ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ МВС УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

РЕАЛІЗАЦІЯ ФІЛОСОФІЇ «INTELLIGENCE-LED POLICING» В СИСТЕМІ КРИМІНАЛЬНОГО АНАЛІЗУ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

МОНОГРАФІЯ

Видано за підтримки Консультативної місії ЄС в Україні

2024

УДК 351.741:(343:303.442.3)

Р-31

DOI: https://doi.org/10.36486/978-966-2310-66-5

Рекомендовано до друку:

вченою радою Державного науково-дослідного інституту МВС України

(протокол № 1 від 28 лютого 2024 року)

вченою радою Одеського державного університету внутрішніх справ

(протокол № 7 від 30 січня 2024 року)

Рецензенти:

Білоус В.Т. – доктор юридичних наук, професор, заслужений юрист України;

Корнієнко М.В. – доктор юридичних наук, професор, заслужений юрист України;

Кулик О.Г. – доктор юридичних наук, професор.

Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: монографія / Користін О., Швець Д., Бутко Б., Денисенко Б. та ін., за заг. ред. Користіна О.Є. – Київ: «ВАІТЕ», 2024. 444 с.

ISBN 978-966-2310-66-5

У монографії на основі аналізу зарубіжної наукової літератури та фахових публікацій, узагальнення практичного досвіду розвинених поліцейських систем світу, із врахуванням сучасного етапу реформування вітчизняних органів правопорядку, концептуально досліджено теоретичні засади та інституційні стандарти кримінального аналізу в системі правоохоронного органу. Зосереджено увагу на обґрунтуванні сучасного концепту розвитку системи кримінального аналізу на основі нової організаційно-управлінської філософії правоохоронної діяльності – intelligence-led policing (ILP). Розкрито ключові елементи моделі ILP. Методологічно науковий пошук зосереджено на обґрунтуванні професійної термінології у визначеній сфері, інституційних компонентів кримінального аналізу та ILP, на формуванні інтелектуальної складової правоохоронного менеджменту та сучасного безпекового світогляду, зокрема у діяльності Національної поліції України.

Системно досліджено та зроблено змістовний аналіз ключових методів й інструментів кримінального аналізу, а також сучасних трендових інформаційно-аналітичних новацій, що активно упроваджуються аналітиками, розвиваючи сучасні підходи розвитку аналітичної розвідувальної компоненти у діяльності вітчизняних правоохоронних органів.

Матеріали, викладені в монографії, будуть корисними для формування системи знань інституційної розбудови кримінального аналізу та аналітичної розвідки, використання у практичній діяльності працівниками Національної поліції України та інших правоохоронних органів, для розроблення типових навчальних програм відповідного спрямування, а також вивчення студентами, курсантами, аспірантами, ад'юнктами та викладачами.

УДК 351.741:(343:303.442.3)

ISBN 978-966-2310-66-5

Присвячується правоохоронцям та усім захисникам, які героїчно виборюють незалежність України та свободу українського народу

ЗМІСТ

ПЕРЕДМОВА

Мора О'Салліван, заступниця голови Консультативної місії ЄС в Україні 8

Джеррі Ретклiфф, PhD, професор університету Темпл (Філадельфія, США). 10

ВИСЛОВЛЕННЯ ПОДЯКИ 12

ВСТУП

Передумови та обґрунтування 14

Мета та особлива роль. 15

АНАЛІТИКА В БЕЗПЕКОВІЙ ДІЯЛЬНОСТІ

РОЗДІЛ 1 Сутність та теоретичне осмислення феномену аналітики 19

РОЗДІЛ 2 Суспільне призначення аналітики 27

РОЗДІЛ 3 Формування та реалізація правоохоронної політики на основі наукового передбачення 33

КОНЦЕПТУАЛІЗАЦІЯ INTELLIGENCE-LED POLICING (ILP) В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

РОЗДІЛ 4 Зміст та інтерпретація терміну «intelligence» в контексті моделі Intelligence-led Policing 45

РОЗДІЛ 5 Кримінальний аналіз в сучасних моделях поліцейської діяльності та новітній концепт на основі аналітичної розвідки 53

РОЗДІЛ 6 Філософія ILP – концепія Джеррі Ретклiффа 69

РОЗДІЛ 7 Актуалізація аналітичної розвідки в національній правоохоронній моделі 79

РОЗДІЛ 8 Забезпечення стандартів Європейського Союзу з прав людини в умовах упровадження ILP. 89

ІНСТИТУЦІЙНА ХРАКТЕРИСТИКА КРИМІНАЛЬНОГО АНАЛІЗУ

РОЗДІЛ 9 Зарубіжні особливості інституційного становлення кримінального аналізу 97

РОЗДІЛ 10 Становлення підрозділів кримінального аналізу Національної поліції України та вимоги до професійної компетентності аналітиків. 105

РОЗДІЛ 11 Термінологія та сутність кримінального аналізу. 113

РОЗДІЛ 12 Типології кримінального аналізу. 123

РОЗДІЛ 13 Процес кримінального аналізу 133

РОЗДІЛ 14 Інформаційне забезпечення кримінального аналізу 147

НАПРЯМИ ТА ОСОБЛИВОСТІ ЗАСТОСУВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ В УМОВАХ ВОЄННОГО СТАНУ

РОЗДІЛ 15 Розвиток системи кримінального аналізу в діяльності Національної поліції України в сучасних умовах 169

РОЗДІЛ 16 Цифрові технології та аналітичні засоби аналізу воєнних злочинів в Україні . . 179

РОЗДІЛ 17 Сучасні пошукові сервіси та інструменти аналізу кіберзлочинів 199

МЕТОДИ, ІНСТРУМЕНТИ ТА ТРЕНДОВІ НОВАЦІЇ КРИМІНАЛЬНОГО АНАЛІЗУ В УКРАЇНІ

РОЗДІЛ 18 Зміст, принципи і типології методів та інструментів кримінального аналізу . . 215

РОЗДІЛ 19 Статистичні методи в кримінальному аналізі 237

РОЗДІЛ 20 Якісний аналіз 263

РОЗДІЛ 21 Темпоральний аналіз 269

РОЗДІЛ 22 Геопросторовий аналіз 281

РОЗДІЛ 23 Методологічні засади OSINT 289

РОЗДІЛ 24 Тенденції злочинності та прогнозування кримінальної активності. 299

РОЗДІЛ 25 Ризик-орієнтований підхід (РОП) в діяльності органів правопорядку. 311

РОЗДІЛ 26 Кібервійна та форсайт кіберстійкості 343

РОЗДІЛ 27 Аналіз соціальних мереж 359

РОЗДІЛ 28 Операції з електронними таблицями і застосуванням Python 367

РОЗДІЛ 29 Основні алгоритми роботи аналітика з i2 Analyst's Notebook та Microsoft Excel. . 387

РОЗДІЛ 30 Аналіз та операції з великими даними в середовищі R 415

РОЗДІЛ 31 Фінансові розслідування для ефективного розслідування складних кримінальних правопорушень 425

РОЗДІЛ 32 Аналітичні продукти. 435

CONTENTS

FOREWORD

Mayra O'Sullivan, Deputy Head of EU Advisory Mission Ukraine 8

Jerry H. Ratcliffe, PhD, professor at Temple University (Philadelphia, USA) 10

ACKNOWLEDGEMENTS 12

INTRODUCTION

Background and rationale. 14

Objective and added value 15

ANALYTICS IN SECURITY ACTIVITIES

CHAPTER 1 The essence and theoretical understanding of the phenomenon of analytics 19

CHAPTER 2 The social purpose of analytics. 27

CHAPTER 3 Formation and implementation of law enforcement policy on the scientific foresight basis. 33

CONCEPTUALIZATION OF INTELLIGENCE-LED POLICING (ILP) IN LAW ENFORCEMENT

CHAPTER 4 Content and interpretation of the term «intelligence» in the context of the Intelligence-led Policing model. 45

CHAPTER 5 Crime analysis in modern models of policing and the latest concept based on intelligence 53

CHAPTER 6 ILP philosophy – the conception of Dr. Jerry H. Ratcliffe. 69

CHAPTER 7 Actualization of intelligence in the national law enforcement model 79

CHAPTER 8 Ensuring European Union human rights standards in the context of ILP implementation. 89

INSTITUTIONAL CHARACTERISTICS OF CRIME ANALYSIS

CHAPTER 9 Foreign features of the institutional formation of crime analysis 97

CHAPTER 10 Establishment of Crime Analysis Units of the National Police of Ukraine and Requirements for Professional Competence of Analysts. 105

CHAPTER 11 Terminology and essence of crime analysis 113

CHAPTER 12 Typologies of crime analysis 123

CHAPTER 13 Crime analysis process. 133

CHAPTER 14 Information support of crime analysis 147

VECTORS AND PECULIARITIES OF APPLICATION OF CRIME ANALYSIS UNDER MARTIAL LAW

CHAPTER 15 Development of the Crime Analysis System in the Activities of the National Police of Ukraine in Modern Conditions 169

CHAPTER 16 Digital technologies and analytical tools for analyzing war crimes in Ukraine 179

CHAPTER 17 Modern search services and tools for analyzing cybercrime 199

METHODS, TOOLS AND TREND INNOVATIONS OF CRIME ANALYSIS IN UKRAINE

CHAPTER 18 Content, principles and typologies of methods and tools of crime analysis. 215

CHAPTER 19 Statistical methods in crime analysis 237

CHAPTER 20 Qualitative analysis 263

CHAPTER 21 Temporal analysis 269

CHAPTER 22 Geospatial analysis 281

CHAPTER 23 Methodological principles of OSINT 289

CHAPTER 24 Crime trends and forecasting of criminal activity. 299

CHAPTER 25 Risk-based approach (RBA) in law enforcement activities. 311

CHAPTER 26 Cyber warfare and cyber resilience foresight 343

CHAPTER 27 Social networks analysis 359

CHAPTER 28 Basic spreadsheet operations and analytical innovations based on Python 367

CHAPTER 29 Basic algorithms of analyst's work with i2 Analyst's Notebook and Microsoft Excel . . 387

CHAPTER 30 Analysis and operations with big data in R environment 415

CHAPTER 31 Financial investigations for effective investigation of complex criminal offenses. . . . 425

CHAPTER 32 Analytical products. 435

DOI: https://doi.org/10.36486/978-966-2310-66-5-22

Нас не має вводити в оману те, як просто сьогодні створити візуалізацію. Ключове – це інтелектуальний процес, а комп'ютер – лише інструмент

Альберто Каїро

РОЗДІЛ 22
Геопросторовий аналіз

Максим Корнієнко
Дмитро Афонін

Геопросторовий аналіз – *це сукупність методів та інструментів кримінального аналізу, які застосовуються на всіх його рівнях (стратегічний, оперативний та тактичний), що направлені на отримання даних за допомогою різних GIS, геологічних, топографічних карт, а також карт маршрутів, як підрозділів поліції, так і злочинців, логістичних карт, схем тощо; картографування кримінальних правопорушень, щодо злочинної діяльності та встановлення взаємозв'язків в цих даних, з метою виявлення нової інформації щодо розслідуваних кримінальних правопорушень.*

МЕТОДИ КЛАСИФІКАЦІЇ ДАНИХ, ОТРИМАНИХ ПРИ ГЕОПРОСТОРОВОМУ АНАЛІЗІ:

Метод природних розривів. Більшість програмних пакетів GIS (*географічна інформаційна система – це система збору, зберігання, аналізу та графічної візуалізації просторових (географічних) даних та пов'язаної з ними інформації про необхідні об'єкти*) використовують метод природних розривів як варіант класифікації даних за замовчуванням [1]. Це хороший метод для визначення природних груп або кластерів значень у даних. Метод визначає «розриви» між групами значень даних. Класи ознак виділяються там, де є відносно великі «викиди» в даних. Цей метод обмежений для аналізу часових інтервалів, наприклад, для порівняння подібних періодів часу, оскільки діапазон даних може суттєво змінюватися в часі (наприклад, за рік), що робить розподіл даних, а отже, і природні розриви, непослідовними між часовими періодами (*рис. 22.1*) [2].

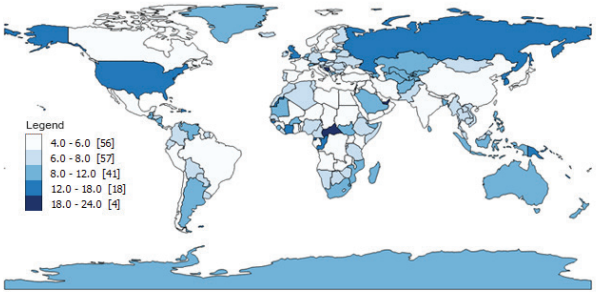


Рисунок 22.1. Хороплетна карта світу з використанням методу природних розривів.

Метод рівних інтервалів. Метод рівних інтервалів розбиває діапазон даних від низьких до високих значень на рівні підгрупи або класу, які задає користувач. Наприклад, кількість злочинів за один цикл коливається від 0 до 250. Щоб визначити п'ять класів, GIS використовує діапазон 250, ділить його на п'ять (50) і створює категорії, кожна з яких містить діапазон 50 (наприклад, 0-50, 51-100, 101-150). Це чудовий метод для порівняння даних за різні періоди часу, якщо користувач встановлює однакові інтервали в першому та другому періодах (*рис. 22.2*) [1].

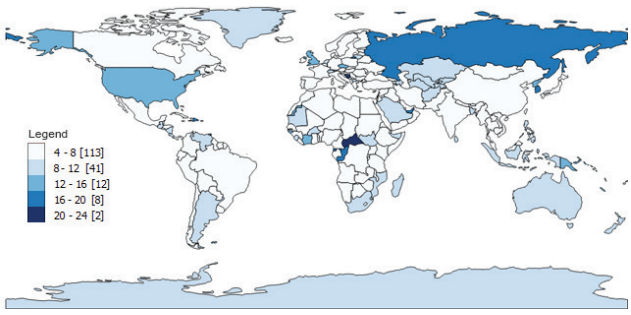


Рисунок 22.2. Хороплетна карта світу з використанням методу рівних інтервалів.

Метод квантилів. *Квантиль – значення, за якого задана випадкова величина не перевищує фіксовану ймовірність* [1]. Якщо ймовірність задана у відсотках, квантиль називається процентилем або перцентилем. Квантилі відносять рівну кількість спостережень або точок даних до кожного класу, як визначено користувачем. Якщо користувач встановлює чотири класи даних (квантилі), 25 відсотків даних або записів потраплять до кожного класу відповідно. Цей метод може вводити в оману залежно від розподілу даних. Класифікація за квантилями добре підходить для лінійно розподілених даних (*рис. 22.3*) [2].

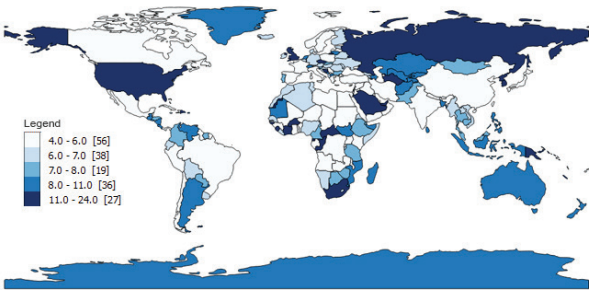


Рисунок 22.3. Хороплетна карта світу з використанням методу квантилів.

Метод стандартних відхилень. Цей метод слід використовувати лише тоді, коли дані наближаються до нормального розподілу [1]. Цей метод обчислює середнє значення розподілу даних, а потім відображає одне, два або три стандартних відхилення вище і нижче середнього значення (*рис. 22.4*).

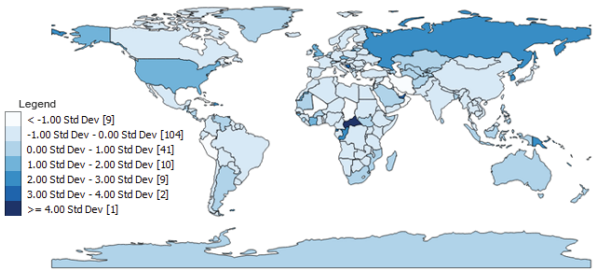


Рисунок 22.4. Хороплетна карта світу з використанням методу стандартних відхилень.

МЕТОДИ КАРТОГРАФУВАННЯ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ

> ***Картографування*** *– це процес складання карт та схематичної візуалізації важливої інформації, яка була в минулому, є на даний час, або буде у майбутньому. Картографування відбувається у одній з двох форм: крапково-символьній та Хороплету [1].*

Метод крапково-символьного картографування. Крапково-символьне картографування злочинної діяльності є методом фіксації даних на карті. У найпростішій формі, кожен символ або крапка на карті представляє собою окремий випадок географічного явища, що картографується. Крапкові карти розподілу корисні для ілюстрації просторової щільності. Труднощі виникають тоді, коли розподіл даних настільки щільний, що точкові символи зливаються в масу, руйнуючи тим самим первісний намір карти: показати дискретні місця подій.

(зображення з сайту www.mappery.com)

Для вирішення проблеми перекриття позначок крапково-символьного типу при високій щільності подій на одній дільниці, використовують пропорційне або градуйоване символьне картографування. Існує певна різниця між градуйованими та пропорційними символами. *Градуйовані символи* – це символи різного розміру, вибрані користувачем для представлення дискретних класифікацій даних [1]. *Пропорційні символи* призначаються програмним забезпеченням для представлення кожного унікального значення в діапазоні даних крапкових символів (*рис. 22.5*) [1].

Рисунок 22.5. Картографування методом символів (значків) на прикладі економічної карти Хорватії

Для крапокового розподілу необхідно використовувати програмне забезпечення GIS, щоб здійснювати обчислення частоти або підрахунок кількості повторень координат місцезнаходження (адрес) у базі даних. Важливою є цілісність даних. При підрахунку частоти програма розшукує унікальні координати місцезнаходження (адреси). При цьому програма може видавати варіанти запису адреси (наприклад, повна та скорочена назва), які після перевірки аналітик повинен об'єднати та зафіксувати як одне місцезнаходження з інтерпретацією її назви [2]. Для того щоб уникнути помилки при обчислені даних, існує багато різних програмних інструментів, направлених на фільтрацію та очищення даних при роботі з GIS картами (*рис. 22.6*).

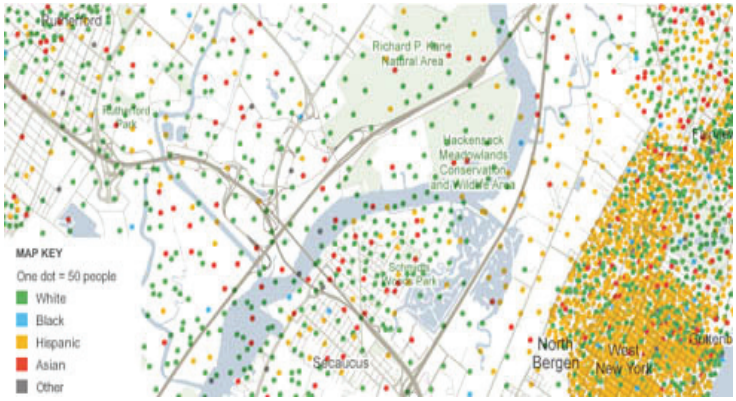


Рисунок 22.6. Картографування методом крапок на прикладі карти із зображенням крапками розселення представників різних етнічних груп (зображення з сайту www.danieljlewis.org)

На основі розрахунку частоти, можливим є створення градуйованої карти символів. Кожному підрахунку або діапазону підрахунків призначаються крапки різного розміру, щоб показати порядкову або інтервальну класифікацію даних. Величина крапок та їх кількість на одному символі визначається за методом розрахунку та вибору розмірів градуйованих символів. Також існує функціональна межа кількості різних розмірів символів, які при вивчені карти можуть бути інтерпретовані [3]. Тому карти максимально спрощуються.

Метод побудови карт Хороплету. Хороплетні карти часто називають також картами символів площі або статистичними картами поверхні [4]. Різниця між крапко-символьною картою та хороплетною полягає в тому, що крапко-символьна карта вказує на окреме місце, тоді як хороплетна карта вказує на сукупність даних на певній території, наприклад, на території обслуговування певного відділу поліції (*рис. 22.7*).

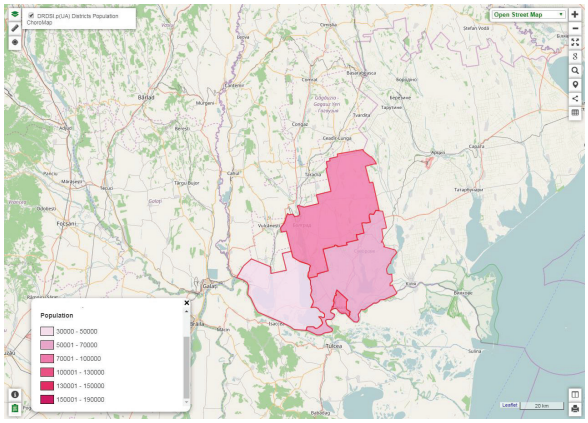


Рисунок 22.7. Картографування методом Хороплету на прикладі кількості населення у районах Дунайського регіону України

Першим важливим рішенням при складанні карти Хороплету є вибір території збору даних. *Територія – це географічна область або досліджувана зона, яка буде використовуватися для аналізу та ілюстрації даних* [4]. Карта складається на різних рівнях (області, району, міста, розташування певних об'єктів, певної групи осіб). Необхідно обрати масштаб та рівень аналізу. Це дуже важливо та напряму пов'язано з вихідними даними, які можливо в подальшому нанести на карту. Дані можуть надходити з різних джерел, але важливим є те, що вони повинні бути представлені у вигляді таблиці, де рядок – це територіальна одиниця (власні найменування), що має унікальний код (який буде використаний для зв'язку з метрикою географічного об'єкта) і яка може мати одну або декілька характеристик (атрибутів). Далі встановлюється зв'язок між геометрією і тематичними даними, який проводиться за допомогою картографічної системи (наприклад, QGIS) на підставі спільного атрибута (KOATUU). Але можливо використовувати інший спільний атрибут (за наявністю). Для налаштування рангів і стилів хороплет-шару використовується спеціальний файл налаштування (config), що входить до складу «Зразка…» [4].

Аналітик налаштовує: *кількість рангів; значення рангів; колір для певного рангу.*

Крок, що завершує процес конструювання хороплети. З директорії Basics (Основи) використовується «Вихідні файли і дані для побудови карт». В структурі «Вихідні файли…» у відповідних каталогах розміщуються [4]: *вихідні файли для карт; вихідні файли для QGIS; базові карти.*

МЕТОДИ ПРОСТОРОВОГО ЗАПИТУ (ПОШУКУ ДАНИХ НА КАРТАХ).

Цей метод пов'язаний з просторовим аналізом але тут він має свої особливості, пов'язані саме з картографуванням злочинної діяльності.

Програмне забезпечення GIS включає систему керування базами даних, зазвичай реляційну систему керування базами даних (RDBMS), для зберігання атрибутів просторових даних. Програмне забезпечення GIS також включає можливість імпортувати дані з інших джерел баз даних або отримувати доступ до даних в інших системах баз даних через з'єднання, такі як Open Database Connectivity (ODBC) [4]. Системи управління базами даних підтримують концепцію запитів для виокремлення підмножини даних. «Знайти» – це найпростіший пошук за атрибутами, зазвичай з метою знайти один запис. Обмежений запит дозволяє отримати підмножину даних, накладаючи обмеження на атрибути, наприклад, пошук всіх інцидентів протягом певного місяця (*рис. 22.8*).

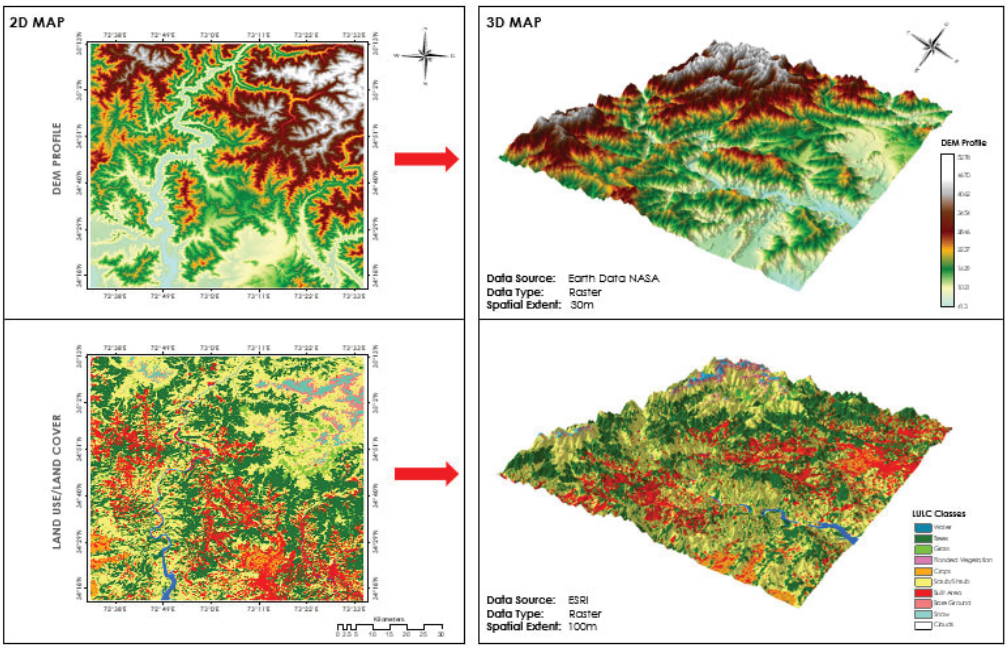


Рисунок 22.8. Приклад використання методу просторового аналізу на квадратній області географічної карти

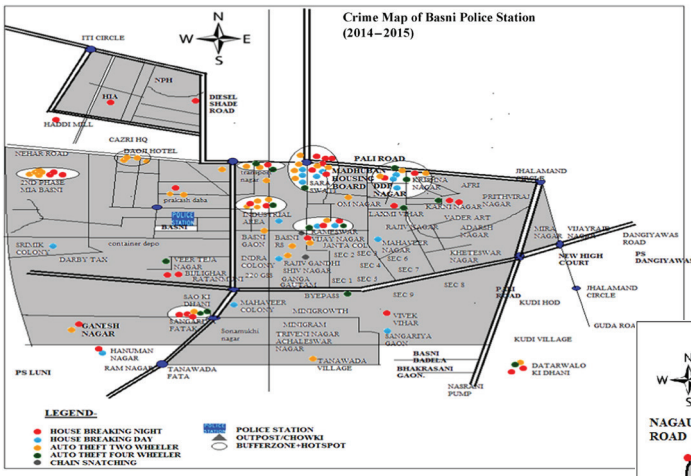


Рисунок 22.9. Карта злочинності Баснінського відділу поліції (2014–2015)

У результаті проведеного кримінального аналізу територій обслуговування восьми обраних відділів поліції, де спостерігалося найвище підвищення рівня вчинення квартирних крадіжок та угонів транспортних засобів в період 2014-2015 років, аналітиками були зроблені наступні висновки [5]:

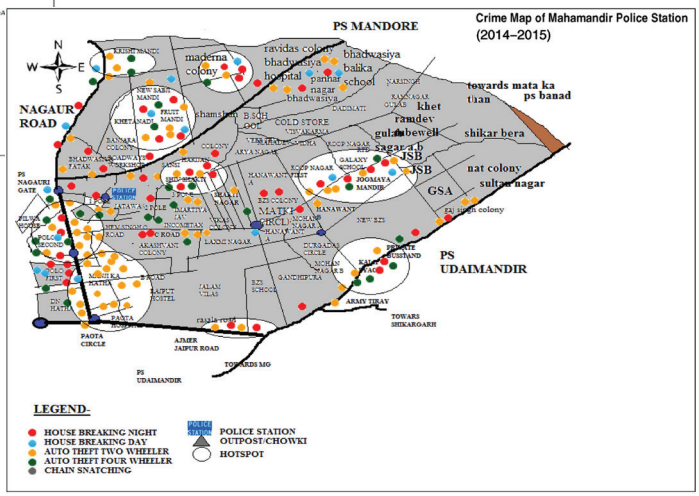


Рисунок 22.10. Карта злочинності відділу поліції Махамандір (2014–2015)

- ✓ *рівень заарештованих обвинувачених був низьким (менше 35%);*
- ✓ *патрулювання поліцейськими нарядами здійснювалося незадовільно та не було збільшено після підвищення рівня кримінальних правопорушень;*
- ✓ *чисельність особового складу поліцейських відділів була меншою за необхідну;*
- ✓ *більшість картографованих зон, на яких було виявлено скупчення місць виявлення слідів кримінальних правопорушень, тобто місць можливого вчинення квартирних крадіжок та угонів транспортних засобів, знаходилися в густо населених районах;*
- ✓ *серед осіб, які знаходилися в цих густонаселених районах, була величезна кількість безробітної молоді, наркоманів, циган, осіб, пов'язаних з криміналом [5].*

Зроблені висновки дали можливість прийняти відповідні управлінські рішення та зменшити рівень квартирних крадіжок та угонів транспортних засобів у місті Джодхпур.

Метод дослідження буфера об'єкта (буферізація даних). *Буфер – це зона навколо об'єкта аналізу, поміченого на карті (точка, лінія або багатокутник), яка просторово пов'язана з самим об'єктом.* Буферизація є поширеним методом у картографуванні злочинної діяльності з метою визначення зони або області аналізу [6]. Створення буфера передбачає визначення віддаленості границі наступної буферної зони. Проходження границі буферної зони визначається задачами, які стоять перед аналітиком, рельєфом місцевості, характеристиками об'єктів аналізу тощо.

Наприклад, якщо необхідно визначити 1000-метрову зону, вільну від наркотиків, навколо школи, необхідно вибрати місце розташування школи і скористатися інструментом буфера у програмному забезпечені GIS. Якщо школу визначити на карті крапкою, то буферна зона відобразиться у вигляді кола з радіусом у відповідному масштабі 1000 метрів. Але якщо школу відобразити у вигляді багатокутника, результатом буде більш точне відображає даного об'єкту з прилягаючою територією (шкільним подвір'ям) (*рис. 22.11*) [6].

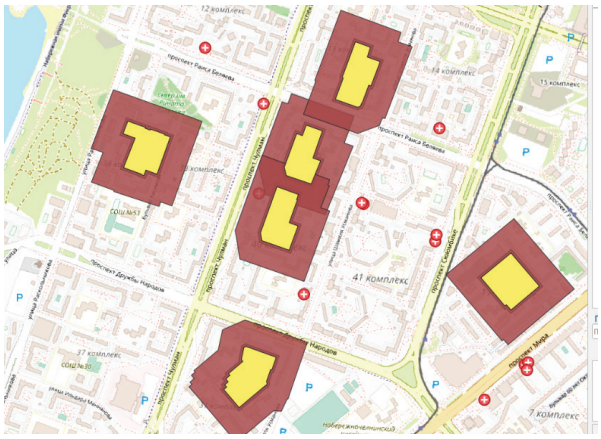


Рисунок 22. 11. Використання методу буферизації на прикладі відображення школи у вигляді багатокутника з прилягаючою територією

Метод буферизація розширює можливості аналітика при досліджені об'єкту. Застосування буфера створює нові дані, які потім можна використовувати для проведення подальшого аналізу. Створивши 1000-метрову буферну зону навколо школи, відкривається новий простір, в якому можна проаналізувати різноманітні характеристики, включаючи осіб які вживають наркотики, їх продаж, наявність сексуальних злочинців, які живуть і працюють там.

Метод зонального (за площами) дослідження об'єктів. *Зона (площа) – це певна територія, розмір якої визначений завданнями аналітика.* Даним методом можливо досліджувати декілька територій за площами та виявляти взаємозв'язки між ними, які можуть бути визначені певними загальними характеристиками між ними або зонами перетинання. Так, при аналізі декількох територій, які за своїми характеристиками наближені одна до одної, можна визначити зони підвищеної небезпеки або вірогіднішого знаходження об'єкту пошуку. Наприклад, інформація про території можливих розбійних нападів, отримана з різних джерел, нанесена на карту, виявляє зони підвищеної вірогідності їх вчинення (*рис. 22.12*) [7].

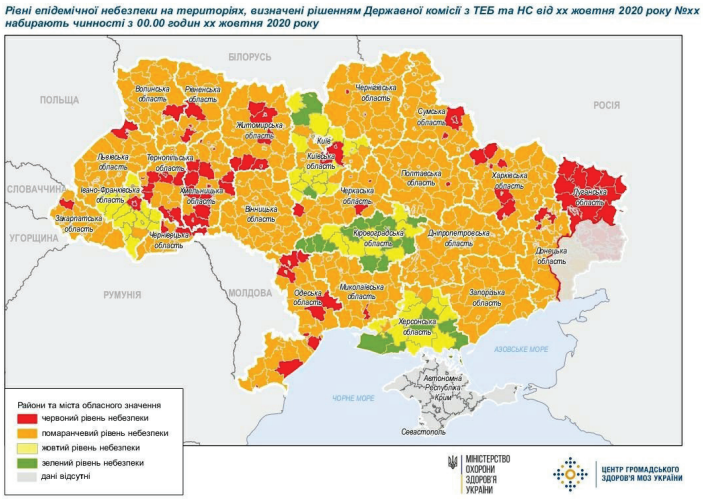
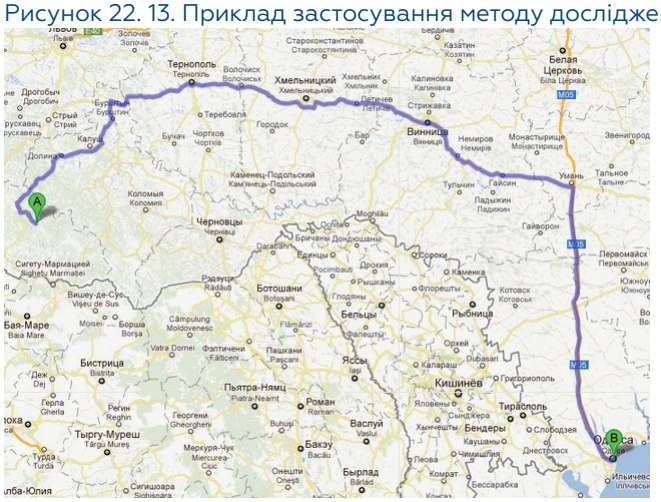


Рисунок 22.12. Приклад застосування методу зонального дослідження (аналізу) об'єктів на карті

Метод дослідження маршруту об'єкта злочинної діяльності.

Рисунок 22. 13. Приклад застосування методу дослідження маршруту об'єкта



Даний метод направлений на визначення та аналіз маршруту руху злочинця, як під час вчинення кримінального правопорушення, так і під час його звичайного життя. Під час аналізу маршруту руху визначаються його довжина, швидкість переміщення, наявність перетинання з іншими маршрутами руху того ж самого або інших злочинців, наявність або відсутність яких-небудь перешкод, які допомагають або навпаки роблять перепони щодо можливості завершити маршрут. Даний метод розповсюджується також на маршрут руху потерпілого або представників правоохоронних органів, у тому числі поліції, під час виконання службових обов'язків (*рис. 22.13*) [8].

МЕТОДИ ПРОГНОЗУВАННЯ (ПРЕВЕНТИВНОГО АНАЛІЗУ) ЗЛОЧИННОСТІ НА ОСНОВІ ГЕОРОЗВІДКИ.

Метод превентивного аналізу (прогнозування) на основі георозвідки – це застосування геоінтелекту або геопросторового інтелекту та його здатність ідентифікувати, фіксувати, зберігати та досліджувати дані для створення геопросторових уявлень за допомогою критичного мислення, геопросторового міркування та аналітичних методів, розробки та представлення знань у вигляді придатному для прийняття управлінських рішень заснованих на етичності [9]. Методи та інструменти георозвідки дозволяють нам аналізувати дані про злочини таким чином, щоб ідентифікувати певні геопросторові перспективи (тенденції) або шаблони, які дозволять нам передбачити майбутні злочинні дії.

Один із інструментів георозвідки, реалізований для аналізу кримінальних правопорушень – це *карти злочинності* [9]. Створення та аналіз цих карт базується на використанні геоінформаційних систем (GIS). GIS дуже корисні для отримання інформації та прийняття обґрунтованих рішень на основі геопросторових даних, оскільки вони дозволяють користувачеві поєднувати дані з багатьох джерел і, отже, проводити аналіз на основі різних змінних. Це дає змогу візуалізувати та проаналізувати кримінальні правопорушення з більшою глибиною та з різних точок зору, включаючи геопросторову перспективу. Використання карт злочинності підтримує поліцейські операції шляхом пошуку злочинних дій, які сталися нещодавно, а також шляхом передбачення того, коли і де існує більша ймовірність того, що в майбутньому може бути вчинений певний злочин. Ці карти можуть відігравати дуже важливу роль у зниженні рівня злочинності, від початкових етапів, пов'язаних зі збором даних, у розробці поліцейських операцій з протидії злочинності як інструменту для визначення найбільш сприятливих районів для розгортання сил, аж до завершальних етапів, пов'язаних із спостереженням та оцінкою реагування на дії поліції, здійснені з метою зменшення злочинності. Карти злочинності також відіграють ключову роль під час передачі результатів, оскільки їх можна використовувати для більш чіткого пояснення закономірностей і тенденцій розповсюдження та виникнення злочинності, що робить їх легшими для розуміння різними підрозділами поліції, які отримують інформацію.

Алгоритми прогнозування злочинної діяльності, засновані на георозвідці, здатні визначити, де і коли існує більша ймовірність того, що в майбутньому можуть бути вчинені кримінальні правопорушення.

Методи прогнозування поділяються на дві великі групи: *методи ретроспективного та перспективного аналізу.*

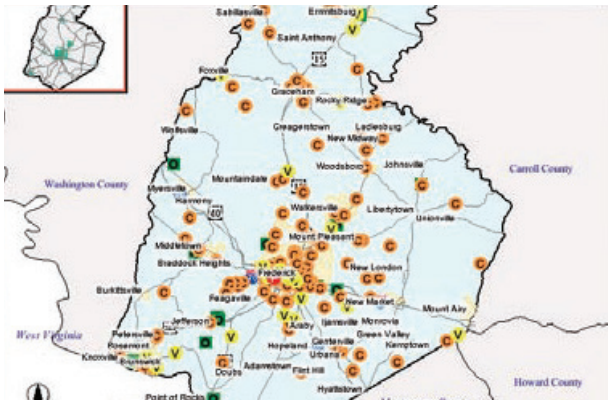
Ретроспективний аналіз

Цей тип аналізу базується на вивченні даних про минулі кримінальні правопорушення. Він включає в себе чотири основних метода:

Аналіз гарячих точок. Цей метод вивчає території, у яких спостерігається висока концентрація злочинності, і використовує місця минулих кримінальних правопорушень, щоб передбачити кримінальні правопорушення, які можуть повторитися в майбутньому (*рис. 22.14*) [10].

> *Гарячу точку можна визначити як конкретне місце або невелику територію, де кількість злочинів перевищує середню, і де ризик віктимізації вищий за середній.*

Гарячі точки динамічні: вони змінюються протягом певного періоду часу, вони змінюють положення, вони змінюють форму, збільшуючись або звужуючи розміри, або навіть зникаючи або знову з'являючись залежно від часу кримінального правопорушення та аналізованого періоду.

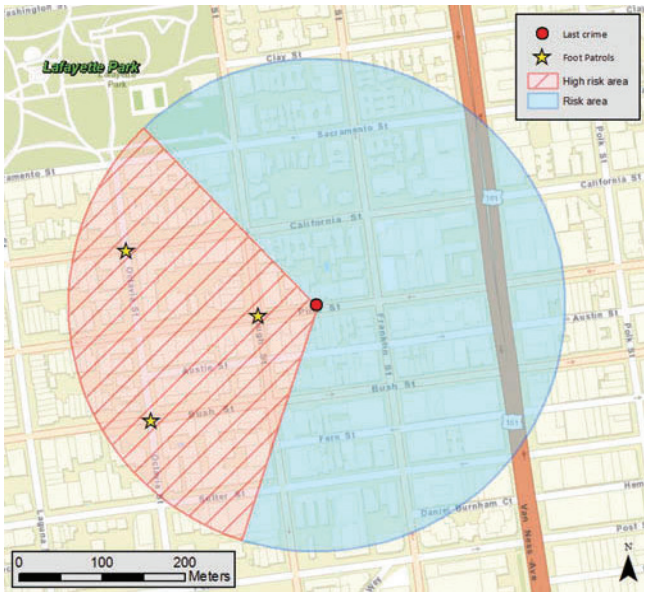


Аналіз гарячих точок є відправною точкою якісного аналізу карти злочинності. На основі аналізу великої кількості даних, аналіз гарячих точок слід використовувати для прогнозування областей підвищеного ризику злочинності на основі злочинів минулих років для вирішення проблем та відповідного планування діяльності поліції [11]. Після визначення гарячої точки аналітичний процес продовжується з визначенням часових закономірностей у цій області або типів певного способу дії, які присутні для отримання корисних результатів.

Рисунок 22.14. Приклад застосування аналізу гарячих точок на карті де позначені місця нападу сексуального насильника

Ретроспективний темпоральний аналіз. Цей метод допомагає аналізувати злочинні дії, щоб виявити тенденції щодо дня та часу, коли вони відбувалися і використовує їх як основу майбутніх прогнозів.

Часопросторовий ретроспективний аналіз. Цей метод поєднує закономірності, виявлені на місці, з тими, які виявлені в часі, щоб передбачити місце та час, коли існує висока ймовірність вчинення кримінального правопорушення в майбутньому.



Аналіз імовірного повторення. Цей метод базується на ідеї, що коли вчиняється кримінальне правопорушення в певному місці, існує підвищена ймовірність того, що аналогічне подібне кримінальне правопорушення може бути вчинено через короткий проміжок часу на прилеглій території (*рис. 22.15*) [11].

Рисунок 22.15. Приклад застосування аналізу ймовірного повторення з метою встановлення зони ризику та ймовірності вчинення грабежів в майбутньому (червоним кольором у центрі кола помічене місця вчинення грабежу у минулому)

Існує принаймні три методи аналізу для виявлення та дослідження гарячих точок різної складності. Вибір того, який аналіз застосовувати, залежить від типу доступних даних, вимог, які необхідно охопити, мети, результатів і типу аудиторії [9]. Вивчення розподілу злочинності за типом перед аналізом є принципово важливим для визначення того, який тип методології слід використовувати. Кожен тип аналізу гарячих точок має різні сильні та слабкі сторони, які необхідно зрозуміти перед виконанням та інтерпретацією результатів.

Метод візуального визначення. Цей метод складається з простої візуальної інтерпретації крапково-символьної карти, на якій показані всі злочинні події. Аналітик візуально визначає області, де точки згруповані разом. Цей метод не є статистично точним, оскільки він залежить виключно від людської інтуїції, але все ж може бути ефективним.

Метод аналізу градуйованої кольорової або хороплетної карти. Аналітик використовує інтенсивність кольору, щоб затінити області на карті відповідно до кількості злочинів, скоєних у цих областях. На результати значною мірою впливатиме розмір одиниці аналізу, прийнятої аналітиком (блоки перепису, групи блоків, райони тощо), тому що вибір занадто великого розміру призведе до приховування менших гарячих точок, розташованих на більших територіях з обмеженими можливостями. Вибір правильної техніки класифікації даних – рівний інтервал, квантиль або природні розриви, також матиме вплив на представлення та аналіз даних [12].

Метод аналізу щільності. Цей третій тип аналізу гарячих точок використовує відображення клітинок сітки. Після розміщення сітки на цікавій області з урахуванням відповідного розміру комірки, яка використовується для аналізу, вибирається радіус пошуку, який обчислює кількість інцидентів у радіусі та ділить це число на розмір зони пошуку. Як правило, найтемніші кольори представляють клітинки з найбільшими оцінками.

Більш точний підхід до аналізу щільності може бути виконаний за допомогою інтерполяції щільності ядра. Вони використовують метод сіткового аналізу для оцінки щільності злочинності на всій досліджуваній території шляхом присвоєння більшої ваги подіям, які відбуваються ближче до центру радіуса пошуку, і меншої ваги подіям, які відбуваються далі. Потім результати надають інформацію про те, де згрупована злочинність, але вони також надають значення щільності для всієї досліджуваної області. Крім того, інтерполяція щільності ядра забезпечує більш реалістичне зображення форми розподілу гарячих точок [12].

Перспективний аналіз

Метод аналізу не базується на минулих подіях, натомість він полягає у визначенні географічних показників, які роблять певне місце більш привабливим для правопорушників, таким чином, поєднуючи їх, підвищується ризик злочинності в певній місцевості.

Індикатори, які підвищують або зменшують ризик злочинності в регіоні, необхідно визначати відповідно до типу досліджуваного кримінального правопорушення, оскільки, наприклад, показники угону транспортного засобу та сексуального насильства не будуть однаковими.

Найвідомішим методом перспективного аналізу є ***моделювання рельєфу ризику (RTM).*** Основна мета картографування злочинності полягає в тому, щоб отримати на карті злочинні події. Після зіставлення даних за адресою або геокодуванням ці точки вносяться до GIS [13]. Місце, де відбува-

ються кримінальні правопорушення, а також зв'язок цих місць одне з одним та іншими даними чи інформацією – є важливим фактором аналізу кримінальних правопорушень.

Початкові результати, ймовірно, не будуть задовільними. Наявність сотень або тисяч точок на карті призводить до перевантаження інформацією, і немає жодних розумних очікувань на спроможність аналітика розпізнати закономірності в інформації. З цієї причини необхідно застосовувати *методи просторового аналізу*, щоб допомогти аналітикам у візуалізації та просторовій інтерпретації даних про злочини (*рис. 22.16*) [13].

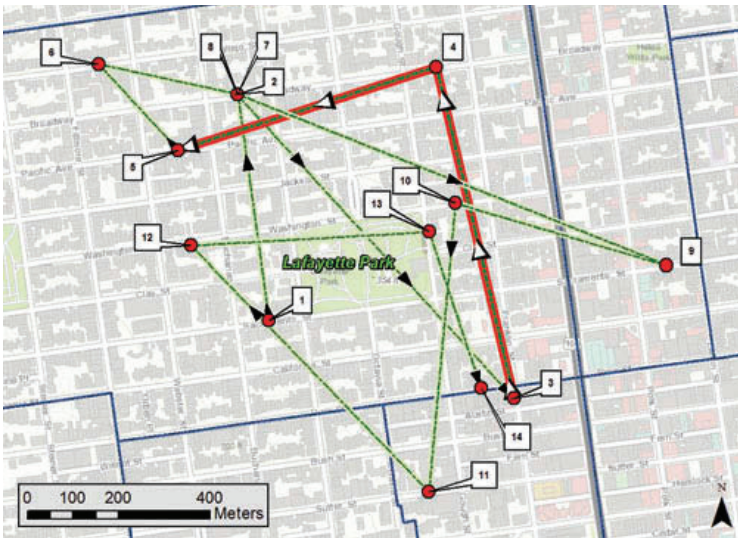


Рисунок 22. 16. Приклад застосування методу просторового аналізу при картографуванні місць вчинення квартирних крадіжок (помічені червоними крапками) в результаті чого аналітиком була виявлена закономірність руху за годинниковою стрілкою коло парку

Як метод визначення ймовірності чи ризику, RTM використовує вплив на розташування цих раніше визначених індикаторів, щоб зробити висновок, що певні злочини відбуватимуться в певних областях, де існують ці індикатори (або їх комбінація). Значення ризику, отримані в результаті застосування моделей аналізу ризику на місцях, є орієнтовним способом показати вразливість місця до злочинності.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Dent, B., Torguson, J. & Hodler, T. (2008). *Cartography: Thematic map design.* The Plenum Series on Demographic Methods and Population Analysis. McGraw Hill-Higher Education.
2. International Association of Crime Analysts (2017). *Exploring crime analysis: Readings on essential skills* (3rd ed.). K. Gallagher, J. Wartell, S. Gwinn, G. Jones & G. Stewart (Eds.). Overland Park.
3. Caplan, J.M. & Kennedy, L.W. (2011). *Risk terrain modeling manual: Theoretical framework and technical steps of spatial risk assessment*. Newark, NJ: Rutgers Center on Public Safety.
4. Географічні карти та картографічний метод дослідження. І том: Географічні карти; 2 том: Картографічний метод дослідження / Т.В. Дудун, С.В. Тітова; упоряд. С.В. Тітова. Київ, 2017. 150 с.
5. Lama, S. & Rathore, S. S. (2018). Crime Mapping and Crime Analysis of Property Crimes in Jodhpur. *International Annals of Criminology*, 55 (02), 1–15. DOI:10.1017/cri.2017.11.
6. Levine, N. (2003). CrimeStat 11. *Crime Mapping News*, 5 (2), 2-4.
7. Harries, K. (1999). *Mapping crime: Principles and practice*. Washington, DC: U.S. Department of Justice, Crime Mapping Research Center.
8. Paynich, R., Cooke, P. & Matthews, C. (2007). *Developing standards and curriculum for GIS in law enforcement*. Presented at 9th NIJ Crime Mapping Conference, Pittsburgh, PA.
9. Boba Santos, R. (2013). *Crime analysis with crime mapping* (3rd ed.). Thousand Oaks, CA: SAGE.
10. Epifanio Pecharromán (2016). Crime Predictive Analysis Based on Geointelligence. *The International Journal of Intelligence, Security, and Public Affairs*, 18:3, 221-248.
11. Eck, J., Chainey, S., Cameron, J., Leitner, M. & Wilson, R. (2005). *Mapping crime: Understanding hotspots*. Washington, DC: National Institute of Justice.
12. Hill, B. & Paynich, R. (2014). *Fundamentals of crime mapping* (2nd Ed.). Burlington, MA: Jones & Barlett Learning.
13. Caplan, J. & Kennedy, L. (2010). *Risk terrain RTM modeling manual. Theoretical framework and technical steps of spatial risk assessment for crime analysis*. Newark, NJ: Rutgers Center on Public Security.

DOI: https://doi.org/10.36486/978-966-2310-66-5-23

до 90 % аналітично-розвідувальних даних надходить із відкритих джерел і лише 10 % – завдяки агентурній роботі.

генерал-лейтенант Самуель Вілсон,
колишній керівник Розвідувального управління Міністерства оборони США (1976-1977)

РОЗДІЛ 23
Методологічні засади OSINT

Олександр Користін
Богдан Денисенко

Процес цифровізації (діджиталізації), та, таким чином, генерування все більшої й більшої кількості даних та інформації онлайн (так само і офлайн), не спинити. Отже, розширюються можливості знаходити, глибше і детальніше перевіряти та верифікувати дані, інформацію щодо осіб, компаній, транспортних засобів, інших об'єктів та елементів дослідження, їх аналізувати, створювати зв'язки, у тому числі причинно-наслідкові зв'язки, створювати інформацію з доданою вартістю, таким чином здійснюючи аналітичну розвідку (intelligence) на основі даних з відкритих джерел (OSINT).

ПОНЯТТЯ ТА ТЕХНОЛОГІЧНИЙ ПРОЦЕС OSINT

Компанія «Reuser's Information Service» (RIS) у своєму тренінгу «OSINT Pathfinder» фокусує увагу на численних маніпуляціях з цим поняттям та зазначає

> ***OSINT** є комплексною, інтегрованою методологією і технологічним процесом, спрямованим на задоволення вимог замовника щодо дієвої аналітичної розвідки здійсненої в процесі синтезу та аналізу, на основі репрезентативної вибірки достовірної, надійної, своєчасної та точної інформації з відкритих джерел.*
>
> *Dr. Arno H.P. Reuser [1]*

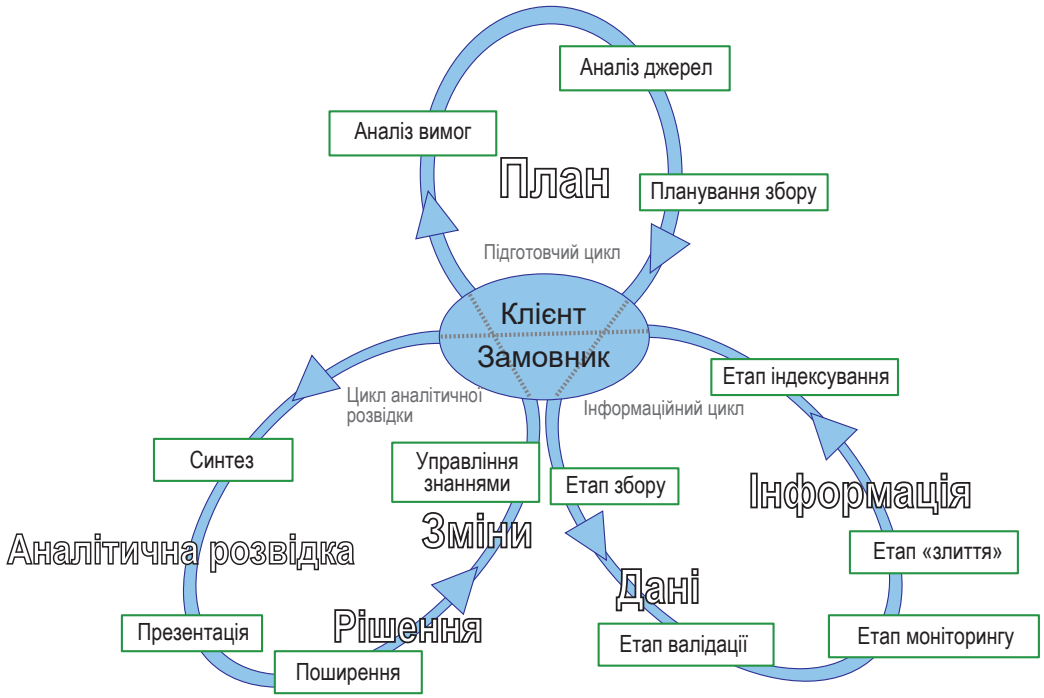


Рисунок 23.1. Цикл OSINT (RIS) [1; 2]

RIS також наголошує на змішуванні понять **OSINT та OSINF**. Оскільки, **OSINF** (Open Source Information) є всією інформацією з відкритих джерел у будь-якому форматі, що може бути здобута будь-яким законним та етично прийнятним шляхом без жодних обмежень, чи то безкоштовно, чи на платній основі. RIS наголошує на таких обмеженнях, та, відповідно, акцентує увагу на тому, що простий збір та надання необробленої, сирої інформації не є OSINT.

Під час збору інформації необхідно враховувати **обмеження** щодо авторського права, ліцензування та інтелектуального права власності.

> *Хакерство, незаконне втручання у комп'ютерні мережі, злом паролів є незаконним та не може вважатись OSINT дослідженням.*

З етичної точки зору, наявність деяких ресурсів у відкритому доступі, у той час як вони не передбачені для відкритого доступу, не може вважатись інформацією з відкритих джерел.

RIS наголошує, що стандартний цикл аналітичної розвідки (intelligence cycle) не відповідає потребам OSINT-дослідження, оскільки кількість кроків такого дослідження може змінюватись (відповідно до потреб конкретного дослідження).

Особливістю **циклу аналітичної розвідки з відкритих джерел (*цикл OSINT*)**, запропонованого RIS, є те, що клієнт, або замовник перебувають в центрі процесу, а сам цикл складається з 3-х підциклів, а саме: підготовчий цикл, інформаційний цикл та цикл аналітичної розвідки (*Рис. 23.1*).

Підготовчий цикл

Цей цикл має на меті отримати якомога більше ясності щодо завдання або вимог дослідження, щоб забезпечити відповідність остаточного продукту потребам замовника. Під час підготовчого циклу розробляється план дій, який оцінюється разом із замовником.

Підготовчий цикл складається з трьох етапів: аналіз вимог, аналіз джерел та планування збору.

Перший етап (аналіз вимог) необхідний для підготовки відповідного аналітичного продукту. Розбиття початкової вимоги на логічні кроки допомагає розкласти основну проблему на підпроблеми. Такі логічні кроки включають визначення підпитань, визначення припущень, визначення та вирішення змінних для запобігання непорозумінь із замовником, застосування кваліфікаторів для обмеження та уточнення дослідницького процесу, тощо. Результатом цього процесу є набір попередніх проблем, які необхідно вирішити (щоб розібратися з припущеннями і упередженнями), і набір питань, на які необхідно відповісти, які визначені таким чином, щоб не було ніякого непорозуміння щодо того, що потрібно зробити.

Коли є достатня ясність щодо постановки завдань, наступним етапом є аналіз джерел даних та інформації. Цей етап передбачає ретельне вивчення того, яке джерело використовувати, встановлення надійності та достовірності кожного окремого джерела, переконатися, що вибір джерел є збалансованим і репрезентативним.

> *Важливо пам'ятати, що відкриті джерела є занадто складними, щоб ставитися до них легковажно.*

Окремий етап аналізу джерел є дуже важливим. Знання того, які джерела використовувати, також допоможе зменшити надлишок інформації. Вибір релевантного, репрезентативного та збалансованого набору джерел значно допомагає зменшити інформаційний потік, оскільки все, що потрібно зробити досліднику, – це лише просуватися вниз за списком **перевірених джерел**. Крім того, втрата орієнтиру в масиві в джерелах більше не є проблемою.

Це призведе до наступного кроку – створення плану збору інформації та плану дій. У цьому плані зазначається, які джерела будуть досліджуватися, яким чином і коли. У плані збору даних, після першого та другого кроку, будуть перераховані очікувані відповіді від кожного джерела й максимальна кількість результатів. У плані також буде вказано, коли слід припинити пошук. Цей крок є важливим в управлінні часом і ресурсами. План допомагає боротися з інформаційним перенасиченням, оскільки все, що потрібно зробити, – це дослідити джерела, а не перебирати мільйони результатів пошуку в універсальній пошуковій системі «Інтернет». План допомагає в управлінні часом, оскільки пошук у заздалегідь визначеному наборі джерел можна спланувати. Цей крок також допомагає в управлінні ресурсами, оскільки тепер можна легко призначити співробітників на конкретні завдання у плані.

Ще один важливий момент – контроль. Робота за планом і ведення щоденника, в якому перелічуються дії, пошук, запити, результати й дати, допоможе досліднику бути відповідальним. Це допоможе продовжити дослідження, не втрачаючи часу та не роблячи все заново. Це також допоможе іншому досліднику продовжити дослідження, якщо перший дослідник недоступний. План збору даних і щоденник є фундаментальними інструментами в аналітичному процесі, а отже, це третій крок нового циклу.

Результатом підготовчого циклу є план дій, який включає аналіз потреб, аналіз джерел та планування збору. Ці плани узгоджуються та затверджуються замовником. Замовник, при цьому, може бачити чи правильно інтерпретовано початкову вимогу і чи деконструкція проблеми є правильною. Замовник може змінити план (можливо навіть суттєво), вимоги, запропонувати рішення, перелік джерел, дати поради та поділитися ідеями. Такий зворотний зв'язок із замовником є безцінним для всього процесу і має додаткову перевагу у вигляді розвитку довірчих відносин.

Якщо необхідно внести зміни до будь-якого з перших трьох етапів, цикл підготовки повторюється, доки всі залучені сторони не будуть задоволені кінцевим продуктом. Лише після цього розпочинається інформаційний цикл.

Підготовчий етап передбачає підготування робочого місця, а саме:

а) бажано проводити дослідження в «ізольованому середовищі», використовуючи віртуальну машину (чи машини), анонімізуючи доступ до ідентифікуючих особливостей машини, з якої здійснюється доступ в мережу;

б) необхідно використовувати віртуальні приватні мережі (VPN), змінюючи ідентифікуючу IP-адресу;

в) за необхідності, створити акаунти для прикриття (виключно в рамках чинного законодавства, з повагою до персональних даних та етичних норм), до реєстрації та супроводження яких використовуючи «незасвічені» номери телефонів (за необхідності) та фото (за можливості).

Є низка сайтів у різних юрисдикціях, які надають можливість отримати одноразовий *СМС* чи альтернативну можливість використання телефонного номеру (з пулу номерів), однак механізми аутентифікації поштових сервісів та соціальних мереж (у більшості випадків) налагодили можливість попередження використання даних номерів для реєстрації, отже цей механізм є не завжди дієвим, однак його необхідно мати на увазі.

Що стосується фото, то наявна низка альтернативних джерел, серед яких є https://thispersondoesnotexist.com/ тощо. Необхідно враховувати, що згенеровані фото неіснуючих людей можуть мати явні сліди обробки та синтезу, тому потребують перегляду деталей згенерованих фото.

Інформаційний цикл

Цей цикл складається з п'яти етапів, на яких здійснюється власне пошук і збір інформації. Інформація збирається, обробляється, індексується, тощо, задля складання інформаційного звіту та його оцінювання разом із замовником.

Інформаційний цикл починається з етапу збору даних з відкритих джерел. Етап збору включає в себе власне пошук даних (або інформації) та роботу над планом збору. На цьому етапі також відбувається безпосередній збір даних. Цей, здавалося б, простий етап може мати свої проблеми, особливо у випадку з вирішенням бюрократичних питань доступу до державних чи корпоративних баз даних, потребує технічних рішень для завантаження та обробки різних форматів інформації, розшифрування інформації, дедуплікації, деархівування, тощо.

> *Не може бути підрозділу OSINT, який працює самостійно. Всі задіяні є, або принаймні повинні бути, частиною команди. Зрештою, аналітик зацікавлений у цьому, у отриманні «повноцінної» інформації [1].*

Оскільки інтернет містить так багато необробленої інформації, необхідною є фаза валідації для того, щоб переконатися, що інформація є достовірною, правильною, корисною й надходить з відповідного джерела. Кожен електронний лист, кожен веб-сайт, кожен документ повинен підлягати режиму валідації. Цей режим повинен бути широко узгодженим, здійсненним і, в межах розумного, простим у застосуванні для всіх зацікавлених сторін. Валідація життєво важлива в сучасному світі, і тому є додатковим етапом.

Світ змінюється швидко, і, оскільки процес створення аналітичного розвідувального продукту може зайняти багато часу, обґрунтованим є початок фази моніторингу на цьому етапі, щоб відстежувати розвиток подій і бути переконаним, що під час процесу не буде пропущено жодних поточних важливих подій. За необхідності, за умови, що інтерес замовника є достатньо чітким, дослідник може адаптувати вимоги на цьому етапі або отримати додатковий зворотний зв'язок від замовника. Це також допоможе впоратися з проблемою часу обігу інформації.

Інформація з усіх цих різних джерел має бути оброблена, щоб видалити дублікати, переформатувати, призначити метадані, розрізнити релевантні та нерелевантні джерела, оновити журнали виконання, додати ключові слова та впорядкувати інформацію у певний осмислений спосіб. Фаза злиття призначена для цього. На цьому етапі створюється інформаційний звіт, що підсумовує результати пошуку інформації.

Очевидно, що дані та інформація повинні зберігатися таким чином, щоб їх можна було знайти знову. Зазвичай більшість спецслужб просто скидають інформацію в якусь мережу без будь-якої індексації. У кращому випадку, використовується якась програма для пошуку інформації, але вони часто погано налаштовані й, безумовно, не відповідають потребам користувачів, оскільки їх розробляє та налаштовує IT-персонал, який, як правило, ніколи не залучає замовника до своїх проєктів. Результатом є величезна колекція приватних бібліотек: на папері, в цифровому вигляді та в особистих спогадах дослідників. Належний процес індексації інформації все ще залишається важливим етапом і заслуговує на окремий крок у циклі.

Кінцевим продуктом інформаційного циклу є звіт OSINF з результатами пошуку, планом дій, початковими висновками та об'єктивним резюме.

> *Звіт OSINF не передбачає проведення аналізу у традиційний спосіб. У ньому немає інтерпретації, пояснення, прогнозування, суджень, **лише «факти»**.*

Звіт надається замовнику, який тепер може прийняти рішення щодо кількох речей. Або замовник задоволений інформацією у такому вигляді, як вона є, і поки що не потребує жодних подальших послуг, або ж замовник недостатньо задоволений інформацією та інформаційний цикл буде повторено знову, або клієнт дуже задоволений і вимагає аналізу та інтерпретації інформації для підготовки аналітичного розвідувального звіту.

Цикл аналітичної розвідки

На цьому етапі здійснюється аналіз зібраної інформації і власне «розвідувальний аналіз», формується аналітичний звіт, який поширюється серед зацікавлених осіб.

Цикл аналітичної розвідки складається з трьох фаз: фаза синтезу, фаза презентації, фаза поширення. Оскільки в дійсності «аналіз» проводиться приблизно на кожному кроці й на кожній фазі, використання цього терміна для позначення фази є недоречним. Як новий термін пропонується термін «синтез». Синтез включає в себе всі види діяльності, які дозволять створити аналітичний розвідувальний звіт з інформаційного звіту: інтерпретацію, розуміння, пояснення, прогнозування, узагальнення, маркування, судження тощо, тобто, всі ті види діяльності, які раніше називалися розвідувальним аналізом. Кінцевим продуктом цього етапу є звіт аналітичної розвідки (аналітичний продукт).

Наступний крок, який часто недооцінюють, – презентація. Яким би якісним не був аналітичний продукт, якщо результати не представлено належним чином, всі зусилля були марними. Багато чудових розвідувальних продуктів було знищено через те, що автор не зміг донести свою думку, або через те, що автор не зміг правильно висловити свої думки у звіті. Причин є багато: звіт занадто великий, щоб замовник зміг його прочитати (належним чином), погано написаний, щоб замовник неправильно інтерпретував текст, погано представлений на нечітких слайдах, погано представлений доповідачем тощо. Тут також має місце доброчесність. Виконавці або навмисно пишуть звіти, у яких у досить нечіткій формі викладено інформацію чи висновки, щоб мінімізувати ризик «помилок», або, з іншого боку, зазначають «свою правду», від якої клієнт відмовляється, тому що це не те, що він хотів прочитати.

Етап поширення аналітичного продукту є ще одним часто недооцінюваним кроком. Хоча кінцевою метою будь-якого аналітичного розвідувального продукту має бути його широке розповсюдження серед усіх зацікавлених сторін (в межах розумного), досить часто окремі агенції (підрозділи) мають дуже суворі правила щодо того, хто має право бачити ту чи іншу частину звіту.

Останній крок – управління знаннями. На цьому етапі вся робота, пов'язана зі створенням аналітичного розвідувального звіту, має бути проаналізована, проіндексована і зберігатися для подальшого використання: використані методологія аналітичної розвідки та збору інформації, стратегії пошуку, дискусії тощо. Очевидно, що на цьому етапі фіксується інформація про те, що спрацювало, і те, що не спрацювало, що може бути використано знову для нового завдання, або, принаймні, як отриманий досвід може бути використаний для наступного проекту.

OSINT-дослідження є багатогранним та може передбачати, серед іншого, визначення IP та MAC-адреси (у разі відсутності обмежень доступу, у тому числі законодавчих обмежень), контактної та додаткової інформації власників ресурсів або елементів, опрацювання фото (у тому числі виявлення метаданих (EXIF data), проведення відповідних геопросторових досліджень, хроно-локації тощо. Список не є вичерпним. Список задач та підходів може доповнюватись та змінюватись відповідно до задач, які стоять перед OSINT-дослідженням, однак загалом (у більшості випадків) задачі звужуються до ідентифікації, верифікації, та опису з метою визначення причинно-наслідкового зв'язку. Відповідно, інструментарій є широким і в більшості випадків не є статичним.

Цикл аналітичної розвідки з відкритих джерел, запропонований RIS [1] у вигляді «пропелера», в його нинішньому вигляді може бути застосований до багатьох дисциплін, але він передбачає, що замовни-

ком є особа або організація, яка завжди активно співпрацює з питань розробки аналітичних продуктів. Незважаючи на те, що цикл RIS відформатований у вигляді «пропелера», все ж він є достатньо лінійним процесом. Він передбачає, що всі OSINT-дослідження можуть бути структуровані, незалежно від майбутнього розвитку подій. Але ідея про те, що будь-яке розвідувальне аналітичне дослідження можна змоделювати, може бути абсолютно неправильною. Можливо, саме тому існує так багато різновидів циклів. Можливо, це також причина, чому так багато професіоналів дізнаються про цикл аналітичної розвідки з відкритих джерел, але ніхто насправді не дотримується його у повсякденній практиці.

ДАНІ, ІНФОРМАЦІЯ

Дані, інформація є основою для аналізу під час будь-якого дослідження, у тому числі OSINT. Кількість даних, інформації збільшується кардинально щоденно. Так, дослідження «International Data Corporation» (IDC), що є провідним світовим постачальником ринкової розвідувальної аналітичної продукції та консультаційних послуг [3], показує, що станом на 2018 рік загальна кількість даних у світі становила 33 зетабайти та передбачалось, що їх кількість зросте до 175 зетабайтів до 2025 року [4]. Дослідженням вже станом на 2020 рік встановлено, що загальний обсяг створених, зібраних, скопійованих і спожитих даних у всьому світі становив 64,2 зетабайти. Переглянутим дослідженням передбачається, що до 2025 року створення даних на глобальному рівні зросте вже до понад 180 зетабайтів [5].

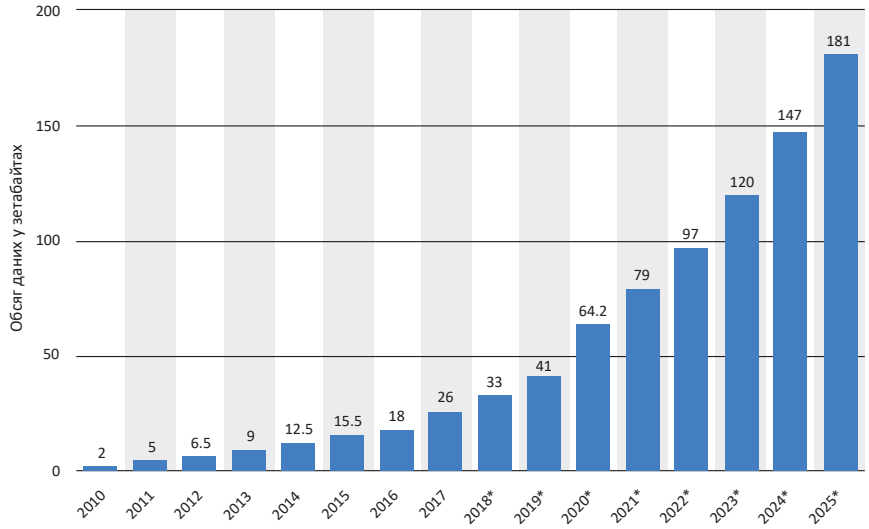


Рисунок 23.2. Загальний обсяг створених, спожитих та збережених даних у всьому світі (2010-2020 роки) та прогноз до 2025 року (Statista, 2023) [1; 5]

У 2018 році прогнозування передбачало, що протягом наступних семи років (до 2025 року) індустрія зберігання даних відвантажить 42 зетабайти (ZB) ємностей (пристроїв для зберігання даних); на пристроях IoT буде створено 90 ZB даних; 49 відсотків даних зберігатимуться в загальнодоступних хмарних середовищах; майже 30 відсотків згенерованих даних буде використовуватися в режимі реального часу [4]. Тенденції зберігаються та розвиваються, доповнюючись розвитком квантумних комп'ютерних можливостей (збільшуючи спроможності опрацювання даних кардинально), можливістю зберігання даних на молекулах ДНК, що є технологічним трендом 2023 року. Порівняно з «комп'ютерним розумінням» бінарного коду (представленим цифрою 1 або 0), ДНК розуміє 4-літерний код, що значно збільшує можливості та об'єми зберігання інформації [6]. Розуміючи потребу у збільшенні можливостей для зберігання даних, як було вказано у викладеному вище прогнозуванні, та відповідно, обмеженими можливостями створення достатніх пристроїв для зберігання «бінарних» даних, ДНК-зберігання є реальним виходом.

> *Для **прикладу**, половини макової насінини достатньо для ДНК-зберігання всіх даних Facebook [7]. Чашка кави, до прикладу, зможе зберегти всі дані світу [8]. Додатковою перевагою цього підходу зберігання даних є стабільність. У випадку зберігання у холодному та сухому місці, файли можуть зберігатись сотні тисяч років [9]. Однак, цей процес зберігання є на даний час дуже вартісним та синтезування 1 мегабайту даних коштує близько 3,500 доларів США [10]. Але, станом на 2019 рік науковці прогнозували, що до 2024 року ціна може впасти до 100 доларів США за синтез 1 терабайту даних, у випадку відповідного інвестування [11].*

У 2020 році обсяг створених та відтворених даних зріс. Зростання було вищим, ніж очікувалося раніше, через збільшення попиту завдяки пандемії COVID-19, оскільки більше людей працювали та навчались з дому й частіше використовували домашні розваги [5]. Водночас це ж дослідження

звертає увагу на те, що лише невеликий відсоток новостворених даних зберігається, оскільки лише два відсотки даних, створених і спожитих у 2020 році, було збережено та зберігається до 2021 року.

Ті незначні можливості **архіваторів**, як Wayback Machine (або інших загальних або спеціалізованих) не задовольняють усі потреби на запити історичних даних, у той же час, є потужним джерелом, у випадку, якщо архіватори все-таки задовольнили збереження відповідних даних.

У сучасному світі все залишає цифрові сліди. Все більше **пристроїв «інтернету речей» (Internet of things/IoT)**, тобто «розумних» пристроїв з'являється та використовується у будь-якій сфері життєдіяльності. Станом на кінець 2020 року, з 21,7 мільярда активних підключених пристроїв у всьому світі, понад 11,7 мільярда (54 %) є IoT пристроями [12]. Графік нижче показує тенденцію у приблизно 20 % щорічного приросту ринку IoT пристроїв.

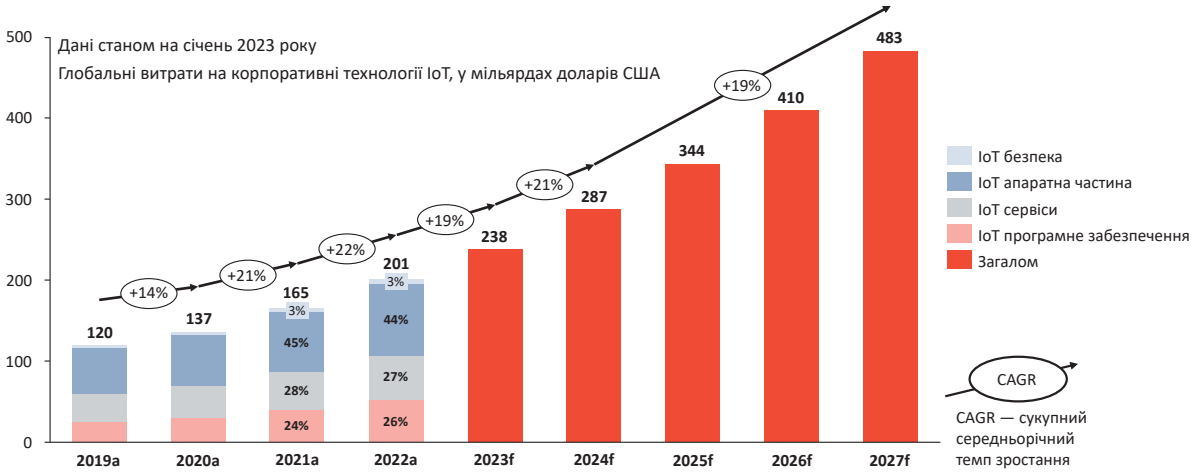


Рисунок 23.3. Аналіз корпоративного ринку IoT (2019-2022 роки) з прогнозуванням до 2027 року (IOT Analytics) [13]

> *IoT пристрої – це пристрої, які мають як мінімум один перетворювач (сенсор/датчик або привід) для безпосередньої взаємодії з фізичним світом і принаймні з одним мережевим інтерфейсом (до прикладу, Ethernet, Wi-Fi, Bluetooth) для взаємодії з цифровим світом [14].*

Виділяють такі основні типи IoT пристроїв, відповідно до їх основного застосування:

Споживацькі (для споживачів) – це насамперед пристрої для щоденного використання, наприклад: побутова техніка, голосова підтримка та освітлювальні прилади;

Комерційні – в основному використовуються в галузі охорони здоров'я та транспорту, наприклад: розумні кардіостимулятори та системи моніторингу;

Військові – використовуються в основному для застосування технологій IoT у військовій сфері (IoMT), наприклад: роботи-спостерігачі та біометрія, людини під час виконання бойових завдань;

Промислові (індустріальні) – використовуються в основному для промислових застосувань (IIoT), наприклад у виробничому та енергетичному секторах, як-от: цифрові системи управління, розумне сільське господарство та промислові великі дані;

Інфраструктурні – використовуються в основному для підключення в «розумних містах», наприклад: датчики інфраструктури та системи управління [15].

Отже, усвідомлюючи зростаючу тенденцію приросту відповідних пристроїв, розуміємо, що інформація про спосіб життя людини (через пристрої, що відслідковують переміщення, як то координати, швидкість, дані щодо зупинок та перебування, стан здоров'я тощо), у тому числі «розумні будинки», пристрої для відео-спостереження та інші можливості, все менше і менше залишають можливостей зберігати анонімність людям, що користуються відповідними технологіями та пристроями. Та, відповідно, дають можливість тим, хто використовує ці зібрані дані, отримувати інформацію щодо способу життя фігуранта, будь-які інші відповідні дані «не виходячи з дому». Це, у свою чергу, викликає занепокоєння у багатьох правозахисних організацій.

Слід також обов'язково наголосити на необхідності використання даних, інформації виключно в рамках обмежень, передбачених законодавством України.

> *Кожен користувач (у тому числі представник правоохоронних органів) залишає цифровий слід в мережі, реєстрі, базі даних. Порушення законодавства про захист персональних даних передбачає відповідальність.*

Найбільшим джерелом даних та інформації є інтернет. Інтернет є мультишаровим та складається з **поверхневої (або індексованої) мережі (Surface Web), глибокої мережі (Deep Web) та темної мережі (Dark Web)**.

Поверхнева мережа є найбільш видимою частиною інтернету та є доступною для індексування пошуковими системами такими як Google, Bing тощо. Здається, що пошукові результати цих систем дають безкінечні результати, однак індексована частина містить менше 5% контенту інтернету. Відповідно, 95+% залишаються у неіндексованій частині шарів глибокої мережі (deep web) та темної мережі (dark web) [17].

Діпнет (на відміну від даркнет) не вимагає конкретного браузера для доступу до відповідного контенту. Його контент не може бути ідентифікованим та індексованим стандартним пошуковими системами, оскільки ця інформація або захищена паролем, або зберігається за певними інтернет-сервісами. Прикладами діпвебу є дані, які містяться в електронних скриньках, онлайн-банкінг або навіть робочий інтранет [17].

На відміну від діпнет, ***дарквеб*** – веб-сайти доступні тільки через спеціалізовані пошуковики такі як, наприклад, The Onion Router (TOR). Контент даркнету в основному розміщується анонімно та значно зашифровано, забезпечуючи додаткові рівні захисту від відстеження та ідентифікації. Як правило, основними способами розслідування у неіндексованих мережах є інфільтрація та/чи прослуховування або перехоплення, відслідковування криптогаманців/операцій та/або соціальних медіа. Є багато рішень ***блокчейн аналізу*** таких як Chainalysis, Bitquery-Coinpath, Messari, Crystal Blockchain, інші [18], однак вони є платними продуктами та вимагають детальних знань та розумінь блокчейну.

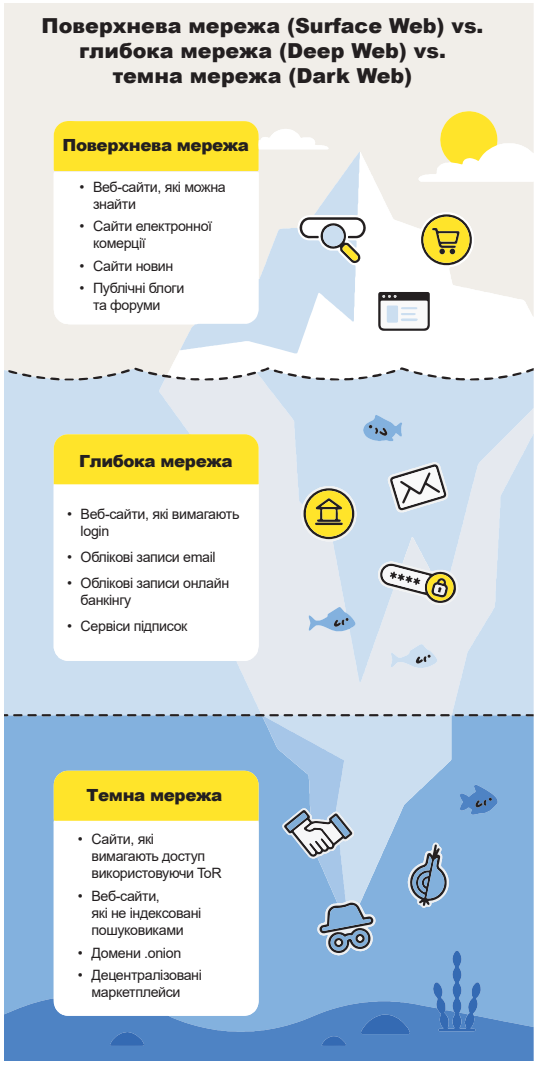


Рисунок 23.4. Мережева структура інтернет: поверхнева, глибока та темні мережі (Norton) [16]

Індексована мережа, або відкритий інтернет є найбільш доступною для пошуку. ***Пошукові сервіси*** дають можливість знайти індексовану інформацію за відповідними алгоритмами та правилами. У багатьох випадках оператори розширеного пошуку (Boolean operators) такі як AND, OR, NOT та інші, мають схожий функціонал для різних пошукових систем, однак є свої особливості, логіка та застосування різними пошуковими системами. Необхідно розуміти логіку, яку мають оператори та вміти створювати відповідно логічні пошукові комбінації, які зможуть звузити пошукові результати до необхідних. Оператори пошуку (розширеного пошуку) широко представлені у численних джерелах. Матеріал є об'ємним та вимагає окремого висвітлення.

Є величезна кількість пошукових систем, які ***RIS категоризує*** відповідно до їх робочих принципів, а саме [1]:

А) Директорії або каталоги (фактично це не зовсім пошукові системи, а підбірка сайтів та сторінок, зроблених людьми та упорядкованих у директорії/каталоги формату пошукового дерева). Прикладом є сайт «Reuser's Repertorium».

Б) Окремі пошукові системи (використовує принцип пошуку за ключовими словами через пошукові роботи). Прикладом є Google, DuckDuckGo, Shodan тощо.

В) Мета-пошукові системи (проводить пошук через низку окремих пошукових систем одночасно). Прикладом є Skyscanner, TripAdvisor тощо.

Г) Вертикальні пошукові системи (спеціальний тип окремих пошукових систем, але обмежений конкретними широкими предметами пошуку). Прикладом є YouTube, IMDb тощо.

Д) Об'єднані пошукові системи (паралельна мульти-пошукова система в реальному часі). Прикладом є Scopus, UNjobs тощо.

Е) Пошукові системи фактів або машина для відповідей на запитання (фактично це не зовсім пошукові системи). Прикладом є Chat GPT, BERT тощо. Штучний інтелект/ШІ (як його називають), який використовується у таких пошукових системах, дає можливість скоротити процес пошуку з

метою отримання, у багатьох випадках, непоганих результатів (відповідей) в процесі дослідження. У той же час, слід пам'ятати про обмеження процесів, які стоять за так званим ШІ, оскільки інтелектуальна частина процесу пошуку там по суті відсутня. На даний час заміни або альтернативи людському інтелекту не винайдено, хоча виписані та сформовані алгоритми й бібліотеки процесів та відповідної інформації намагаються до цього наблизитись. Про це говорить низка теоретиків та практиків застосування алгоритмів машинного та глибокого навчання. Так, доктор Ленс Б. Еліот (всесвітньо відомий експерт зі ШІ, який поєднує практичний досвід у галузі з глибокими науковими дослідженнями) зазначає, що остання ера штучного інтелекту широко використовує машинне навчання (ML) та глибоке навчання (DL), які використовують обчислювальну відповідність патернів. Звичайний підхід полягає в тому, що ви збираєте (формуєте) дані про завдання щодо прийняття рішень та вводите дані в комп'ютерні моделі ML/DL. Ці моделі прагнуть знайти математичні патерни. Після виявлення таких патернів, якщо вони будуть знайдені, система штучного інтелекту потім використовуватиме ці патерни у разі зустрічі з новими даними. Після надання нових даних для прийняття поточного рішення застосовуються патерни, використані на «старих» або історичних даних. Таким чином, сьогодні немає жодного ШІ, який би був подібним здоровому глузду чи зміг би когнітивно здивувати щодо наявності чіткого людського мислення [19]. У той же час, не варто недооцінювати цей напрям розвитку високих технологій, оскільки машинне навчання (ML) та глибоке навчання (DL) дозволяють автоматизувати та спростити процеси обрахування та опрацювання даних, створюючи продукти (результати) для подальшого осмислення людиною.

Заслуговує на увагу й пошукова система **Shodan**, яка спрямована на пошук апаратної частини, IoT, зокрема веб-камери, бейбі-камс, камер спостереження, роутерів тощо. Визначає також IP-адресу, HTTP-хедери. Але має певні обмеження, що стосуються його виключного платного використання.

Як зазначає «Мольфар», усі чи майже всі створені інструменти використовують джерела OSINT, тобто більшість доступних інструментів є агрегаторами відкритої інформації. Проте деякі інструменти OSINT містять унікальні дані, наприклад, FlightRadar24 – інтерактивна мапа з трекінгом геолокації цивільних та деяких військових літаків в режимі реального часу. Або MarineTraffic – аналогічний сайт для трекінгу геолокації кораблів [20].

Вибір пошукової системи залежить від задачі, яку потрібно вирішувати, тобто саме від напряму, мети пошуку та функціоналу пошукової системи. Не менш важливо враховувати актуальність пошукових механізмів (перш за все, стан підтримання функціонування самого індексування, у тому числі його якості). Пошук, для прикладу, за фото з використанням TinEye можливо доповнити використовуючи Google Images, Google Lens, PimEyes тощо. Список не є вичерпним та залежить від контексту.

На перетині вказаної категоризації пошукових систем з'являються так звані гібридні бази (або швидше об'єднані пошукові або мета-пошукові системи доступу до баз даних з аналітичним функціоналом), які скорочують процес аналітичного дослідження (перш за все щодо компаній та пов'язаних осіб). Прикладом є Orbis, Sayari, Youcontrol тощо.

> *Пошукові системи та/або бази даних є лише інструментом в руках аналітика або дослідника, який повинен бачити механізм, алгоритм пошуку, можливості пошуку відповідно до конкретно визначеної мети, задач дослідження.*

Створення методології з OSINT-дослідження є завжди складною задачею, оскільки, у випадку фокусування на інструментах дослідження (чого як правило вимагають практичні співробітники), є велика ймовірність, що інструмент вже застарів (або вже не працює) до моменту упровадження та практичного використання методології.

У зв'язку з цим, основною рекомендацією є: *не обмежуватися формою (інструментом), а фокусуватися на змісті (баченні, розумінні).*

Очевидно, що бачення та розуміння того, як повинно виглядати дослідження передбачає використання інструментів для досягнення мети такого дослідження. Водночас, наявність вузького інструментарію (конкретних обмежених інструментів фактично та вузьких вмінь користування ними відповідно) обмежує функціоналом конкретних інструментів і можливості дослідження, що є проявом когнітивного обмеження та вимагає системного перегляду підходу до організації роботи, перегляду робочих процесів. Так само, під час формування бачення розвитку цього напряму дослідження необхідно враховувати тенденції та новітні технології, зокрема й ті, які розглянули раніше (до прикладу розвиток IoT, тенденції зберігання даних тощо).

Розуміючи відповідні тенденції, враховуючи, що все більше й більше злочинів мають цифрові сліди та використовують цифрові можливості, на початку 2021 року Консультативна місія Європейського Союзу (КМЄС), ініціювала програму «Детектив-2030» (Д30) [21], яка у подальшому була ребрендована та переформатована у «Цифровий детектив» (D30). Детективи, аналітики правоохоронних відомств (НПУ, НАБУ, АРМА) та представники ВУЗів МВС України, а також ДНДІ МВС України беруть участь у

D30, спрямованій на розширення можливостей правоохоронних органів у сфері здійснення цифрових розслідувань. Ціль програми і проста, і складна одночасно: розвиватись, еволюціонувати, щоб не відставати від технологій, які використовують злочинці. Відповідно до стратегії ЄС щодо боротьби з організованою злочинністю 2021-2025, більше 80 % злочинів зараз мають цифровий компонент [22]. Тому, серед іншого, учасники програми отримали глибокі тренінги з OSINT, а також цифрової криміналістики, з базового та спеціалізованого розуміння в IT, зокрема щодо мереж та безпекових особливостей мереж, кібер-безпеки тощо. Серед очікуваних результатів програми не лише діяльність з розширення відповідних спроможностей відомств, але й розробка стратегічної візії щодо стандартів для майбутніх працівників органів правопорядку в Україні, формування відповідних професійних компетентностей детективів, з додатковими знаннями та навичками роботи у сфері цифрових технологій, забезпечення впровадження проактивних методів правоохоронної та безпекової діяльності.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Reuser, A.H.P. (2017). *The RIS Open Source Intelligence Cycle. The Journal of Mediterranean and Balkan Intelligence*, 10 (2), 29-43.
2. Reuser`s Information Services. Retrieved from https://opensourceintelligence.biz/osint-unlocked/
3. International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events. Retrieved from https://www.idc.com/about
4. IDC: Expect 175zettabytes of data worldwide by 2025. Retrieved from https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html
5. Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025. Retrieved from https://www.statista.com/statistics/871513/worldwide-data-created/
6. 5 Important Data Storage Trends 2024-2026. Retrieved from https://explodingtopics.com/blog/data-storage-trends
7. DNA: The Ultimate Data-Storage Solution. Retrieved from https://www.scientificamerican.com/article/dna-the-ultimate-data-storage-solution/
8. Could all your digital photos be stored as DNA? Retrieved from https://news.mit.edu/2021/dna-data-storage-0610
9. DNA could store all of the world's data in one room. New algorithm delivers the highest-ever density for large-scale data storage. Retrieved from https://www.science.org/content/article/dna-could-store-all-worlds-data-one-room
10. DNA Data Storage. Integrated information storage technology for writing large amounts of digital information in DNA using an enzyme-driven, sustainable, low-cost approach. Retrieved from https://wyss.harvard.edu/technology/dna-data-storage/
11. DNA is the future for data storage. That future is coming very soon. Retrieved from https://www.synbiobeta.com/read/dna-is-the-future-for-data-storage-that-future-is-coming-very-soon
12. At 12 billion, IoT connections to surpass non-IoT devices in 2020. Retrieved from https://telecom.economictimes.indiatimes.com/news/at-12-billion-iot-connections-to-surpass-non-iot-devices-in-2020/79318722
13. Global IoT market size to grow 19% in 2023—IoT shows resilience despite economic downturn. Retrieved from https://iot-analytics.com/iot-market-size/
14. Information Technology Laboratory. Computer security resource center. Retrieved from https://csrc.nist.gov/glossary/term/iot_device
15. What Are IoT Devices? Definition, Types, and 5 Most Popular for 2024. Retrieved from https://www.simplilearn.com/iot-devices-article
16. What is the dark web and how do you access it? Retrieved from https://us.norton.com/blog/how-to/how-can-i-access-the-deep-web
17. Where to Gather Intelligence for Deep & Dark Web Investigations. Retrieved from https://www.maltego.com/blog/where-to-gather-intelligence-for-deep-dark-web-investigations/
18. 12 Best Blockchain Analysis Tools. Retrieved from https://medium.com/coinmonks/12-best-blockchain-analysis-tools-2fb8bd62db5c
19. Forbes. Retrieved from https://www.forbes.com/sites/lanceeliot/2022/09/03/unpacking-the-best-top-ten-quotes-about-artificial-intelligence-leveraging-modern-day-ai-ethics-thinking/?sh=3c0dda2a473f
20. Useful apps. Retrieved from https://molfar.com/useful-apps
21. Програма «Детектив-2030»: пристосувати правоохоронну та судову систему до цифрової ери. URL: https://www.euam-ukraine.eu/ua/news/detective-2030-programme-making-law-enforcement-and-the-judiciary-fit-for-the-digital-age/
22. Fighting organised crime – EU strategy for 2021-25. Retrieved from https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12735-Fighting-organised-crime-EU-strategy-for-2021-25_en

РЕАЛІЗАЦІЯ ФІЛОСОФІЇ
«INTELLIGENCE-LED POLICING»
В СИСТЕМІ КРИМІНАЛЬНОГО АНАЛІЗУ
НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

МОНОГРАФІЯ

Користін О., Швець Д., Бутко Б., Денисенко Б. та ін.,
за заг. ред. Користіна О.Є

Комп’ютерна верстка: Вадим Петрунін

Підписано до друку 05.04.2024. Формат 60х90 1/8
Папір офсетний. Друк офсетний.
Обл.-вид. арк. 27,75 Тираж 600 прим. Зам. 128.

Видавництво ТОВ "Компанія ВАІТЕ"
01042, м. Київ, вул. Саперне поле, 26, к. 27.
Свідоцтво про внесення до Державного реєстру суб'єктів видавничої
справи серія ДК № 2570 від 27.07.2006 р.