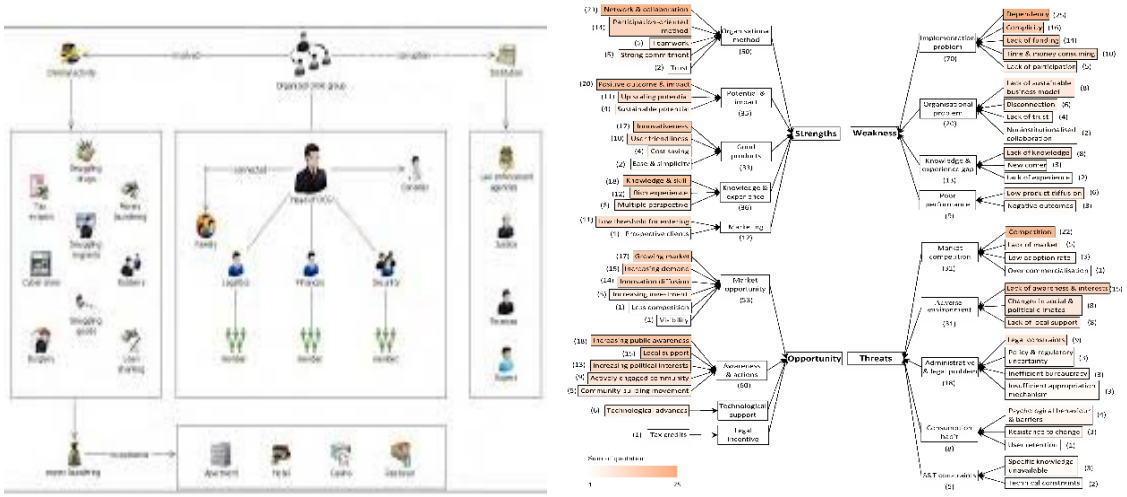

Рис. 9

– ***оцінка оперативних можливостей*** – такий аналіз оцінює перекриття джерелами інформації, щоб зберегти фокусування операції на попередньо узгоджені цілі, особливо в разі значного плану збору розвідувальних даних або іншої масштабної операції;

– ***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 має своєю метою виявлення явних або прихованих ознак скоєних злочинів або тих, що плануються, на основі 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 тощо; 2) неструктуровані дані – текстові дані, графічні файли, відео- та аудіо- файли; дані із соцмереж, мессенджерів, IoT тощо. 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; 2) такі, що виявляють сховані, непрямі ознаки на основі так званих «слабких сигналів» шляхом побудови системи спеціальних індикаторів (Ларина, Овчинский, 2018).

2. Особливості і порівняльний огляд наявних інструментальних систем для вирішення завдань правоохоронних органів щодо кримінальної аналітики

Інструментальні платформи з програмним забезпеченням правоохоронних органів розробляються під конкретну систему кримінальних обліків конкретної країни і цілком відповідають структурам інформаційно-пошукових систем, у яких накопичується інформація про протиправні інциденти, осіб, об'єкти тощо. Самі інциденти кваліфікуються згідно з чинним кримінальним або адміністративним законодавством країни.

Разом із цим, зараз для забезпечення потреб правоохоронних органів існують міжнародні стандарти і методи інтелектуального аналізу, що застосовуються для розслідування злочинів, виявлення кримінальних подій та різноманітних видів кримінального аналізу, зокрема в межах моделі ILP (Intelligence Led Policing) – поліцейської діяльності, керованої аналітикою, та інших моделей предикативної поліцейської діяльності.

Нижче подано огляд найбільш відомих аналітичних платформ, які використовуються у правоохоронних органах різних країн.

Crime Center (Shotspotter). Запатентована система датчиків, алгоритмів та штучного інтелекту, яка точно виявляє, знаходить і попереджає поліцію про стрілянину (Струков та ін., 2020). Є складовою частиною RTCC – Real-time crime center (ситуаційно-аналітичні центри реального часу) поліції США. Головним 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 стріляниною або вибухом. Може інтегруватися в інші ГІС-платформи правоохоронних органів (рис. 10).

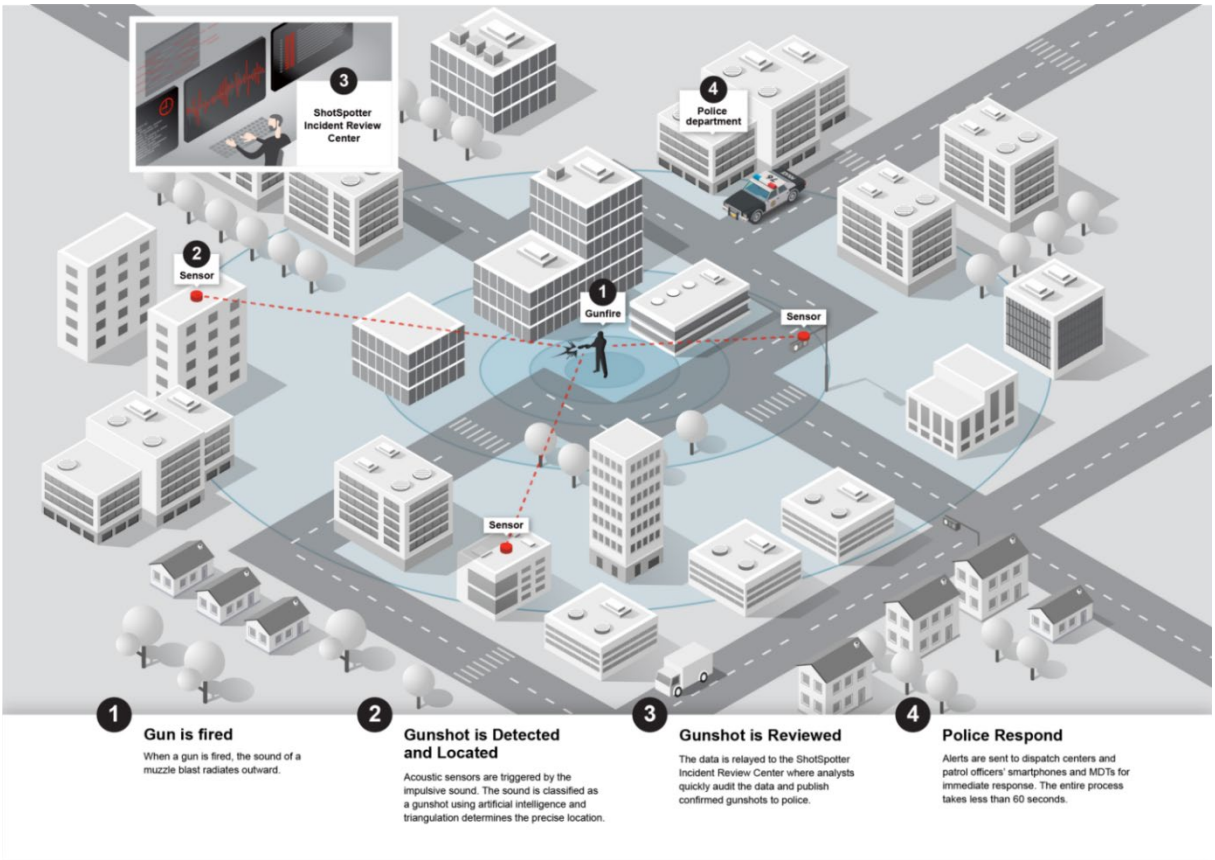

Рис. 10

Maltego. Пропонується як інструмент для графічного аналізу інтернет-посилань, пошукового інструменту у відкритих джерелах Інтернету в реальному часі та збору інформації, а також подання цієї інформації візуально на основі графів, завдяки чому шаблони та зв'язки між різними джерелами та відповідною інформацією легко ідентифікуються (Узлов, Струков, 2017).

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. 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 потрібні їх доволі важка конвертація та розроблення логістичної моделі й моделі асоціативних правил. Застосовується здебільшого для OSINT (рис. 11).

IBM i2 Analyst's Notebook. Це візуальне аналітичне середовище, яке дає змогу максимально ефективно використовувати величезні обсяги інформації, накопичені державними службами та підприємствами. Завдяки інтуїтивно зрозумілому інтерфейсу з урахуванням контексту воно дає можливість аналітикам швидко зіставляти, аналізувати і наочно уявляти 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 (Корнейко, Школьніков, Овсянюк, 2020).

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;

– поліпшене розуміння структури, ієрархії і способів дій злочинних, терористичних і шахрайських організацій;

– спрощення обміну складними даними, що дає змогу ухвалювати своєчасні й точні оперативні рішення;

– можливість отримання вигоди завдяки швидкому впровадженню, яке забезпечує швидке зростання продуктивності, завдяки надійним рішенням для візуальної аналітики (рис. 12).

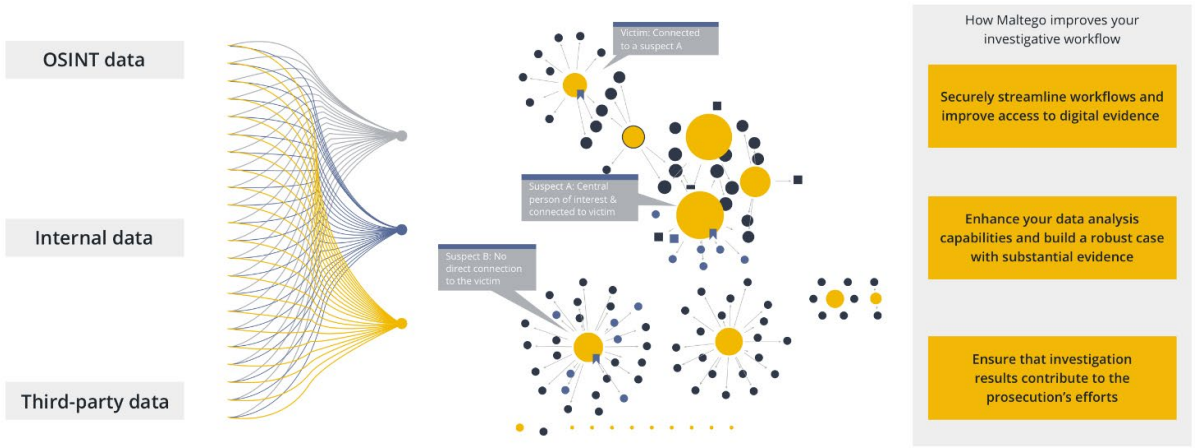

Рис. 11

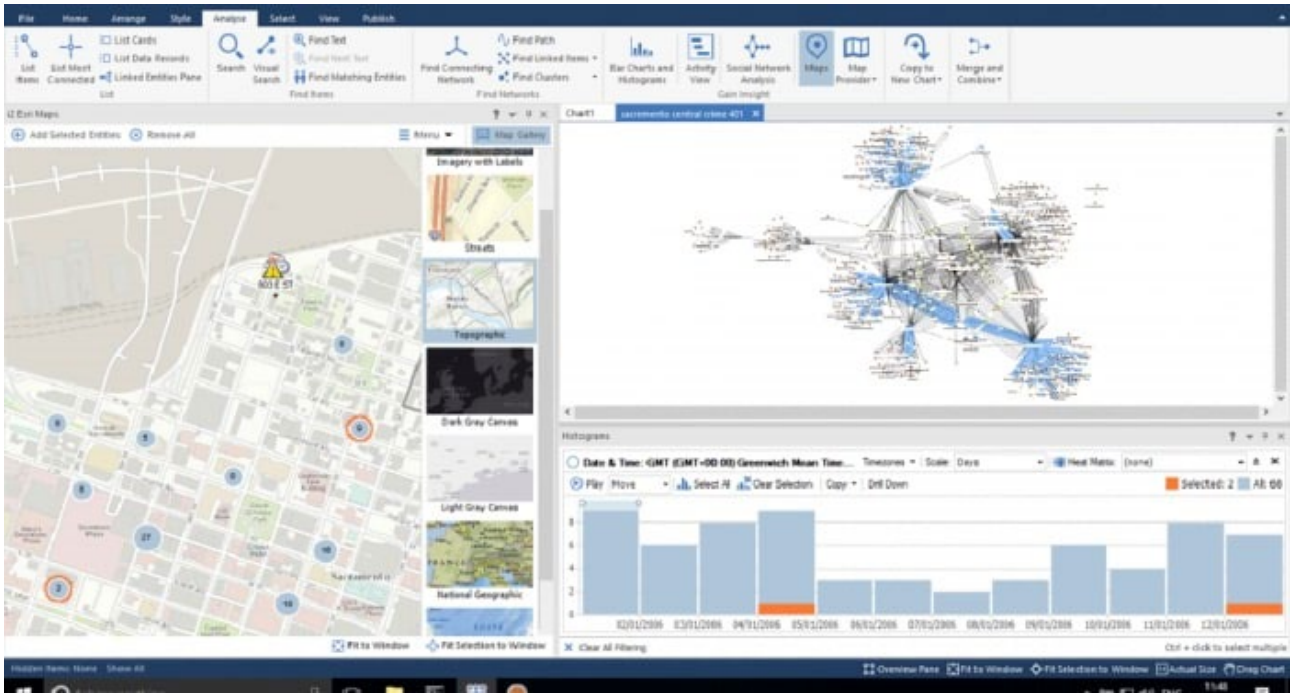

Рис. 12

IBM i2 Analyst's Notebook є максимально розкрученою серед аналітиків системою, яка була започаткована на початку 2000 років, має кілька версій. Систему орієнтовано на побудову різноманітних схем, але потрібна велика кількість операцій ручної обробки даних, бо вона 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 і є коштовною.

Command Central Aware Motorola – це набір інструментів, який містить у собі ГІС як платформу для відображення всієї інформації та візуального аналізу, інструменти інтелектуальної

обробки та керування відеопотоками 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 ухвалити перші управлінські рішення. У разі рішення розміщує відповідну інформацію на одному дисплеї або групі дисплеїв і переміщує інші джерела у фоновий режим, де це не відвертає увагу від поточного завдання.

Інтелектуальне програмне забезпечення для моніторингу може виявляти контрольовані шаблони або сценарії у відеопотоках, що допомагає виявляти протиправні дії. Людина-оператор може не помітити, що рюкзак залишився притуленим до стіни, яка прилягає до входу в центр громадського транспорту, але штучний інтелект комп'ютера це зробить. Подібним чином програмне забезпечення «бачитиме» людей, які рухаються проти потоку руху або йдуть нехарактерно повільно чи швидко, вказуючи на те, що їх поведінка відрізняється від такої в тих, хто їх оточує. Транспортний засіб, що в'їжджає у зону, зарезервовану для пішоходів, негайно буде позначений, а оператора буде попереджено 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 дає можливість 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 наявні системи управління справами, системи управління доказами, арештами, судовими даними, іншими даними про злочини й даними автоматизованої диспетчеризації (CAD), а також має підключення до федеральних сховищ, оперативних баз і даних з державних сховищ. Уміє обробляти як структуровані та слабоструктуровані, так і неструктуровані дані, такі як сховища документів та електронні листи. Palantir – наймасштабніший продукт з капіталізацією більш ніж 500 млн доларів США. Розроблявся для потреб федеральних агентств і має багатий арсенал інструментів штучного інтелекту для роботи з Big Data і Big Stream Data. Працює з гетерогенними даними. Частково використовується Europol (Струков та ін., 2020).

SmartCOP. Інтелектуальна платформа SmartCOP для відділів поліції має повністю інтегровану лінійку програмних продуктів, що охоплює 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 у реальному часі для обробки дзвінків, диспетчеризації, мобільних даних, записів та управління інформацією для оптимізації ефективності операцій. SmartCOP пропонує багатофункціональне рішення, яке забезпечує гнучкість та охоплює інтегровану картографію (використовується ESRI), картки запуску AVL та пов'язані історичні дані. SmartCOP є простим у використанні та дуже легко налаштовується. Платформа будувалася під національну систему обміну інформацією США (National Information Exchange Model). На європейському ринку не представлена.

ePOOLICE – це система раннього виявлення загроз із боку організованих злочинних угруповань (далі – ОЗУ) з використанням методів обчислювального сканування і розвідувальних систем (Ларина, Овчинский, 2018; Струков та ін., 2020). Проєкт спільно фінансувався країнами ЄС і Європейським Союзом у межах Сьомої Рамкової програми досліджень і розробок (FR7). Програма FR7-SEC-2012-1 розробляється в межах загальноєвропейської програми «Безпека і суспільство», її розділів «Форсайт», «Сценарії» та «Безпека». Мета проєкту полягає у створенні ефективної загальноєвропейської системи середовищного сканування для попередження злочинів, що готуються, діючих і виникаючих ОЗУ (Бурдін, 2020, с. 16). Підсумком реалізації проєкту ePOOLICE став працездатний прототип ефективної системи раннього попередження загроз, що виникають із боку ОЗУ. Згідно з рішенням ЄС проєкт передбачає:

– проведення науково-технологічних досліджень з метою розроблення ефективних систем сканування, аналізу і прогнозування загроз із боку ОЗУ, при цьому сканування має здійснюватися в загальнодоступному Інтернеті, соціальних мережах і медіа, а також у новому інформаційному середовищі, що дедалі більше фрагментується, включно з комунікаційними мережами месенджерів, інтернетом грошей та інтернетом речей;

– виявлення ознак, індикаторів або індексів, що описують ранні або «слабкі» сигнали загроз, що формуються 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.

Як ключові аспекти прототипу системи можна виділити:

– управління інформацією і знаннями в умовах середовищної невизначеності та інформаційної неповноти, що ґрунтується на розпізнаванні патернів, що сигналізують про загрози, а також активності ОЗУ;

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

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

– використання методології динамічної складності та спеціальних методів подання складних явищ і процесів у простих таблицях і візуальних образах, що дозволяють конденсувати інформацію;

– дотримання міжнародних і певних країн правових, етичних і режимних вимог до таких систем.

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

Оскільки отримання достовірних даних про внутрішні процеси в конкретних ОЗУ є не лише вельми складним, але і вкрай коштовним, програма здійснює розпізнавання загроз ОЗУ шляхом моніторингу середовища їх активності. У межах цього моніторингу не лише виділяються вразливі точки локації і сфери можливої активності ОЗУ, але й виявляються індикатори, події тощо у зовнішньому середовищі, які є діагностичними ознаками підготовки ОЗУ до злочинів.

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

Зараз ГУНП в Харківській області провело 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 (Узлов та ін., 2018). Комплекс має назву «RICAS». Згідно зі Звітом про оцінку потреб щодо впровадження моделі поліцейської діяльності, керованої аналітикою (Intelligence-Led Policing/ ILP) в Національній поліції України від грудня 2016 р., проведеним EUAM та UNDP, «систему можна використовувати на державному рівні в якості платформи для аналітичного супроводу та підтримки процесу прийняття рішень». У процесі експлуатації комплексу підтверджується його гнучкість та спроможність інтегрувати будь-які дані з можливістю часового та просторового аналізу їх зв'язків між собою. Комплекс розроблено із застосуванням найновіших технологій у галузі 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 є досить значними (Узлов та ін., 2015). Система дає змогу відшукати приховані зв'язки між заданими об'єктами та відображувати знайдені зв'язки як у вигляді геоінформації, так і у вигляді хронологічної стрічки подій. Також упроваджується модуль аналізу неструктурованої інформації, що надає можливість здійснювати пошук за аналогією або за заданими критеріями в режимі реального часу фактично у будь-яких текстових масивах.

RICAS побудовано на ґрунті таких припущень:

– будь-яка кримінальна інформація містить дані про час та місце скоєння, що можуть бути відображені не лише у вигляді текстового опису (населений пункт, вулиця, будинок), а й у формі географічних координат і 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 в разі збільшення масштабів даних та візуалізації даних в єдиному інформаційному просторі (на мапі) з урахуванням розвитку в часі.

RICAS не є відокремленою системою, її побудовано як інтелектуальний інструмент аналізу наявних баз даних, що дає змогу не лише виконувати запити й отримувати результати в

текстовому вигляді, а й проводити пошук за неочевидними критеріями, аналізувати перетини зв'язків та ступінь близькості об'єктів, осіб і подій з одночасною наочною візуалізацією результатів аналізу у просторі та часі. Система оперує засобами математичного моделювання та інтелектуального семантичного аналізу, наочного темпорального аналізу, аналізу поведінкового профілю та аналізу прихованих зв'язків. Для уніфікації пошукових функцій та швидкої побудови поведінкового профілю використовується алгоритм «тегування» (побудови ключових реквізитів), а також антиципаційний алгоритм (схема передбачення) – коли мета пошуку відома заздалегідь і треба лише встановити зв'язки. Семантичне ядро системи дає змогу виконувати складні запити, що містять статичні й динамічні складові: обмеження в часі, методу скоєння злочину, дислокації об'єктів та інші.

Ураховуючи автоматизацію процесу обробки інформації та побудови новітніх реквізитів (зв'язків і перетинів, класифікацію та кластеризацію) в режимі реального часу, завдяки збільшенню обсягів інформаційних джерел і підключенню до хмарного сервісу RICAS не лише інформаційних систем органів внутрішніх справ, а й інших відкритих державних реєстрів, систем обліку осіб, речей і подій кримінальний аналіз буде значно точнішим і повнішим для формування доказової бази в конкретних провадженнях, а прогнозування стану криміногенної обстановки дасть змогу ефективніше проводити профілактичні заходи та попереджувати злочинні прояви з більшою долею вірогідності.

Аналітичні можливості розглянутих інтелектуальних платформ відображено 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 зв'язків Link Analysis			+	+	+	+	+	+
• Візуальна аналітика на картографії Crime Mapping		+	+	+	+	+		
• Демографічний / соціальний аналіз тенденцій			+	+	+	+		
• Мережевий аналіз			+	+	+	+	+	+
• Оцінка оперативних можливостей				+	+	+		+
• Аналіз результатів				+	+	+		
• Моніторинг доступного кіберпростору				+	+			
• Необхідність адаптації до ІП НПУ МВС України	Так	Так	Так	Так	Так	Ні	Так	Так

ВИСНОВКИ. У роботі подано огляд сучасних найбільш розвинених інтелектуальних платформ, які використовуються для потреб кримінального аналізу і відповідають сучасним вимогам до таких систем. Виконано їх порівняльний аналіз, виокремлено й узагальнено функціональні компоненти таких систем, що дає змогу на етапі вибору необхідної платформи формулювати вимоги до її функціонального наповнення. На підставі проведеного дослідження можна сформулювати такі вимоги до функціональних характеристик інтелектуальних систем автоматизованого аналізу для потреб кримінального аналізу: система має надавати співробітникам максимально повні результуючі дані для ефективного вирішення завдань правоохоронних органів за такими напрямами:

– постійний моніторинг соціально-економічної та криміногенної ситуації на різному рівні відповідальності, в різних сферах життєдіяльності регіонів, негативних процесів та їх впливу на соціально-економічну ситуацію з установленням 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 ситуацій, латентних конфліктів, схем відмивання коштів та процесів у кримінальному середовищі на всіх рівнях відповідальності;

– виявлення латентних схем, механізмів і 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 чинних законів та нормативних актів; виявлення схем відмивання коштів, здобутих незаконним шляхом, суб'єктів підприємницької діяльності, підприємств державної власності або установ бюджетної сфери, які в них задіяні;

– розкриття та профілактика злочинів; координація підрозділів у розкритті серійних злочинів або злочинів, учинених стійкими злочинними групами з ознаками організованості; розроблення методичних рекомендацій з розкриття злочинів;

– своєчасне інформування керівництва про оперативну обстановку в регіоні за напрямами роботи, територіями та стратегічно важливими об'єктами; надання керівниками територіальних і структурних підрозділів керівництву своєчасної та об'єктивної інформації про володіння ситуацією в районі чи за напрямом роботи; стратегічне прогнозування та підтримка ухвалення тактичних рішень керівництвом на всіх рівнях відповідальності, забезпечення оперативного аналізу процесів за наслідками ухвалених рішень.

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

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Бортник С. М. Перспективи розвитку аналітичних систем предикативної аналітики // Застосування інформаційних технологій у діяльності правоохоронних органів : матеріали круглого столу (м. Харків, 14 груд. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2020. С. 9–11.

2. Бурдін М. Ю. Розпізнавання осіб злочинців і терористів на базі нейронних мереж // Застосування інформаційних технологій у діяльності правоохоронних органів : матеріали круглого столу (м. Харків, 14 груд. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2020. С. 12–14.

3. Інформаційні технології у правоохоронній діяльності. Частина 1: Високотехнологічні тренди у правоохоронній сфері зарубіжних країн : навч. посіб. / В. М. Струков, Д. Ю. Узлов, Ю. В. Гнусов та ін. ; за заг. ред. В. М. Струкова ; Харків. нац. ун-т внутр. справ. Харква : Діса плюс, 2020. 276 с.

4. Ковтун І. В. Інформаційно-аналітична діяльність штабів органів внутрішніх справ у сфері розслідування кримінальних правопорушень. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2012. № 3. С. 520–528.

5. Корнейко О. В., Школьніков В. І., Овсянюк Д. І. Використання сучасних інформаційно-аналітичних технологій в діяльності центру кримінальної аналітики Національної академії внутрішніх справ // Інформаційні технології в освіті та практиці : матеріали Всеукр. наук.-практ. конф. (м. Львів, 18 груд. 2020 р.) / МВС України, Львів. держ. ун-т внутр. справ. Львів, 2020. С. 8–11.

6. Ларина О. С., Овчинский В. С. Искусственный интеллект. Большие данные. Преступность. М. : Книжный мир, 2018. 166 с.

7. Основи кримінального аналізу : підручник / А. М. Бабенко, О. М. Заєць, В. А. Некрасов та ін. ; за заг. ред. О. Є. Користіна. Одеса, 2019. 296 с.

8. Основи кримінального аналізу : посібник з елементами тренінгу / О. Є. Користін, С. В. Албул, А. В. Холостенко та ін. Одеса : ОДУВС, 2016. 112 с.

9. Прикладний кримінальний аналіз на базі інформаційно-аналітичної системи «RICAS»: Методичні рекомендації щодо аналітичної діяльності та кримінального аналізу на базі інформаційно-аналітичної системи «RICAS» / Д. Ю. Узлов, І. В. Дегтярьова, В. М. Струков та ін. Харків : Юрайт, 2018. 92 с.

10. Узлов Д. Ю., Струков В. М. Використання методів і технологій штучного інтелекту в кримінальному аналізі // Застосування інформаційних технологій в діяльності Національної поліції України : матеріали наук.-практ. семінару (м. Харків, 21 груд. 2018 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. С. 17–19.

11. Узлов Д. Ю., Струков В. М. Сучасні інструментальні засоби кримінального аналізу // Проблеми застосування інформаційних технологій правоохоронними структурами України та вищими навчальними закладами зі специфічними умовами навчання : зб. наук. ст. за матеріалами доп. Міжнар. наук.-практ. конф. (м. Львів, 22 груд. 2017 р.) / МВС України, Львів. держ. ун-т внутр. справ. Львів, 2017. С. 162–164.

12. Узлов Д. Ю., Струков В. М., Власов О. В. Використання інтелектуального аналізу даних у протидії інформаційній злочинності // Актуальні питання протидії кіберзлочинності та торгівлі людьми : матеріали Всеукр. наук.-практ. конф. (м. Харків, 23 листопада 2018 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. С. 325–328.

13. Узлов Д. Ю., Струков В. М., Власов О. В. Методологічний апарат аналітичної роботи в Національній поліції України // Застосування інформаційних технологій в діяльності Національної поліції України : матеріали наук.-практ. семінару (м. Харків, 21 груд. 2018 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. С. 64–66.

14. Узлов Д. Ю., Струков В. М., Григорович А. Б., Петрусенко А. И., Доскаленко С. И. Применение интеллектуальной системы криминального анализа в реальном времени (RICAS) для аналитического сопровождения оперативно-розыскной деятельности и досудебного расследования. *Право і безпека*. 2015. Вип. 2 (57). С. 132–139.

15. Швець Д. В. Стратегічні напрямки використання новітніх технологій цифрового світу у попередженні злочинів // Застосування інформаційних технологій у діяльності правоохоронних органів : матеріали круглого столу (м. Харків, 14 груд. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2020. С. 7–9.

16. Boba R. Introductory Guide to Crime Analysis and Mapping. Washington, 2001. 74 p.

17. Ismailov K. Y. Peculiarities of human rights and freedom while applying intelligence-led policing (ILP). *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. 2019. Spec. Iss. 1. Pp. 36–41.

18. Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies / U. S. Department of Justice Office of Community Oriented Policing Services. 2nd ed. Michigan, 2009. 465 p.

19. OSCE Guidebook. Intelligence-Led Policing / OSCE. Vienna, 2017.105 p.

20. S. Gwinn, Bruce C., Cooper J. P., Hick S. Exploring Crime Analysis: Readings on Essential Skills. 2nd ed. Kansas, 2019. 222 p.

21. Scott M. Problem-Oriented Policing: Reflections on the First 20 Years. Washington, 2000. 46 p.

22. Strukov V., Uzlov D. Web-based Protected Geoinformation System of Criminal Analysis (RICAS) for Analytical Support for Crimes Investigation // Problems of Infocommunications. Science and Technology : International Scientific-Practical Conference (Kharkiv, 10–13 October 2017). Kharkiv, 2017. Pp. 508–511.

23. Uzlov D., Popov S., Vlasov O., Bodyanskiy Y. Adaptive Matrix Model for a Crime Forecasting Task // Data Stream Mining & Processing : Third International Conference (Lviv, 21–25 August 2020). Lviv, 2020. Pp. 96–101.

24. Uzlov D., Strukov V., Vlasov O. Using Data Mining for Intelligence-Led Policing and Crime Analysis // Conference Problems of Infocommunications. Science and Technology : International Scientific-Practical Conference (Kharkiv, 9–12 October 2018). Kharkiv, 2018. Pp. 499–502.

25. Westphal C. Data Mining for Intelligence, Fraud and Criminal Detection. Advanced Analytic & Information Sharing Technologies. Boca Raton : CRC Press, 2009. 426 p.

Надійшла до редакції: 14.09.2021

СТРУКОВ В. М., УЗЛОВ Д. Ю., ГНУСОВ Ю. В. ИНСТРУМЕНТАЛЬНЫЕ ИНТЕЛЛЕКТУАЛЬНЫЕ ПЛАТФОРМЫ ДЛЯ УГОЛОВНОГО АНАЛИЗА

Целью данной работы является сравнительный анализ наиболее известных зарубежных и отечественных платформ интеллектуального анализа данных для криминального анализа. На основе обзора действующих платформ криминального анализа и практического опыта сформулирован перечень функциональных составляющих

аналитических инструментов криминального аналитика, которые в настоящее время применяются в различных интеллектуальных платформах криминального анализа и в практической деятельности правоохранительных органов. Выделены типичные особенности интеллектуального программного обеспечения правоохранительных органов в целом и криминального анализа в частности. Выполнен сравнительный обзор функционала аналитических инструментов интеллектуального программного обеспечения правоохранительных органов зарубежных стран и отечественных разработок, на основе которого сформулированы требования к функциональным характеристикам интеллектуальных систем автоматизированного анализа для нужд криминального анализа.

Ключевые слова: *криминальный анализ, аналитический инструмент, интеллектуальная платформа, функциональная составляющая, профайлинг, анализ связей.*

STRUKOV V. M., UZLOV D. YU., GNUSOV YU. V. INSTRUMENTAL INTELLIGENT PLATFORMS FOR CRIMINAL ANALYSIS

The aim of the work is a comparative analysis of the most well-known foreign and domestic intelligent data mining platforms for criminal analysis. The relevance of this work is due to the peculiarities of the Fourth Industrial Revolution, the processes of which are rapidly unfolding at the present stage and have a critical impact on all areas, including law enforcement. Such features include: 1) "information explosion", which is intensifying, 2) accelerating the pace of development of modern technologies; 3) the cost of high-tech tools, which is rapidly declining, and such tools become available to ordinary citizens (including criminals). The consequences of illegal actions of perpetrators with the use of modern high-tech tools are analyzed. It is determined that the consequences of such actions can be large-scale, forcing law enforcement agencies around the world to move from a reactive to a predicative model of activity. A fundamentally important condition for the implementation of the predicative model is the use of highly intelligent tools to prevent crime. An analytical review of the most modern intellectual platforms used for the needs of criminal analysis and meeting modern requirements for such systems is given. Based on the review of existing platforms of criminal analysis and practical experience, a list of functional components of analytical tools of criminal analyst, which are currently used in various intellectual platforms of criminal analysis and in the practice of law enforcement was formulated. Typical features of intelligent software of law enforcement agencies in general and criminal analysis in particular are highlighted. A comparative overview of the functionality of analytical tools of intelligent software of law enforcement agencies of foreign countries and domestic developments is given. Features of functional components of intellectual systems of criminal analytics are named. Based on the study, the requirements for the functional characteristics of intelligent systems of automated analysis for the needs of criminal analysis are formulated. Using the results of this study will provide an opportunity at the stage of choosing the necessary platform to formulate requirements for its functional content.

Key words: *criminal analysis, analytical tool, intelligent platform, functional component, profiling, connection analysis.*

Цитування (ДСТУ 8302:2015): Струков В. М., Узлов Д. Ю., Гнусов Ю. В. Інструментальні інтелектуальні платформи для кримінального аналізу. *Право і безпека*. 2021. № 4. С. 64–79. DOI: https://doi.org/10.32631/pb.2021.4.07.

Citation (APA): Strukov, V. M., Uzlov, D. Yu., & Gnusov, Yu. V. Instrumental intelligent platforms for criminal analysis. *Law and Safety, 4*(83), 64–79. https://doi.org/10.32631/pb.2021.4.07.